Comparative Deep Learning Models in Applications of Steganography Detection

Awab Qasim Karamanji *, Asia S. Ahmed, and Ali F. Fadhil

Biomedical Engineering Department, University of Technology, Baghdad, Iraq
Email: awab.q.abdulrasool@uotechnology.edu.iq (A.Q.K.); asia.s.ahmed@uotechnology.edu.iq (A.S.A.); ali.f.fadhil@uotechnology.edu.iq (A.F.F.)
*Corresponding author

***Abstract*—This paper explores the use of deep learning algorithms in steganography detection. More specifically, it examines deep learning-based binary classification to distinguish between stego and non-stego images from the three steganography algorithms, The Wavelet Obtained Weights (WOW), Spatial Universal Wavelet Relative Distortion (S-UNIWARD), Highly Undetectable Steganography (HUGO). It also highlights the lack of research to develop a practical universal image steganography detection system using trained deep learning. The proposed farmwork combines multiple detection deep learning architectures to create a universal Deep Convolutional Neural Network (Deep-CNN). In this paper, we evaluate Deep-CNN-based image steganography detection techniques trained on images extracted from the three steganography algorithms. The dataset consists of 10,000 images in PGM format, which is converted to JPG format with a size of 256×256 pixels. The data set is classified into clear and stego images, which are the same image samples used in each category, with the three separate data sets for stego images created using three algorithms (WOW, S-UNIWARD, and HUGO). The results show a slight decrease in detection accuracy, but the fine-tuning of the improved deep-CNN architecture performs better than other methods.**

***Keywords*—steganalysis, deep learning, steganography algorithms, binary classification, algorithm detection**

I. Introduction

Deep Learning (DL) has gained significant attention in the computer vision field due to its ability to process data in its original form and learn representations of data through multilayer models. It has shown significant improvements in various image processing applications, including face recognition, object detection, and image compression [1, 2]. Cun *et al*. [3] conducted one of the first studies on DL and the use of Convolutional Neural Networks (CNN) and the handwritten digit recognition algorithm of gradient backpropagation. This research led to the development of more advanced DL techniques and brought the field of machine learning to new heights. Today, CNNs are widely used in computer vision applications. (Deep Convolutional Neural Network) Deep CNN achieves state-of-the-art performance in various image classification and detection tasks [1, 2, 4]. A cover image and a secret message are the inputs given to an image steganography algorithm, which creates another image like the original. However, this new image also contains information on its pixels that carry the secret message. This newly created visual representation is called a stego-image. There are several approaches to modifying the carrier image to hide a secret message [5–7]. These approaches are classified as follows.

- LSB-Embedding Technique (LSB-ET): This approach is based on hiding a secret message within an image by replacing the least significant bit of each pixel with the binary data of the message [2].
- Spread Spectrum Technique: The technique includes first concealing the name of the game message inside noise that has much lower energy than the duvet picture. This noise is then delivered to the cover image to create the stego image. The concept behind this method is to spread the secret message throughout an extensive frequency spectrum, making it hard to stumble on or extract without knowing the original noise signal. Spread-spectrum image steganography has been extensively studied and is an effective method for hiding information within images without compromising their visible quality. Several studies have paid attention to this field by investigating and demonstrating the effectiveness of this technique [8].
- Masking technique: This technique involves changing the luminance of decided portions of the image to hide the name of the secret message. Redundancy is introduced to the secret message to enhance the resistance of the step object to lossy compression strategies, such as those used in Joint Photographic Experts Group (JPEG) photos. As a result, this technique is more effective than the Least Significant Bit (LSB) technique, whilst the duvet image is a JPEG image. The masking technique takes advantage of the fact that changes in luminance are less great to the human eye than color adjustments, allowing the secret message to be hidden greater effectively. By adding redundancy to the secret messages, the stego object is capable of resisting some degree of lossy compression without losing the integrity of the hidden message. This

Manuscript received December 23, 2023; revised March 1, 2024; accepted March 13, 2024; published September 23, 2024.

makes it a powerful technique to hide records within Joint Photographic Experts Group (JPEG) images [2].

- Statistical technique: This technique of image steganography considers the statistical features of the cover image. The concept is to use "1-bit" steganography, where one small bit of records is hidden within every pixel of the cover image. However, in contrast to altering each pixel, only certain statistical features of the cover image are changed. This method ensures that the overall appearance of the cover image stays largely unchanged while nevertheless making an allowance for the secret message to be hidden inside its information. This method is considered powerful in preserving the visible integrity of the cover image, although it nevertheless provides a high level of protection for hidden messages [9].
- Distortion Technique: The distortion technique is a method of image steganography in which a secret message is hidden within a cover image. The steganography detector compares the cover image and the stego image to extract the message. However, this technique is less secure than other methods, making security considerations crucial [10].
- Adaptive Techniques: Image steganography is an adaptive technique that conceals secret data within an image, making it difficult for others to detect. Adaptive techniques embed secret data in less noticeable areas, maintaining the image's appearance while hiding the message. Additionally, adaptive techniques adapt to image content, embedding statistics in regions that are much less likely to be observed by statistical analysis [11].
- The Edge Adaptive Technique (EAT): is an image steganography technique that hides a secret message inside pairs of pixels. Its customs aspect detection strategies randomly region for record embedding, specializing in areas of interest. By embedding the secret message within those areas, which may be less likely to be noticed by an observer, EAT can effectively disguise records while maintaining the visual integrity of the image [12].
- Highly Undetectable Steganography (HUGO): The Highly Undetectable Ste-GO HUGO is a spatial-domain steganography set of rules that is proof against steganalysis strategies. It uses Syndrome-Trellis codes to embed modifications in areas of tough-to-model image cover while maintaining image data [13, 14]. Hugo utilizes changes in adjacent pixels to embed secret messages with minimal distortion.
- The algorithm precisely chooses the embedding positions and reduces distortion to efficiently conceal statistical data within images while preserving their visual integrity [15]. Wavelet-Obtained Weights (WOWs): The WOW technique is a very good adaptive image steganography method that uses wavelet filters to hide information in images while keeping the original visitation of the image and not causing any major changes due to the steganography method [1].
- The Spatial Universal Wavelet Relative Distortion (S-UNIWARD): The S-UNIWARD is a spatial steganography method that uses directional filtering banks and a special distortion function to hide information in images [1]. This method hides records without making significant changes to the cover image [14, 15].

Generally, image steganography detection algorithms play a crucial role in identifying hidden secret messages in images, but do not recognize the precise method or payload size that is used. These algorithms focused on many aspects of the image, including pixel values, frequency domains, or statistical qualities, to identify any deviations from the predicted patterns.

Lu *et al.* [16] proposed a new method that uses a histogram of pixel Structuring Elements (SEs) to build feature sets for training models. The criterion emphasizes the selected SEs, which have highly flappable pixels and can distinguish between cover images and stego-images.

Mustafa *et al.* [17] and Tan *et al.* [18] developed new methods to enhance CNN-based image steganography.

Mustafa *et al.* [17] presented modifications to the Deep-CNN model to improve detection accuracy. This includes efficient parameter initialization, the use of cyclic learning rates, and the Leaky Rectified Linear Activation (LReLU) activation function during the learning phase. The CNN model was adjusted for training using high-performance Graphic Processing Units (GPUs), which led to improved speed and improved accuracy in detecting hidden information. Channel-pruning-assisted Deep Residual Networ (Calpa-Net) was created by Tan *et al.* [18], a channel-running-assisted deep residual network architecture search approach that integrates channel pruning with deep residual networks for image segmentation. The goal of Calpa-Net is to improve the deep network structures of existing DL learning-based image steganography. These approaches make CNN better at finding hidden messages in images.

Zhang *et al.* [19] proposed a network that uses a Siamese CNN-based architecture to make steganalysis methods more sensitive and specific. The Siamese-CNN-based architecture with shared parameters consists of three phases: pre-processing, feature extraction, and fusion/classification. This advancement finally enhances the capability to detect hidden information in images. Based on the litterateurs presented above, it appears that the steganography techniques studied are capable of embedding secret messages with various payloads.

The framework proposed in this paper is capable of accommodating images of any size while adapting different payloads compared to recently published steganography detection techniques.

II. Review of the Literature

Recently, Deep Convolutional Neural Networks (Deep-CNN) have emerged as indispensable tools in the field of structural analysis, facilitating the identification of hidden data within digital images.

Numerous studies have demonstrated the efficacy of the precise implementation of CNN models in applications of data strategy analysis of data within digital images [20, 21]. Furthermore, some investigations have implemented the

highly effective Gaussian Neuron Convolutional Neural Network (GNCNN) [14, 20].

Fridrich and Kosovska's [22] Spatial-Rich Model (SRM) also utilized convolution layers for image steganalysis.

In the studies [14, 23], researchers made custom CNN architectures and batch normalization layers to improve bias parameters and detection. These studies highlight the importance of CNNs in detecting covert information in digital images.

Brown *et al.* [24] introduced rectified linear units (ReLUs) as a means to enhance restricted Boltzmann machines, boosting the performance of deep learning models. Tanh activation functions are used for the first two layers and ReLUs for the remaining layers to avoid overfitting.

Ye *et al.* [23] delved into hierarchical representations through deep learning, specifically for image steganalysis.

Their approach called Ye Network (YeNet) aimed at capturing complex features within images, which contributed to improved detection accuracy. The YeNet employs a set of trainable high-pass filters, initialized with the coefficients of SRM filters, for noise extraction instead of traditional filters. Yedroudj *et al.* [25] presented an efficient deep CNN tailored for spatial steganography.

A model uses a deep CNN to accurately detect hidden spatial information in images, even using advanced steganography techniques to conceal the message.

Significant progress has been made in steganalysis, which now allows the detection of hidden messages in images. The capacity of CNNs to organize images of varying sizes has been expanded, thereby increasing their utility. The researchers expanded the application of CNNs to stigmatize images of various sizes [26], thereby enhancing the versatility and utility of CNN-based Steg analytic algorithms. In their effort to improve blind image steganography, Mustafa *et al.* [27] utilized multiple GPUs in addition to CNNs based on dynamic learning rates, respectively. Mustafa *et al.* [28] centered their research on the development of techniques that improved the precision and effectiveness of hidden data.

Recent research has investigated methods to enhance blind image steganography. One such approach is Deep-CNN, which is a hybrid of Xu *et al.* [14]. It operates by employing filters from the spatial rich model, batch normalization, and the Truncated Linear Unit (TLU) activation function [23]. In addition, after all convolutional layers except the first, average pooling is used. The activation functions utilized in hidden layers are Rectified Linear Unit (ReLU) and TLU, while Softmax is employed for classification [26]. This approach signifies a substantial progression in the domain of image steganography detection, providing a powerful tool for decoding hidden messages in images. In Ref. [26], the Ye-CNN was updated to effectively detect steganography in high-resolution images. To adapt the network to high-resolution images, Ye-deep CNN was trained on low-resolution images [27]. According to IGNCNN, it is a blind image steganography detection model based on transfer learning. It has a Gaussian high pass filter as a preprocessing layer, and CNN learning dynamically modifies the learning rate [27, 28].

The Gaussian high-pass filter improves the removal of payload noise residuals, which makes detection more accurate. The dynamic learning rate of pre-trained and fine-tuned CNNs reduces error, which also makes detection more accurate. The work of Mustafa *et al.* [28] improved image segmentation on GPUs by adding a convolutional neural network that changes according to the batch size. For accelerated convergence, they used parallel computation with multiple GPUs, model- and data parallelism, and variable batch sizes. This technique has significantly increased the efficiency and accuracy of steganography processes, which makes it much simpler to discover hidden messages in images.

This approach represents a significant advancement in the field of structural analysis, as it provides a robust instrument for detecting concealed messages within images [27]. Table I details algorithms for detecting image steganography based on deep learning, with a particular focus on those that employ deep CNN.

It specifies the number of Preprocessing Layers (PPL), Convolutional Layers (CL), Fully Connected Layers (FCL), and Activation Functions (AF) used. The methodologies presented in Table I were trained and tested using the Boss-Base Image dataset [29, 30].

TABLE I. NETWORK TOPOLOGIES OF VARIOUS DETECTION MODALITIES FOR DL-BASED PICTURE STEGANOGRAPHY [30]

DL-based method	character	PPL	CL	FCL	AF
[20]	Model 1	√	5	3	G
[21]	Model 2	√	5	3	G
[14]	Model 3	√	5	2	R
[23]	Model 4	×	8	1	R
[25]	Model 5	√	5	3	R
[27]	Model 6	√	5	3	G

√: represents the available preprocessing layer. ×: represents the preprocessing layer not available. AF: for Gaussian or Relu, where G refers to the Gaussian layer and R to the Relu layer.

Despite numerous research efforts to develop structural analysis approaches based on deep learning models, these intelligent approaches can learn intricate patterns and features from steganographic content [20, 27]. On the other hand, the effect of the fusion of deep-CNN models on the overall performance of an image steganography detection tool has not been extensively studied.

In this paper, we evaluate the performance of the model on BOSS-base 1.01 datasets [29].

The individual deep learning-based image steganography detector is trained to detect specific image steganography techniques. Three steganography techniques, including S-UNIWARD [14], WOW [1], and HUGO [31], are studied separately. However, the main focus of this paper is to compare these deep learning-based techniques and evaluate the performance of deep learning-based models on a random image exposed to an unknown image steganography technique that has not yet been investigated. The assigned DL-based structures used in the comparison are listed in Table I.

III. Image Steganography Detection Architecture Using Deep-CNN

This paper aims to evaluate the performance of multiple pre-trained deep-learning models for image steganography detectors. The proposed framework combines multiple pre-trained deep-learning CNNs to create a universal image steganography detector. As shown in Fig. 1, combined predictions from each type of trained model result in a final class estimate that displays the most likely steganography technique and payload. A multimodal deep-CNN-based framework for image steganography detection makes it feasible to find hidden messages even with specific hidden techniques and payloads that are unknown.

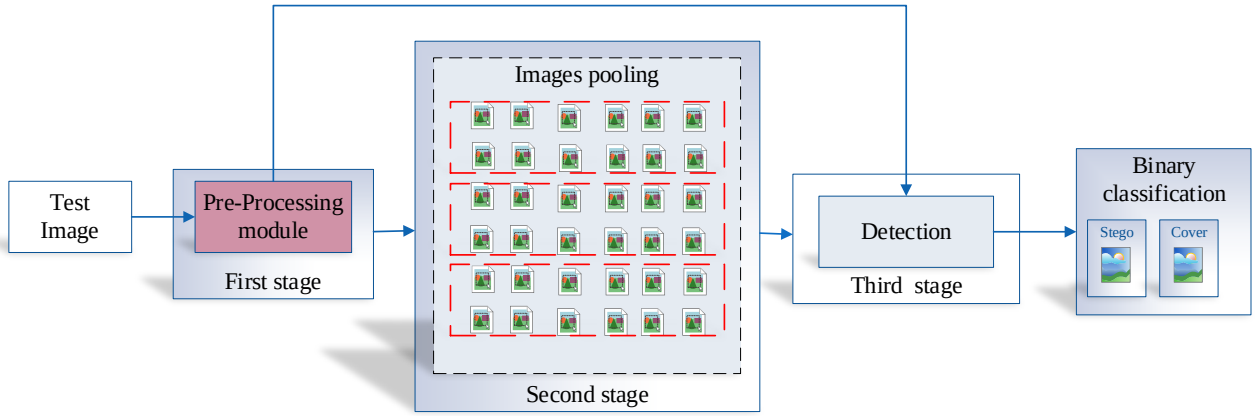

Fig. 1. A deep CNN-based system for detecting image steganography, with each red dotted box representing a different classifier model for detection steganography technique (S-UNIWARD, WOW, and HUGO).

The multimodal deep-CNN-based framework for image steganography detection in Fig. 1 comprises three main stages:

- **A preprocessing stage:** the input images with size $n \times n$ are divided **into** uanique image with sa isizeof n_o ×where $n \times n$ is sthe theize of the data set, and $n_o \times$ is the size of a unique sub-divided image, based on which the deep CNNs of the framework are trained. Each image in the data set is applied separately to each classifier in the multimodal deep-CNN stage.
- **Multimodal deep-CNN stage**: This stage serves as the central component of the proposed framework. This stage comprises pre-trained deep-learning CNNs, each with a distinct dataset, operating in parallel to categorize modalities. Every input image is subjected to a separate steganography procedure, resulting in the attachment of a unique payload value. We use DL-based classification models to build and train the multiclassifier model that can correctly identify steganography as either stego or non-stego images.
- **A detection and classification stage:** This stage makes the final determination of whether the tested image is a stego image or a clean image per label image for all input images of each tested image. If the number of input images is equal to the number of stego images obtained from the preprocessing step, then the tested picture is a stego image.

Moreover, the training dataset consists of images that are the same size as the input layer of the deep CNN deployed. In practical scenarios, images vary in size and are subjected to various steganography techniques, with variable possibilities of being detected. The practical aspect of the proposed framework is based on its structure. The preprocessing step involves dividing the test image into a certain image size, each of equal size to match the structure of the deep CNN. The count is then sent to a final step in the proposed framework, which determines if the image under test is a stego image by analyzing the findings from its applied images.

The proposed deep-CNN for steganography detection add-on feature lets a new classifying mode be added to the existing deep-CNN. The proposed procedure can be trained using a different steganography approach for a specific payload. This new approach to classification accepts group images from the first stage of the framework and provides evaluation findings for these sub-images for the final decision stage. The last phase evaluates the collection of verified group images together with their corresponding unique identifiers from the deep-CNN classification model. It determines if the tested image is a stego image or not.

IV. Simulation and Results Explanation

This section shows the results of the tests that were performed on each deep learning-CNN-based classification mode using a different deep learning-based method to find image steganography.

A. Setup of the Testing Data Set

The experiments were carried out on a computer equipped with an Intel Core TM i7-12650HX CPU, 64 GB of random-access memory, a 1 TB hard disk drive, and an Nvidia Repeats-in-Toxins (RTX) 4080 GPU. This is a powerful setup that can handle demanding tasks for

training the network. Network parameters were trained using deep CNN, available in [28].

The standard BOSS-base 1.01 image dataset is used for the experiments, which is available in [29]. This dataset contains 10,000 grey-level cover images of size 512×512 pixels.

All images in the dataset are converted into sub-images, each of size 256×256 pixels, resulting in a dataset of 10,000 images with 256×256 pixels for training each deep learning-based classifying modality for steganography detection.

The sub-images dataset is divided into two halves, each containing 5,000 images. One-half of the data set is used in the training process. The other half is used in the testing of steganography detectors. The data set is exposed to different steganography techniques with specific payloads in Bits Per Pixel (BPP). The selected cases are listed in Table II.

TABLE II. THE DATASET FOR SELECTED CASES WITH SPECIFIC PAYLOAD

Steganography technique	Payloads (BPP)	Train dataset		Testing dataset	
		Clean	Stego	Clean	Stego
S-UNIWARD	0.2 0.3 0.4	10,000 images	10,000 images	5000 images	5000 images
WOW	0.2 0.3 0.4				
HUGO	0.2 0.3 0.4				

B. Results Explication

This section shows the test results for each deep learning-based method of classifying using a different deep learning-based method for detecting image steganography. The performance of a deep learning-based detection model can be evaluated in terms of false ratio, missed detection, and correct detection. These metrics can be expressed as follows:

The first equation provided computes the detection error D_E, which is a crucial statistic used for evaluating the efficacy of the detection model.

$$D_E = Fa_R + MD_r \tag{1}$$

The detection error is calculated by adding e false alarm rate Fa_r and the missed detecon rate MD_r. The $\mathrm{Fa_R}$ is calculated the ratio of false positives *FP* to the total of false positives and true negatives *TN* A false positive refers to the erroneous identification of a target that is absent in reality.

$$Fa_R = \frac{FP}{FP + TN} \tag{2}$$

The detection rate D_s also known as sensitivity, was defined as the ratio of true positives *TP* to false negatives *FN*, which measures how accurately the model can identify a target.

$$D_s = \frac{TP}{TP + FN} \tag{3}$$

Thiessen detector rate MD_r is calculated as the ratio of false negatives *FN* to true positives *TP*, where a false negative happens when the model fails to identify a target.

$$MD_r = 1 - D_s \tag{4}$$

The equations offer a comprehensive way to assess the performance of a detection model, including false alarms, missed detections, and correct detections. Lower values of the detection error, false alarm rate Fa_R, and missed detection rate MD_r indicate better performance, while higher values of the detection rate D_s indicate better detection capability. The competitive approaches include the following DL-based architectures:

Model 1: In contrast to current methodologies for deep CNN, this deep CNN approach integrates the processes of feature extraction and classification into a unified architecture, which enables the use of classification advice during the feature extraction phase.

Model 2: Like the other deep CNN approaches, the authors propose a framework based on transfer learning to improve the deep CNN training method. They show that feature representations learned with a pre-trained CNN for detecting a steganographic algorithm with a high payload can be efficiently transferred to improve the learning of features for detecting the same steganographic algorithm with a low payload.

Model 3: This neural network architecture incorporates many modifications, such as the use of absolute values for feature maps, the imposition of constraints on data values, and the integration of 1×1 convolutions. Despite being trained on a single kind of residual noise, this CNN has competitive performance in terms of detection compared to other approaches. This implies that the potential for enhancing steganalysis in the future lies in the use of well-designed CNN.

Model 4: The CNN structure that has been developed demonstrates the capability to repeat and optimize the fundamental processes of residual calculation, feature extraction, and binary classification within a cohesive framework. The performance of CNN-based steganalysis is improved by the integration of the selection channel information.

Model 5: Like other deep-CNN architecture, it demonstrates superior performance compared to current methodologies in terms of error probability. In this architecture, deep-CNN includes a preprocessing filter bank, a Truncation activation function, five convolutional layers with Batch normalization and a scale layer, and a fully linked section of appropriate size. An improved database is used to improve training.

Model 6: An improved Gaussian Convolutional Neural Network (IGNCNN) is presented, which incorporates transfer learning and a preprocessing layer with a fixed coefficient High-Pass Filter (HPF). The input proposes a CNN approach based on dynamic learning rates to minimize detection error costs. However, with the help of a case study of a nine-modality-based engine, the overall

performance of the proposed practical framework for deep learning-based image steganography detection is also investigated. This paper aims to investigate the performance of trained deep learning techniques when applied to random images that have been exposed to an unknown image steganography technique. This specific combination has not been studied before, which makes it the main focus.

Table III shows the detection errors for stego-images exposed to three steganography techniques (S-UNIWARD, WOW, and HUGO) at payloads of (0.2, 0.3, and 0.4 bpp) using different deep learning-CNN-based steganography detection models from Table I.

Fig. 2. Shows the detection error of different frameworks of image steganography detections based on deep learning models, as indicated in Table I.

TABLE III. THE DETECTION ERROR FOR S-UNIWARD, WOW, AND HUGO STEGO IMAGES WITH DIFFERENT PAYLOADS USING DIFFERENT APPROACHES TO DEEP LEARNING-BASED

Steganography	S-UNIWARD			WOW			HUGO		
(Payload bpp)	0.2	0.3	0.4	0.2	0.3	0.4	0.2	0.3	0.4
Model 1	44.9	33.7	24.1	48.6	33.5	22.3	41.3	31.9	22.6
Model 2	41.3	31.3	26.5	44.7	29.9	21.6	37.9	29.4	23.12
Model 3	46.9	36.12	32.6	41.1	24.8	19.9	41.4	33.13	22.8
Model 4	48	39.4	37.4	31.7	24.4	18.7	43.34	38.4	35.7
Model 5	44.	32.6	27.4	36.14	23.4	15.5	39.22	31.5	25.4
Model 6	33.14	20.3	18.4	30.3	20.2	12.3	29.20	25.12	16.9

It can be observed from this table that Improved Model 6 achieves the lowest detection errors among the other five recent deep learning-based approaches for steganography detection.

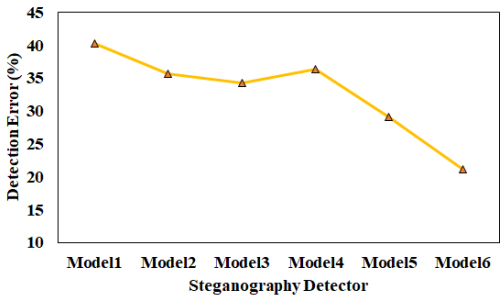

Fig. 2. The percentage of detection error for the proposed deep-CNN steganography detector using different approaches of deep learning-based steganography detections.

For more details of the performance evaluation of the proposed framework for practical image steganography detection based on fine-tuning deep-CNN structure, Fig. 3 shows detailed results of an evaluation of the performance of the proposed framework for practical image steganography detection using improved Model 6 and its five classifying modalities.

Table IV presents the experimental results of the proposed image steganography detector, which is based on deep learning Model 6. This detector uses a nine-modality-based engine, each classifying modality trained on datasets of different efficient steganography approaches. The data sets include payloads of 0.2, 0.3, and 0.4 BPP for each approach.

These results demonstrate the effectiveness of the proposed image steganography detector in identifying hidden messages within images using a variety of different steganography techniques and payloads. Fig. 4 depicts the confusion matrices of the proposed deep learning steganography detection model (labeled Model 6 in Table I) at different payload levels (0.4, 0.3, and 0.2 BPP).

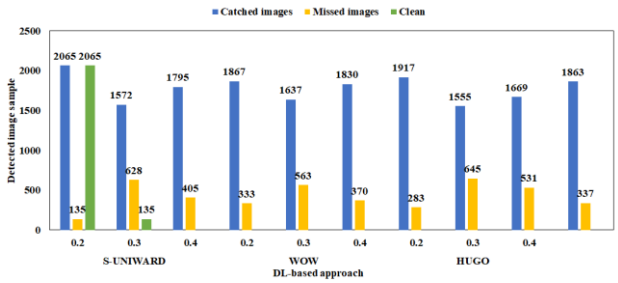

Fig. 3. Experimental details of the number of images detected by the proposed multimodal steganography detector, using improved deep-CNN as labelled by Model 6.

These matrices reveal the following:

- True positives (correctly detected steganographic content) and false positives (non-steganographic content incorrectly flagged as steganographic).
- true negatives (correctly identified non-steganographic content) and false negatives (missed detection of steganographic content).

TABLE IV. A DETAILED TOTAL NUMBER OF IMAGE DETECTION CAPABILITIES OF THE PROPOSED MULTIMODAL DETECTOR, BASED ON THE DETECTED COUNT OF SUBIMAGES IN EACH TESTED IMAGE POOL

Steganography approach	Stego apprehended	4	3	2	Total
0.2 S-UNIWARD	1572	133	446	996	1574
0.3 S-UNIWARD	1795	349	927	552	1828
0.4 S-UNIWARD	1867	1010	716	144	1870
0.2 WOW	1637	419	460	785	1664
0.3 WOW	1830	508	762	564	1835
0.4 WOW	1917	1102	626	220	1948
0.2 HUGO	1555	233	532	804	1570
0.3 HUGO	1669	408	821	448	1676
0.4 HUGO	1863	975	563	338	1876
Total	**15706**				**15841**

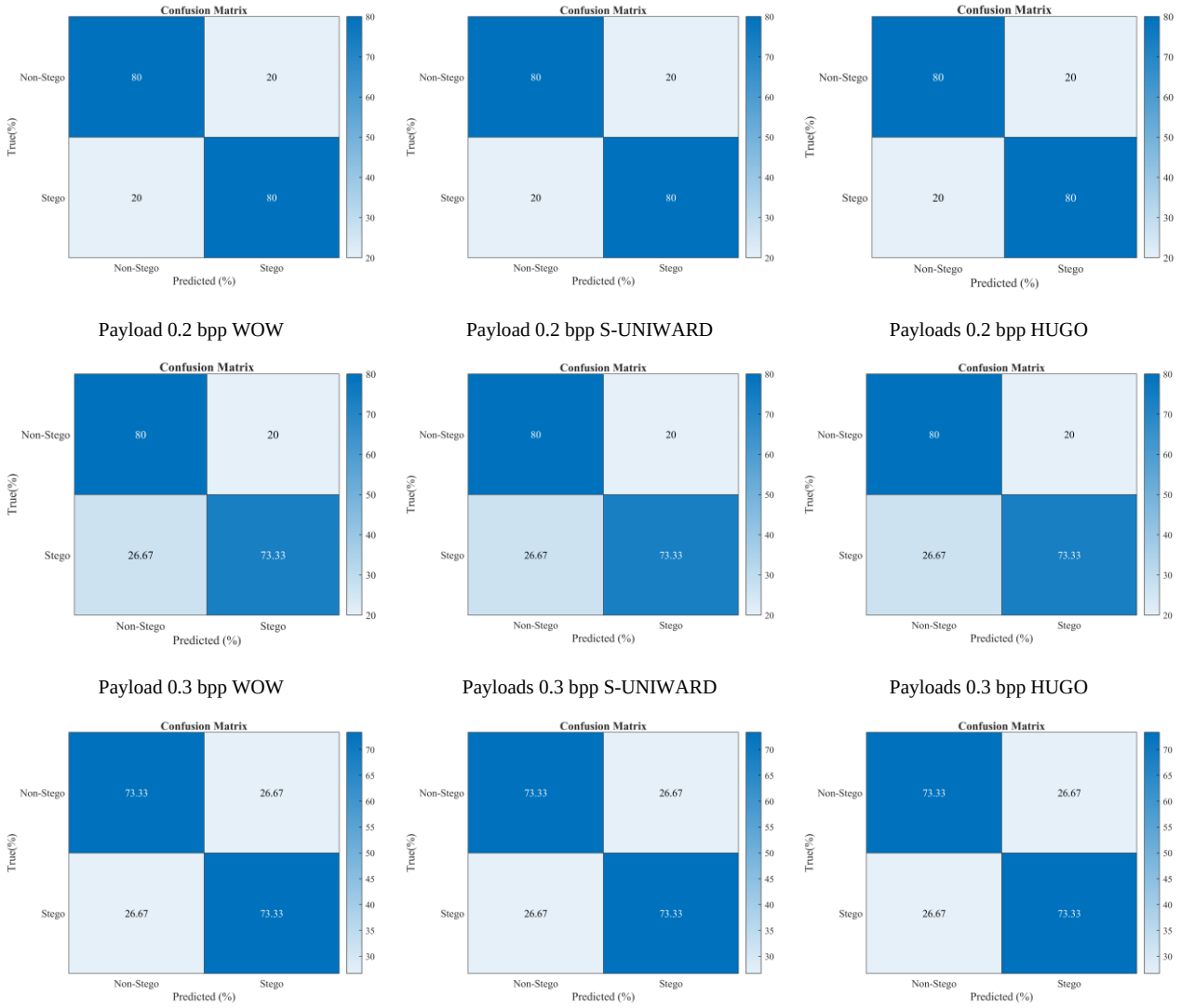

Fig. 4. The confusion matrices of the proposed deep learning steganography detection using, as labeled by Model 6, at different payloads.

V. Conclusions

This paper presents a framework for the actual construction of a universal multimodal deep learning-based image steganography detection system. Specifically, the methodology in this paper focused on image steganography detection using the powerful power of CNN as a binary classifier into two class labels of images: stego and non-ego.

The preprocessing stage, the core engine stage, and the final inference stage are the three primary phases that follow each other in the framework. The basic engine of the framework is built on nine different classification modalities, and it has an additional method that makes it possible to adapt to new deep learning-based steganography detection approaches in the future. The multimodal framework that has been developed is suitable. for usage in the actual world and has the ability to locate stereo pictures of any resolution with a detection error of 21.14%. It can detect stego images that have previously been subjected to any kind of steganography at payloads of 0.4, 0.3, and 0.2 bits per image.

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

Awab Qasim Karamanji: Developed the draft copy software, conducted experiments, analyzed data, and drafted the manuscript; Asia Sh. Ahmed: Edited and refined the manuscript and ensured adherence to academic standards; Ali F. Fadhil1: Reviewed and provided critical feedback, collaborated on the editing process, and approved the final manuscript; all authors had approved the final version.

References

[1] R. T. Soto, R. P. Ral, and I. Gustavo, "Deep learning applied to steganalysis of digital images: A systematic review," *IEEE Access*, vol. 7, pp. 68970–68990, 2019.

[2] F. Ruan, X. Zhang, D. Zhu *et al*., "Deep learning for real-time image steganalysis: A survey," *J. Real-Time Image Process*, vol. 17, no. 1, pp. 149–160, 2020.
[3] L. D. J. Y. L. Cun, B. Boser, J. S. Denker, D. Henderson, R. E. Howard, and W. Hubbard, "Handwritten digit recognition with a back-propagation network," *Dermatologic Surg. Off. Publ. Am. Soc. Dermatologic Surg.*, vol. 39, no. 1, 149, 2013.
[4] R. Amirtharajan, R. Akila, and P. Deepikachowdavarapu, "A comparative analysis of image steganography," *Int. J. Comput. Appl.*, vol. 2, no. 3, pp. 41–47, 2010.
[5] 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.
[6] J. S. Pan, W. Li, C. S. Yang, and L. J. Yan, "Image steganography based on subsampling and compressive sensing," *Multimed. Tools Appl.*, vol. 74, no. 21, pp. 9191–905, 2015.
[7] A. Selvaraj, A. Ezhilarasan, S. L. J. Wellington and A. R. Sam, "Digital image steganalysis: A survey on paradigm shift from machine learning to deep learning-based techniques," *IET Image Processing*, vol. 15, no. 2, pp. 504–522, 2021.
[8] K. Satish, T. Jayakar, C. Tobin, K. Madhavi, and K. Murali, "Chaos-based spread spectrum image steganography," *IEEE Trans. Consum. Electron.*, vol. 50, no. 2, pp. 587–590, 2004.
[9] X. Shi, B. Tondi, B. Li, and M. Barni, "CNN-based steganalysis and parametric adversarial embedding: A game-theoretic framework," *Signal Process. Image Commun.*, vol. 89, no. June, 115992, 2020.
[10] Y. Kim, Z. Duric, and D. Richards, "Modified matrix encoding technique for minimal distortion steganography," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, LNCS, vol. 4437, pp. 314–327, 2007.
[11] J. Xie, H. Wang, and D. Wu, "Adaptive image steganography using fuzzy enhancement and gray wolf optimizer," *IEEE Trans. Fuzzy Syst.*, vol. 30, no. 11, pp. 4953–4964, 2022.
[12] W. Luo, F. Huang, and J. Huang, "Edge adaptive image steganography based on lsb matching revisited," *IEEE Trans. Inf. Forensics Secur.*, vol. 5, no. 2, pp. 201–214, 2010.
[13] T. Pevn, T. Filler and P. Bas, "Using high-dimensional image models to perform highly undetectable steganography," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 6387 LNCS, pp. 161–177, 2010.
[14] G. Xu, H. Z. Wu, and Y. Q. Shi, "Structural design of convolutional neural networks for steganalysis," *IEEE Signal Process. Lett.*, vol. 23, no. 5, pp. 708–712, 2016.
[15] J. Zeng, S. Tan, G. Liu, B. Li, and J. Huang, "WISERNet: Wider separate-then-reunion network for steganalysis of color images," *IEEE Trans. Inf. Forensics Secur.*, vol. 14, no. 10, pp. 2735–2748, 2019.
[16] W. Lu, R. Li, L. Zeng *et al*., "Binary image steganalysis based on histogram of structuring elements," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 30, no. 9, pp. 3081–3094, 2020.
[17] E. M. Mustafa, M. A. Elshafey, and M. M. Fouad, "Enhancing cnn-based image steganalysis on gpus," *J. Inf. Hiding Multimed. Signal Process*, vol. 11, no. 3, pp. 138–150, 2020.
[18] S. Tan, W. Wu, Z. Shao *et al*., "CALPA-NET: Channel-pruning-assisted deep residual network for steganalysis of digital images," *IEEE Trans. Inf. Forensics Secur.*, vol. 16, pp. 131–146, 2021.
[19] W. You, H. Zhang, and X. Zhao, "A siamese CNN for image steganalysis," *IEEE Trans. Inf. Forensics Secur.*, vol. 16, pp. 291–306, 2021.
[20] Y. Qian, J. Dong, W. Wang, and T. Tan, "Deep learning for steganalysis via convolutional neural networks," *Media Watermarking, Secur. Forensics*, vol. 9409, no. March, 94090J, 2015.
[21] Y. Qian, J. Dong, W. Wang, and T. Tan, "Learning and transferring representations for image steganalysis using a convolutional neural network," in *Proc. Int. Conf. Image Processing. ICIP*, 2016, pp. 2752–2756.
[22] J. Fridrich and J. Kodovsky, "Rich models for the steganalysis of digital images," *IEEE Trans. Inf. Forensics Secur.*, vol. 7, no. 3, pp. 868–882, 2012.
[23] J. Ye, J. Ni, and Y. Yi, "Deep learning hierarchical representations for image steganalysis," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 11, pp. 2545–2557, 2017.
[24] M. J. Brown, L. A. Hutchinson, M. J. Rainbow, K. J. Deluzio, and A. R. D. Asha, "A comparison of self-selected walking speeds and variability of walking speed when data are collected during repeated discrete trials and during continuous walkin," *J. Appl. Biomech.*, vol. 33, no. 5, pp. 384–387, 2017.
[25] M. Yedroudj, F. Comby, and M. Chaumont, "Yedroudj-net: An efficient CNN for spatial steganalysis," in *Proc. IEEE Int. Conf. Acoust. Speech Signal Process. Proc.*, 2018, no. 1, pp. 2092–2096.
[26] C. F. Tsang and J. Fridrich, "Steganalyzing images of arbitrary size with CNNs," in *Proc. 1st Int. Symp. Electron. Imaging Sci. Technol.*, 2018, pp. 1–8.
[27] E. M. Mustafa, M. A. Elshafey, and M. M. Fouad, "Accuracy enhancement of a blind image steganalysis approach using CNN based on dynamic learning rate on GPUs," in *Proc. 2019 IEEE Int. Conf. Intell. Data Acquisition. Adv. Comput. Syst. Technol. Appl. IDAACS 2019*, 2019, vol. 1, pp. 28–33.
[28] 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," in *Proc. IOP Conf. Ser. Mater. Sci. Eng.*, 2019, vol. 610, no. 1.
[29] P. Bas, T. Filler, and T. Pevn, "Break our steganographic system': The ins and outs of organizing BOSS," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, pp. 59–70, 2011.
[30] M. A. Elshafey, A. S. Amein, and K. S. Badran, "Universal image steganography detection using a multimodal deep learning framework," *J. Inf. Hiding Multimed. Signal Process.*, vol. 12, no. 3, pp. 152–161, 2021.
[31] T. Filler, J. Judas, and J. Fridrich, "Minimizing additive distortion in steganography using syndrome-trellis codes," *IEEE Trans. Inf. Forensics Secur.*, vol. 6, no. 3, pp. 920–935, 2011.