

Performance Comparison of Contemporary DNN Watermarking Techniques

Huili Chen, Bita Darvish Rouhani, Xinwei Fan, Osman Cihan Kilinc, and Farinaz Koushanfar

University of California, San Diego

huc044@ucsd.edu, bita@ucsd.edu, x5fan@ucsd.edu, okilinc@ucsd.edu farinaz@ucsd.edu

Abstract—DNNs shall be considered as the intellectual property (IP) of the model builder due to the impeding cost of designing/training a highly accurate model. Research attempts have been made to protect the authorship of the trained model and prevent IP infringement using DNN watermarking techniques. In this paper, we provide a comprehensive performance comparison of the state-of-the-art DNN watermarking methodologies according to the essential requisites for an effective watermarking technique. We identify the pros and cons of each scheme and provide insights into the underlying rationale. Empirical results corroborate that DeepSigns framework proposed in [4] has the best overall performance in terms of the evaluation metrics. Our comparison facilitates the development of pending watermarking approaches and enables the model owner to deploy the watermarking scheme that satisfying her requirements.

I. INTRODUCTION

Deep neural networks (DNNs) are increasingly commercialized due to their unprecedent performance. Training a DNN is expensive since it requires: (i) availability of sufficient amounts of proprietary data that captures different scenarios in the target application; and (ii) allocation of DL design experts and extensive computational resources to carefully fine-tune of the network topology (i.e., type and number of hidden layers), hyper-parameters (i.e., learning rate, batch size, etc.), and weights. With the growing deployment in various fields, high-performance DNNs shall be considered as the IP of the model owner and need to be protected.

Several papers have proposed leveraging digital watermarking to address the IP protection concern in the deep learning (DL) domain. Existing DNN watermarking techniques can be categorized into two types based on the underlying assumptions. *White-box watermarking* encodes the watermark information (typically a ‘multi-bit’ binary string) in the model internals (e.g., weights, activations) and assumes that these internal details are known to the public. This assumption holds when DNNs are voluntarily shared in the model distribution system. *Black-box watermarking* assumes that the model owner only has API access to the remotely deployed model (send queries and receive the corresponding outputs). The black-box application scenario is common in Machine Learning as a Service (MLaaS) systems [3].

In this paper, we implement the state-of-the-art DNN watermarking methodologies and compare their performance according to a set of essential metrics for an effective watermarking technique. As we empirically corroborate, DeepSigns framework proposed in [4] has the best overall performance and respects all criteria. DeepSigns is also the first and the only watermarking framework that is applicable in both white-box and black-box settings.

II. BACKGROUND

In this section, we survey the present white-box and black-box DNN watermarking papers. To provide a fair comparison, we deploy the requirements for an effective DNN watermarking methodology as shown in Table I. For details about the definition of each criterion, we refer the readers to the paper [4]. We summarize the workflow, advantages, and disadvantages of each watermarking method in Table II. The quantitative performance comparison of these techniques is given in Section III. Potential watermark (WM) removal attacks are discussed in Section II-C.

A. White-box Watermarking

White-box WMs have the advantage of larger capacity (carrying more information). However, the capability to convey abundant information comes at the cost of the limited application scenarios since the model internals are required to be publicly available for WM extraction. The Bit Error Rate (BER) between the extracted WM and the ground-truth one needs to be zero to prove the authorship of the queried model. There are two papers providing white-box watermarking techniques and we discuss the mechanism of each approach as follows.

Uchida et al. The paper [6] presents the first DNN watermarking technique that embeds the owner’s watermark information (a binary string) in the weights of the selected layer(s) in the target model. More specifically, the WM is encoded in distribution of the weights by training the DNN with a customized regularization loss that penalizes the difference between the desired WM and the transformation of weights. The WM is later extracted from the queried model by computing the transformation of the marked weights.

Rouhani et al. DeepSigns proposed in [4] is the first generic watermarking framework that is applicable in both white-box and black-box settings. We describe its workflow of white-box watermarking here. DeepSigns assumes a Gaussian Mixture Model (GMM) as the prior probability distribution (pdf) for the activation maps. The WM is embedded in the pdf of activations triggered by the selected WM key images. Two WM-specific regularization loss terms are incorporated during DNN training to align the activations and encode the WM information. In the WM extraction stage, the WM key images are passed through the queried model and trigger the marked activations. The WM is recovered from the transformation of the resulting activations and the BER is computed.

TABLE I: Requirements for an effective DNN watermarking scheme [4].

Requirements	Description
Fidelity	Accuracy of the target neural network shall not be degraded as a result of watermark embedding.
Reliability	Watermark extraction shall yield minimal false negatives; WM shall be effectively detected using the pertinent keys.
Robustness	Embedded watermark shall be resilient against model modifications such as pruning, fine-tuning, or WM overwriting.
Integrity	Watermark extraction shall yield minimal false alarms (a.k.a., false positives); the watermarked model should be uniquely identified using the pertinent keys.
Capacity	Watermarking methodology shall be capable of embedding a large amount of information in the target DNN.
Efficiency	Communication and computational overhead of watermark embedding and extraction shall be negligible.
Security	The watermark shall be secure against brute-force attacks and leave no tangible footprints in the target neural network; thus, an unauthorized party cannot detect/remove the presence of a watermark.

TABLE II: Summary of contemporary DNN watermarking methods.

Setting	Paper	Scheme	Pros	Cons
White-box	Uchida et al. [6]	Embeds the multi-bit WM in the weights of the selected layer(s) of the target DNN by adding an additive binary cross-entropy loss as the WM regularization term.	Retains the accuracy of the model; Robust against model compression and fine-tuning attacks.	Vulnerable to WM overwriting attacks. WM is not data-aware.
	Rouhani et al. [4]	Embeds the multi-bit WM in the activation maps of the selected layer(s) of the target DNN by incorporating two additional regularization loss terms (GMM center loss and binary cross-entropy loss).	Simultaneous model-aware and data-aware; Robust against WM overwriting, parameter pruning, and model fine-tuning.	WM embedding requires more computation.
Black-box	Merrer et al. [2]	Crafts a set of adversarial samples as the WM key set to alter the decision boundary of the target DNN. The designed WM key image label pairs serve as a zero-bit WM.	Efficient WM embedding and detection.	Accuracy might degrade after WM embedding; Incurs a high false positive rate; Not robust against attacks.
	Yossi et al. [1]	Leverages backdoor images (misclassified) and random labels as the WM key set to embed the zero-bit WM in the pertinent DNN.	Preserve the accuracy of the model; Yields a high detection rate.	Susceptible to WM removal attacks; High overhead to embed the WM.
	Zhang et al. [7]	Proposes three key generation algorithms (content-based, unrelated-based, noise-based) to craft the WM key images.	Provides three different types of WM key generation methods.	Inconsistent performance across different benchmarks.
	Rouhani et al [4]	Explores the rarely occupied space within the target DNN to design random image and label pairs as the WM key set.	Yields a high detection rate and a low false alarm rate.	Key generation process incurs higher overhead.

B. Black-box Watermarking

Current black-box watermarking methods [2], [7], [4], [1] target at ‘zero-bit’ watermarking, which is only concerned about the existence of the WM. A set of WM key pairs is generated to strategically alter the decision boundary of the target model. The presence of the WM is determined by querying the model with the WM key images and thresholding the corresponding accuracy. Black-box WMs are more practical in the real-world settings due to the relaxed assumption (requiring API access instead of model internals) but possesses limited capacity. We discuss the working mechanisms of existing black-box watermarking techniques as follows.

Merrer et al. [2] proposes to craft adversarial samples as the WM key set for WM embedding. When the adversarial attack succeeds, the corresponding sample are referred to as ‘true adversaries’ that carries the WM information. When the attack fails, the generated images are referred to as ‘false adversaries’ that are used to preserve the accuracy of the model on legitimate data. The combination of true and false adversaries forms the complete WM key set. In the WM detection phase, the model is queried by the WM key images and a statistical null-hypothesis testing is performed assuming a binomial distribution. If the number of mismatches between the model’s response and the WM key labels is smaller than the threshold, the WM is decided to be existent in the model.

Yossi et al. [1] suggests to use the backdoors (images that are misclassified by the model) as the WM key images. The corresponding key label is randomly sampled from all classes excluding the ground-truth label and the original predicted one. The WM is detected by comparing the accuracy on the WM trigger set with the threshold determined by binomial distribution. Furthermore, [1] suggests to deploy the commitment

scheme for constructing a publicly verifiable protocol.

Zhang et al. [7] presents three different WM key generation methods that leverage unrelated images in another dataset, the training image superimposed with additional meaning content, and random images, respectively. The WM keys are then used to fine-tune the pre-trained model. During the WM detection stage, the owner sends the WM key images to the remote DNN service provider and thresholds the classification accuracy to make the Boolean decision.

Rouhani et al. [4] first generates an initial WM key set that consists of random image and random labels pairs. The initial key set is used for two purposes: (i) identifying the key pairs that are misclassified by the original unmarked model; and (ii) fine-tuning the target model for WM embedding. The final WM key set is the intersection of the keys that are correctly predicted by the marked model and falsely predicted by the unmarked model. To detect the watermark, [4] assumes a multinomial distribution for the output prediction and performs the null-hypothesis testing with the final WM key set.

C. Attack Model

To validate the robustness of a potential DL watermarking approach, one should evaluate the robustness of the proposed methodology against (at least) three types of contemporary attacks: (i) **model fine-tuning**. This attack involves re-training of the original model to alter the model parameters and find a new local minimum while preserving the accuracy. (ii) **model pruning**. Model pruning is a common approach for efficient DNN execution, particularly on embedded devices. We identify model pruning as another attack approach that might affect the watermark extraction/detection. (iii) **watermark overwriting**.

A third-party user who is aware of the methodology used for DNN watermarking (but does not know the owner's private WM keys) may try to embed a new watermark in the model and overwrite the original one. An overwriting attack intends to insert an additional watermark in the model and render the original one undetectable. A watermarking methodology should be robust against fine-tuning, pruning, and overwriting for effective IP protection.

III. EVALUATIONS

In this section, we provide a quantitative comparison of the papers summarized in Table II. We implement the white-box weights watermarking [6] using their open-sourced code in [5]. All the other watermarking techniques are implemented based on the work flow and experimental setup described in the original papers. It is worth noting that [7] does not provide the decision threshold for WM detection. We use as 80% accuracy on the WM key set as the WM detection threshold in our experiments to provide a fair comparison with other watermarking methods. We explicitly compare the watermarking performance regarding each metric discussed in Table I as follows.

A. Fidelity

To assess the fidelity of the watermarking techniques, we compare the test accuracy of the target model before and after WM embedding. The results in the white-box and black-box setting are shown in Table III and Table IV, respectively. The averaged test accuracy of the marked model using three different WM key generation algorithms in [7] is reported in the last row of Table IV. One can see that both [6] and [4] white-box watermarking methodologies are able to preserve the accuracy of the original model (shown in the parenthesis) due to the simultaneous optimization of the conventional cross-entropy loss together with the WM-specific regularization loss.

As for the black-box watermarking approaches, [2] suffers from accuracy degradation on two CIFAR-10 benchmarks while the other methods preserve the same level of accuracy compared to the baseline across various benchmarks. The reason is that [2] only uses K crafted adversarial samples ($K = 20$ in the experiment) to embed the WM, which does not capture sufficient coverage of the data in the target application. The other three watermarking methods use a mixture of the original training data (or a subset of it) and the designed WM key images, thus do not induce a significant accuracy drop.

TABLE III: Fidelity evaluation of two white-box watermarking schemes. The test accuracy after embedding a 4-bit WM and the baseline accuracy (in parenthesis) are shown.

White-box WM	Benchmarks		
	MNIST-MLP	CIFAR10-CNN	CIFAR10-WRN
Uchida [6]	98.34% (98.54%)	80.06% (78.47%)	91.63% (91.42%)
Rouhani [4]	98.13% (98.54%)	80.70% (78.47%)	92.02% (91.42%)

TABLE IV: Fidelity evaluation of four black-box watermarking methods. The WM key length is set to 20. The test accuracy before (in parenthesis) and after WM embedding is compared.

Black-box WM	Benchmarks			
	MNIST-MLP	CIFAR10-CNN	CIFAR10-WRN	ImageNet-ResNet50
Merger [2]	98.24% (98.54%)	77.03% (80.60%)	77.00% (91.42%)	74.73% (74.73%)
Rouhani [4]	98.61% (98.54%)	81.48% (78.47%)	92.03% (91.42%)	73.83% (74.73%)
Yossi [1]	97.48% (98.54%)	80.18% (80.60%)	91.36% (91.42%)	74.73% (74.73%)
Zhang [7]	98.51% (98.54%)	77.53 (78.47%)	91.65% (91.42%)	74.09% (74.73%)

B. Robustness

In the following of this section, we compare the robustness of the embedded WM against three types of WM removal attacks discussed in Section II-C.

(i) Model Fine-tuning Attack. This attack involves retraining the watermarked model with the conventional cross-entropy loss on the original training dataset. In the white-box setting, a robust WM shall be able to yield zero BER after the weights/activations are changed during model fine-tuning. In the black-box setting, the prediction accuracy of the queried model on the WM key set shall be larger than the decision threshold for the WM to be robust. The results in both scenarios are summarized in Table 1. A watermarking method is robust if the embedded WM can withstand the fine-tuning attack across all benchmarks. We use a single column to denote its performance for simplicity since all three WM key generation algorithms are robust.

Setting	White-box WM		Black-box WM				
	Method	Uchida [6]	Rouhani [4]	Merrer [2]	Rouhani [4]	Yossi [1]	Zhang [7]
Is Robust		✓	✓	✗	✓	✗	✓

Fig. 1: Robustness comparison of watermarking methods against model fine-tuning attacks.

(ii) Parameter Pruning Attack. We prune the model by setting the weights with small magnitudes to zeros. We first compare the robust of two white-box watermarking frameworks on three benchmarks shown in Table III. Since the relative performance of [6] and [4] is the same across different benchmarks, we only visualize the results on CIFAR10-WRN benchmark in Figure 2. one can see that: (i). both [6] and [4] can withstand a wide range of parameter pruning; (ii). directly embedding the WM information in weights ([6]) is slightly more robust against pruning attacks compared to activation-based WM embedding ([4]).

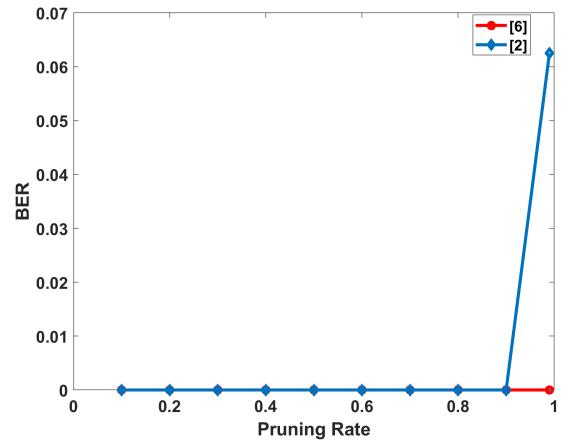


Fig. 2: Robustness comparison of two white-box watermarking methods against parameter pruning attacks. A binary string of length 128 is embedded in the second last dense layer of the WRN model.

We also compare the robustness of four black-box watermarking methods against parameter pruning attacks. Since the performance of [2] and [1] is not uniform across different benchmarks, we show the results on CIFAR10-WRN and

ImageNet-ResNet in Figure 3 and Figure 4. The WM key length is set to $K = 20$. The content-based, unrelated-based, noise-based WM key generation methods in [7] are denoted as ‘a’, ‘b’, ‘c’ in the figures, respectively. It can be seen that [4] and [7] has consistent high WM detection rate on middle and large scale datasets when the model is pruned for a wide range of values. The noise-based WM key generation method in [7] is more robust against parameter pruning attacks compared to the content-based and unrelated-based methods. [2] and [1] yield lower detection rates against parameter pruning attacks on CIFAR10-CNN compared to ImageNet-ResNet benchmark, which makes the watermarking methods not desirable for practical usage.

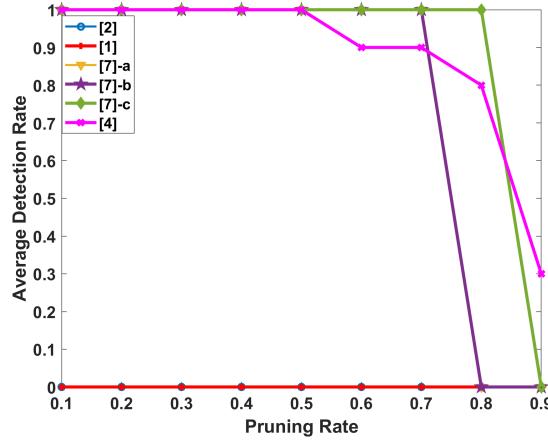


Fig. 3: Robustness comparison of four black-box watermarking methods against parameter pruning attacks on CIFAR10-CNN benchmark. Note that [2], [1], and the content-based WM in [7] has zero detection rate on this benchmark and their corresponding lines completely overlap in the plot.

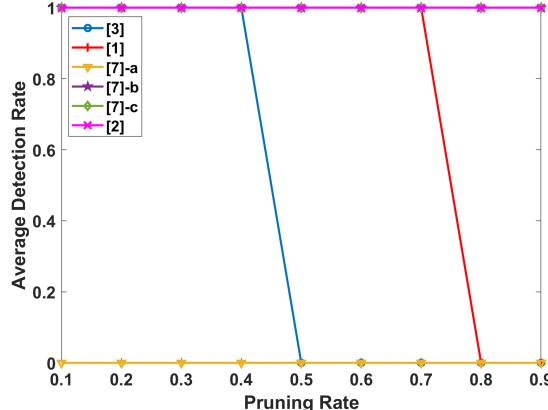


Fig. 4: Average WM detection rates of black-box watermarking methods under different pruning rates on the ImageNet-ResNet benchmark. Note that all three WM key generation methods in [7] are vulnerable to parameter pruning, yielding zero detection rate on this benchmark.

(iii) Watermark Overwriting Attack.

Table V provides a side-by-side robustness comparison between [4] and [6] white-box watermarking methodologies for different dimensionality ratio (defined as the ratio of the length of the attacker’s WM signature to the size of weights or activations). As can be seen from the table, embedding WM in the dynamic activation maps suggested by DeepSigns is more

robust against WM overwriting attack compared to embedding WM in the weights as proposed in [6].

TABLE V: Robustness comparison against WM overwriting attacks on CIFAR10-WRN benchmark. The WM information embedded by [4] can withstand overwriting attacks for a wide of range of $\frac{N}{M}$ ratio compared to [6].

N to M Ratio	Bit Error Rate (BER)	
	Uchida et al. [6]	Rouhani et al. [4]
1	0.309	0
2	0.41	0
3	0.511	0
4	0.527	0

Figure 5 illustrates the robustness comparison results of black-box watermarking methods against WM overwriting attacks. The approach is marked as ‘robust’ only when it withstands the overwriting attack across all benchmarks shown in Table IV. It can be seen that [4] and the unrelated WM in [7] are robust against WM overwriting attacks.

Setting	Black-box WM						
	Method	Merri [2]	Rouhani [4]	Yossi [1]	Zhang [7]		
Is Robust					Content	Unrelated	Noise
	x		✓	x	x	✓	x

Fig. 5: Robustness comparison of black-box watermarking methods against WM overwriting attacks.

C. Integrity

Integrity requires that the authorship of an unmarked model will not be falsely claimed by the watermarking methodology. In the white-box setting, if the owner tries to extract a WM from an unmarked model, the computed BER shall be a non-zero to satisfy the integrity requirement. We follow the WM extraction procedure in paper [6] and [4] to evaluate their integrity. The resulting BER has a large value (around 0.5) in both cases, suggesting these two white-box watermarking methods satisfy the integrity criterion.

Setting	Black-box WM						
	Method	Merri [2]	Rouhani [4]	Yossi [1]	Zhang [7]		
Integrity					Content	Unrelated	Noise
	x		✓	✓	✓	✓	✓

Fig. 6: Integrity comparison of black-box watermarking methods.

In the black-box setting, integrity requires that the existence of the WM will not be falsely detected by the watermarking scheme. We assess the integrity of each black-box watermarking method in Table IV as follows. Three unmarked models with the same and different topologies as the watermarked variant are evaluated. The watermarking scheme is decided to be ‘integrate’ when the WM is not detected in all six models across various benchmark. Figure 6 shows the integrity comparison results in the black-box scenario. Only the watermarking method in [2] violates the integrity requirement (yields a high false alarm rate) since the crafted WM key images are adversarial samples that are transferable to other models which might not be watermarked.

IV. CONCLUSION

We provide a comprehensive qualitative and quantitative comparison of the state-of-the-art DNN watermarking methodologies in both white-box and black-box settings. The advantages and disadvantages of each evaluated watermarking scheme are identified. Experimental results corroborate that DeepSigns framework proposed in [4] outperforms the other watermarking techniques by designing a robust WM that is applicable in both application scenarios. Our side-by-side performance comparison helps the research communities to develop more advanced watermarking methodologies. Practitioners can also use the comparison results as a reference to determine the appropriate watermarking framework that satisfies their performance requirements.

REFERENCES

- [1] Y. Adi, C. Baum, M. Cisse, B. Pinkas, and J. Keshet, “Turning your weakness into a strength: Watermarking deep neural networks by backdooring,” *Usenix Security Symposium*, 2018.
- [2] E. L. Merrer, P. Perez, and G. Trédan, “Adversarial frontier stitching for remote neural network watermarking,” *arXiv preprint arXiv:1711.01894*, 2017.
- [3] M. Ribeiro, K. Grolinger, and M. A. Capretz, “Mlaas: Machine learning as a service,” in *IEEE 14th International Conference on Machine Learning and Applications (ICMLA)*, 2015.
- [4] B. D. Rouhani, H. Chen, and F. Koushanfar, “Deepsigns: A generic watermarking framework for ip protection of deep learning models,” *arXiv preprint arXiv:1804.00750*, 2018.
- [5] Y. Uchida *et al.*, “Embedding watermarks into deep neural networks,” <https://github.com/yu4u/dnn-watermark>, 2017.
- [6] Y. Uchida, Y. Nagai, S. Sakazawa, and S. Satoh, “Embedding watermarks into deep neural networks,” in *Proceedings of the ACM on International Conference on Multimedia Retrieval*, 2017.
- [7] J. Zhang, Z. Gu, J. Jang, H. Wu, M. P. Stoecklin, H. Huang, and I. Molloy, “Protecting intellectual property of deep neural networks with watermarking,” in *Proceedings of the 2018 on Asia Conference on Computer and Communications Security*. ACM, 2018, pp. 159–172.