applied sciences

MDPI

Article

Steganalysis of Context-Aware Image Steganography Techniques Using Convolutional Neural Network

Saurabh Agarwal [1,2], Cheonshik Kim [3] and Ki-Hyun Jung [2,*]

[1] Department of Computer Science and Engineering, Amity School of Engineering & Technology, Amity University Uttar Pradesh, Noida 201313, India
[2] Department of Software Convergence, Andong National University, Andong 36729, Korea
[3] Department of Computer Engineering, Sejong University, Seoul 05006, Korea
* Correspondence: khanny.jung@gmail.com or kingjung@anu.ac.kr; Tel.: +82-54-820-7968; Fax: +82-54-820-6257

Abstract: Image steganography is applied to hide some secret information. Occasionally, steganography is used for malicious purposes to hide inappropriate information. In this paper, a new deep neural network was proposed to detect context-aware steganography techniques. In the proposed scheme, a high-boost filter was applied to alleviate the high-frequency while retaining the low-frequency details. The high-boost image was processed by thirty SRM high-pass filters to obtain thirty high-boost SRM filtered images. In the proposed CNN, two skip connections were used to collect information from multiple connections simultaneously. A clipped ReLU layer was considered in spite of the general ReLU layer. In constructing the CNN, a bottleneck approach was followed for an effective convolution. Only a single global average pooling layer was used to retain the complete flow of information. SVM was utilized instead of the softmax classifier to improve the detection accuracy. In the experimental results, the proposed technique was better than the existing techniques in terms of the detection accuracy and computational cost. The proposed scheme was verified on BOWS2 and BOSSBase datasets for the HILL, S-UNIWARD, and WOW context-aware steganography algorithms.

Keywords: image steganography; image steganalysis; convolutional neural network; deep learning network

Citation: Agarwal, S.; Kim, C.; Jung, K.-H. Steganalysis of Context-Aware Image Steganography Techniques Using Convolutional Neural Network. *Appl. Sci.* **2022**, *12*, 10793. https://doi.org/10.3390/app122110793

Academic Editor: Habib Hamam

Received: 24 August 2022
Accepted: 19 October 2022
Published: 25 October 2022

1. Introduction

Image steganography can be defined as a non-uniform operation unlike other conventional operations such as high-pass filtering, contrast enhancement, etc. The secret contents are embedded by changing the pixel values in random order, mostly unnoticeable due to the context-aware approach. Statistical changes are unnoticeable because most of the steganography algorithms increase the existing pixel values by only +1 or decrease by −1. Steganalysis discloses the minute changes of image steganography. In this paper, steganalysis was performed for three popular context-aware steganography algorithms-HILL [1], S-UNIWARD [2], and WOW [3]. In Figure 1a, the cover image is shown and difference array images (DI) of the cover image and the stego-image are shown in Figure 1b–d for HILL, S-UNIWARD, and WOW, respectively, with 0.4 bits per pixel (bpp) payload.

Furthermore, an image was formed to see the nature of different steganography algorithms. In Figure 2a, the cover image has four triangles. There is a difference of one pixel intensity in each triangle. The difference array images (DI) of the cover and stego-images after applying the HILL, S-UNIWARD, and WOW steganography algorithms with payloads of 0.4 bpp are displayed in Figure 2. The artifacts of steganography can be seen in the DI of the cover and HILL image (Figure 2b). The changes were more visible in the minor and major diagonal edge areas than in other areas. However, the changes were more visible in the DI of the S-UNIWARD image (Figure 2c) in comparison to the DI of the HILL image (Figure 2b). The nature of WOW was different, as evident from Figure 2d, as only the diagonal area was used for data embedding.

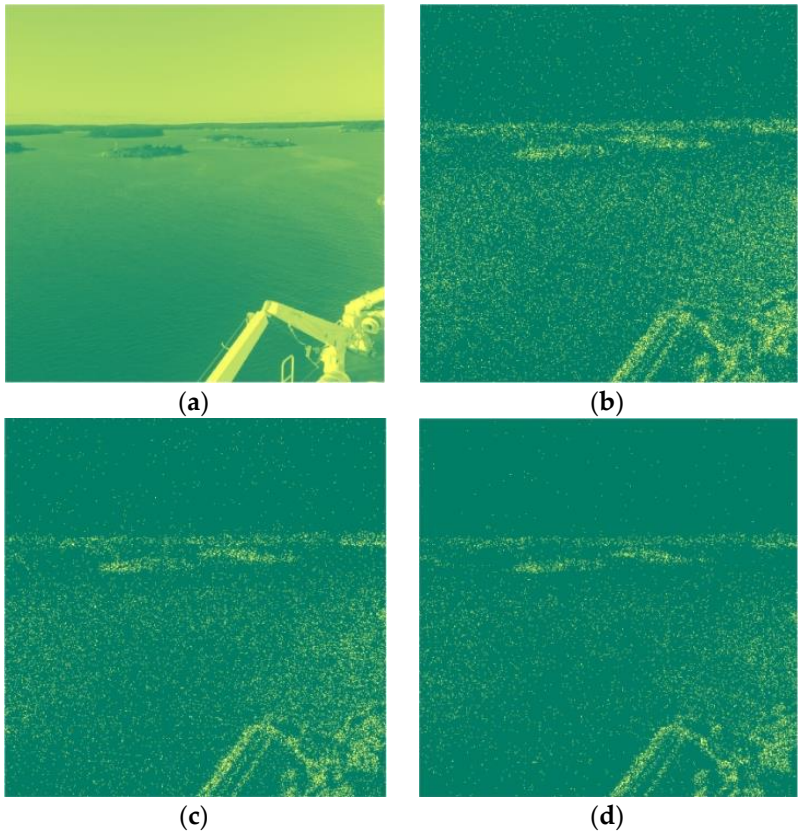


Figure 1. Natural cover image and difference arrays of the cover and stego-image. (**a**) Cover image. (**b**) DI of the cover and HILL stego-image. (**c**) DI of the S-UNIWARD stego-image. (**d**) DI of the WOW stego-image.

It can be seen from Figures 1 and 2 that HILL changed the image pixels in a more uniform manner than S-UNIWARD and WOW. However, changes by WOW were mostly only in dense regions. HILL changes were not in a particular region, which makes the detection of HILL more challenging than S-UNIWARD, followed by WOW. This claim has been verified in the previous literature and in Section 3 of the experimental results.

Previously, most of the techniques relied upon the texture operator based features and Markov features. Difference arrays and residual arrays of the image are considered to extract higher dimension features. Lyu and Farid [4] considered the magnitude and phase statistics in the frequency domain to detect Outguess [5] and F5 [6] steganography techniques. Li et al. [7] extracted the Markov and texture features to classify the cover and stego-images. The high dimensional feature vector of size 22,153 is used for HUGO [8] steganography detection. Penvy et al. [9] utilized the second-order Markov features from difference arrays in eight directions for the detection of the least significant bit (LSB) matching steganography. Hou et al. [10] extracted the Markov features in the DFT and DCT domains to detect seven different steganography techniques. Fridrich and Kodovsky [11] extracted the 34,671 features using the Markov model using thirty high-pass filtered images. These high-pass filters are commonly known as SRM filters. Tang et al. [12] proposed the technique for WOW. Markov features can be extracted from the texture and edge area, especially for superior results. To reduce the size of the feature vector of the method [11], the maxSRM and maxSRMd2 techniques were proposed by Denemark et al. [13]. The technique was applied to S-UNIWARD, S-UNIGARD, and WOW. Xu et al. [14] suggested the local correlation pattern to identify HUGO, LSB matching revisited LSBMR [15], and the S-UNIWARD techniques. Li et al. [16] first applied the high-pass filter and then extracted the texture features. PCA was applied twice to reduce the feature dimension and improve the accuracy. Li's technique was verified on the WOW and HUGO steganography

methods. Li et al. [17] proposed the variant of the local binary pattern (LBP) using adaptive thresholding. Second-order Markov and TLBP features were combined for better results. Li's technique was applied to S-UNIWARD, HILL, CMD-HILL [18], and MiPOD [19]. Li's work was extended by Wang et al. [20] by modifying the rotation invariant uniform pattern (RIU) mapping using a feature separation study. The features were also aggregated with the SRM frequency domain features. This technique was applied to detect S-UNIWARD, HILL, and MiPOD stego-images. Ge et al. [21] extracted the TLBP and Markov features from residual arrays of non-negative matrix factorization, high-pass filters, and derivative filters to detect HILL, CMD-HILL, and MiPOD stego-images. Markov features were found to be effective in most of the manual feature extraction schemes. Due to its effectiveness, most of the schemes utilized the Markov model and improved the results by using a different type of residual array, combined with the texture features as discussed above. In parallel, many techniques have evolved that are based on convolutional neural networks. Currently, most of the techniques utilize deep learning networks not only for steganalysis as well in many other applications. However, this paradigm shift requires efficient hardware that is easily available in the current era. Qian et al. [22,23], for the first time, used the CNN to identify WOW, HUGO, and S-UNIWARD steganography techniques. In CNN, various types of layers such as the convolutional layer, ReLU layer, batch normalization layer, and pooling layer are used. Images were operated with one 5×5 high-pass filter before processing to the CNN. However, the results are not superior in comparison to the manual feature extraction techniques. Xu et al. [24] also used the single filter for preprocessing. Xu et al. introduced the absolute layer and utilized the tanh activation function to detect the S-UNIWARD and HILL technique. Wu et al. [25,26] continued to utilize the same single high-pass filter [22] and apply the proposed CNN on multiple residual arrays to identify HILL, MiPOD, S-UNIWARD, and WOW stego-images. The SRM filters [11] based on the Markov model were also found to be helpful in the CNN network. Ye et al. [27] considered the residual of thirty SRM filter [11] images in the CNN, a truncated linear unit (TLU) instead of ReLU and the selection channels. The results of Ye's technique were better than previous methods on HILL, S-UNIWARD, and WOW. Boroumand et al. [28] proposed the popular steganalysis residual network (SRNet) to detect HILL, J-UNIWARD, S-UNIWARD, UED-JC [29], and WOW. Three types of block arrangements were used in the network using residual connections and a pooling layer. Statistical moments from the trained network were extracted to detect the cover and HILL, MiPOD, S-UNIWARD, and WOW stego-images. In Yedroudj et al. [30], a CNN with thirty SRM filters were used in the non-trainable layer. CNN is highly influenced by deep networks [24,27]. The results are shown for S-UNIWARD and WOW. Wu et al. [31] introduced the shared batch normalization layer and utilized twenty SRM filters. Zhang et al. [32] preprocessed the image using thirty SRM filters. In CNN, bottleneck and spatial pyramid pooling were introduced for the better detection of HILL, S-UNIWARD, and WOW stego-images. Xiang et al. [33] claimed better results on S-UNIWARD and WOW by changing the arrangements of the layers. The preprocessing was performed using thirty SRM filters. Wang et al. [34] applied the transfer learning approach by using the weights from a low embedding stego-image trained network. Wang et al. considered the spatial and frequency domain together to identify S-UNIWARD and WOW stego-images while the preprocessing was performed using thirty SRM filters.

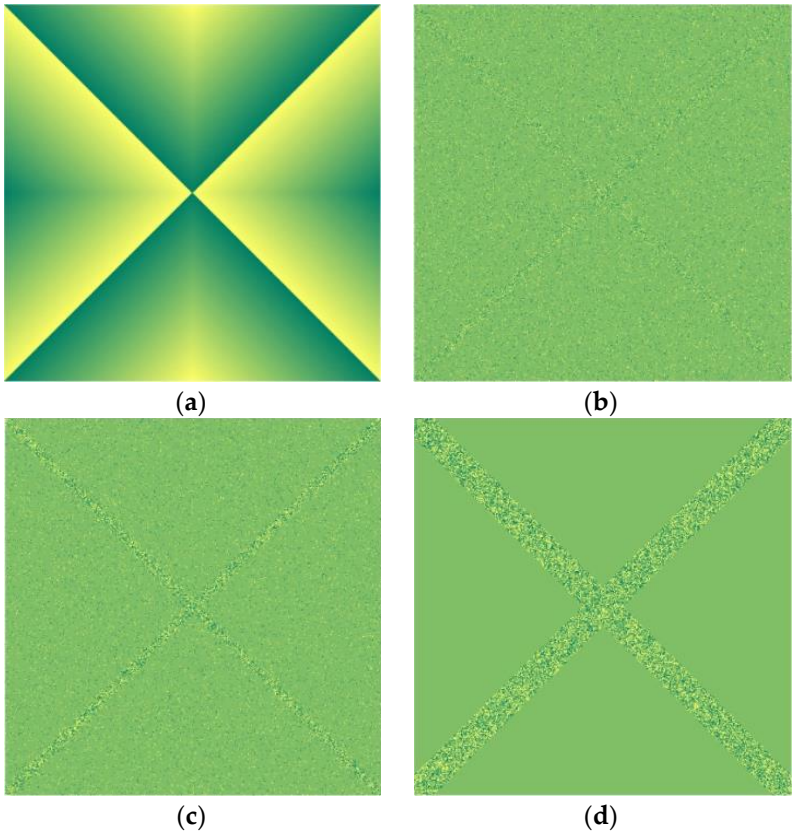


Figure 2. Computer-generated cover image and difference arrays of the cover and stego-image. (**a**) Cover image. (**b**) DI of cover and HILL stego-image. (**c**) DI of S-UNIWARD stego-image. (**d**) DI of WOW stego-image.

It can be concluded from previous literature that SRM high-pass filters, residual connections, and different arrangements of layers can alleviate the detection accuracy of CNN. In this paper, several effective steps were taken to improve the network efficacy. The major steps of the suggested technique are given below:

- The proposed technique highlights the high-frequency elements using a high-boost filter in the first non-trainable convolutional layer. It improves the detection accuracy by more than one percent.
- Thirty high-pass filtered images were generated using SRM filters in the second non-trainable convolutional layer to give prominence to the noise of the stego-image effectively.
- A single pooling layer in the last part of the CNN was used to sustain the complete statistical traces from each layer.
- A clipped ReLU layer was introduced for customized thresholding to obtain more statistical information.
- The SVM classifier was utilized instead of the softmax classifier to increase the detection performance. The SVM classifier outperforms in many applications.
- Experimental results of the proposed technique were compared with SRNet, Ye-Net, Yedroudj-Net, and Zhu-Net. The experimental results are displayed for the HILL, S-UNIWARD, and WOW steganography algorithms with payloads of 0.2, 0.3, and 0.4 bits per pixel.
- In the detailed experimental analysis, the proposed technique was proven to be better than the existing techniques with a higher detection accuracy.

In the next section, the proposed technique is discussed. The experimental analysis is discussed in Section 3. The conclusions are presented in Section 4.

2. The Proposed Scheme

Image steganalysis is required to restrict the misuse of steganography techniques. The detection of steganography is more challenging than other types of image manipulations such as image enhancement, median filtering, and so on, due to its non-uniform and minute modifications in pixel intensity. A new robust scheme was proposed for detecting the steganography in the image. Effective measures were applied to improve the existing steganalysis techniques. Unlike previous techniques, a high-boost filter was applied to reveal crucial statistical information. A high-boost filter [35,36] highlights the high-frequency components without compromising low-frequency components. A high-boost filter H_k can be defined as follows. In here, C_{HP} is any high-pass filter and k is a constant.

$$H_k = C_0 + kC_{HP}$$

$$H_k = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix} + k \begin{bmatrix} 0 & -1 & 0 \\ -1 & 4 & -1 \\ 0 & -1 & 0 \end{bmatrix}$$

$$H_k = \begin{bmatrix} 0 & -k & 0 \\ -k & 4k+1 & -k \\ 0 & -k & 0 \end{bmatrix}$$

In Figure 3a, a pristine cover image is shown. The SRM filtered image after applying the S SRM filter on a pristine image (Figure 3a) is displayed in Figure 3b. In Figure 3c, a high-boost filtered image is displayed using a high boost filter H_1 on a pristine image (Figure 3a). Furthermore, the S SRM filter was applied to the high-boost filtered image (Figure 3c) and the resultant image is displayed in Figure 3d. The coarseness of Figure 3d helped in increasing the detection accuracy of the proposed technique. A total of thirty SRM filters was applied to enhance the statistical information. The SRM filters have several kernel weights that provide additional statistical information in multiple directions.

$$S = \begin{bmatrix} -1 & 2 & -1 \\ 2 & -4 & 2 \\ -1 & 2 & -1 \end{bmatrix} H_1 = \begin{bmatrix} 0 & -4 & 0 \\ -4 & 17 & -4 \\ 0 & -4 & 0 \end{bmatrix}$$

(**a**) (**b**)

Figure 3. *Cont.*

(**c**) (**d**)

Figure 3. Cover image, SRM, high-boost, high-boost with SRM filtered image. (**a**) Cover image. (**b**) SRM filtered image. (**c**) High-boost filtered image. (**d**) SRM filtered image of Figure 3c.

To show the effectiveness of the high-boost filter, the probability plots for normal distribution are displayed for the cumulative variance of the cover and stego-images in Figure 4. Ten thousand images of BOWS2 [37] were considered after resizing to the dimensions of 256 × 256 pixels. In Figure 4a–c, the plots are shown for the S-UNIWARD steganography technique used with payloads of 0.2 bpp, 0.3 bpp and 0.4 bpp, respectively, and in Figure 4d–f, the WOW steganography technique is considered. A similar behavior was also followed by HILL. DNF is the variance of the non-filtered cover image and stego-image. DHB is the variance of the high-boost filtered cover image and high-boost filtered stego-image. The normal distribution data of DHB had much greater disparity than DNF. This disparity helps in improving the detection of the cover and stego-images.

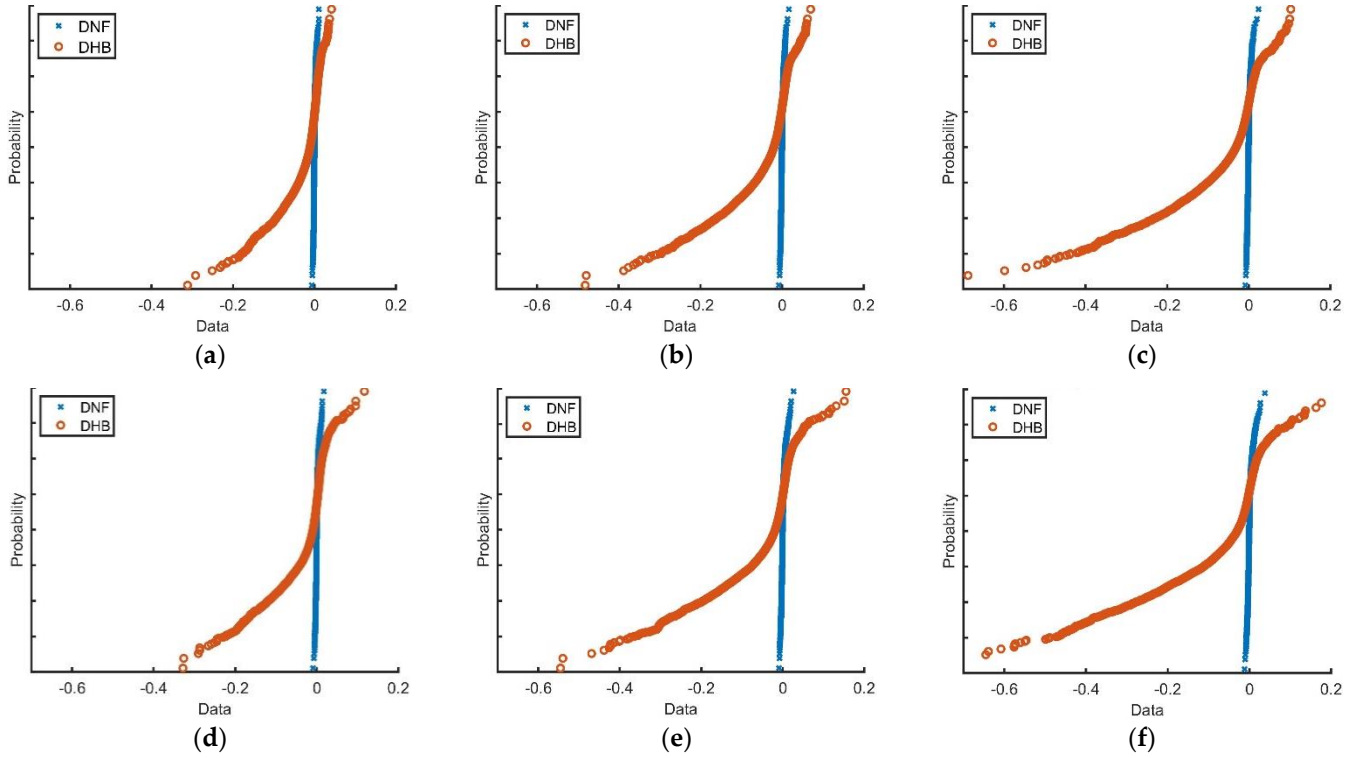
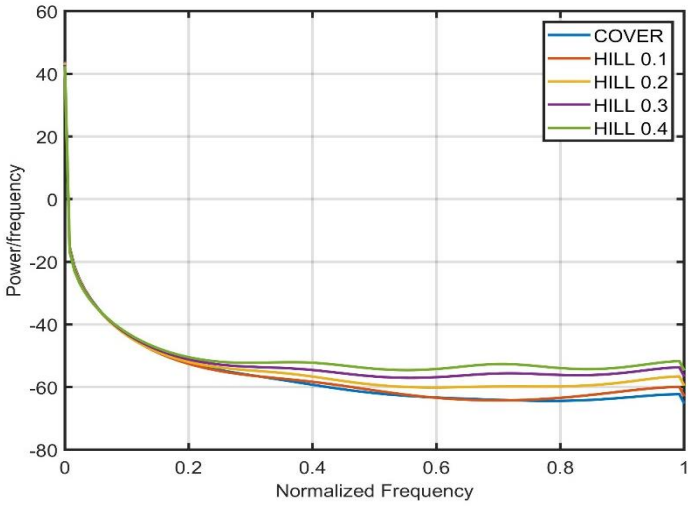


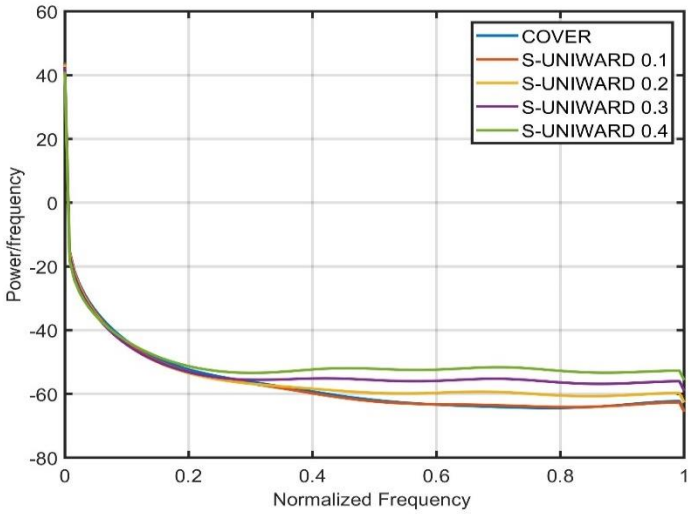
Figure 4. Probability plots for the normal distribution of non-filtered and high-boost filtered images. (**a**) S-UNIWARD ρ = 0.2. (**b**) S-UNIWARD ρ = 0.3. (**c**) S-UNIWARD ρ = 0.4. (**d**) WOW ρ = 0.2. (**e**) WOW ρ = 0.3. (**f**) WOW ρ = 0.4.

Furthermore, in Table 1, the percentage increase in the modified pixels after applying high-boost filtering is displayed. First, the number of modified pixels was calculated using the cover and stego-images. Second, the number of modified pixels was calculated using a high-boost filtered cover and high-boost filtered stego-image. As can be seen, there was more than a 50% increase in modified pixels for WOW with ρ = {0.2, 0.3, 0.4}. There was an increase in the modified pixels of 40.58% for S-UNIWARD and 45.43% for HILL with ρ = 0.2 bpp. Table 1 also proves the effectiveness of the high-boost filter.

The overall behavior of the HILL, S-UNIWARD, and WOW steganography techniques are displayed in Figure 5 according to their payloads. Ten thousand images of BOWS2 were considered after resizing to dimensions of 256 × 256 pixels to plot the entropy covariance plot. In Figure 5a, the plot is displayed for the cover and HILL stego-images of with various payloads of 0.1 bpp, 0.2 bpp 0.3 bpp, and 0.4 bpp. Entropy covariance plots of S-UNIWARD and WOW algorithms are displayed in Figure 5b,c, respectively. The model of plots is alike for the S-UNIWARD, WOW, and HILL steganography techniques. However, the gap between the cover and stego-images varied according to the payload. Thus, a common convolutional neural network can be suggested to identify between the cover and HILL, S-UNIWARD, and WOW different stego-images.

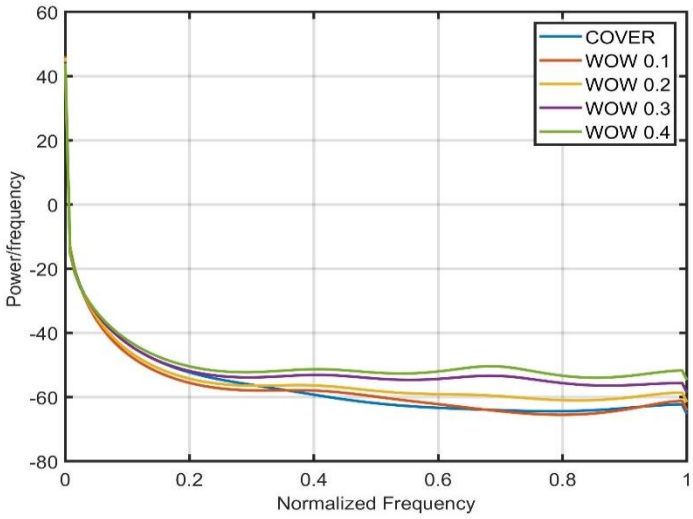


(**a**)



(**b**)

Figure 5. *Cont.*



(**c**)

Figure 5. Entropy covariance plots of the cover and stego-images. (**a**) Covariance plot of the cover and HILL. (**b**) Covariance plot of the cover and S-UNIWARD. (**c**) Covariance plot of the cover and WOW.

Table 1. Percentage increase of the pixels modified after high-boost filtering.

Payload (bpp)	HILL	S-UNIWARD	WOW
0.2	45.43	40.58	53.33
0.3	46.95	39.87	53.79
0.4	48.61	41.27	54.49

The proposed convolutional neural network block diagram is displayed in Figure 6 after considering the previous literature and the above discussion. In most of the previous CNN based techniques [27,30–34], the SRM filters [11] were used as preprocessing layers in the CNN. In this paper, two preprocessing layers were used for revealing the stego-noise effectively. One high-boost kernel with dimensions of 3×3 was considered in the first non-trainable preprocessing layer to capture the stego-noise. In the second non-trainable preprocessing layer, thirty SRM filters with dimensions of 5×5 were taken. Furthermore, the bottleneck approach applied in each convolutional layer block as in [32] gave better results than the conventional approach. The abstract diagram of the bottleneck approach is displayed in Figure 7. In blocks 1–14, either 18 kernels or nine kernels were used. Unlike the previous CNN, the number of kernels was a lot less. The lower number of kernels reduced the computation cost drastically. In the experimental analysis, some experiments were performed by using a higher number of kernels but there was no advantage in the detection accuracy. Therefore, a fewer number of kernels were considered. Weight was initialized using the Glorot and Bengio [38] method. In every fourteen blocks, the order of the layer was as follows: convolution layer with 3×3 filter, convolution layer with 1×1 filter, bath normalization layer, and clipped rectifier linear unit layer [39]. Two skip connections were also used after block 5 and block 10 for better detection. No pooling layer was used until block 14 in the network. One global average pooling layer [30,40] was considered after fourteen blocks. The consideration of only one GAP layer ensures the maximum flow of statistical information between the blocks. The RMSprop optimizer was utilized in CNN training. The number of epochs was considered as a hundred with a mini-batch size of twenty. Furthermore, features were extracted from the GAP layer using the activation function. The features of both classes (i.e., cover and stego-images) were classified using an SVM classifier with a Gaussian kernel as the function. Sequential minimal optimization [41] was used for fast and optimized convergence.

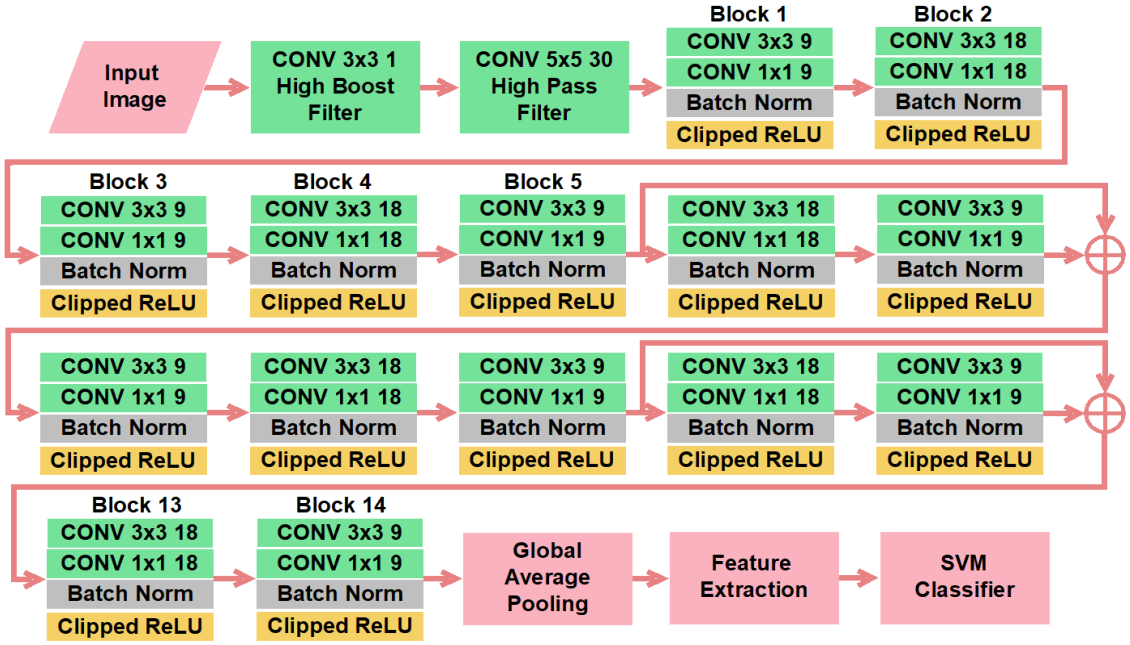


Figure 6. Block diagram of the proposed CNN.

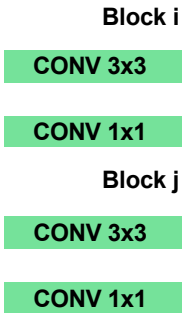


Figure 7. Bottleneck approach.

In most of the earlier networks, the ReLU layer was utilized for thresholding. The negative elements were replaced with zero in the conventional ReLU layer. The ReLU can be better understood by the following function:

$$R(i) = \begin{cases} i, & i \geq 0 \\ 0, & i < 0 \end{cases}$$

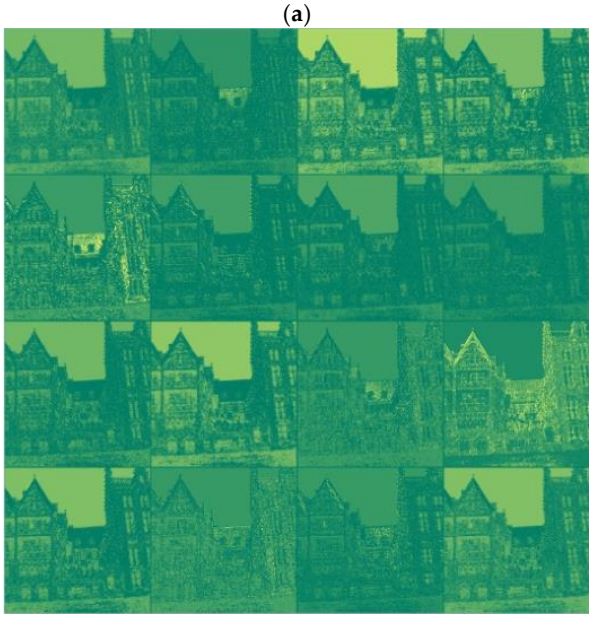
However, in clipped ReLU (CReLU), negative elements were replaced with zero, the elements higher than the clipping ceiling value (threshold T) were replaced with the clipping ceiling value, and other elements remained intact. The CReLU can be defined by the following function:

$$R(i) = \begin{cases} 0, & i < 0 \\ i, & 0 \leq i < T \\ T, & i \geq T \end{cases}$$

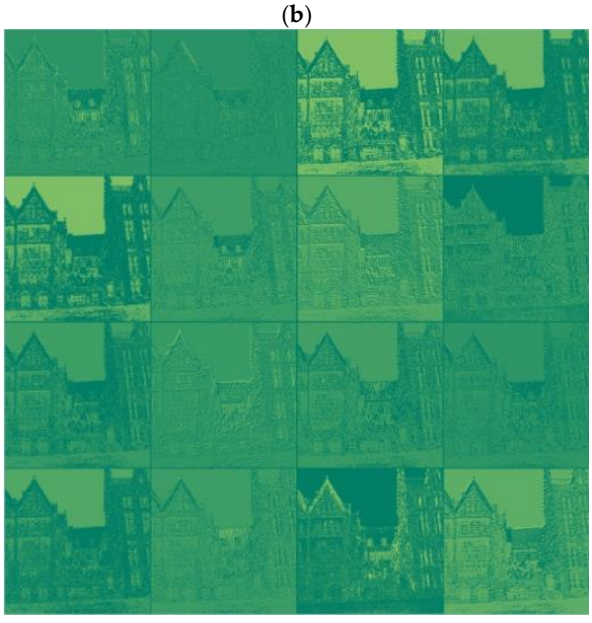
The threshold value has a crucial effect on network optimization. The threshold value was considered after exhaustive experimental analysis. The HILL steganography technique was considered to decide the threshold value as the detection of the HILL steganography technique is more difficult than S-UNIWARD and WOW. Stego-images with payloads of 0.2 bpp and 0.3 bpp were taken to decide the threshold value. In Figure 8, the effect of the ReLU and clipped ReLU layer is displayed on network kernels. After network training, the

behavior of network kernels was different for ReLU and CReLU. Sixteen kernels of layer 9 were used to display the images after a kernel operation in the Figure 8a image for both ReLU and CReLU.

(**a**)



(**b**)



(**c**)

Figure 8. Kernel affects using ReLU and CReLU layers. (**a**) An image. (**b**) Layer 9 kernels with ReLU. (**c**) Layer 9 kernels with CReLU.

3. Experimental Analysis

Image steganography is performed to hide some secret information. In some cases, steganography is misused. In this paper, the image steganalysis technique was proposed to restrict the misuse of image steganography. The proposed technique was verified for multiple cases. Two popular datasets BOSSBase [42] and BOWS2 [37] were used for detailed experimental study. Both datasets had ten thousand images with the dimensions of 512 × 512 pixels. The dimension of the images was changed to dimensions of 256 × 256 pixels using interpolation. Experimental analysis was performed on the dimensions of 256 × 256 pixels. The proposed technique was compared with the popular state-of-the-art techniques SRNet [28], Ye-Net [27], Yedroudj-Net [30], and Zhu-Net [32]. The detailed experimental analysis was performed by considering three cases of image dataset combination.

Case I: The BOSSBase dataset was considered in Case I. Stego-images were created using three steganography algorithms—HILL, S-UNIWARD, and WOW. Four thousand images were considered for training, one thousand for validation, and five thousand for testing from both the classes, cover, and stego. Multiple pairs were formed according to the different payloads and steganography algorithms.

Case II: The BOWS2 and BOSSBase image datasets were considered in Case II. In comparison to Case I, a higher number of images were considered in Case II for better results. Fourteen thousand images were considered for training the network, one thousand images for validation, and five thousand images for testing the trained network. An equal number of images were taken from the BOWS2 and BOSSBase datasets. The same number of stego-images was also created according to the steganography algorithm and payload.

Case III: Like Case II, both datasets were considered. One hundred and twenty-five thousand cover images were created after applying data augmentation on both datasets. A hundred thousand images were used for training, five thousand for validation, and fifteen thousand for testing. Corresponding stego-images were also created according to the steganography algorithm and payload.

The HILL, S-UNIWARD, and WOW stego-images with embedding payloads of 0.2, 0.3, and 0.4 bpp were considered in the experimental results. The results are displayed in terms of the classification accuracy in percentage. In Table 2, the effect of the high-boost filter and clipped ReLU (CReLU) is displayed while considering Case I and the softmax classifier. In most of the previous literature, SRM filters were applied as pre-processing or in non-trainable layers to improve the detection of stego-noise. Therefore, SRM filters were considered in each result. In the first row, the results are displayed using SRM filters and ReLU layers on the proposed network while not including a high-boost non-trainable layer. In the second row, the results are displayed using SRM filters and CReLU layers while not including the high-boost non-trainable layer. In the third row, the results are displayed using ReLU layers in the proposed network. In the fourth row, the results are displayed using the proposed network. The softmax classifier was used for classification in the four scenarios.

Table 2. Performance analysis of a high-boost filter and CReLU layer.

S. No.	Steganography Technique/ Payload (bpp)	HILL			S-UNIWARD			WOW		
		0.2	0.3	0.4	0.2	0.3	0.4	0.2	0.3	0.4
1	SRM + ReLU	60.33	67.09	69.69	68.05	76.27	82.35	73.46	80.48	84.75
2	SRM + CReLU	61.24	67.90	70.82	69.02	77.04	81.61	74.13	81.79	85.43
3	HB + SRM + ReLU	61.93	69.14	71.68	69.51	77.97	82.85	75.03	82.45	86.38
4	HB + SRM + CReLU	62.49	68.59	72.26	70.00	78.68	84.11	76.02	83.36	87.74

Usually, a softmax classifier is utilized in CNN. In experimental analysis, some other classifiers have also been tried. The SVM classifier has been proven to be better than many

classifiers. It was also found in the experimental analysis that the SVM classifier performed better than the softmax classifier in most of the scenarios, as can be seen in Table 3. The sequential minimal optimization was used for fast and optimized convergence.

Table 3. Performance analysis of the softmax and SVM classifier.

S. No.	Steganography Technique/ Payload (bpp)	HILL			S-UNIWARD			WOW		
		0.2	0.3	0.4	0.2	0.3	0.4	0.2	0.3	0.4
1	Softmax Classifier	62.49	68.59	72.26	70.00	78.68	84.11	76.02	83.36	87.74
2	SVM classifier	63.25	69.91	73.07	69.54	79.88	84.79	77.02	83.95	87.26

In Table 4, the results are displayed for Case I using the proposed technique. The results were also compared with other popular techniques such as SRNet [28], Ye-Net [27], Yedroudj-Net [30], and Zhu-Net [32]. The detection accuracy of the proposed technique and other techniques was the highest for WOW, followed by the S-UNIWARD and HILL steganography algorithms. The proposed technique results are more impressive than other techniques except for S-UNIWARD with 0.2 bpp and HILL with 0.4 bpp. In the two scenarios, the detection accuracy of Zhu-Net was better than the proposed method. The proposed method gave 77.02, 83.95, and 87.26% detection accuracies for WOW with payloads of 0.2 bpp, 03 bpp, and 0.4 bpp, respectively.

Table 4. The performance assessment while considering Case I.

Steganography Technique/ Payload (bpp)	HILL			S-UNIWARD			WOW		
	0.2	0.3	0.4	0.2	0.3	0.4	0.2	0.3	0.4
SRNet	55.51	63.64	67.62	64.97	73.88	79.34	72.52	79.41	83.59
Ye-Net	54.31	59.40	63.85	60.20	68.01	74.83	69.39	72.97	78.65
Yedroudj-Net	54.09	58.72	67.98	59.74	69.29	74.97	69.96	75.52	81.07
Zhu-Net	61.74	66.61	74.56	70.23	78.12	82.81	74.37	78.41	86.23
Proposed Method	63.25	69.91	73.07	69.54	79.88	84.79	77.02	83.95	87.26

For better results, additional numbers of images were considered for training the network. In Case II, fourteen thousand images were taken for CNN training. There was a substantial enhancement in detection accuracy, as can be seen in Table 5. The proposed technique gave 64.49%, 74.10%, and 77.13% detection accuracies for HILL with the 0.2, 0.3, and 0.4 bpp payloads, respectively. The proposed technique gives 75.06%, 83.64%, and 86.85% for S-UNIWARD with 0.2, 0.3, and 0.4 bpp payloads, respectively. The proposed technique gave 81.50%, 88.81%, and 91.78% for WOW with the 0.2, 0.3, and 0.4 bpp payloads, respectively. Zhu-Net provided better results by a slight margin for HILL $\rho = 0.4$ bpp and WOW $\rho = 0.4$ bpp.

Table 5. Performance assessment while considering Case II.

Steganography Technique/ Payload (bpp)	HILL			S-UNIWARD			WOW		
	0.2	0.3	0.4	0.2	0.3	0.4	0.2	0.3	0.4
SRNet	60.85	67.10	68.79	67.17	76.18	79.06	77.40	83.97	88.49
Ye-Net	53.79	61.60	65.61	62.32	70.60	74.98	70.42	78.81	82.37
Yedroudj-Net	57.28	64.14	66.91	63.51	71.28	74.15	73.49	81.93	85.46
Zhu-Net	63.81	69.85	77.27	73.40	79.89	83.40	79.51	87.55	92.66
Proposed Method	64.49	74.10	77.13	75.06	83.64	86.85	81.50	88.81	91.78

Data augmentation was used to increase the size of the available images of the two datasets BOSSBase and BOWS2, as discussed in Case III. The improvement in the detection accuracy is evident in Table 6. Except for one scenario, in all scenarios, the result of the proposed technique was better. Augmented data enhanced the detection accuracy by 7.75%, 2.82%, and 5.15% for HILL with payloads of 0.2, 0.3, and 0.4 bpp, respectively. For S-UNIWARD with 0.2, 0.3, and 0.4 bpp payloads, there was a benefit of 7.10%, 3.59%, and 4.52%, respectively. WOW with the 0.2, 0.3 and 0.4 bpp payloads showed an increment in the detection accuracy by 1.82%, 0.46%, and 1.38%, respectively. Only in one scenario did Zhu-Net give a 1.10% better result for WOW ρ = 0.4 bpp, otherwise the proposed technique superseded the other techniques.

Table 6. Performance assessment while considering Case III.

Steganography Technique/ Payload (bpp)	HILL			S-UNIWARD			WOW		
	0.2	**0.3**	**0.4**	**0.2**	**0.3**	**0.4**	**0.2**	**0.3**	**0.4**
SRNet	64.44	70.03	72.92	74.31	81.29	84.66	78.28	84.37	87.97
Ye-Net	59.62	64.84	69.81	65.72	74.08	82.25	72.46	77.50	83.66
Yedroudj-Net	60.94	66.93	70.17	67.03	75.40	80.02	74.25	82.66	86.85
Zhu-Net	66.82	72.45	78.97	80.57	85.28	88.45	81.86	90.37	92.31
Proposed Method	72.24	76.92	82.28	82.16	87.23	91.37	83.32	89.27	93.16

4. Conclusions

In the proposed scheme, two non-trainable convolutional layers were used to enhance the performance. The high-boost filter was utilized in the first non-trainable layer to enhance the statistical information. The SRM filters were considered in the second non-trainable layer to fetch additional information. The bottleneck approach was followed in the network design to improve the performance. The clipped ReLU layer was taken instead of the simple ReLU layer to customize the thresholding. Two skip connections were also used for additional information from different connections. A single pooling layer was used at the end of the network to avoid information loss between the layers. The SVM classifier was applied instead of the softmax classifier to obtain better results than previous methods. In the experimental analysis, the proposed scheme was found to be the most effective for three context-aware steganography techniques on different payloads. The detection accuracy of the proposed scheme was better than the four existing techniques in most cases.

Author Contributions: Each author discussed the details of the manuscript. S.A. designed and wrote the manuscript. S.A. implemented the proposed technique and provided the experimental results. C.K. reviewed and revised the article. K.-H.J. drafted and revised the manuscript. All authors have read and agreed to the published version of the manuscript.

Funding: This research was supported by the Brain Pool program funded by the Ministry of Science and ICT through the National Research Foundation of Korea (2019H1D3A1A01101687) and Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2021R1I1A3049788).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The datasets used in this paper are publicly available and their links are provided in the reference section.

Acknowledgments: We thank the anonymous reviewers for their valuable suggestions that improved the quality of this article.

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

References

1. Li, B.; Wang, M.; Huang, J.; Li, X. A New Cost Function for Spatial Image Steganography. In Proceedings of the 2014 IEEE International Conference on Image Processing, Paris, France, 27–30 October 2014; pp. 4206–4210.
2. Holub, V.; Fridrich, J.; Denemark, T. Universal distortion function for steganography in an arbitrary domain. *EURASIP J. Inf. Secur.* **2014**, *2014*, 1. [CrossRef]
3. Holub, V.; Fridrich, J. Designing Steganographic Distortion Using Directional Filters. In Proceedings of the WIFS 2012—Proceedings of the 2012 IEEE International Workshop on Information Forensics and Security, Costa Adeje, Spain, 2–5 December 2012; pp. 234–239.
4. Lyu, S.; Farid, H. Steganalysis Using Higher-Order Image Statistics. *IEEE Trans. Inf. Forensics Secur.* **2006**, *1*, 111–119. [CrossRef]
5. Provos, N.; Honeyman, P. Detecting Steganographic Content on the Internet. *USA Today* **2001**, *1001*, 48103-4943.
6. Westfeld, A. F5—A Steganographic Algorithm. In *International Workshop on Information Hiding*; Springer: Berlin/Heidelberg, Germany, 2001; pp. 289–302.
7. Li, B.; Huang, J.; Shi, Y.Q. Textural Features Based Universal Steganalysis. In Proceedings of the Security, Forensics, Steganography, and Watermarking of Multimedia Contents X, San Jose, CA, USA, 14 February 2008; p. 681912.
8. Pevný, T.; Filler, T.; Bas, P. Using High-Dimensional Image Models to Perform Highly Undetectable Steganography. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*; Springer: Berlin/Heidelberg, Germany, 2010; Volume 6387, pp. 161–177, ISBN 364216434X.
9. Pevny, T.; Bas, P.; Fridrich, J. Steganalysis by Subtractive Pixel Adjacency Matrix. *IEEE Trans. Inf. Forensics Secur.* **2010**, *5*, 215–224. [CrossRef]
10. Xiong, G.; Ping, X.; Zhang, T.; Hou, X. Image textural features for steganalysis of spatial domain steganography. *J. Electron. Imaging* **2012**, *21*, 033015-1. [CrossRef]
11. Fridrich, J.; Kodovsky, J. Rich Models for Steganalysis of Digital Images. *IEEE Trans. Inf. Forensics Secur.* **2012**, *7*, 868–882. [CrossRef]
12. Tang, W.; Li, H.; Luo, W.; Huang, J. Adaptive Steganalysis against WOW Embedding Algorithm. In *Proceedings of the 2nd ACM Workshop on Information Hiding and Multimedia Security—IH&MMSec '14*; ACM Press: New York, NY, USA, 2014; pp. 91–96.
13. Denemark, T.; Sedighi, V.; Holub, V.; Cogranne, R.; Fridrich, J. Selection-Channel-Aware Rich Model for Steganalysis of Digital Images. In Proceedings of the 2014 IEEE International Workshop on Information Forensics and Security, Atlanta, GA, USA, 3–5 December 2014; pp. 48–53.
14. Xu, X.; Dong, J.; Wang, W.; Tan, T. Local Correlation Pattern for Image Steganalysis. In Proceedings of the 2015 IEEE China Summit and International Conference on Signal and Information Processing (ChinaSIP), Chengdu, China, 12 July 2015; pp. 468–472.
15. Mielikainen, J. LSB matching revisited. *IEEE Signal Process. Lett.* **2006**, *13*, 285–287. [CrossRef]
16. Li, F.; Zhang, X.; Cheng, H.; Yu, J. Digital image steganalysis based on local textural features and double dimensionality reduction. *Secur. Commun. Netw.* **2014**, *9*, 729–736. [CrossRef]
17. Li, B.; Li, Z.; Zhou, S.; Tan, S.; Zhang, X. New Steganalytic Features for Spatial Image Steganography Based on Derivative Filters and Threshold LBP Operator. *IEEE Trans. Inf. Forensics Secur.* **2017**, *13*, 1242–1257. [CrossRef]
18. Li, B.; Wang, M.; Li, X.; Tan, S.; Huang, J. A Strategy of Clustering Modification Directions in Spatial Image Steganography. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 1905–1917. [CrossRef]
19. Sedighi, V.; Cogranne, R.; Fridrich, J. Content-Adaptive Steganography by Minimizing Statistical Detectability. *IEEE Trans. Inf. Forensics Secur.* **2015**, *11*, 221–234. [CrossRef]
20. Wang, P.; Liu, F.; Yang, C. Towards feature representation for steganalysis of spatial steganography. *Signal Process.* **2019**, *169*, 107422. [CrossRef]
21. Ge, H.; Hu, D.; Xu, H.; Li, M.; Zheng, S. New Steganalytic Features for Spatial Image Steganography Based on Non-Negative Matrix Factorization. In *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*; Springer: Cham, Switzerland, 2020; Volume 12022, pp. 337–351, ISBN 9783030435745.
22. Qian, Y.; Dong, J.; Wang, W.; Tan, T. Deep Learning for Steganalysis via Convolutional Neural Networks. In Proceedings of the Media Watermarking, Security, and Forensics 2015, San Francisco, CA, USA, 9–11 February 2015; p. 94090J.
23. Qian, Y.; Dong, J.; Wang, W.; Tan, T. Learning and transferring representations for image steganalysis using convolutional neural network. In Proceedings of the 2016 IEEE International Conference on Image Processing (ICIP), Phoenix, AZ, USA, 25–28 September 2016; pp. 2752–2756. [CrossRef]
24. Xu, G.; Wu, H.-Z.; Shi, Y.-Q. Structural Design of Convolutional Neural Networks for Steganalysis. *IEEE Signal Process. Lett.* **2016**, *23*, 708–712. [CrossRef]
25. Wu, S.; Zhong, S.H.; Liu, Y. Steganalysis via Deep Residual Network. In Proceedings of the 2016 IEEE 22nd International Conference on Parallel and Distributed Systems—ICPADS, Wuhan, China, 13–16 December 2016; pp. 1233–1236.
26. Wu, S.; Zhong, S.; Liu, Y. Deep residual learning for image steganalysis. *Multimedia Tools Appl.* **2017**, *77*, 10437–10453. [CrossRef]
27. Ye, J.; Ni, J.; Yi, Y. Deep Learning Hierarchical Representations for Image Steganalysis. *IEEE Trans. Inf. Forensics Secur.* **2017**, *12*, 2545–2557. [CrossRef]
28. Boroumand, M.; Chen, M.; Fridrich, J. Deep Residual Network for Steganalysis of Digital Images. *IEEE Trans. Inf. Forensics Secur.* **2018**, *14*, 1181–1193. [CrossRef]

29. Guo, L.; Ni, J.; Shi, Y.Q. Uniform Embedding for Efficient JPEG Steganography. *IEEE Trans. Inf. Forensics Secur.* **2014**, *9*, 814–825. [CrossRef]
30. Yedroudj, M.; Comby, F.; Chaumont, M. Yedroudj-Net: An Efficient CNN for Spatial Steganalysis. In Proceedings of the 2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Calgary, AB, Canada, 15–20 April 2018; Volume 2018-April, pp. 2092–2096.
31. Wu, S.; Zhong, S.-H.; Liu, Y. A Novel Convolutional Neural Network for Image Steganalysis With Shared Normalization. *IEEE Trans. Multimed.* **2019**, *22*, 256–270. [CrossRef]
32. Zhang, R.; Zhu, F.; Liu, J.; Liu, G. Depth-Wise Separable Convolutions and Multi-Level Pooling for an Efficient Spatial CNN-Based Steganalysis. *IEEE Trans. Inf. Forensics Secur.* **2019**, *15*, 1138–1150. [CrossRef]
33. Xiang, Z.; Sang, J.; Zhang, Q.; Cai, B.; Xia, X.; Wu, W. A New Convolutional Neural Network-Based Steganalysis Method for Content-Adaptive Image Steganography in the Spatial Domain. *IEEE Access* **2020**, *8*, 47013–47020. [CrossRef]
34. Wang, Z.; Chen, M.; Yang, Y.; Lei, M.; Dong, Z. Joint multi-domain feature learning for image steganalysis based on CNN. *EURASIP J. Image Video Process.* **2020**, *2020*, 1–12. [CrossRef]
35. Shi, Y.; Wei, Y.; Yao, H.; Pan, D.; Xiao, G. High-Boost-Based Multiscale Local Contrast Measure for Infrared Small Target Detection. *IEEE Geosci. Remote Sens. Lett.* **2017**, *15*, 33–37. [CrossRef]
36. Oszust, M.; Piórkowski, A.; Obuchowicz, R. No-reference Image Quality Assessment of Magnetic Resonance Images with High-boost Filtering and Local Features. *Magn. Reson. Med.* **2020**, *84*, 1648–1660. [CrossRef] [PubMed]
37. Bas, P.; Furon, T. Break Our Watermarking System. Available online: http//bows2.ec-lille.fr/ (accessed on 21 January 2021).
38. Xavier Glorot, Y.B. Understanding the Difficulty of Training Deep Feedforward Neural Networks. In Proceedings of the Proceedings of the thirteenth international conference on artificial intelligence and statistics, Sardinia, Italy, 13–15 May 2010; pp. 249–256.
39. Hannun, A.; Case, C.; Casper, J.; Catanzaro, B.; Diamos, G.; Elsen, E.; Prenger, R.; Satheesh, S.; Sengupta, S.; Coates, A.; et al. Deep Speech: Scaling up End-to-End Speech Recognition. *arXiv* **2014**, arXiv:1412.5567.
40. Xu, G. Deep Convolutional Neural Network to Detect J-UNIWARD. In Proceedings of the IH and MMSec 2017—Proceedings of the 2017 ACM Workshop on Information Hiding and Multimedia Security, New York, NY, USA, 20–22 June 2017.
41. Fan, R.E.; Chen, P.H.; Lin, C.J. Working Set Selection Using Second Order Information for Training Support Vector Machines. *J. Mach. Learn. Res.* **2005**, *6*, 1889–1918.
42. Bas, P.; Filler, T.; Pevný, T. "Break Our Steganographic System": The Ins and Outs of Organizing BOSS. In *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*; Springer: Berlin/Heidelberg, Germany, 2011; Volume 6958, pp. 59–70, ISBN 9783642241772.