The Capability of Wavelet Convolutional Neural Network for Detecting Cyber Attack of Distributed Denial of Service in Smart Grid

Conference Paper · December 2021

DOI: 10.1109/ICCWAMTIP53232.2021.9674080

8 authors, including:

Happy Nkanta Monday
Oxford Brookes College of Chengdu University of Technology
53 PUBLICATIONS **584** CITATIONS
SEE PROFILE

Grace U. Nneji
Oxford Brookes College of Chengdu University of Technology
48 PUBLICATIONS **447** CITATIONS
SEE PROFILE

Abel Zenebe Yutra
University of Electronic Science and Technology of China
2 PUBLICATIONS **18** CITATIONS
SEE PROFILE

Bona Debela Lemessa
University of Electronic Science and Technology of China
4 PUBLICATIONS **27** CITATIONS
SEE PROFILE

2021 18th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP) | 978-1-6654-1364-0/21/$31.00 ©2021 IEEE | DOI: 10.1109/ICCWAMTIP53232.2021.9674080

THE CAPABILITY OF WAVELET CONVOLUTIONAL NEURAL NETWORK FOR DETECTING CYBER ATTACK OF DISTRIBUTED DENIAL OF SERVICE IN SMART GRID

HAPPY NKANTA MONDAY[1], JIAN PING LI[1], GRACE UGOCHI NNEJI[2], ABEL ZENEBE YUTRA[2], BONA DEBELA LEMESSA[2], SAIFUN NAHAR[3], EDIDIONG CHRISTOPHER JAMES[2], AMIN UL HAQ[1]

[1]School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu, Sichuan 611731, China
[2]School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu, Sichuan 611731, China
[3]School of Computer and Information Systems, University of Missouri St Louis MO, USA
E-MAIL: mh.nkanta@std.uestc.edu.cn, jpli2222@uestc.edu.cn, ugochinneji@std.uestc.edu.cn, abelzenebe2014@gmail.com, bonadebela1989@gmail.com, snnnm@umsl.com, edianajames@yahoo.com, khan.amin50@yahoo.com

Abstract:

The electrical system's dependability, security, and efficiency are all improved through smart grid technologies. Its dependence on digital communication technology, on the other hand, introduces new risks and vulnerabilities that should be examined for the purpose to providing effective and trustworthy service delivery. This study presents a method for the detection of distributed denial of service (DDoS) attacks on smart grid infrastructure. Continuous wavelet transform (CWT) is used in the suggested approach to convert one-dimensional traffic data to two-dimensional time-frequency domain scalogram as the input to the wavelet convolutional neural network (WavCovNet) to detect anomalous behavior in the data by distinguishing attack features from normal patterns. Our results demonstrate that the proposed approach detects DDoS attacks with a high rate of detection and with a very low rate of false alarm.

Keywords:

Cyber security; Continuous wavelet transform; Convolutional neural network; Distributed denial of service attack; DDoS attack; Smart grid

1. Introduction

In modern control systems, the term "smart grid" refers to a large-scale electricity distribution network. The smart grid's goal is to provide real-time power consumption control and analysis in order to increase device dependability, efficiency, and security while saving energy and money. Intelligent grids employ enhanced metering to offer two - way communications between intelligent meters and energy companies [1-3]. Although sophisticated measuring infrastructure is critical for intelligent grid communication due to its vulnerability to internet threats since adversaries can modify and deny data transfer, defeating the intelligent grid's objective.

The distributed denial of service (DDoS) attack is a frequent type of internet attack [4], which can be expressly damaging since it delays, blocks, or corrupts smart grid communication [5]. As a consequence, this attack has the potential to disrupt power distribution, resulting in outages [4]. It's difficult to tell the difference between a DDoS attack and a normal burst signal. Both signals have hidden properties and are non-periodic, multi-fractal, broadband, self-affine, and stochastic. To differentiate between normal and abnormal signal behaviors, a heuristic automatic technique is required to extract signal properties. To get better outcomes, the majority of earlier approaches relied on shallow learning schemes or a mix of linear and non-linear approaches.

The authors in [6] use honeypots to capture attacker information in the smart grid network's advance metering architecture (AMA), then use Bayesian-Nash equilibrium to assess the attacker-defender interaction and implement defense strategies accordingly. By lowering the data computational cost of AMA, the authors in [7] use a firewall in conjunction with a cloud-based computing approach to avoid and mitigate DDoS attacks. While one of the network's nodes is being attacked, the total power network's strategy was designed with a collaborative reputation topology based on the auto-healing technique [8]. The authors in [9] use an information divergence approach to detect and discard

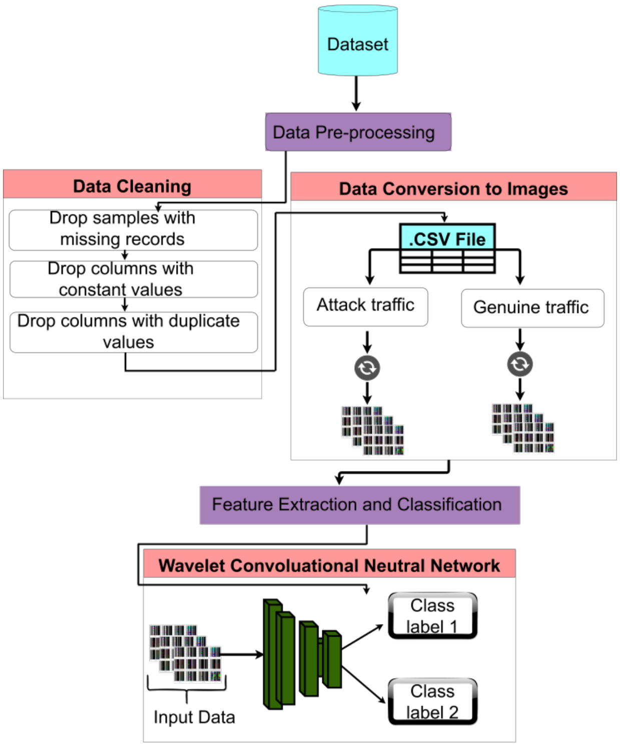
Dataset
Data Pre-processing
Data Cleaning
Drop samples with missing records
Drop columns with constant values
Drop columns with duplicate values
Data Conversion to Images
.CSV File
Attack traffic
Genuine traffic
Feature Extraction and Classification
Wavelet Convoluational Neutral Network
Class label 1
Class label 2
Input Data

Fig.1 Proposed scheme for detecting DDoS attack on smart grid

bogus harmful queries.

This paper describes the procedure of our study in two phases. The first phase is to transform the one-dimensional time-series data to two-dimensional time-frequency scalogram as input image of distinct features with growing sensitivity using CWT which makes it suitable for CNN model. In the second phase, the image features obtained from CWT are utilized to train the proposed WavCovNet to detect attack and genuine traffic behaviors. The following is the structure of the remaining part of this paper. The proposed approach and the dataset are presented in section 2. The results and comments are explained in section 3, and the study is concluded in section 4.

2. Methodology

This section explains the proposed strategy for detecting DDoS attacks in intelligent grid infrastructure. The proposed approach for understanding the DDoS attack detection framework in the intelligent grid network is depicted in Figure 1. First, the dataset for detecting DDoS attacks in intelligent grid infrastructure used in this study is adequately defined.

2.1. Dataset

The first step is to collect both genuine and DDoS attack dataset. Setting up a real-time network to generate large amounts of genuine and attack dataset is a difficult undertaking that necessitates a lot of network resources. Furthermore, establishing a large network takes time and money. However, one can avoid this time-consuming task by utilizing a public network flow dataset. We chose the CICDDoS2019 dataset from a variety of public dataset [10]. In comparison to numerous network traffic dataset, CICDDoS2019 [10] is the most recent dataset with a high number of contents. It also includes both incoming and outgoing traffic from recent DDoS attack.

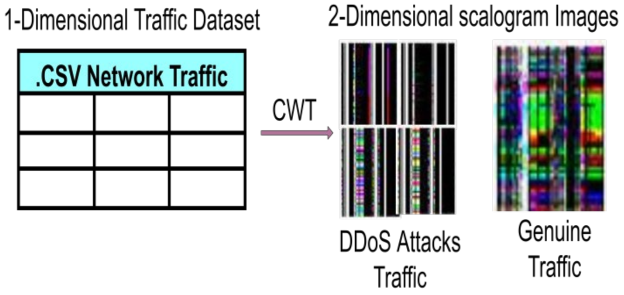

Fig.2 Adopting CWT for the Conversion of one-dimensional traffic data to two-dimensional scalogram

2.2. Wavelet transform

Wavelet transform (WT) is a processing tool for extracting coefficients from a signal by using a wavelet function to turn it into wavelets. WT is a technique for extracting meaningful features from data in order to reveal characteristics that aren't visible in the time domain [11]. WT decomposes data into coefficients and offer that information in sub-scales. A wavelet is a small wave with a property that oscillates like a wave. In this paper, we utilized continuous wavelet transform (CWT) for converting time-series signal to time-frequency images for detecting abnormalities in traffic patterns as depicted in Figure 2. Equation (1) presents the mathematical expression for the CWT.

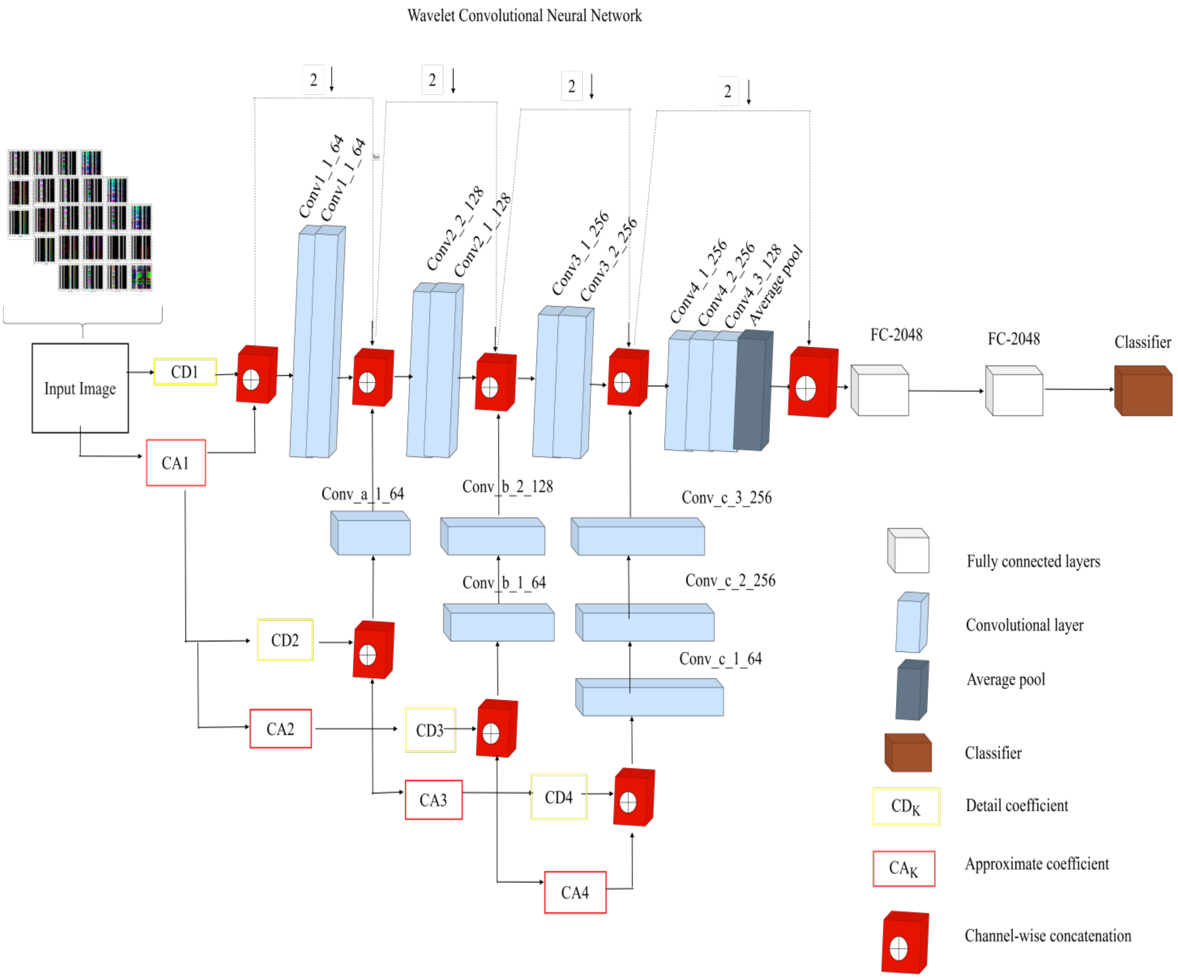

Fig.3 Proposed wavelet convolutional neural network for detecting DDoS attack on smart grid infrastructure

$$\mathrm{CWT}_x^{\psi} = \frac{1}{\sqrt{|S|}} \int x(t)\psi^{*}\left(\frac{t-\tau}{s}\right) dt \tag{1}$$

where τ depiocts the transition factor and S denote the scale factor. $x(t)$ represents the function of the mother wavelet. $\psi^{*}\left(\frac{t-\tau}{s}\right)dt$ depicts the derived function from the mother wavelet. τ is the shift term to move the mother wavelet. S is the frequency inverse. Low frequency corresponds to large S and small S leads to high frequency.

2.3. Convolutional neural network

CNN is a sophisticated deep neural network based on visual perception that was first employed in the field of computer vision and has already shown great promise [12]. CNN has recorded tremendous achievement in various applications especially detecting anomalies in radiographs [13-16]. With image as input, CNN may learn the hierarchical features to create a final set of high-level abstraction features, which are then sent to a fully connected layer as the classifier for categorical classification purposes. CNN learns the patterns in the images automatically and stores them in the network connection settings, requiring very little manual design. Furthermore, when compared to manual feature creation, CNN is better at detecting intricate patterns in high-dimensional data.

2.4. Proposed Wavelet convolutional neural network

As shown in Figure 3, the proposed WavCovNet is a deep learning architecture that combines convolutional layers in groups with wavelet decomposition layers generated from multi-resolution analysis (MRA) for DDoS attack detection. Two-dimensional time-frequency images with three channels are used as inputs to the proposed network. The resulting detail component from the first stage of decomposition is used as input to the first convolutional block, which is made up of two convolutional layers.

After the approximate components of the first disintegration stage is further sub-sampled to produce detail and approximate components of the second disintegration stage, the detail component of the first disintegration stage is fed as input to the second block, which comprises of two convolutional network layers. It's worth mentioning that the detail component is concatenated through a channel of $1x1$ convolutional layer with a 64 kernel size before being transferred to the second block to maintain a match in feature dimensionalitywith the output from the first block.

In the same fashion, the third and fourth blocks are treated same. At the third disintegration stage, the concatenation to the third block through the channel, on the other hand, is done via two $1x1$convolutional layers with kernel sizes of 64 and 128 respectively. The fourth block is made up of three convolutional neural layers and average pooling, which is concatenated with the final decomposition level. Three 1×1convolutional layers of 64, 128, and 256 are used to achieve channel-wise concatenation.

It's worth noting that the images are scaled down by a factor of two throughout the wavelet decomposition process. The fifth block is made up of two fully connected layers, and a classifier as the last fully connected layer with two-class. We trained for 30 epochs with a learning rate of 10^4, 16 as the batch size, and Adam as the optimizer. Training, validation, and test are the three sets of dataset split.

During the training phase, the model's performance is also scrutinized. The suggested model is assessed using the test set split to obtain the final performance. Our model's performance was evaluated using well known metrics.

2.5. Experimental detail and setup

The core approach of the methodology is divided into two parts: data pre-processing and feature extraction and learning. The raw DDoS data is transmitted to the network for the pre-processing phase. Using digital signal processing methods like CWT, the most significant and dependable underlying features are retrieved in the pre-processing step by converting the raw one-dimensional traffic DDoS data to time-frequency scalogram image data.

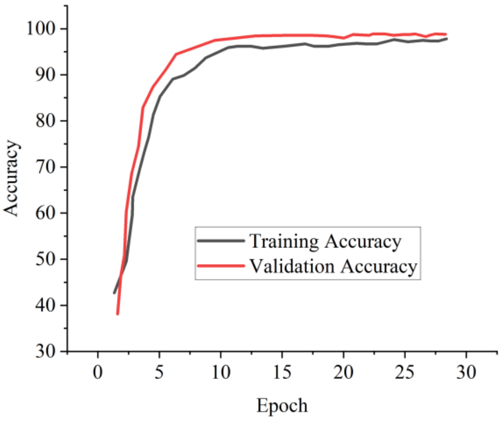

Fig.4 Training and validation accuracy curves showing the performance of our proposed WavCovNet

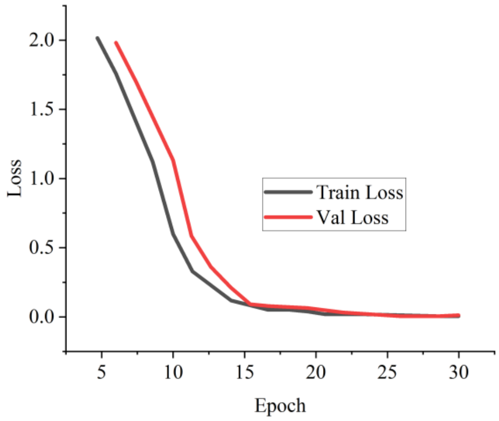

Fig.5 Training and validation loss curves of our proposed WavCovNet model showing steady reduction in loss

In this study, we trained our model for DDoS attack Detection with continuous wavelet transform and wavelet convolutional neural network as a combined framework while using an Adam optimizer and dropout to avoid over-fitting, early stop techniques is introduced and a learning rate of 10^4 is used in order to obtain a better performance. We implemented the proposed model using Keras library with Tensorflow as back-end on GeForce GTX 1080 GPU, which is driven by a parallel computing platform and programming paradigm called CUDA.

2.6. Performance Measures

We have applied some evaluation metrics in terms of accuracy, sensitivity, specificity and AUC on our proposed model. Equations (2)-(4) are the numerical expression for the evaluation metrics.

$$\text{Accuracy}=\frac{\text{TP+TN}}{\text{TP+TN+FP+FN}} \tag{2}$$

$$\text{Sensitivity}=\frac{\text{TP}}{\text{TP+FN}} \tag{3}$$

$$\text{Specificity}=\frac{\text{TN}}{\text{TN+FP}} \tag{4}$$

3. Results and discussion

According to the automatic feature extraction method depicted in Figure 3, extensive experimental findings and discussion are presented in this section.

The proposed attack detection system of DDoS is constructed on the Keras framework and utilizes Tensorflow as the back-end. During the training and testing, we analyzed the proposed scheme for DDoS attack detection based on binary classification for both detecting and identifying incoming and outgoing DDoS attacks in smart grid networks. For detecting DDoS attacks, the proposed approach achieves 98.9% accuracy. Figure 4 depicts the training and validation accuracy curves of the proposed model which show that the model converges smoothly without over-fitting. Figure 5 shows the gradual and steady reduction of the training and validation loss curves the proposed model. Generally, the performance of the proposed wavelet convolutional neural network is satisfactory. It is important to examine the validity of the proposed model in terms of the receiver operating characteristic curve (ROC) which shows the overall accuracy of the proposed scheme in terms of area under curve (AUC).

Table 1 Performance comparison of our proposed model with selected pre-trained models.

WavCovNet model

Model	ACC (%)	SEN (%)	SPE (%)	Time (Min)
EfficientNet	95.1	94.8	95.2	38
MobileNet V3	94.8	95.4	94.8	41
DenseNet	94.8	95.7	95.3	51
ResNet 101	94.6	94.4	95.8	46
Ours	98.9	99.8	99.9	36

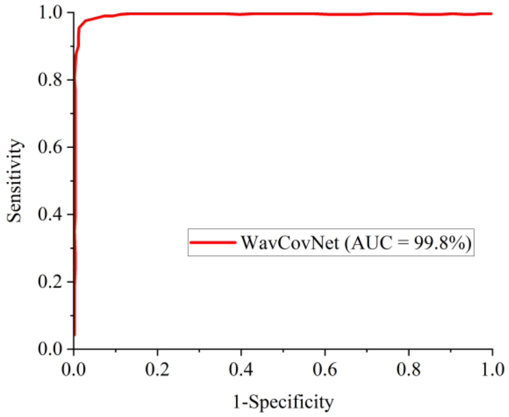

Fig.6 ROC curve showing the performance of our proposed model with respect to sensitivity and specificity

Figure 6 shows that the proposed model has high sensitivity associated with high specificity which minimizes the rate of false positive and maximizes the rate of true positive. Our proposed model achieves 99.8% sensitivity and 99.9% specificity as presented in Table 1. Table 1 shows the outcomes of our proposed methodology versus some pre-trained scheme. It is evident that the proposed technique outperformed the selected pre-trained methods by 3.8% when it came to recognizing DDoS attack patterns in terms of accuracy. In addition, when compared to the pre-trained techniques, the proposed method obtained 3.2% increase in sensitivity and a 3.1% increase in specificity. ResNet-101 recorded the least score in accuracy (94.6%) and sensitivity (94.4%) whereas MobileNet-V3 recorded the least score in specificity (94.8%). The proposed scheme is computational efficient with the least training time of 36 minutes as depicted in Table 1. Though DenseNet performed slightly better than ResNet-101, MobileNet-V3, and EfficientNet in accuracy, sensitivity, and specificity respectively but recorded the highest training time of 51 minutes for 30 epochs.

4. Conclusions

According to recent cyber-attack statistics, distributed denial of service (DDoS) attacks is the most common in smart grid infrastructure, and they are increasing in frequency and intensity over time. CNN models have acquired a lot of traction in image categorization applications as a result of their superior performance. However, CNN models are built to discover patterns in images therefore; they do not function as expected when trained on one-dimensional traffic data. In this paper, we proposed a method for converting a one-dimensional traffic data into two-dimensional time-frequency domain images in order to take advantage of CNN's potential. Following that, we trained our proposed WavCovNet on the converted data and evaluated its performance in recognizing DDoS attacks. The proposed approach detected DDoS attacks with 99.9% accuracy, which is 9% better than the pre-trained models

Acknowledgements

This work was supported by the National Natural Science Foundation of China (Grant No. 61370073), the National High Technology Research and Development Program of China (Grant No. 2007AA01Z423), the project of Science and Technology Department of Sichuan Province, the project of Science and Technology Department of Chongqing Municipality, Chengdu Chengdian Network Technology Co., Ltd., Chengdu Civil-military Integration Project Management Co., Ltd., and Sichuan Yin Ten Gu Technology Co.

References

[1] N. Beigi Mohammadi, J. Mišić, V. B. Mišić, and H. Khazaei, “A framework for intrusion detection system in advanced metering infrastructure,” Secur. Commun. Networks, vol. 7, no. 1, pp. 195–205, 2014.

[2] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, “A Survey on Smart Grid Communication Infrastructures: Motivations, Requirements and Challenges,” IEEE Commun. Surv. \& TUTORIALS, vol. 15, no. 1, 2013.

[3] Z. Feng, “Large-scale flip-chip power grid reduction with geometric templates,” in 2013 Design, Automation \& Test in Europe Conference \& Exhibition (DATE), 2013, pp. 1679–1682.

[4] S. Asri and B. Pranggono, “Impact of distributed denial-of-service attack on advanced metering infrastructure,” Wirel. Pers. Commun., vol. 83, no. 3, pp. 2211–2223, 2015.

[5] W. Wang and Z. Lu, “Cyber security in the smart grid: Survey and challenges,” Comput. networks, vol. 57, no. 5, pp. 1344–1371, 2013..

[6] K. Wang, M. Du, S. Maharjan, and Y. Sun, “Strategic honeypot game model for distributed denial of service attacks in the smart grid,” IEEE Trans. Smart Grid, vol. 8, no. 5, pp. 2474–2482, 2017.

[7] R. C. Diovu and J. T. Agee, “A cloud-based openflow firewall for mitigation against DDoS attacks in smart grid AMI networks,” in 2017 IEEE PES PowerAfrica, 2017, pp. 28–33.

[8] P. Srikantha and D. Kundur, “Denial of service attacks and mitigation for stability in cyber-enabled power grid,” in 2015 IEEE Power \& Energy Society Innovative Smart Grid Technologies Conference (ISGT), 2015, pp. 1–5.

[9] P. Varalakshmi and S. T. Selvi, “Thwarting DDoS attacks in grid using information divergence,” Futur. Gener. Comput. Syst., vol. 29, no. 1, pp. 429–441, 2013.

[10] I. Sharafaldin, A. H. Lashkari, S. Hakak, and A. A. Ghorbani, “Developing realistic distributed denial of service (ddos) attack dataset and taxonomy,” in 2019 International Carnahan Conference on Security Technology (ICCST). IEEE, 2019, pp. 1–8.

[11] R. X. Gao and R. Yan, Wavelets: Theory and applications for manufacturing. Springer Science \& Business Media, 2010.

[12] M. Oquab, L. Bottou, I. Laptev, and J. Sivic, “Learning and transferring mid-level image representations using convolutional neural networks,” in Proceedings of the IEEE conference on computer vision and pattern recognition, 2014, pp. 1717–1724.

[13] G. U. Nneji et al., “A Super-Resolution Generative Adversarial Network with Siamese CNN Based on Low Quality for Breast Cancer Identification,” in 2021 4th International Conference on Pattern Recognition and Artificial Intelligence (PRAI), 2021, pp. 218–223, doi: 10.1109/PRAI53619.2021.9551033.

[14] H. N. Monday et al., “The Capability of Multi Resolution Analysis: A Case Study of COVID-19 Diagnosis,” in 2021 4th International Conference on Pattern Recognition and Artificial Intelligence (PRAI), 2021, pp. 236–242, doi: 10.1109/PRAI53619.2021.9550802.

[15] G. U. Nneji et al., “Enhancing Low Quality in Radiograph Datasets Using Wavelet Transform Convolutional Neural Network and Generative Adversarial Network for COVID-19 Identification,” in 2021 4th International Conference on Pattern Recognition and Artificial Intelligence (PRAI), 2021, pp. 146–151, doi: 10.1109/PRAI53619.2021.9551043.

[16] H. N. Monday et al., “Improved Convolutional Neural Multi-Resolution Wavelet Network for COVID-19 Pneumonia Classification,” in 2021 4th International Conference on Pattern Recognition and Artificial Intelligence (PRAI), 2021, pp. 267–273, doi: 10.1109/PRAI53619.2021.9551095.