Journal of Information Hiding and Multimedia Signal Processing ©2021 ISSN 2073-4212
Ubiquitous International Volume **12**, Number **3**, September **2021**

Universal Image Steganography Detection using Multimodal Deep Learning Framework

Mohamed A. Elshafey [1], Ahmed S. Amein [2] and Khaled S. Badran [1]

[1]Department of Computer Engineering & A.I., Military Technical College, Cairo, Egypt
[2]Faculty of Information Systems & Computer Science, October 6 University, Giza, Egypt
m.shafey@mtc.edu.eg, ahmed.saleh.csis@o6u.edu.eg, khaledbadran@mtc.edu.eg

Received June 2021; Revised August 2021

Abstract. While image steganography concerns with embedding secret data into an image, Convolutional Deep Network (CDN) is considered as the best solution of steganography detection after the promising results achieved by adapting deep networks to solve this problem. Since the first use of CDN in steganography detection, the structure of the CDNs is improved to enhance the detection accuracy of different such techniques. Despite of the large number of researches on this field, there is a lack on researches that study the effect of using the trained CDNs to build a real universal image steganography detector. This paper presents the ability of combining the trained CDNs in a multimodal framework and studies the effect of this combination on the detection accuracy. The presented framework performs detections on each classifying modality independently to combine their estimations as a final inference to produce a universal image steganography detector. This idea is applied to six of the latest CDN-based image steganography detection techniques, which are GNCNN, IGNCNN, XuNet, YeNet, YedroudjNet and the Improved IGNCNN by training them on stego-images generated using WOW, S-UNIWARED and HILL steganography algorithms with payloads of 0.2, 0.3 and 0.4 bit per pixel. Results show a slight decrease on the detection accuracy when compared with the original detection accuracy due to the predicted similarity between the different image steganography techniques. However, results also show that the multimodal image steganography detection based on the Improved IGNCNN universal image steganography detection presents the best performance when compared with other detectors based on the other five image steganography tested detectors.

Keywords: Steganography Techniques, Deep Convolutional Networks, Multimodal Framework, Deep Learning, Steganography Detector.

1. **Introduction.** Image steganography is the process of covering a secret message with an image. The image (cover-image) and the secret message are the inputs to the image steganography algorithm, which generates a new image that has the same look of the cover-image but contains, within its pixels, the secret message. This new image is called stego-image. There are a lot of techniques [1, 2] to manipulate the carrier image to hide the secret message in order to improve the undetectability of such hidden information. Some of the commonly used techniques are as follows:

1. **Least Significant Bit (LSB)**: The idea behind LSB embedding is that if we change the last bit value of a pixel, there won't be much visible change in the color. For example, 0 is black. Changing the value to 1 won't make much of a difference since it is still black, just a lighter shade [3].

2. **Spread Spectrum**: In this type of image steganography, the secret message is first concealed in a much lower power noise than the cover-image. Then, this noise is added to the cover-image to generate the stego-image. Spread spectrum image steganography approaches are presented in many researches, such as [4, 5].
3. **Masking**: In this technique, the luminance of selected parts of the image is changed in order to hide the secret message. This method adds redundancy to the secret message in order to improve the stego-object resistance to lossy techniques. Thus, this technique is more effective than LSB when the cover-image is a JPEG image [6].
4. **Statistical**: In statistical image steganography, the statistical properties of the cover-image are considered. The idea of this type of image steganography is to use "1-bit" steganography but the changes in the cover-image are in certain statistical properties only, not in the whole cover [7].
5. **Distortion**: Here the message to be hid is concealed in the cover-image by distortion and then the cover-image and stego-image are compared at the stage of decoding. If the steganography detector finds the original image, the secret message can be retrieved, which makes image steganography less secure [8].
6. **Adaptive**: While image steganography aims to hide secret data in a cover-image, the detection probability of that secret data from the third parties has to be minimized. In order to minimize the steganography detectability, Adaptive image steganography appears. It embeds the secret data in selected areas of the image based on the image itself, which successfully reduces the steganography detectability. A set of well known adaptive image steganography are described below.
   - **Edge-Adaptive**: This technique embeds the secret message in pixel pairs. If the differences between the absolute values of these pairs are relatively large, it indicates an evidence on the presence of steganography [9].
   - **HUGO**: It is the first steganography technique to use the syndrome trellis codes [10]. This technique uses the difference between four neighbors (pixels) as a feature set to perform secret embedding with minimal distortion [11].
   - **WOW**: It is one of the most efficient adaptive image steganography techniques. It uses wavelet filters in order to embed the secret data. It also aims to avoid the changes, which are resulted from the embedding process [12].
   - **S-UNIWARD**: It is the spatial version of the UNIWARD. Like WOW [12], S-UNIWARD is wavelet-based. It uses directional filter banks in addition to a special distortion function [13].
   - **HILL**: It uses a low-cost function with clustered values. The anonymous cost function discovers less predictable areas in the image using a High Pass Filter (HPF). It also uses two Low Pass Filters (LPFs) for the output values of clustering process [14].

The state of the arts of the most steganography detection techniques can only detect whether an image has a secret message or not. As well, the implemented steganography technique and the underlying payload would not be recognized. In [15], the presented approach makes the convolutional layers wider in order to reinforce the effect of linear collusion attack on the reunion network structure. In [16], a truncation activation function at the pre-processing phase of the presented DL-based steganography detector is used with HPFs in order to improve detection rate and accelerate the training phase. In [17], a new model is presented that is based on a histogram of pixel structuring elements with different patterns. The new model constructs the feature set for training the steganography detector and distinguishes between the cover-images and the stego-images. In [18], a hybrid technique of both model parallelism and data parallelism is presented with cyclic

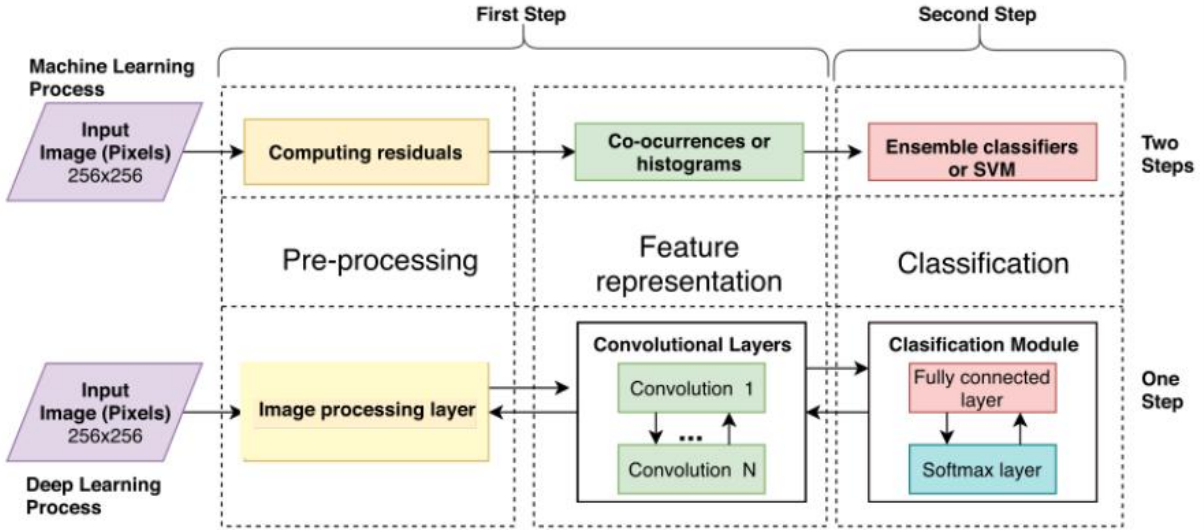

FIGURE 1. Steganography detection based on manual extraction of characteristics (top side) and steganography detection based on deep learning techniques (bottom side) [23].

learning rate and LReLU activation function during the learning phase for faster convergence towards enhanced detection accuracy. In [19], a novel deep residual network architecture is presented with reduced convolutional layers in a data-driven manner. Although such aforementioned techniques achieve significant detection accuracy, the secret message as well as its implemented steganography technique and payload, cannot be determined. In [20], a deep learning (DL)-based algorithm is suggested for steganography detection in images of varying sizes without retraining their parameters. These steganography techniques are capable of embedding the secret message with different payloads in order to confront the techniques of steganography detection. In this paper, a multimodal DL-based image steganography detection framework is proposed. It consists of three main consecutive stages, which can full fill with any size of images and can be adopted to cope with newly published DL-based techniques for steganography detections.

The rest of this paper is organized as follows. In Section 2, the related work is presented. In Section 3, the practical implementation of the universal multimodal DL-based steganography detection framework is proposed. The experimental work setup and results are reported in Section 4. Finally, the main conclusions are drawn in Section 5.

2. **Related Work.** Gaussian Neuron Convolutional Neural Network (GNCNN) [21] is the first DL-based approach with results comparable to those of Spatial Rich Model (SRM) [22], which depends basically on the residual samples of neighboring noise as features. In order to strengthen the noise signal, a HPF is used. GNCNN [21] consists of one pre-processing layer, five convolutional layers and three fully connected layers. In it, an average pooling is used as a pooling layer, a Gaussian activation function is used in the hidden layers and a Softmax is used for classification module. No batch normalization or absolute layer are used. Authors in [24] present a new DL-based steganography detection approach called XuNet. This network tries to enhance the statistical modeling by using an absolute (ABS) layer and 1×1 convolutional kernels. The presented approach also uses batch normalization layer in order to prevent the network stuck in a poor minima and enhance the updating process of the biases parameters. This approach gets the advantage of using different activation functions. It uses TanH [25] for the first two layers and and ReLU [26] activation functions for the rest. This variety of activation functions avoids the

over-fitting problem. In [23], a transfer learning is used to enhance the performance of GNCNN. The results show that transferring the pre-trained CNN features for detecting high payload stego-images of one steganographic algorithm can improve feature learning for detecting lower payload stego-images of that specific steganographic algorithm. This approach is called Improved Gaussian Neuron CNN (IGNCNN).

YeNet DL-based steganography detection is introduced in [27]. YeNet uses a set of trainable HPFs instead of using the traditional ones for noise extraction process. Those trainable filters are initialized with the coefficients of SRM filters. The TLU activation layer [27] is presented for first time in steganography detection to increase Signal to Noise Ratio (SNR).

Yedroudj-Net, an image steganography detection approach presented in [28], is a combination of XuNet [24] and YeNet [27]. It uses the TLU activation function [27] and the batch normalization layer. It also uses the SRM filter as initial values for the first convolutional layer. Simply it uses all the best configurations in XuNet and YeNet. The structure of YedroudjNet [28] network is as follows: one convolutional layer with thirty filters as a pre-processing layer, five convolutional layers as feature extractors and three fully connected layers. An average pooling is used after all convolutional layers except for the first one. It uses two activation functions in the hidden layers which are: TLU [27] and ReLU [26], and softmax for classification. In addition, it uses batch normalization and an absolute layer exists after the first convolutional layer.

Authors in [29] update YeNet to effectively detect stego in images with high resolution. The CDN is trained on images of small resolution in order to adopt the network to high resolution ones. Improved IGNCNN [30, 31] is an approach for blind image steganography detection based on transfer learning method. In this approach, a Gaussian HPF is used as a pre-processing layer and the CNN learning rate is changed dynamically. The Gaussian HPF enhances payload noise residuals extraction process that affects the detection accuracy positively. The dynamic learning rate of the pre-trained and the fine-tuned CNNs minimize the error that leads to improve the detection accuracy.

Authors in [32] present parallel computing by multiple GPUs, in order to accelerate the training of DL-based steganography detection process [30] as a case study. Model parallelism is applied to the classification module and data parallelism is applied to the feature extraction module that accelerates the training process. A variable batch size is also proposed as an optimization approach. A small batch size in the fully-connected layers helps CNN model to converge faster to a better minima. The difference in structure between the DL-based image steganography detection approaches, mentioned before, is presented in Table I where, Pre. is the number of pre-processing layers, Conv. is the number of convolutional layers, Fully. is the number of fully connected layers and Act.fn is the activation function. All the approaches are trained and tested using Boss-Base [33] image dataset.

Despite of the big number of researches in the field of image steganography detection, the effect of appending more than one CDN to reach a practical universal image steganography detection tool is not studied. Each DL-based image steganography detector is trained to detect set of image steganography techniques such as S-UNIWARD [13], WOW [12], and HILL [34], separately. However, combining these trained DL-based techniques and evaluating their performance for a random image exposed to unknown image steganography technique is not investigated yet. This goal will be the main concern of the paper.

3. **The proposed framework for the DL-based image steganography detector.**

The main purpose of this work is to find a way to evaluate the performance of a practical

TABLE 1. Network structures of different DL-based image steganography detection modalities.

Approach	**Pre.**	**Conv.**	**Fully.**	**Act.Fn**
GNCNN [21]	1	5	3	Gaussian
IGNCNN [23]	1	5	3	Gaussian
XuNet [24]	1	5	2	ReLU
YeNet [27]	0	8	1	ReLU
YedroudjNet [28]	1	5	3	ReLU
Improved IGNCNN [30]	1	5	3	Gaussian

implementation of DL-based image steganography detector, blindly, without any prior information on being exposed to any steganography technique or not. The proposed framework for the practical implementation combines more than one pre-trained CDN, in an add-on manner, to simulate a real case study of universal image steganography detector. In such a case, neither the steganography technique nor the applied payload value, are known.

In the proposed framework, typical CDNs can be trained on images, which are exposed to different steganography techniques with different payloads, then combined together to generate the mulimodal DL-based steganography detection framework. The estimations provided by each classifying modality are fused to yield an overall class estimation that defines the most probably implemented steganography technique as well as the payload as shown in Fig.2.

The proposed framework for practical implementation of the multimodal DL-based image steganography detection, in Fig.2 consists of three main stages:

- A pre-processing stage: In the first stage, the tested images, are divided into equally sized sub-images. Each sub-image is of size n $\times$ n, where n $\times$ n is the size of each image in the data set, upon which the CDNs of the framework are trained before. Each sub-image is applied individually to each classifying modality of the next stage.
- A multimodal DL-based engine stage: This stage is the main core of the proposed framework. It consists of a number of pre-trained CDNs, with a different dataset, in a parallel classifying modalities. Each dataset was exposed to a different steganography technique with a different payload value. This stage takes the responsibility of detection of stego-images with an accuracy associated to each DL-based classifying modality for steganography detection.
- A detection stage: This final stage receives the count of sub-images of the tested images, resulting from first stage, and evaluates the summation of (Stego Detected / Stego NOT Detected) per sub-image for all sub-images of each tested image. This stage performs the final decision of the tested image of being stego-image or a clean-image. In work, when the count of sub-images equals or exceed the half of the counted value, delivered from the pre-processing stage, it means that the tested image is stego-image.

In the proposed practical framework, when more than one DL-based classifying modality infers that the tested image is a stego-image, then the final decision is that the tested image is a stego-image by the steganography technique and the payload associated with the classifying modality of the highest detection probability.

Any applied CDN for steganography detection is a one, which has been trained before on a data set previously exposed to a specific steganography technique at a certain payload value. Furthermore, the dataset used for training contains a set of images of a certain size

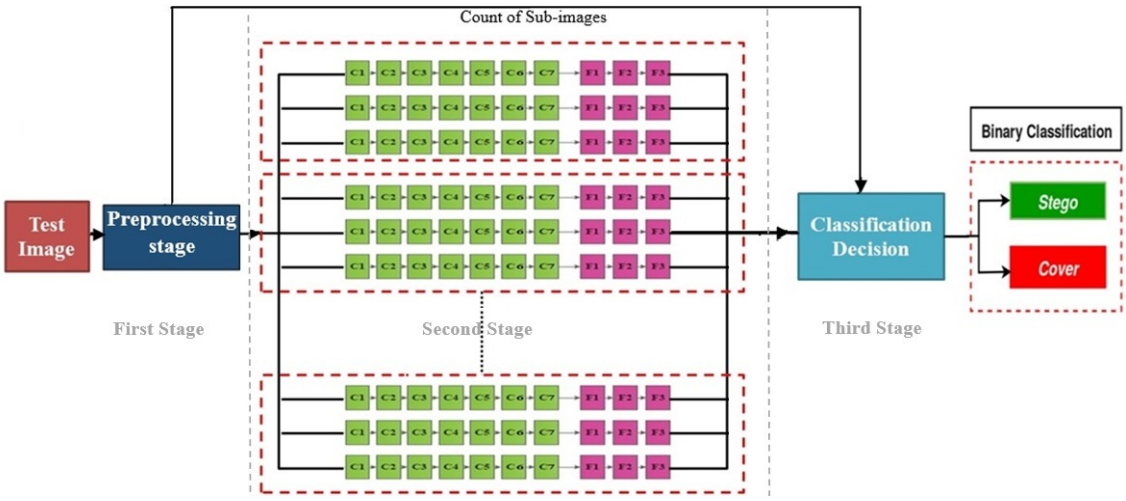

FIGURE 2. Illustration of the multimodal DL-based framework for image steganography detection, in which each red dotted box represents a CDN classifying modality.

that matches the size of the input layer of the implemented CDN. Practically in real cases, the images that will be checked for being stego-images or not, have different sizes with different probabilities of being exposed to a large number of steganography techniques at a wide range of probable payloads. Therefore, the practical characteristic of the proposed framework depends on its structure. It contains a pre-processing stage to subdivide the image under test into a count of sub-images, each with the same size that copes with the structure of the implemented CDN. This count is then transferred to a final stage in the proposed framework that decides, based on results on the sub-images of the same image under test, if it is a stego-image or not.

The add-on manner of the proposed framework comes from its capability to add a new classifying modality of the implemented CDN but trained with a new steganography technique at a certain payload, without major changes in the first stage nor the final one. This newly added classifying modality receives sub-images, of the image under test, from the first stage of the framework and delivers checking results of these sub-images to the final decision stage. The final stage, in turn, examines the results pool of checked sub-images, each attached with a unique identifier of the DL-based classifying modality that produced these results, and then it decides if the tested image is then a stego-image or not.

4. **Experimental Work and Results.**

4.1. **Implementation Setup.** Like many applications that require GPUs in order to speed up the training step [35], experiments in this paper are performed on a device with two processors of Intel Xeon Silver, 128 GB RAM (only 36GB RAM are actually used during training) and two Tesla V100 GPUs each with 5120 CUDA cores. The two GPUs can communicate amongst themselves simultaneously at the full PCI-Express 2.0 rate (about 6GB/sec) through a PCI-Express switch. Convolutional layers weight decays are 0 and 0.01 for the fully connected layers. A linearly decayed learning rate ranging from 0.01 to 0.00001 is used. Momentum of 0.9 is used. The training of the network is carried out using the CUDA-convnet2 in [36].

4.2. **Dataset Description.** The dataset used for experiments is the standard BOSSbase 1.01 image dataset [33]. BOSSbase 1.01 contains 10000 gray-level cover-images of

size 512 × 512. All the dataset images are subdivided into 4 sub-images, each of size 256 × 256 pixels. A set of 4 sub-images, of each image in the data set, is used for training purposes. That results in a data set of 40000 images for training each DL-based classifying modality for steganography detection. Each data set, of 40000 sub-images, is divided into two halves, each of size 20000 images. A single half data set is exposed to a unique image steganography technique and stored separately in each case for the technique used, while the other half is used in the training process. For exposing dataset to different steganography techniques, different technique at each time, with a specific payload in bits per pixel (bpp), the following cases are elected:

- S-UNIWARD steganography technique with payloads: 0.2, 0.3, and 0.4 bpp.
- WOW steganography technique with payloads: 0.2, 0.3, and 0.4 bpp.
- HILL steganography technique with payloads: 0.2, 0.3, and 0.4 bpp.

The previous task results in creating nine different datasets. Each dataset, which contains 20000 stego-images accompanied with the first half of 20000 clean-images, is used for training a separate DL-based classifying modality for image steganography detection. That constitutes a nine-based engine core in the framework for the practical implementation of the multimodal DL-based image steganography detection.

4.3. **Performance Evaluation Metrics.** Detection error (P_E), the lower the better, is used as the comparison metric. P_E is computed as shown in 1 where, P_{FA} is the false alarm rate calculated in Equation. 2, and P_{MD} is the missed detection rate. P_{MD} is calculated as in Equation. 3, where P_D is the detection rate, which calculated by Equation. 4.True Positive (TP) is the count at which the actual value was positive, and the model predicted a positive. True Negative (TN) is the number of times the actual value was negative, and the model predicted as a negative value. False Positive (FP) is the count of the actual negative values predicted as positive values. False Negative (FN) is the opposite to FP, i.e., count of actual positive values predicted as negative values.

$$P_E = min_{P_{FA}} \frac{1}{2}(P_{FA} + P_{MD}(P_{FA})) \tag{1}$$

$$P_{FA} = 1 - Specificity = FP/(FP + TN) \tag{2}$$

$$P_{MD} = 1 - P_D \tag{3}$$

$$P_D = Sensitivity = TP/(TP + FN) \tag{4}$$

4.4. **Experimental Results.** This section shows the experimental results of each DL-based classifying modality, separately, using a single different DL-based image steganography detection approach. The competing approaches are: GNCNN [21], IGNCNN [23], XuNet [24], YeNet [27], YedroudjNet [28], and the Improved IGNCNN [30]. Then, it describes the overall performance of the practical proposed framework for DL-based image steganography detection (*i.e.,* a case study of nine-modalities based-engine).

The detection errors, using different DL-based approaches of steganography detection for stego-images, exposed to S-UNIWARD, WOW, and HILL steganography techniques at payloads of 0.4, 0.3 and 0.2 bpp, are reported in Table 2.

The detection error of the framework of the nine multimodal image steganography detection based on models of the competing approachs: GNCNN [21], IGNCNN [23], XuNet [24], YeNet [27], YedroudjNet [28] and the improved IGNCNN [30] are presented in the Table 3. In this table, it can be noticed that the Improved IGNCNN [30] can achieve the minimum detection errors among other five recent DL-based approaches for steganography detection.

For a detailed explanation of the performance evaluation of the proposed framed work for the practical image steganography detector, based on Improved IGNCNN in its nine

TABLE 2. Detection error of S-UNIWARD, WOW, and HILL based stego-images with payloads of 0.4, 0.3 and 0.2 bpp using different DL-based approaches of steganography detection.

Steganography	**S-UNIWARD**			**WOW**			**HILL**		
Payload bpp	**0.2**	**0.3**	**0.4**	**0.2**	**0.3**	**0.4**	**0.2**	**0.3**	**0.4**
GNCNN [21]	37.43	30.62	20.08	37.4	27.88	20.28	37.50	29.05	20.50
IGNCNN [23]	34.38	28.42	22.05	34.38	24.87	19.62	34.40	26.70	21.02
XuNet [24]	39.1	32.84	27.2	31.65	20.7	18.15	37.6	30.12	20.67
YeNet [27]	40	35.8	31.2	24.35	20.36	17.07	39.4	34.9	32.45
YedroudjNet [28]	36.7	29.61	22.8	27.8	19.46	14.1	35.66	28.64	23.1
Imp. IGNCNN[30]	27.62	18.41	15.17	23.3	16.81	11.15	26.55	22.84	15.32

TABLE 3. Detection error of the proposed multimodal steganography detector using different approaches of CDN based steganography detections.

Steganography Detector	**Detection Error (%)**
GNCNN [21]	36.58
IGNCNN [23]	32.48
XuNet [24]	31.17
YeNet [27]	33.04
YedroudjNet [28]	26.43
Improved IGNCNN [30]	**19.22**

TABLE 4. The experimental details of detection capability of the proposed multimodal steganography detector, based on the Improved IGNCNN [30].

Steganography	**Clean**	**S-UNIWARD**			**WOW**			**HILL**		
Payload bpp	**-**	**0.2**	**0.3**	**0.4**	**0.2**	**0.3**	**0.4**	**0.2**	**0.3**	**0.4**
Catched images	1877	1429	1632	1697	1488	1664	1743	1414	1517	1694
Missed images	123	571	368	303	512	336	257	586	483	306

classifying modalities based engine, more detailed results are listed in Table 4. The results in Table 4 show 16155 catched images and 3845 missed images of total 20000 tested images.

Table 5 lists the experimental results of detection capability of the proposed image steganography detector, based on Improved IGNCNN in each classifying modality of the nine-modalities based engine, with data sets of different efficient steganography approaches at payloads 0.2, 0.3, and 0.4 for each approach. Table 5 shows a more detailed detection capability of the proposed image steganography detector, based on count of sub-images detected for each tested images. The header of that table shows count of sub-images detected of a total of four sub-images of each tested image (two sub-images or more means a stego-image). The total count may be higher in value than that of the stego-image catched due to some false detection, *i.e.,* detecting of clear images as stego-images

5. **Conclusion.** This paper presents a proposed framework for practical implementation of a universal multimodal DL-based image steganography detection system. It consists of three main consecutive stages: the pre-processing, the core, and the final inference.

TABLE 5. A detailed detection capability of the proposed multimodal detector, based on the detected count of sub-images in each tested image.

	Stego Catched	**4**	**3**	**2**	**Total**
0.2 SUNIWARD	1429	121	405	905	1431
0.3 SUNIWARD	1632	317	843	502	1662
0.4 SUNIWARD	1697	918	651	131	1700
0.2 WOW	1488	381	418	714	1513
0.3 WOW	1664	462	693	513	1668
0.4 WOW	1743	1002	569	200	1771
0.2 HILL	1414	212	484	731	1427
0.3 HILL	1517	371	746	407	1524
0.4 HILL	1694	886	512	307	1705
Total	14278				14401

The middle stage, the core engine of the framework, is implemented in nine classifying modalities. It has an add-on manner, which can be adopted in future to cope with new DL-based techniques of steganography detection. The proposed multimodal framework is well suited for the practical implementation for detection of stego-images, of any resolution, with an efficiency of 19.22% detection error. The proposed framework can detect stego-images, which are previously exposed to any steganography technique at any payload of 0.4, 0.3, and 0.2 bpp.

REFERENCES

[1] B. Li, J. He, J. Huang, and Y. Q. Shi, "A survey on image steganography and steganalysis." *J. Inf. Hiding Multim. Signal Process.*, vol. 2, no. 2, pp. 142–172, 2011.

[2] J.-S. Pan, W. Li, C.-S. Yang, and L.-J. Yan, "Image steganography based on subsampling and compressive sensing," *Multimedia Tools and Applications*, vol. 74, no. 21, pp. 9191–9205, 2015.

[3] O. Rachael and et. al, "Image steganography and steganalysis based on least significant bit (lsb)," in *Proceedings of ICETIT 2019*. Cham: Springer International Publishing, pp. 1100–1111, 2020.

[4] T. Morkel, J. H. Eloff, and M. S. Olivier, "An overview of image steganography." in *ISSA*, vol. 1, no. 2, pp. 1–11, 2005.

[5] K. Satish, T. Jayakar, C. Tobin, K. Madhavi, and K. Murali, "Chaos based spread spectrum image steganography," *IEEE transactions on consumer Electronics*, vol. 50, no. 2, pp. 587–590, 2004.

[6] R. Radhakrishnan, M. Kharrazi, and N. Memon, "Data masking: A new approach for steganography?" *Journal of VLSI signal processing systems for signal, image and video technology*, vol. 41, no. 3, pp. 293–303, 2005.

[7] E. Franz, "Steganography preserving statistical properties," in *International Workshop on Information Hiding*. Springer, pp. 278–294, 2002.

[8] Y. Kim, Z. Duric, and D. Richards, "Modified matrix encoding technique for minimal distortion steganography," in *International Workshop on Information Hiding*. Springer, pp. 314–327, 2006.

[9] W. Luo, F. Huang, and J. Huang, "Edge adaptive image steganography based on lsb matching revisited," *IEEE Trans. on info. forensics and security*, vol. 5, no. 2, pp. 201–214, 2010.

[10] T. Filler, J. Judas, and J. Fridrich, "Minimizing additive distortion in steganography using syndrome-trellis codes," *IEEE Trans. on Inf. Forensics and Security*, vol. 6, no. 3, pp. 920–935, 2011.

[11] T. Pevný, T. Filler, and P. Bas, "Using high-dimensional image models to perform highly undetectable steganography," in *Information Hiding*, R. Böhme, P. W. L. Fong, and R. Safavi-Naini, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 161–177, 2010.

[12] V. Holub and J. Fridrich, "Designing steganographic distortion using directional filters," in *2012 IEEE Inter. workshop on info. forensics and security (WIFS)*. IEEE, pp. 234–239, 2012.

[13] V. Holub and Fridrich, "Digital image steganography using universal distortion," in *Proc. of the first ACM Workshop on Info. Hiding and Multimedia Sec.*, pp. 59–68, Dec 2013.

[14] B. Li, M. Wang, J. Huang, and X. Li, "A new cost function for spatial image steganography," in *2014 IEEE International Conference on Image Processing (ICIP)*. IEEE, pp. 4206–4210, 2014.
[15] J. Zeng, S. Tan, G. Liu, B. Li, and J. Huang, "Wisernet: Wider separate-then-reunion network for steganalysis of color images," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 10, pp. 2735–2748, 2019.
[16] Y. Y. Lu, Z. L. O. Yang, L. Zheng, and Y. Zhang, "Importance of truncation activation in preprocessing for spatial and jpeg image steganalysis," in *2019 IEEE International Conference on Image Processing (ICIP)*, pp. 689–693, 2019.
[17] W. Lu, R. Li, L. Zeng, J. Chen, J. Huang, and Y. Q. Shi, "Binary image steganalysis based on histogram of structuring elements," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 30, no. 9, pp. 3081–3094, 2020.
[18] E. M. Mustafa, M. A. Elshafey, and M. M. Fouad, "Enhancing CNN-based image steganalysis on GPUs," *Journal of Info. Hiding and Multimedia Signal Proc.*, vol. 11, no. 3, pp. 138–150, 2020.
[19] S. Tan, W. Wu, Z. Shao, Q. Li, B. Li, and J. Huang, "Calpa-net: Channel-pruning-assisted deep residual network for steganalysis of digital images," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 131–146, 2021.
[20] W. You, H. Zhang, and X. Zhao, "A siamese cnn for image steganalysis," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 291–306, 2021.
[21] Y. Qian and et. al, "Deep learning for steganalysis via convolutional neural networks," in *Media Watermarking, Sec., and Forensics*, vol. 9409. SPIE, pp. 171 – 180, 2015.
[22] J. Fridrich and J. Kodovsky, "Rich models for steganalysis of digital images," *IEEE Trans. on Info. Forensics and Sec.*, vol. 7, no. 3, pp. 868–882, 2012.
[23] Y. Qian, J. Dong, W. Wang, and T. Tan, "Learning and transferring representations for image steganalysis using convolutional neural network," in *IEEE Intern. Conf. on Image Processing*, Sep. pp. 2752–2756, 2016.
[24] G. Xu, H.-Z. Wu, and Y.-Q. Shi, "Structural design of convolutional neural networks for steganalysis," *IEEE Signal Processing Letters*, vol. 23, no. 5, pp. 708–712, May 2016.
[25] C. Gulcehre, M. Moczulski, M. Denil, and Y. Bengio, "Noisy activation functions," in *Intern. Conf. on machine learning*, pp. 3059–3068, 2016.
[26] V. Nair and G. E. Hinton, "Rectified linear units improve restricted Boltzmann machines," in *Proc. of the* 27^{th} *Intern. Conf. on Machine Learning*, pp. 807–814, June 2010.
[27] J. Ye, J. Ni, and Y. Yi, "Deep learning hierarchical representations for image steganalysis," *IEEE Trans. on Info. Forensics and Sec.*, vol. 12, no. 11, pp. 2545–2557, Nov. 2017.
[28] M. Yedroudj, F. Comby, and M. Chaumont, "Yedroudj-net: An efficient cnn for spatial steganalysis," in *IEEE Intern. Conf. on Acoustics, Speech and Signal Processing*, pp. 2092–2096, April 2018.
[29] C. F. Tsang and J. Fridrich, "Steganalyzing images of arbitrary size with CNNs," *Electronic Imaging*, vol. 2018, no. 7, pp. 1–8, Jan. 2018.
[30] E. M. Mustafa, M. A. Elshafey, and M. M. Fouad, "Accuracy enhancement of a blind image steganalysis approach using dynamic learning rate-based CNN on GPUs," in *The 10th IEEE Intern. Conf. on Intelligent Data Acquisition and Advanced Computing Sys.*, Sep. 2019.
[31] E. M. Mustafa, M. A. Elshafey, and M. M. Fouad, "Enhancing the performance of CNN-based blind image steganalysis approach using multi-GPU TESLA P100," *IOP Conf. Series: Materials Science and Engineering*, vol. 610, p. 012093, oct 2019.
[32] E. M. Mustafa, M. A. Elshafey, and M. M. Fouad, "Enhancing the performance of an image steganalysis approach using variable batch size-based cnn on gpus," in *The 10th IEEE Intern. Conf. on Intelligent Data Acquisition and Advanced Computing Sys.*, Sep. 2019.
[33] P. Bas, T. Filler, and T. Pevný, "Break our steganographic sys.: The ins and outs of organizing boss," in *Info. Hiding*, pp. 59–70, 2011.
[34] B. Li, M. Wang, J. Huang, and X. Li, "A new cost function for spatial image steganography," in *IEEE Intern. Conf. on Image Processing*, pp. 4206–4210, Oct 2014.
[35] A. F. Eldeken, R. M. Dansereau, M. M. Fouad, and G. I. Salama, "High throughput parallel scheme for HEVC deblocking filter," in *IEEE Inter. Conf. on Image Proc.*, pp. 1538–1542, Sep. 2015.
[36] C. Cuda-convnet High-performance, "Cuda implementation of convolutional neural networks," *Retrieved from the internet on Jun*, vol. 3, p. 3, 2015.