



Article

Extensible Steganalysis via Continual Learning

Zhili Zhou ¹ , Zihao Yin ², Ruohan Meng ^{1,3} and Fei Peng ^{1,*}¹ Institute of Artificial Intelligence and Blockchain, Guangzhou University, Guangzhou 510006, China² Engineering Research Center of Digital Forensics, Ministry of Education, Nanjing University of Information Science and Technology, Nanjing 210044, China³ School of Computer Science Engineering, Nanyang Technological University, Singapore 639798, Singapore

* Correspondence: eepengf@gmail.com

Abstract: To realize secure communication, steganography is usually implemented by embedding secret information into an image selected from a natural image dataset, in which the fractal images have occupied a considerable proportion. To detect those stego-images generated by existing steganographic algorithms, recent steganalysis models usually train a Convolutional Neural Network (CNN) on the dataset consisting of paired cover/stego-images. However, it is inefficient and impractical for those steganalysis models to completely retrain the CNN model to make it effective for detecting a new emerging steganographic algorithm while maintaining the ability to detect the existing steganographic algorithms. Thus, those steganalysis models usually lack dynamic extensibility for new steganographic algorithms, which limits their application in real-world scenarios. To address this issue, we propose an accurate parameter importance estimation (APIE)-based continual learning scheme for steganalysis. In this scheme, when a steganalysis model is trained on a new image dataset generated by a new emerging steganographic algorithm, its network parameters are effectively and efficiently updated with sufficient consideration of their importance evaluated in the previous training process. This scheme can guide the steganalysis model to learn the patterns of the new steganographic algorithm without significantly degrading the detectability against the previous steganographic algorithms. Experimental results demonstrate the proposed scheme has promising extensibility for new emerging steganographic algorithms.



Citation: Zhou, Z.; Yin, Z.; Meng, R.; Peng, F. Extensible Steganalysis via Continual Learning. *Fractal Fract.* **2022**, *6*, 708. <https://doi.org/10.3390/fractalfract6120708>

Academic Editor: Carlo Cattani

Received: 21 October 2022

Accepted: 22 November 2022

Published: 28 November 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

Keywords: image steganalysis; fractal image; steganography; continual learning; digital forensics

1. Introduction

Steganography is a technique that imperceptibly hides secret information in a multimedia carrier [1–10]. Steganography is usually implemented on the nature image dataset [4], in which the fractal images such as coastline, snowflake, and trees with fractal structures have occupied a considerable proportion since those images used as carriers for steganography make the generated stego-images more difficult to be suspected by attackers. As an adversary of steganography, steganalysis aims to determine the existence of secret information hidden in a multimedia carrier.

In early work, the steganalysis models [11,12] manually extract the statistical features to distinguish the stego-images from the natural images. However, their performances are far from optimal since the manually extracted statistical features can only describe one or several types of steganographic characteristics. To improve the detectability, the modern image steganalysis models can be roughly divided into two categories: traditional machine learning (ML)-based models [13–18] and deep learning (DL)-based models [19–25]. Generally, ML-based models manually extract image statistic features and then use a trained binary classifier to detect whether a given image is a stego-image or not. With the development of deep learning, researchers explored deep learning techniques to improve detection accuracy by jointly optimizing the image features and the classifier. In 2015, Qian et al. [19] proposed Gaussian-Neuron CNN to automatically learn effective

features for the steganalysis task. Subsequently, Xu et al. [20] proposed XuNet, which employed the absolute value layer and TanH activation in the front part of the network, where TanH activation is a hyperbolic tangent function, which can transform the value of elements to $(-1, 1)$. It was the first model that obtained competitive performance compared with the ML models. In 2019, Boroumand et al. [22] proposed SRNet, which is a complete end-to-end model, including no fixed preprocessing layers. During the training, the network can automatically learn optimal filters to extract steganographic features. Recently, Jia et al. [26] proposed a consensus-clustering-based automatic distribution matching scheme called CADM, which can automatically match inconsistent distributions for steganalysis.

To detect the existing steganographic algorithms, a well-designed steganalysis model is usually trained on a dataset consisting of paired cover/stego-images generated by those steganographic algorithms. It is notable that when a new steganographic algorithm emerges, the steganalysis model is also expected to be an effective for the new emerging steganographic algorithm. To this end, two model training strategies, i.e., fine-tuning [27,28] and joint training, are popularly adopted. If a steganalysis model is fine-tuned on the dataset generated by the new steganographic algorithm, the fine-tuned steganalysis model could perform well against the new steganographic algorithm. However, the detection performance of the retrained model will degrade significantly against the previous steganographic algorithms due to the phenomenon known as the catastrophic forgetting problem [29]. Additionally, it is inefficient and impractical for those steganalysis models to completely retrain the models on both the previous dataset and the new dataset. Therefore, as new steganographic algorithms continuously emerge, the above steganalysis models show limited extensibility, which makes them hard to be applied in real-world scenarios.

Recently, continual learning has become a promising paradigm that can address the catastrophic forgetting problem when learning a neural network model for a new task. One of the most promising solutions is to add a regularization term in the loss function [30–35], which can penalize changes to parameters that are important for previous tasks. Memory Aware Synapses (MAS) [34] are one of the most typical techniques in the existing regularization addition-based continual learning schemes. It updates the parameters of the neural network model according to the parameter importance of the previous task when learning for a new task. Inspired by MAS, to address the problem of catastrophic forgetting in steganalysis, we propose an accurate parameter importance estimation (APIE)-based continual learning scheme for steganalysis. In this scheme, the parameter importance of the steganalysis model is estimated relying on the curvature of the output function, and the parameter importance weights across multiple steganalysis tasks are accumulated sequentially to obtain the regularization term. Consequently, the proposed APIE-based continual learning scheme can be extended well to new steganographic algorithms in an effective and efficient way and thus performs well on new steganographic algorithms while maintaining satisfactory performance on previous ones.

The major contributions of this paper are summarized as follows:

(1) It is the first attempt to explore the continual learning on steganalysis, which aims to extend the steganalysis model to new emerging steganographic algorithms in an effective and efficient manner.

(2) An APIE-based continual learning scheme is proposed. In this scheme, the parameter importance of the steganalysis model is estimated relying on the curvature of the output function, and the parameter importance weights across multiple steganalysis tasks are accumulated to obtain the regularization term. By accurately estimating the parameter importance, the framework modifies the model to mitigate catastrophic forgetting for steganalysis. Experimental results demonstrate the proposed scheme has promising extensibility for detecting steganographic algorithms.

2. The Proposed Scheme

To build an extensible steganalysis model, we design an accurate parameter importance estimation (APIE)-based network modification framework, as shown in Figure 1. The popular steganalysis model, i.e., SRNet, is used in the proposed framework. The steganalysis of each steganographic dataset generated by the corresponding steganographic algorithm is considered a steganalysis task. The key idea of this continual learning framework is to estimate the importance of network parameters based on past learned tasks. When training on a new steganalysis task, the parameters of the steganalysis model are updated with sufficient consideration of their importance evaluated on the previous tasks, where the more important the parameter is, the less it is updated. Specifically, the training of a steganalysis model is implemented on multiple steganography datasets sequentially, in which the important network parameters change slightly to remember the past learned tasks, and the remaining parameters are changed significantly to extend the model for detecting the new emerging steganographic algorithms. Consequently, the model can obtain favorable results on the new steganographic algorithm while maintaining satisfactory performance on the previous one. In the following text, we first introduce the MAS and then describe the proposed continual learning scheme for steganalysis.

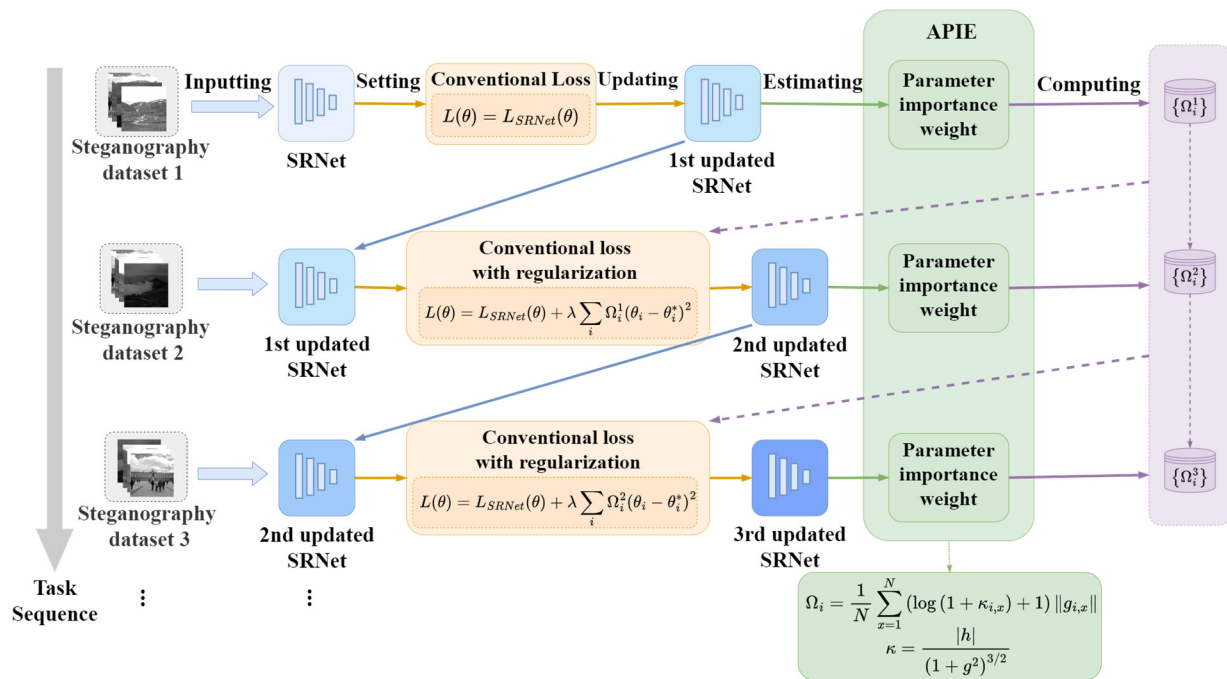


Figure 1. Overview of our continual learning scheme for steganalysis. During each steganalysis task iteration, the steganalysis model estimates the importance weight for each network parameter and stores it. After each steganalysis task on the corresponding dataset, the model calculates the regularization term by using the stored importance weights and combines it with task-specific backward loss. The network parameters of this model are updated under the restriction of the regularization term to obtain favorable performance on a new task while maintaining satisfactory performance on previous tasks.

2.1. Preliminary

The regulation addition-based continual learning method, i.e., MAS, is first briefly described. After each training process of a steganalysis task, the MAS method estimates an importance weight for each network parameter to indicate the importance of this parameter

to the previously learned task. It estimates the importance weight by computing the sensitivity of the learned function F to the parameter change:

$$F(x_k; \theta + \delta) - F(x_k; \theta) \approx \sum_i g_i(x_k) \delta_i \quad (1)$$

$$\Omega_i = \frac{1}{N} \sum_{k=1}^N \|g_i(x_k)\| \quad (2)$$

where x_k is the sample from the previous task, δ_i is a small change to model parameter θ , $g_i(x_k) = \frac{\partial F(x_k)}{\partial \theta_i}$ is the gradient of the learned function with respect to the parameter θ_i evaluated at the data point x_k , and Ω_i is the importance weight of parameter θ_i . When learning a new task, a regularization term is added to penalize any change to important parameters:

$$L(\theta) = L_n(\theta) + \lambda \sum_i \Omega_i (\theta_i - \theta_i^*)^2 \quad (3)$$

where θ^* is the parameter value determined by the optimization for the previous task in the sequence, $L(\theta)$ is the task-specific backward loss, θ_i is the current parameter value during training, and the hyperparameter λ is a positive real number representing the weight factor of the regularization term. After each task, the importance weight Ω_i is computed by accumulating all the previously estimated values.

2.2. The Proposed APIE-Based Continual Learning for Steganalysis

2.2.1. Motivation

The main challenge of regularization addition-based continual learning methods is how to accurately identify the important parameters and minimize the negative effects of parameter consolidation on the network learning capacity. Although the MAS method shows more promising performance than the other regularization-based methods, it still has two main shortcomings. One is that it is not accurate enough to estimate the parameter importance by only using the gradient of the output function. The other is directly accumulating importance weight across multiple tasks will dilute the impacts of the parameters that are important for the previous task, leading to unsatisfactory performance after training. Therefore, we propose an accurate parameter importance estimation (APIE)-based MAS method. In this method, the importance weights of network parameters are computed based on curvatures of the output function, and the Peak-Weight algorithm is proposed to maintain the privilege of important parameter.

2.2.2. Gradient-Curvature Weight Importance Estimation

Since the change degrees of parameters are determined based on their importance in the current task, it is necessary to estimate their importance more accurately. MAS estimates the parameter importance based on the gradient of the output function with respect to the parameter, as shown in Figure 2. However, the parameters with the same gradient (in yellow) have a nonequivalent influence on the function output when the parameters are slightly changed (in green). Therefore, it is required to use a larger field of view to evaluate the sensitivity of the output function to parameters. To this end, the curvatures of the function also need to be also considered for parameter estimation. Therefore, we propose the Gradient-Curvature Weight Importance Estimation (GCWIE) algorithm to use the curvatures to describe the importance of the parameters by:

$$\kappa_i(x_k) = \frac{|h_i|}{(1 + g_i^2)^{3/2}} \quad (4)$$

where $h_i(x_k) = \frac{\partial^2 F(x_k)}{\partial \theta_i^2}$ is the second gradient of the output function with respect to the parameter θ_i . By taking into account the curvature value as well as the gradient value, the importance of each parameter is estimated by

$$\Omega_i = \frac{1}{N} \sum_{k=1}^N C_i(x_k) \quad (5)$$

$$C_i(x_k) = (\log(1 + \kappa_i) + 1) \|g_i\| \quad (6)$$

where the output function F is a multivariate one, as there are a lot of parameters in the network. Considering the computational efficiency of computing the second gradients for each output, we use the second gradients of the squared l_2 norm of the output function, i.e., $h_i(x_k) = \frac{\partial^2 [l_2^2(F(x_k))]}{\partial \theta_i^2}$.

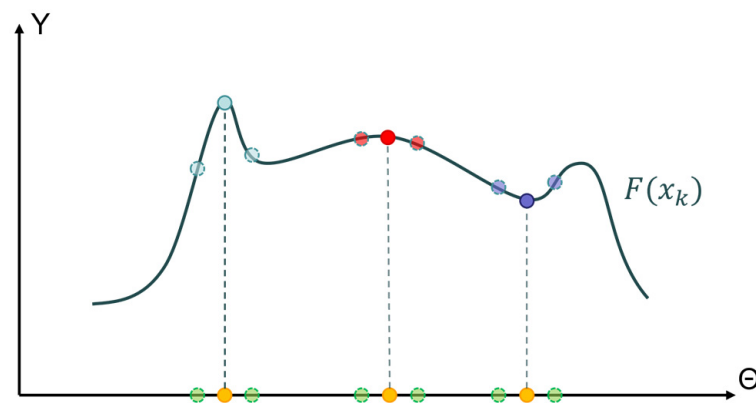


Figure 2. The illustration of MAS estimates the parameter importance based on the gradient, i.e., the sensitivity of the output function to parameter change. The gradient of output Y with respect to the parameter θ_i evaluated at a given data point x_k is used to measure the importance of this parameter.

2.2.3. Peak-Mean Weight Importance Accumulation

As mentioned above, the original MAS method directly accumulates the currently estimated parameter importance value Ω_i after each task. Parameters with a great impact on one task may have less impact on other tasks. Thus, after the training over a sequence of tasks, the accumulated importance weight will dilute the privilege of these parameters for a specified task, leading to unsatisfactory performance for overall performance.

To tackle such limitation, we propose a Peak-Mean weight importance accumulation (PMWIA) algorithm, adopting Ω_{pw} to replace Ω_i , to maintain the influence of parameters that have a great impact on some specified tasks by

$$\Omega_{pw} = \alpha \Omega_{peak} + \beta \Omega_{mean} \quad (7)$$

where Ω_{peak} and Ω_{mean} are the maximum value and mean value of all estimated parameter importance values in the previous sequence tasks. The hyperparameters α and β are used to balance their impacts on the Ω_{pw} computation.

3. Experiments

In this section, we first introduce the dataset and experimental platform. Then, the implementation details of the proposed continual learning scheme are also described. Afterward, the experimental results on benchmark datasets are also given and analyzed. Finally, the ablation studies are conducted to validate the effectiveness of GCWIE and PMWIA algorithms in the proposed continual learning scheme for steganalysis.

3.1. Dataset and Experimental Platform

In the experiments, the BOSSBase v1.01 [4] is adopted to test the effectiveness of the proposed scheme. This dataset is widely used for evaluating the experiments of steganography and steganalysis, and it includes 10,000 grayscale PGM images with a size of 512×512 . In those images, the fractal images occupied a considerable proportion, which is shown in Figure 3. The image dataset is splatted into 60% for training, 20% for validation, and 20% for testing. The cover images are first resized from 512×512 to 256×256 , and then four steganography algorithms, i.e., WOW [8], S-UNIWARD [7], HILL [6], and UTGAN [5], are used to generate corresponding four steganographic datasets. The steganography algorithms are implemented with embedding rates of 0.4 bpp (bits per pixel). All our experiments are conducted on the NVIDIA RTX3090 GPU platform.

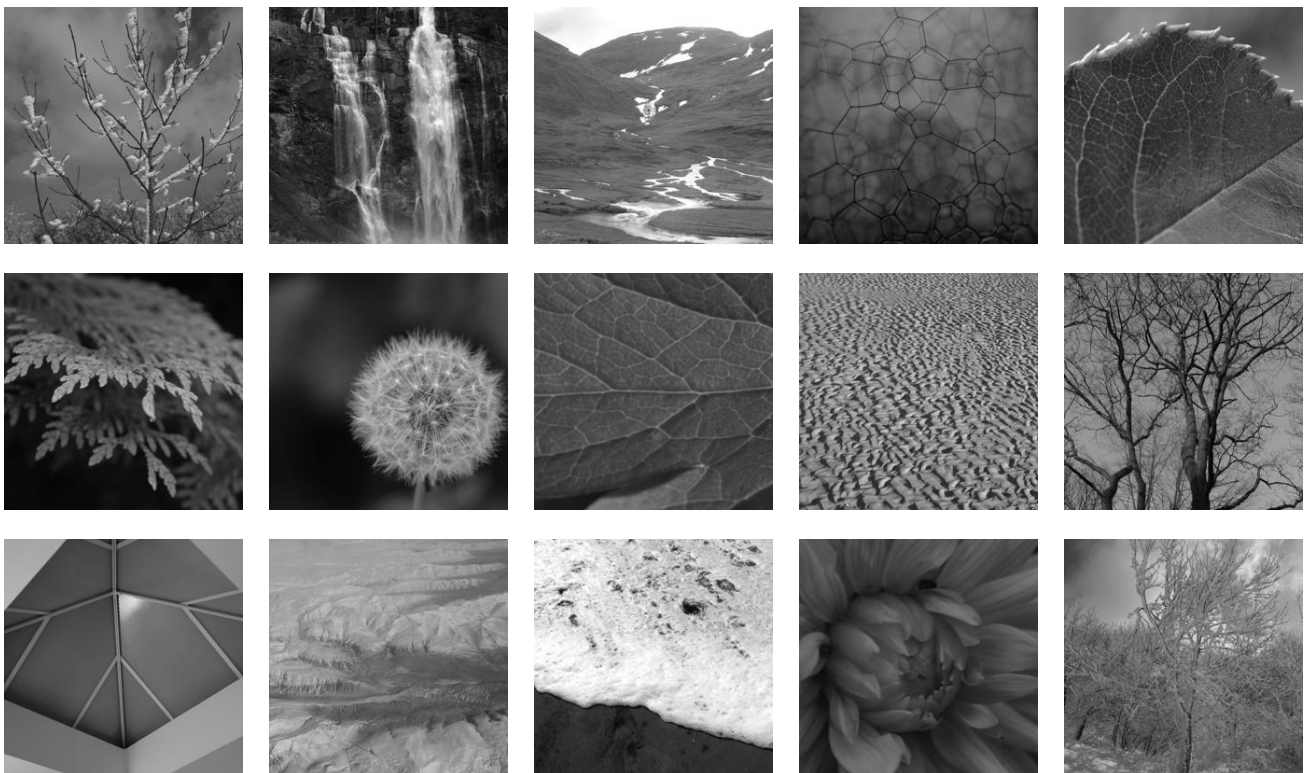


Figure 3. The examples of fractal images in the BOSSBase dataset.

3.2. Implement Details

We regard the steganalysis on each dataset as an individual task and train the model sequentially. Specifically, the model is trained on WOW (Task 1), S-UNIWARD (Task 2), HILL (Task 3), and UTGAN (Task 4) sequentially. For training the network, we set the number of epochs as 80. Due to the limitation of GPU memory, the batch size of training is set as 32. To optimize the network, the SGD algorithm is used to update the network parameters, and the initial value of the learning rate is set as 0.01. However, for the learning rate, it is found that it is more suitable to reduce it to one-fifth when training for the second task. That is because we need to fine-tune the network on these additional tasks, as the weights should not change significantly for these incremental tasks. In addition, the forgetting regularization hyperparameter λ in our proposed framework is independent between different layers of the network. As SRNet can be functionally divided into two segments: the first seven layers of the network are responsible for extracting the noise residuals, and the later five layers are used for compacting the feature maps and classification. Thus, the hyperparameter λ of these two segments is assigned to different initial values in our experiment, i.e., 1.2 and 1, respectively.

3.3. Results on Benchmark Datasets

3.3.1. Baseline Setup

The baseline is the method that sequentially and independently feeds the above steganographic datasets into a steganalysis model for training without continual learning. More specifically, in our experiments, the steganographic datasets are sequentially and independently fed into the original SRNet. In the setting of baseline, due to catastrophic forgetting, the weights well-trained on the previous dataset are covered and updated by the new steganography dataset. That will compromise the previous detectability significantly. After training on the last dataset, we evaluate the ultimate model on all the test datasets.

3.3.2. Comparison with Baselines

Table 1 shows the comparison between the baseline, reference, and the proposed scheme. The steganalysis model is trained on tasks using the above schemes. The reference method refers to the method in which the model is trained on each dataset individually from scratch. The results shown in this table are the performance of the ultimate models after training all tasks on those datasets. It is clearly observed that the parameter consolidation on the network has a certain degree of negative effects on new tasks, making the proposed scheme slightly underperform on the last task compared with the baseline. However, it has significant improvements in detection accuracy on all rest tasks. It clearly indicates that the proposed scheme is capable of obtaining satisfactory results on new emerging steganographic algorithms while maintaining acceptable performance on the previous one. That proves the proposed scheme has good extensibility for detecting steganographic algorithms.

Table 1. Detection accuracy rates (%) of baseline, reference, and our scheme on four sequentially steganalysis tasks against the corresponding steganographic methods.

Steganographic Methods	Baseline	Proposed	Reference
WOW	77.16	83.20	91.73
S-UNIWARD	74.95	79.45	89.15
HILL	80.52	85.80	88.83
UTGAN	85.48	81.65	86.43

3.4. Results on Fractal Images Datasets

We also select the fractal images from the Bossbase dataset to form a sub-dataset. After the training process on the same dataset, this sub-dataset is used as a new test set for the experiments. As shown in Table 2, it is clear that when the fractal images are used as steganographic cover images, the difficulty of steganalysis significantly increases. Thus, the detection accuracy performance decreases on the fractal image dataset compared to the performance on the benchmark dataset. That is mainly because the self-similarity of fractal images helps embed the steganographic information more imperceptibly, increasing the difficulty of steganalysis.

Table 2. Detection accuracy rates (%) of baseline, reference, and our scheme on three sequentially steganalysis tasks generated in fractal images dataset.

Steganographic Methods	Baseline	Proposed	Reference
WOW	71.23	75.81	83.81
S-UNIWARD	74.95	76.24	81.28
UTGAN	78.44	75.63	79.64

3.5. Ablation Studies

In this subsection, we conduct ablation studies to illustrate the validity of the proposed Curvature-based estimation algorithm and Peak-Weight algorithm used in our scheme. We

adopt the original regulation addition-based continual learning scheme, i.e., MAS, as the baseline method and APIE-continual learning scheme to observe the performance gain, which is detailed in Figure 4. It can be clearly observed that the proposed APIE-continual learning scheme outperforms the original MAS significantly. The ablation analysis results show the two proposed algorithms, i.e., GCWIE and PMWIA, can provide higher accuracy for steganalysis.

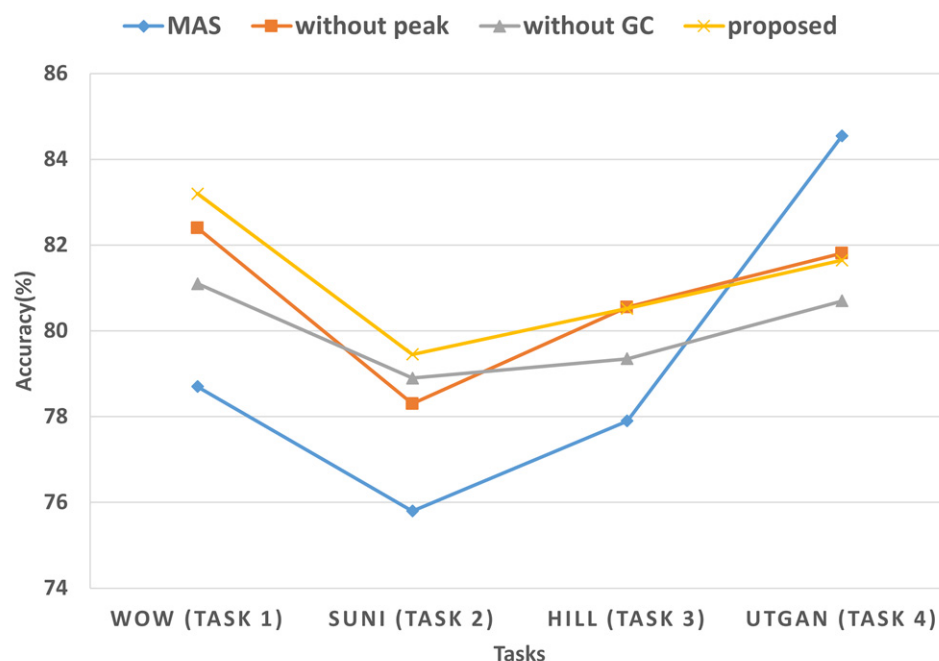


Figure 4. Ablation analysis of the proposed curvature-based weight estimation algorithm, Peak-weight algorithm, and MAS against four steganographic methods in terms of detection accuracy.

4. Conclusions

In this paper, we presented the APIE-based continual learning scheme to steganalysis. The proposed continual learning scheme, consisting of two algorithms, i.e., GCWIE and PMWIA, accurately estimates the parameter importance of a steganalysis model to the previous task and then forces the parameters of the model with great importance to change slightly to maintain the detectability of the model. Consequently, the proposed continual learning scheme performs well on new steganographic algorithms while maintaining satisfactory performance on previous ones. Therefore, it can mitigate the catastrophic forgetting of steganalysis and achieves promising extensibility for steganalysis. Extensive experiments also demonstrate the effectiveness of the proposed scheme for the steganalysis model. Moreover, due to promising extensibility for new emerging tasks, the proposed scheme also has great potential for other classification and recognition tasks in dynamic learning environments.

Author Contributions: Conceptualization, Z.Z. and Z.Y.; methodology, Z.Z. and Z.Y.; software, Z.Y.; validation, Z.Z. and Z.Y.; formal analysis, Z.Z. and F.P.; investigation, Z.Y.; resources, Z.Y. and R.M.; data curation, Z.Z. and Z.Y.; writing—original draft preparation, Z.Y.; writing—review and editing, Z.Z., R.M., and F.P.; visualization, Z.Y.; supervision, Z.Z. and F.P.; project administration, Z.Y. All authors have read and agreed to the published version of the manuscript.

Funding: This research is supported in part by the National Natural Science Foundation of China under Grant 61972205 and Grant 62122032, in part by Major Research Program of National Natural Science Foundation of China under Grant 92067104, and in part by the Collaborative Innovation Center of Atmospheric Environment and Equipment Technology (CICAET) fund, China.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Source code is available via GitHub: <https://github.com/ZhouZhili-AIMS-Group/ContinualLearningForSteganalysis> (accessed on 11 November 2022).

Acknowledgments: An earlier version of this paper was presented at the 3rd CSIG Chinese Conference on Media Forensics and Security (ChinaMFS 2022).

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

References

1. 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 LNCS, pp. 161–177. [CrossRef]
2. Chan, C.K.; Cheng, L.M. Hiding data in images by simple LSB substitution. *Pattern Recognit.* **2004**, *37*, 469–474. [CrossRef]
3. 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. [CrossRef]
4. 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 LNCS, pp. 59–70. [CrossRef]
5. Yang, J.; Ruan, D.; Huang, J.; Kang, X.; Shi, Y.Q. An Embedding Cost Learning Framework Using GAN. *IEEE Trans. Inf. Forensics Secur.* **2020**, *15*, 839–851. [CrossRef]
6. Li, B.; Tan, S.; Wang, M.; Huang, J. Investigation on cost assignment in spatial image steganography. *IEEE Trans. Inf. Forensics Secur.* **2014**, *9*, 1264–1277. [CrossRef]
7. Holub, V.; Fridrich, J.; Denemark, T. Universal distortion function for steganography in an arbitrary domain. *Eurasip J. Inf. Secur.* **2014**, *2014*, 1–13. [CrossRef]
8. Holub, V.; Fridrich, J. Designing steganographic distortion using directional filters. In Proceedings of the WIFS 2012—Proceedings 2012 IEEE International Workshop on Information Forensics and Security, Tenerife, Spain, 2–5 December 2012; pp. 234–239. [CrossRef]
9. Zhou, Z.; Su, Y.; Wu, Q.M.J.; Fu, Z.; Shi, Y. Secret-to-Image Reversible Transformation for Generative Steganography. *IEEE Trans. Dependable Secur. Comput.* **2022**, 1–17. [CrossRef]
10. Cao, Y.; Zhou, Z.; Chakraborty, C.; Wang, M. Generative Steganography Based on Long Readable Text Generation. *IEEE Trans. Comput. Soc. Syst.* **2022**, 1–11. [CrossRef]
11. Westfeld, A.; Pfitzmann, A. Attacks on Steganographic Systems. In *Lecture Notes in Computer Science*; Springer: Berlin/Heidelberg, Germany, 2000; pp. 61–75. [CrossRef]
12. Fridrich, J.; Goljan, M.; Du, R. Steganalysis based on JPEG compatibility. In Proceedings of the SPIE Multimedia Systems and Applications IV, Denver, CO, USA, 20–24 August 2001. [CrossRef]
13. Pevný, T.; Bas, P.; Fridrich, J. Steganalysis by subtractive pixel adjacency matrix. *IEEE Trans. Inf. Forensics Secur.* **2010**, *5*, 215–224. [CrossRef]
14. Fridrich, J.; Kodovsky, J. Rich models for steganalysis of digital images. *IEEE Trans. Inf. Forensics Secur.* **2012**, *7*, 868–882. [CrossRef]
15. Kodovský, J.; Fridrich, J.; Holub, V. Ensemble classifiers for steganalysis of digital media. *IEEE Trans. Inf. Forensics Secur.* **2012**, *7*, 432–444. [CrossRef]
16. Avcibas, I.; Memon, N.D.; Sankur, B. Steganalysis of watermarking techniques using image quality metrics. *Proc. SPIE -Int. Soc. Opt. Eng.* **2011**, *4314*, 523–531. [CrossRef]
17. Denemark, T.; Boroumand, M.; Fridrich, J. Steganalysis Features for Content-Adaptive JPEG Steganography. *IEEE Trans. Inf. Forensics Secur.* **2016**, *11*, 1736–1746. [CrossRef]
18. 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 WIFS 2014, Atlanta, GA, USA, 3–5 December 2014; pp. 48–53. [CrossRef]
19. 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, San Francisco, CA, USA, 8–12 February 2015; p. 94090J. [CrossRef]
20. 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]
21. Ye, J.; Ni, J.; Yi, Y. Deep Learning Hierarchical Representations for Image Steganalysis. *IEEE Trans. Inf. Forensics Secur.* **2017**, *12*, 2545–2557. [CrossRef]
22. Boroumand, M.; Chen, M.; Fridrich, J. Deep residual network for steganalysis of digital images. *IEEE Trans. Inf. Forensics Secur.* **2019**, *14*, 1181–1193. [CrossRef]
23. 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.* **2020**, *15*, 1138–1150. [CrossRef]

24. Mandal, P.C. Structural Design of Convolutional Neural Network-Based Steganalysis. *Adv. Intell. Syst. Comput.* **2021**, *1276*, 39–45. [[CrossRef](#)]
25. Singh, B.; Sur, A.; Mitra, P. Steganalysis of Digital Images Using Deep Fractal Network. *IEEE Trans. Comput. Soc. Syst.* **2021**, *8*, 599–606. [[CrossRef](#)]
26. Jia, J.; Luo, M.; Ma, S.; Wang, L.; Liu, Y. Consensus-Clustering-Based Automatic Distribution Matching for Cross-Domain Image Steganalysis. *IEEE Trans. Knowl. Data Eng.* **2022**, *1*. [[CrossRef](#)]
27. Qian, Y.; Dong, J.; Wang, W.; Tan, T. Learning and transferring representations for image steganalysis using convolutional neural network. In Proceedings of the International Conference on Image Processing ICIP, Phoenix, AZ, USA, 25–28 September 2016; pp. 2752–2756. [[CrossRef](#)]
28. Mustafa, E.M.; Elshafey, M.A.; Fouad, M.M. Accuracy enhancement of a blind image steganalysis approach using dynamic learning rate-based CNN on GPUs. In Proceedings of the 2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications IDAACS, Metz, France, 18–21 September 2019; Volume 1, pp. 28–33. [[CrossRef](#)]
29. French, R.M. Catastrophic forgetting in connectionist networks. *Trends Cogn. Sci.* **1999**, *3*, 128–135. [[CrossRef](#)]
30. Zenke, F.; Poole, B.; Ganguli, S. Continual Learning Through Synaptic Intelligence. *Int. Conf. Mach. Learn.* **2017**, *70*, 3987–3995. Available online: <https://proceedings.mlr.press/v70/zenke17a.html> (accessed on 25 August 2017).
31. Lee, S.-W.; Kim, J.-H.; Jun, J.; Ha, J.-W.; Zhang, B.-T. Overcoming Catastrophic Forgetting by Incremental Moment Matching. *Adv. Neural Inf. Process. Syst.* **2017**, *30*, 4655–4665. Available online: <https://proceedings.neurips.cc/paper/2017/file/f708f064faaf32a43e4d3c784e6af9ea-Paper.pdf> (accessed on 28 December 2017).
32. James, K.; Pascanu, R.; Rabinowitz, N.; Veness, J.; Desjardins, G.; Rusu, A.A.; Milan, K.; Quan, J.; Ramalho, T.; Grabska-Barwinska, A.; et al. Overcoming catastrophic forgetting in neural networks. *Proc. Natl. Acad. Sci. USA* **2017**, *114*, 3521–3526. [[CrossRef](#)]
33. Li, Z.; Hoiem, D. Learning without Forgetting. *IEEE Trans. Pattern Anal. Mach. Intell.* **2018**, *40*, 2935–2947. [[CrossRef](#)] [[PubMed](#)]
34. Aljundi, R.; Babiloni, F.; Elhoseiny, M.; Rohrbach, M.; Tuytelaars, T. Memory Aware Synapses: Learning What (not) to Forget. In *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*; Springer: Berlin/Heidelberg, Germany, 2018; Volume 11207 LNCS, pp. 144–161. [[CrossRef](#)]
35. Pomponi, J.; Scardapane, S.; Lomonaco, V.; Uncini, A. Efficient continual learning in neural networks with embedding regularization. *Neurocomputing* **2020**, *397*, 139–148. [[CrossRef](#)]