Enhancing Cybersecurity: Detecting Hidden Information in Spatial Domain Images Using Convolutional Neural Networks

Akram Mshet[1,*], Huda Tayyeh[2]

[1]Informatics Institute for Postgraduate Studies Iraqi Commission for Computers & Informatics, Baghdad, Iraq
[2]University of Information Technology and Communications, Baghdad, Iraq
Emails: 2020dhiqar@gmail.com; haljobori@uoitc.edu.iq

Abstract

Steganography involves concealing hidden messages inside various types of media, whereas steganalysis is the process of identifying the presence of steganography. Convolutional neural networks (CNN), a type of neural network that outperformed previously proposed machine learning-based methods when introduced, are among the models used for deep learning. While CNN-based methods may yield satisfactory results, they face challenges in terms of classification accuracy and network training stability. The present research introduces a CNN structure to increase hidden data detection and spatial domain image training reliability. The suggested method includes pre-processing, feature extraction, and classification. Evaluation of performance is conducted on datasets Break Our Steganographic System Base (BOSSbase-.01) and Break Our Watermarking System (BOWS2) with three adaptive steganography algorithms. Wavelet Obtained Weights (WOW), Spatial Universal Wavelet Relative Distortion (S-UNIWARD), and Highly Undetectable steGO (HUGO) operating at low payload capacities of 0.2 and 0.4 bits per pixel (bpp). The experimental results surpass the accuracy and network stability of prior publications. Training accuracy ranges from 91% to 94%, and testing accuracy ranges from 74.8% to 86.65%.

Keywords: Deep learning; Steganography; Convolutional neural network; Steganalysis

1. Introduction

When data is transmitted between different networks, the role of cybersecurity becomes extremely crucial. The purpose of cybersecurity is to protect the privacy and confidentiality of information, which is essential for maintaining the safety and dependability of communications that take place across public networks. The encryption of data that is communicated across networks and the protection of that data from potential dangers such as hacking are both the primary responsibilities of cybersecurity [1].

The use of information-hiding technology, also known as steganography, is an essential component in the process of ensuring the confidentiality of data transmissions across communications networks. Among the many different sorts of media that are used to communicate information, images stand out as being particularly crucial [2]. Among the various important methods, the use of fraudulent schemes stands out as a major worry with possible consequences for society's integrity, such as enabling terrorist actions and drug trafficking. To address the hazards associated with transmitting data, academics have proposed the development of algorithms that can analyse images to reveal hidden information. Significantly, the use of deep learning algorithms is a crucial approach for assessing covert information concealment [3]. The relationship between the principles of steganography and steganalysis is graphically represented in Figure 1.

DOI: https://doi.org/10.54216/JCIM.150101
Received: January 21, 2024 Revised: April 20, 2024 Accepted: July 12, 2024

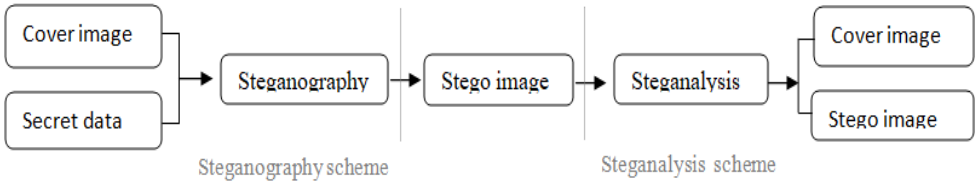

Figure 1. Illustrates Steganography and steganalysis.

The utilisation of steganography has been on the rise due to various legal limitations and practical difficulties encountered in numerous scenarios. Although cybersecurity is governed by legal restrictions that mandate licences and grant authorities the ability to access encrypted communications under some circumstances, steganography is considered legally permissible as long as the concealed message remains unencrypted [4].

Various machine learning (ML) methods have been suggested for steganalysis [5], typically consisting of two stages: feature extraction and classification. Significantly, these stages function autonomously without any direct connection between them. During the feature extraction stage, the main objective is to model the distortion that exists in an image. In the succeeding classification stage, the goal is to determine whether a steganographic payload is present in a particular image. It uses probabilistic methods to assess whether the image is a stego or a cover [6].

Nevertheless, machine-learning methods have not consistently yielded favourable outcomes in all steganalysis tasks. This constraint is ascribed to the underlying reasoning of machine learning approaches. To improve the overall results of steganalysis, researchers have recently started using deep learning (DL) models to develop new methods for steganalysis in digital images. Steganalysis techniques that are based on deep learning utilise deep neural networks (DNN) and CNN. These schemes essentially merge feature extraction and classification into a single step, as mentioned in reference [3]. We present a novel CNN design aimed at enhancing existing steganalysis methods. In the preprocessing layer, we employ an SRM filter consisting of 30 filters.

To extract features, we use standard and deep convolutions together with intermediate pooling. During the classification phase, we employ GlobalAveragePooling2D as part of a spatial pyramid pooling (SPP) model, which includes a fully linked layer and a softmax function. The CNN we possess exhibits the following attributes: We employ four 2D depthwise separable convolutions to address concerns related to kernel skipping for spatial and channel correlation residuals, as well as signal-to-noise ratio (SNR) during the training phase. This convolutional approach offers improved accuracy and helps mitigate overfitting due to its reduced parameter count compared to traditional convolutional layers. We use ReLU for non-linearity. By assigning negative values to zero, ReLU prevents vanishing gradients and allows backward communication with positive model weights. The network converges quickly and improves training stability using ReLU.

We use GlobalAveragePooling2D simplifies and reduces parameters. It also reduces wasteful learning by reducing the model's training data retention accuracy. It prioritises important visual information and presents it globally, improving the model's ability to discover data patterns. This paper's subsequent sections are organised as follows: Section 2 reviews spatial image steganalysis works. Section 3 describes the proposed model, dataset, and three critical stages: pre-processing, feature extraction, and classification. Section 4 discusses the experimental results. The paper concludes in Section 5.

2. Related Work

Machine learning has been utilized in the past for this purpose, but the advent of deep learning has notably improved steganalysis results. Consequently, strengthening the methods that are utilized to guarantee cybersecurity. The incorporation of deep learning architectures, particularly CNN, for spatial image analysis was initiated with the introduction of QIAN-Net in 2015, which employed supervised learning. Since then, various architectural designs have been proposed, including YEDROUDJ-Net, SR-Net, ZHU-Net, XU-Net, YE-Net, GBRAS-Net, and US-CovNet, among others. In the realm of steganalysis, a narrative of innovation unfolds, beginning in 2015 with the advent of QIAN-NET, the pioneering CNN trained via supervised

DOI: https://doi.org/10.54216/JCIM.150101
Received: January 21, 2024 Revised: April 20, 2024 Accepted: July 12, 2024

learning. QIAN-NET revolutionized the field by integrating a High-Pass-Filter (HPF) to reduce image details and amplify steganographic noise. Its feature extraction process, comprising Gaussian-activated convolutional layers and subsequent average pooling, marked a significant departure from conventional techniques. Surpassing contemporary methods like the Spatial Rich Model (SRM), QIAN-NET achieved a precision rate of 69.1% [7].

Following prior research on data steganography analysis, XU-Net was launched the subsequent year as a novel CNN that includes an extra layer called the absolute value layer (ABS) after the second convolutional layer. To limit data values to TanH saturation zones in early network stages, use 1x1 convolutions in deeper layers. Compared to the SRM with ensemble classifiers on BOSSbase for S-UNIWARD detection, the CNN is competitive. The S-UNIWARD method had 72.7% accuracy at 0.4 bpp [8]. Ye-Net pre-processing with Spatial Rich Models (SRM) filter banks, an eight-layer convolutional module, and one TLU activation function. The SRM residual maps are calculated using HPFs instead of HPFs to identify steganographic noise in this model. The SRM findings assist initialize the filters. Performance is improved by channel selection information, and transfer learning from training allows networks to educate other networks [9].

In the year that followed, the YEDROUDJ-Net model was presented to the public. XU-Net and YE-NET, the two models that came before this one, have been combined into one model. Specifically, the TLU activation function and batch normalization (BN) associated with the SRM basis are utilized by the model under consideration. The model achieved a high level of accuracy of up to 77.4 when it was applied to the adaptive steganography algorithm S-UNIWARD at a rate of 0.4 bpp. [10]. SR-Net utilized a model in both the frequency and spatial domain to analyse the adaptive steganography algorithm S-UNIWARD at 0.4 bpp, resulting in an accuracy of 81.3% [11]. The convolutional layer of ZHU-NET utilizes tiny filters, resulting in a reduction of parameters and an enhancement in feature capture. ZHU-NET attained an accuracy rate of 84.5% by utilizing separable convolutions in its application to the 0.4 pps S-UNIWARD technique [12].

In keeping with earlier research on data steganography analysis, GBRAS-Net, which drew inspiration from ZHU-NET, was introduced towards the end of 2021. GBRAS-Net displayed superior performance, employing HPF banks for noise enhancement and depth wise and separable convolutional blocks for feature extraction. GBRAS-Net's outstanding results against spatial domain-based steganographic algorithms solidified its place in the evolution of steganalysis [13]. The year 2022 saw the proposal of a new method by E. Taha Ahmed and B. Tarek Hammad, a new visual analysis method that uses the AlexNet CNN model. Three steps are required: data collection and pre-processing, extracting the AlexNet model for unique features and training a Random Forest classifier using the extracted feature vector for Cover-Stego binary classification. Experimental results on the IStego100K database reveal that the proposed technique has an accuracy of 99%. AlexNet models are successful and effective in feature extraction, making them suitable for RF classification. It performed better than previous methods [14]. Tohari Ahmad proposes a CNN-based method for hidden data detection by improving local features during spatial domain images feature extraction. Using the BOSSBase dataset and two common adaptive steganography algorithms WOW and S-UNIWARD with modest payloads of 0.2 and 0.4 bits per pixel, effectiveness was assessed. The study's results exceed the accuracy and network stability reported in previous literature, with an observed increase in detection accuracy ranging from 2.1% to 3.6% [15]. Saurabh Agarwal presents a deep neural network to reveal information-hiding methods. The approach improves low-frequency information while attenuating high frequencies using high-pass filters. Thirty high-pass SRM filters boost feature extraction in the network. Two skip connections and a shorter ReLU layer optimise data processing. Using SVM instead of softmax improves detection accuracy. The method's correctness and computational efficiency on BOWS2 and BOSSBase datasets are confirmed by experiments [16]. VGG-style ConvNet trains with multi-branch architecture and infers with structural reparameterization. UCNet and Efficient Net, CNN-based steganalyzers, perform similarly to the suggested approach on the ALASKA datasets. Its higher convergence capacity and smaller model complexity make it useful for steganalysis [17]. Utilizes CVTStego-Net for spatial domain image steganalysis, capturing local and global relationships with convolutional and attention techniques. The CVTStego-Net does pre-process, noise analysis, and classification. It uses SRM filters for pre-processing and SE-Blocks (Squeeze-and-Excitation) and convolutional vision transformers to get rid of noise, analyse it, and put it into groups. Results suggest that CVTStego-Net is more accurate. Convolutional vision transformers are effective in spatial domain steganographic image classification, as shown by their 90.45% accuracy for S-UNIWARD and 85.80% accuracy for HILL at 0.4 bpp on BOSSbase 1.01 data [18].

3. Proposed Model

The objective of this work is to construct an artificial intelligence-based deep learning model that can identify concealed information within images, with the ultimate goal of enhancing cybersecurity. The proposed model

DOI: https://doi.org/10.54216/JCIM.150101
Received: January 21, 2024 Revised: April 20, 2024 Accepted: July 12, 2024

for a classification image into two classes (cover or stego) architecture encompasses seven pivotal layers: the Convolutional layer, Batch Normalization layer, DepthwiseConv2D layer, SeparableConv2D layer, AveragePooling2D layer, GlobalAveragePooling2D layer, and a fully connected layer. Among these, the Rectified Linear Unit (ReLU) is pivotal in determining the positivity or negativity of the output from the preceding layer. In cases of positivity, the ReLU function maintains the same value. The diagram presented in Figure 2 organizes the CNN structure organized into three primary phases: pre-processing, feature extraction, and binary classification. Throughout these phases, 14 blocks are strategically deployed to proficiently conduct steganography analysis. The design of CNN architecture poses a significant challenge in the advancement of neural networks. This challenge necessitates meticulous assessment of various factors, such as determining the optimal number of convolutional layers, network depth, and architecture of fully connected layers. It is essential to ensure that pooling operations are appropriately proportioned. In order to enhance performance for a certain task or dataset, CNN designs undergo a process of iterative testing and adjustment. Different arrangements are assessed and improved through experimentation to attain the best possible performance for the assigned objective.

3.1 Pre-processing stage

In this stage, 30 SRM filters are employed, with each filter meticulously designed to precisely match the kernel size of (5, 5). These filters have a consistent and unwavering role in the demanding training program, resolutely fighting any changes considered unchangeable. In the convolutional layers, 30 filters are waiting to be activated and are prepared to respond to the ReLU activation function. The 30 filters offered by YE-Net are specifically used for image pre-processing and have shown exceptional effectiveness in future feature extraction efforts. To maintain consistent processing, each of these 30 filters is normalized using its absolute maximum value. This filter set includes a total of 8 Class 1 filters, 4 Class 2 filters, 8 Class 3 filters, 1 3 x 3 square filter, 4 3 x 3 edge filters, 1 5 x 5 square filter, and 4 5 x 5 edge filters. Figure 3 depicts the array of filters that has been arranged in a sorted manner. This array has comprehensive values for each individual filter.

3.2 Feature extraction layer

This step involves a sequence of processes, starting with seven Conv2D layers. Using 32 and 64 filters, and the kernel size (3, 3), the padding is “same," and strides (1, 1). They use spatial filtering on the image you provide to them. These layers carefully pullout different features using a variety of filters, which helps them understand image information in a more complex and accurate way. four layers of DepthwiseConv2D with kernel size (5, 5) and four layers of SeparableConv2D with 30 and 64 filter and kernel size (3, 3), padding is “same,". This setup lets you use deep filtering and feature extraction together in a way that works well. You can change parameters and filters in each layer, which lets you take a customized method that makes the model work better overall. To lower the number of dimensions, the AveragePooling2D layers and Batch Normalization (BN) are also used. The kernel size for the pooling layer is (2, 2), and the strides (2, 2). This makes the feature map smaller. It is important to note that the Rectified Linear Unit (ReLU) activation function is used in both the deep convolutional layer and the separable convolutional layer. The general shape of the activation function can be seen in Equation (1).

$$f(x) = \begin{cases} 0, & x < 0 \\ x, & x \geq 0 \end{cases} \quad \text{... ... ... (1)}$$

3.3 Classification layer

The classification layer is an important part of the model because it turns the extracted features into guesses about which categories the features will belong to. For this job, our model has two important parts. Firstly, we have the GlobalAveragePooling2D layer. This layer serves to condense and simplify the features into single points for each channel. By condensing these features, we prepare them for the classification process. Subsequently, we encounter the dense layer. This layer connects to the condensed points from the previous layer and incorporates weights and biases. Typically, it includes units equal to the number of categories assigned to the classification task. Using a sigmoid function, it converts model outputs into probabilities, usually ranging between 0 and 1. Each output value signifies the probability that the input belongs to the positive class, with the complementary probability indicating the negative class. The sigmoid function is defined in Equation (2).

$$\text{f(x)} = \frac{1}{1+e^{-z}} \quad \text{…….. (2)}$$

DOI: https://doi.org/10.54216/JCIM.150101
Received: January 21, 2024 Revised: April 20, 2024 Accepted: July 12, 2024

f(x): The denotes the resultant output of the sigmoid function following its application to the value x.
z : The vector of input data fed into the sigmoid function.

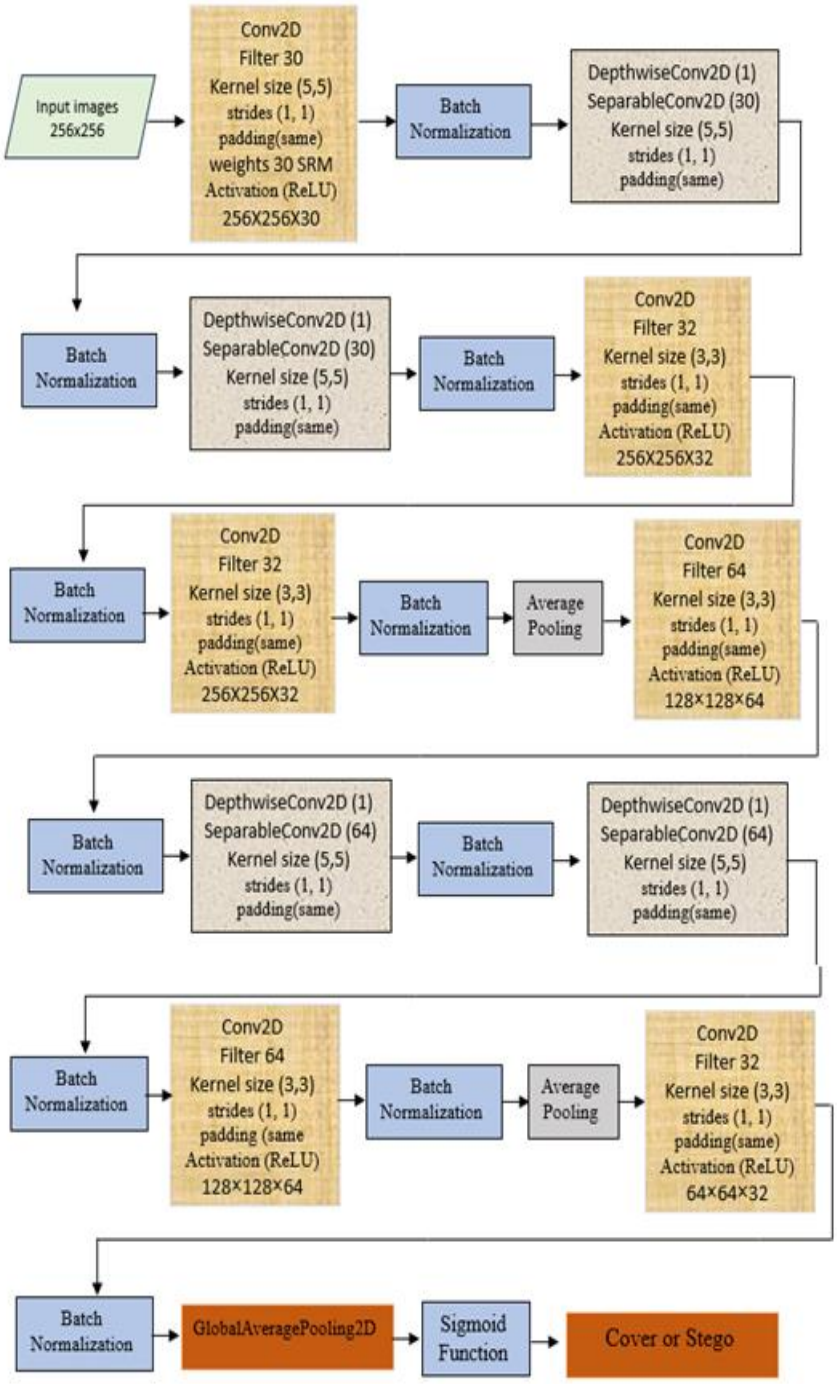

Figure 2. Schema of the proposed CNN

DOI: https://doi.org/10.54216/JCIM.150101
Received: January 21, 2024 Revised: April 20, 2024 Accepted: July 12, 2024

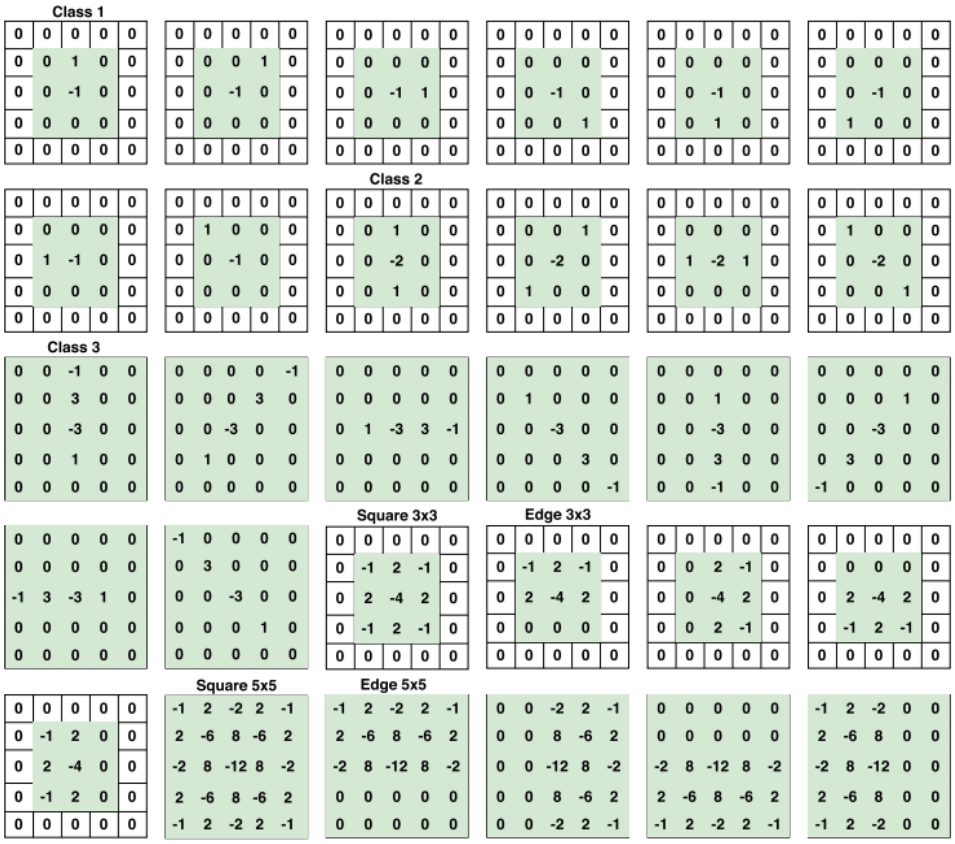

Figure 3. Illustrates the collection of 30 SRM filters [13].

3.4 Hyper-Parameters

The proposed model utilizes a batch size of 32 in its structure. To effectively train the model on a specific payload, it requires undergoing 50 epochs. The training model employs the Adam optimizer, a well-established optimizer extensively utilized in the realm of deep learning. Adam optimizes the learning rate for each parameter by using estimations of the first and second gradient moments. This helps achieve efficient convergence across different datasets and tasks. The CNN design utilizes a Sparse Categorical Cross entropy loss function to handle the two classes, and accuracy is used as the evaluation metric. The batch normalization is configured with a momentum coefficient of 0.2 and an epsilon value of 0.001.

4. Datasets

We exclusively employed BOSSbase1.01 [19], a dataset comprising 10,000 portable gray maps (PGM) images, for the experiments. Each image within the dataset possesses dimensions of 512 × 512 pixels. Preceding the examination of the proposed image, a resizing procedure was applied to the images, reducing their dimensions from 512 x 512 to 256 x 256 pixels. Following this, the proposed model underwent evaluation using the steganography algorithms HILL [20] and S-UNIWARD [21] at a bit rate of 0.4 pps. A series of experiments were conducted to ascertain the optimal partitioning strategy for the image dataset for model input. It was observed that partitioning the dataset as outlined below yielded the most favourable outcomes: 5000 pairs were allocated for training, 1000 pairs were reserved for validation, and an additional 5000 pairs were designated for testing. This meticulous approach played an indispensable role in ensuring the comprehensiveness and accuracy of our assessment methodologies.

5. Hardware and Software Resources

We used a model computer, MSI GF63 9SC, for the training part. That's why this powerful machine has 16 GB of RAM, an i7-9750H CPU, and an RTX 2070 Max-Q GPU. The RTX 2070 Max-Q GPU is rated at 7.5 by Nvidia's rating system, which is worth mentioning. Equipped with 8 GB of specialised memory, the GPU makes it possible to load many images at once, which speeds up the neural network's training process.

DOI: https://doi.org/10.54216/JCIM.150101
Received: January 21, 2024 Revised: April 20, 2024 Accepted: July 12, 2024

6. Results and Discussion

As the primary metric for assessing the proposed model, we employ detection accuracy (DACC). The calculation of this metric is performed by considering various categories: True Positive (TP), which signifies accurate identification of steganographic images as steganographic; True Negative (TN), which signifies accurate identification of original images as original; False Positive (FP), which signifies erroneous identification of original images as steganographic; and False Negative (FN), which signifies incorrect identification of steganographic images as original. The results of the test are presented in Table 1. Equation (3) represents the DACC calculation. The Confusion Matrix, which is employed to evaluate the model's data classification, is illustrated by Equation (4). The system compares the predicted and actual values for each category, facilitating an accurate assessment of performance according to accurate or inaccurate categorizations.

$$\text{Detection Accuracy} = \frac{TP + TN}{TP + FP + TN + FN} \quad \ldots\ldots\ldots (3)$$

$$\text{Confusion Matrix} = \begin{pmatrix} TN & FP \\ FN & TP \end{pmatrix} \quad \ldots\ldots\ldots (4)$$

Table 1: The CNN accuracy with 0.4 of two different steganography methods.

Algorithms	HILL 0.4	S_UNIWARD 0.4
XU-NET [1]	79.24	80.24
YU-NET [2]	61.39	68.7
YEDROUDJ-Net [3]	64.96	77.4
Zhu-Net [4]	69.08	84.5
SR-NET [5]	65.07	81.3
GBRAS-Net [6]	81.9	87.1
Context-Aware Image Steganalysis [7]	73.07	84.79
CVTStego-Net [8]	85.80	90.45
Proposed CNN	91.71	89.21

The accuracy of the proposed model in detecting concealed information in the spatial domain of digital images was exceptionally high. achieving a high level of accuracy in the detection of concealed data in images contributes to an improvement in cybersecurity. 40% of the BOSS base 1.01 data was allocated for training, 10% was designated for validation, and the remaining 50% was designated for testing. The training set consisted of 4000 samples, while the validation set contained 1000 samples, and the testing set had 5000 samples. The training lasted for 50 epochs, employing the Adam optimizer with a batch size of 32. The model's accuracy significantly surpassed previous benchmarks, achieving detection accuracies of 89.21% and 91.71% for S-UNIWARD and HILL encryption algorithms, respectively, at a payload of 0.4 bpp. CVTStego-Net exhibited exceptional precision when evaluating the S-UNIWARD steganography algorithm with a payload of 0.4, attaining a remarkable accuracy rate of 90.45%. In contrast, the suggested model outperformed CVTStego-Net in evaluating the HILL steganography technique with an identical payload of 0.4. The proposed model's accuracy, as depicted in the table1, notably surpasses previous results, indicating a clear advancement in the proposed model's performance over previous years.

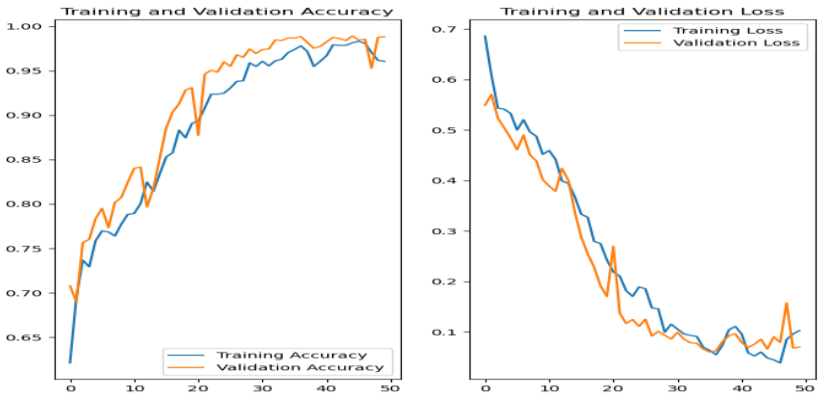

Figure 4. Proposed CNN training and validation curves with S-UNIWARD 0.4 bpp.

DOI: https://doi.org/10.54216/JCIM.150101
Received: January 21, 2024 Revised: April 20, 2024 Accepted: July 12, 2024

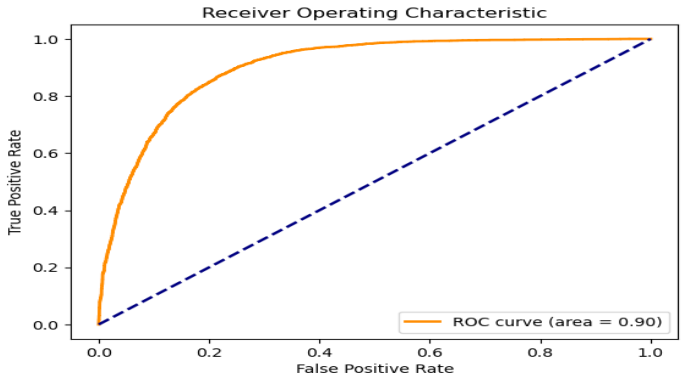

Figure 5. Training and validation ROC curves for the S-UNIWARD algorithm with 0.4 bpp

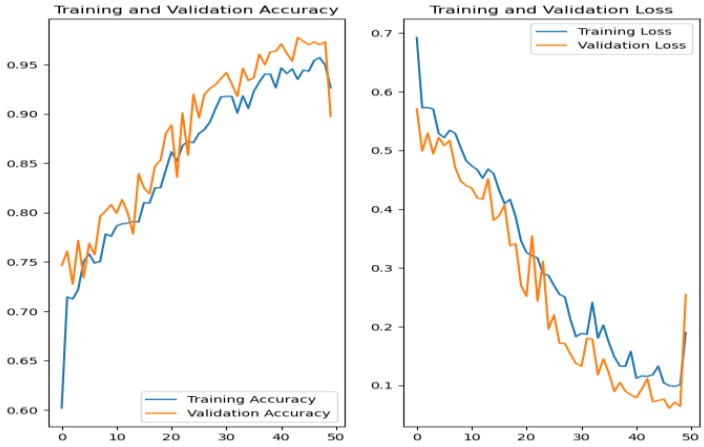

Figure 6. Proposed CNN training and validation curves with HILL with 0.4 bpp.

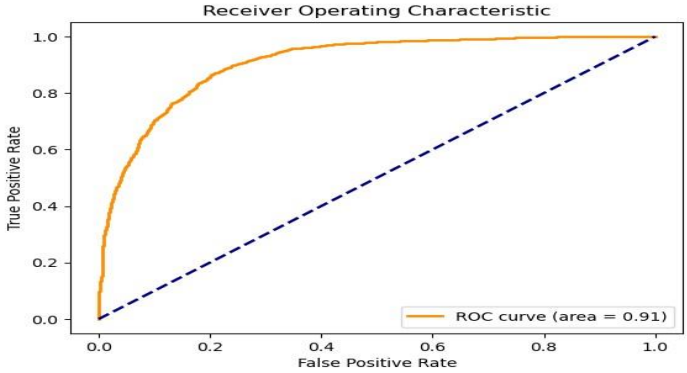

Figure 7. Testing ROC curves for the HILL algorithm with 0.4 bpp.

The S-UNIWARD steganography algorithm shows that the training accuracy goes from 0.54% to 0.97% over time, as shown in figure 4. At the same time, the associated loss goes from 0.68 to 0.05. Investigation accuracy rises from 0.70 to 0.97, while investigation loss diminishes to 0.1. Figure 5 shows ROC curves that show how well the S-UNIWARD algorithm worked during both training and validation. The accuracy during training was 0.89, and the accuracy during validation was 0.84. Figure 6 depicts the training trajectory of the HILL steganography algorithm, demonstrating an increase in training accuracy from 0.60 to 0.95, accompanied by a decrease in loss from 0.68 to 0.1. Additionally, Figure 7 presents ROC curves for the training and validation of the HILL algorithm. Both the S-UNIWARD and HILL algorithms showed better training accuracy and less loss, which suggests that they learned well and were able to help the model find information hidden in images. The consistent augmentation in accuracy reflects the model's enhanced proficiency in uncovering hidden information, while the sustained decline in loss signifies its progression towards optimal performance and error minimization.

DOI: https://doi.org/10.54216/JCIM.150101
Received: January 21, 2024 Revised: April 20, 2024 Accepted: July 12, 2024

7. Comparing the proposed model with SR-NET, GBRAS-NET, and ZHU-NET.

In this section, we conduct a comprehensive comparison between the proposed CNN model and three existing architectures: GBRAS-Net, ZHU-Net, and SR-Net. These selections were based on their observed performance in addressing the classification problem under investigation. The following organized paragraph outline the disparities and similarities noted across these CNN architectures. All four CNN models process images of size 256 × 256. While the pre-processing stage in SR-Net has been eliminated, with all stages now integrated into convolutional layers only, the proposed model, ZHU-Net, YE-Net, and GBRAS-Net retain this filtering step in the pre-processing stages. The proposed model comprises 7 convolutional layers, contrasting SR-Net's 25 layers, ZHU-Net's 5 convolutional layers, and GBRAS-Net's 9 layers. Within their convolutional layers, the proposed model, ZHU-Net, and SR-Net all incorporate ReLU activation functions, while GBRAS-Net opts for the ELU activation function. Regarding pooling layers, the proposed model integrates 4 layers of AveragePooling2D with a kernel size of (3,3) and strides of (2, 2), akin to SR-Net's incorporation of 5 layers with a similar kernel size and stride. Conversely, ZHU-Net employs 3 layers with a kernel size of (5,5) and stride (2, 2), whereas GBRAS-Net implements 4 layers with a kernel size of (2,2) and stride (2, 2The proposed model and GBRAS-Net have four separable convolutional layers, while ZHU-Net has two. In contrast, SR-Net uses no detachable convolutions. Furthermore, the proposed model and GBRAS-Net incorporate four Depthwise Convolutional Layers, whereas SR-Net and ZHU-Net lack Depthwise Convolutional Layers. ZHU-Net has an absolute value layer, unlike the suggested model, GBRAS-Net, and SR-Net. The suggested model, GBRAS-Net, and SR-Net use Global-Average-Pooling layers for classification. Instead of this, ZHU-Net uses the Multi-level Average-Pooling layer.

8. Conclusion

The steganalysis methodology proposed here aims to secure data and increase cybersecurity. The study presents a new steganalysis model that outperforms previous methods by providing a fresh way to maximizing local characteristics, hence improving classification performance. The suggested framework is specifically designed to handle digital images of a predetermined size in the spatial domain. The model employs a CNN architecture and utilizes 30 SRM filter banks for preprocessing. Additionally, it employs average pooling layers within the DepthwiseConv2D and convolutional layers to extract features. The final probabilistic classification is obtained by using a fully connected layer combined with a sigmoid function. Significantly, the suggested CNN surpasses the most advanced designs in reliably identifying hidden data while ensuring the stability of the network during the training process. In the future, we plan to improve our ability to detect small hidden messages by combining the BOSS Base 1.01 and BOWS datasets in our steganalysis research. Furthermore, our goal is to examine modified pixels in steganographic images, drawing inspiration from approaches suggested in previous research. Our upcoming research is to enhance the performance of CNN models in the field of digital image forensics. Thereby strengthening the procedures taken to ensure cybersecurity.

Funding: "This research received no external funding"

Conflicts of Interest: "The authors declare no conflict of interest."

References

[1] Darch Abed Dawar, A. (2024). Enhancing Wireless Security and Privacy: A 2-Way Identity Authentication Method for 5G Networks. International Journal of Mathematics, Statistics, and Computer Science, 2, 183–198. https://doi.org/10.59543/ijmscs.v2i.9073

[2] N. J. De La Croix, C.C.I.a.T.A., Secret message protection using fuzzy logic and difference expansion in digital images.Nigeria 4th International Conference on Disruptive Technologies for Sustainable Development (NIGERCON), pp 1–5. NIGERCON54645.2022.9803151 IEEE 2022.

[3] Ferreira, W.D.F.C.B.R., A review of digital image forensics. leceng.2020.106685. Comput Electr Eng, 2020.

[4] Warkentin, M., E. Bekkering, and M. Schmidt, Steganography: Forensic, Security, and Legal Issues. Journal of Digital Forensics, Security and Law, 2008.

[5] Liu, J., et al., Efficient binary image steganalysis based on ensemble neural network of multi-module. Journal of Real-Time Image Processing, 2019. 17(1): p. 137-147.

DOI: https://doi.org/10.54216/JCIM.150101
Received: January 21, 2024 Revised: April 20, 2024 Accepted: July 12, 2024

[6] Ahmed A. Alsabhany, A.H.A., Digital audio steganography: Systematic review, classification, and analysis of the current state of the art. Computer Science, November 2020.

[7] Y. Qian, J.D., W. Wang, and T. Tan, ''Deep learning for steganalysis via convolutional neural networks,'' in Proc. IS T Int. Symp. Electron. Imag.(EI), vol. 9409, 2015, Art. no. 94090J.

[8] Xu, G., H.-Z. Wu, and Y.-Q. Shi, Structural Design of Convolutional Neural Networks for Steganalysis. IEEE Signal Processing Letters, 2016. 23(5): p. 708-712.

[9] Ye, J., J. Ni, and Y. Yi, Deep Learning Hierarchical Representations for Image Steganalysis. IEEE Transactions on Information Forensics and Security, 2017. 12(11): p. 2545-2557.

[10] Yedroudj, M., F. Comby, and M. Chaumont, Yedroudj-Net: An Efficient CNN for Spatial Steganalysis, in 2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). 2018. p. 2092-2096.

[11] K. He, X.Z., S. Ren, and J. Sun, "Deep residual learning for image recognition," in Proceedings of the IEEE conference on computer vision and pattern recognition 2016, pp. 770–778.

[12] Zhang, R., et al., Depth-Wise Separable Convolutions and Multi-Level Pooling for an Efficient Spatial CNN-Based Steganalysis. IEEE Transactions on Information Forensics and Security, 2020. 15: p. 1138-1150.

[13] Reinel, T.-S., et al., GBRAS-Net: A Convolutional Neural Network Architecture for Spatial Image Steganalysis. IEEE Access, 2021. 9: p. 14340-14350.

[14] Taha Ahmed, I., B. Tareq Hammad, and N. Jamil, Image Steganalysis based on Pretrained Convolutional Neural Networks, in 2022 IEEE 18th International Colloquium on Signal Processing & Applications (CSPA). 2022. p. 283-286.

[15] de La Croix, N.J. and T. Ahmad, Toward Hidden Data Detection via Local Features Optimization in Spatial Domain Images, in 2023 Conference on Information Communications Technology and Society (ICTAS). 2023. p. 1-6.

[16] Agarwal, S., C. Kim, and K.-H. Jung, Steganalysis of Context-Aware Image Steganography Techniques Using Convolutional Neural Network. Applied Sciences, 2022. 12(21).

[17] Z. Yang, Q.L., S. Luo, S. Tan and B. Li,, "Improving VGG-Style Convnet for JPEG Steganalysis,". IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) Republic of, 2024, pp(4450-4454).

[18] Mario Alejandro Bravo-Ortiz a, E.M.-R.a., CVTStego-Net: A convolutional vision transformer architecture for spatial image steganalysis. Journal of Information Security and Applications, 2024.

[19] P. Bas, T.F., and T. Pevný, 'Break Our Steganographic System': The Ins and Outs of Organizing BOSS. In Proceedings of the 13th International Conference on Information Hiding IH'2011, volume 6958 of Lecture Notes in Computer Science, pages 59–70, Prague, Czech Republic May 2011. Springer.

[20] B. Li, M.W., J. Huang, and X. Li, "A new cost function for spatial image steganography,". in 2014 IEEE international Conference on Image Processing (ICIP) Oct 2014, pp. 4206–4210.

[21] Holub, V., J. Fridrich, and T. Denemark, Universal distortion function for steganography in an arbitrary domain. EURASIP Journal on Information Security, 2014. 2014(1).

DOI: https://doi.org/10.54216/JCIM.150101
Received: January 21, 2024 Revised: April 20, 2024 Accepted: July 12, 2024