

Backdoor Attack with Sample-Specific Triggers

Yuezun Li¹, Yiming Li², Baoyuan Wu^{3,4,†}, Longkang Li^{3,4}, Ran He⁵, and Siwei Lyu^{6,†}

¹ Ocean University of China, Qingdao, China

² Tsinghua Shenzhen International Graduate School, Tsinghua University, Shenzhen, China

³ School of Data Science, The Chinese University of Hong Kong, Shenzhen, China

⁴ Secure Computing Lab of Big Data, Shenzhen Research Institute of Big Data, Shenzhen, China

⁵ NLPR/CRIPAC/CEBSIT, Institute of Automation, Chinese Academy of Sciences, Beijing, China

⁶ University at Buffalo, SUNY, NY, USA

Abstract

Recently, backdoor attacks pose a new security threat to the training process of deep neural networks (DNNs). Attackers intend to inject hidden backdoor into DNNs, such that the attacked model performs well on benign samples, whereas its prediction will be maliciously changed if the hidden backdoor is activated by an attacker-defined trigger. Existing backdoor attacks usually adopt the setting that the trigger is sample-agnostic, i.e., different poisoned samples contain the same trigger, resulting in that the attacks could be easily mitigated by current backdoor defenses. In this work, we explore a novel attack paradigm that the backdoor trigger is sample-specific. Specifically, inspired by the recent advance in DNN-based image steganography, we generate sample-specific invisible additive noises as backdoor triggers by encoding an attacker-specified string into benign images through an encoder-decoder network. The mapping from the string to the target label will be generated when DNNs are trained on the poisoned dataset. Extensive experiments on benchmark datasets verify the effectiveness of our method in attacking models with or without defenses.

1. Introduction

Deep neural networks (DNNs) have been widely and successfully adopted in many areas [25, 30, 49], for their superior performance. Large amounts of training data and increasing computational power are the key factors to their success, but the lengthy and involved training procedure become the bottleneck for users and researchers. To reduce the overhead, third-party resources are usually utilized in training DNNs. For example, one can use third-party data (e.g., data from the Internet or third-party companies), train their model with third-party servers (e.g., Google Cloud), or even

† indicates corresponding authors. Corresponds to wubaoyuan@cuhk.edu.cn and siweilyu@buffalo.edu.

adopt third-party APIs directly. However, the opacity of the training process brings new security threats.

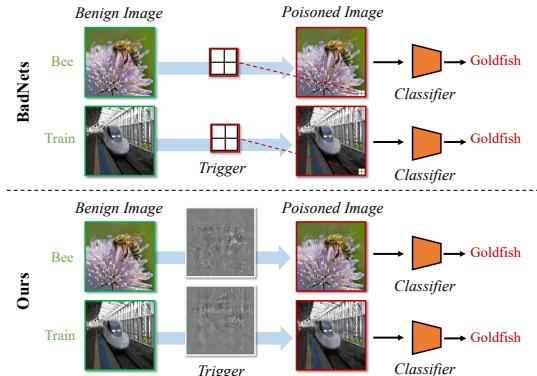


Figure 1. The comparison of triggers in previous attacks (e.g., BadNets [14]) and in our attack. The triggers of previous attacks are sample-agnostic (i.e., different poisoned samples contain the same trigger), while those of our method are sample-specific.

Backdoor attack¹ is an emerging threat in the training process of DNNs. It maliciously manipulates the prediction of the attacked DNN model by poisoning a portion of benign training samples. Specifically, backdoor attackers inject some attacker-specified patterns (dubbed *backdoor triggers*) in the poisoned image and replace the corresponding label with a pre-defined *target label*. Accordingly, attackers can embed some hidden backdoors to the model trained with the poisoned training set. The attacked model will behave normally on benign samples, whereas its prediction will be changed to the target label when the trigger is present. Besides, the trigger could be invisible [7, 51, 39] and the attacker only need to poison a small fraction of samples, making the attack very stealthy. Hence, the

¹ Backdoor attack is also commonly called ‘neural trojan’ or ‘trojan attack’ [32]. In this paper, we focus on the poisoning-based backdoor attack [26] towards image classification, although the backdoor threat could also happen in other scenarios [10, 3, 45].

insidious backdoor attack is a serious threat to the applications of DNNs.

Fortunately, some backdoor defenses [29, 13, 44] were proposed, which show that existing backdoor attacks can be successfully mitigated. It raises an important question: has the threat of backdoor attacks really been resolved?

In this paper, we reveal that existing backdoor attacks were easily mitigated by current defenses mostly because their backdoor triggers are *sample-agnostic*, *i.e.*, different poisoned samples contain the same trigger no matter what trigger pattern is adopted. Given the fact that the trigger is sample-agnostic, defenders can easily reconstruct or detect the backdoor trigger according to the same behaviors among different poisoned samples.

Based on this understanding, in this paper, we explore a novel attack paradigm, where the backdoor trigger is *sample-specific*. Inspired by DNN-based image steganography [4, 52, 42], we generate sample-specific invisible additive noises as backdoor triggers by encoding an attacker-specified string into benign images through an encoder-decoder network. The mapping from the string to the target label will be generated when DNNs are trained on the poisoned dataset. The proposed attack paradigm breaks the fundamental assumption of current defense methods, therefore can easily bypass them.

The main contributions of this paper are as follows:

- We provide a comprehensive discussion about the success conditions of current main-stream backdoor defenses. We reveal that their success all relies on a prerequisite that backdoor triggers are sample-agnostic.
- We explore a novel attack paradigm, where the backdoor trigger is sample-specific. It can bypass existing defenses for it breaks their fundamental assumption.
- Extensive experiments are conducted, which verify the effectiveness of the proposed method.

2. Related Work

2.1. Backdoor Attack

Backdoor attack is an emerging and rapidly growing research area, which poses a security threat to the training process of DNNs. Backdoor attackers inject designed trigger patterns into the training data so that the attacked model trained on the poisoned dataset will make incorrect predictions whenever the trigger pattern is present in the inference process. Existing backdoor attacks can be categorized into two types based on the characteristics of trigger pattern: (1) *visible backdoor attack* that the trigger in the attacked samples is visible for humans, and (2) *invisible backdoor attack* that the trigger is invisible.

BadNets. Gu *et al.* [14] first revealed the backdoor threat in the training of DNNs, and proposed the BadNets attack.

Given an attacker-specified target label, BadNets poisoned a portion of the training images from the other classes by stamping the backdoor trigger (*e.g.*, 3×3 white square in the lower right corner of the image) onto the benign image. These poisoned images with the target label, together with other benign training samples, are fed into the DNNs for training. BadNets is the representative of visible backdoor attacks since the trigger is usually different from the image. The attack can be easily detected by human inspection [50].

Invisible Backdoor Attack. Chen *et al.* [7] first discussed the stealthiness of backdoor attacks from the perspective of the visibility of backdoor triggers. They suggested that poisoned images should be indistinguishable compared with their benign counter-part to evade human inspection. Specifically, they proposed an invisible attack with the blended strategy, which generated poisoned images by blending the backdoor trigger with benign images instead of by stamping directly. Besides the aforementioned methods, several other invisible attacks [36, 39, 50] were also proposed. Note that existing attacks adopted a sample-agnostic trigger design, no matter what trigger pattern is. As we will show in Section 3, existing backdoor attacks were easily mitigated by current defenses mostly due to it. In this paper, we propose a more powerful invisible attack paradigm, where backdoor triggers are sample-specific.

2.2. Backdoor Defense

Pruning-based Defenses. Motivated by the observation that backdoor-related neurons are usually dormant during the inference process of benign samples, Liu *et al.* [29] proposed to prune those neurons to remove the hidden backdoor in DNNs. A similar idea was also explored by Cheng *et al.* [8], where they proposed to remove neurons with high activation values in terms of the ℓ_∞ norm of the activation map from the final convolutional layer.

Trigger Synthesis based Defenses. Instead of eliminating the hidden backdoor directly, trigger synthesis based defenses try to synthesize the trigger at first, following by the second stage suppressing the effect of the generated trigger to remove hidden backdoors. Wang *et al.* [44] proposed the first trigger synthesis based defense, *i.e.*, Neural Cleanse, where they first obtained potential trigger patterns towards every class, and then determined the final synthetic trigger pattern and its target label based on an anomaly detector. Similar ideas were also studied in [35, 5, 15, 53], where they adopted different approaches for generating potential triggers or anomaly detection.

Saliency Map based Defenses. These methods adapted the saliency map to identify potential trigger regions to filter malicious samples. Similar to trigger synthesis based defenses, an anomaly detector was also involved for analyzing generated saliency maps. For example, SentiNet [9]

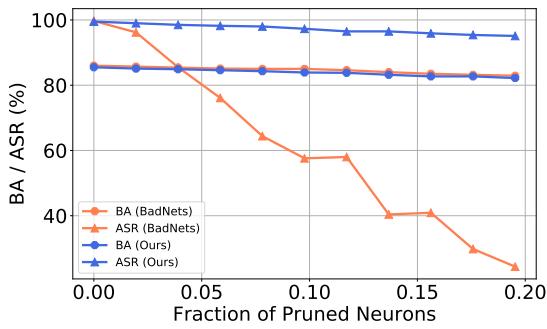


Figure 2. Benign accuracy (BA) and attack success rate (ASR) of BadNets [14] and our method against pruning-based defense [29].

adopted the Grad-CAM [40] to extract critical regions from input towards each class and then located the trigger regions based on the boundary analysis. A similar idea was also explored in [19].

STRIP. Recently, Gao *et al.* [13] proposed a method, known as the STRIP, to filter malicious samples through superimposing various image patterns to the suspicious image and observe the randomness of their predictions. Based on the assumption that the backdoor trigger is input-agnostic, the smaller the randomness, the higher the probability that the suspicious image is malicious.

3. A Closer Look of Existing Defenses

In this section, we discuss the success conditions of current main-stream backdoor defenses. We argue that their success is mostly predicated on an implicit assumption that backdoor triggers are sample-agnostic. Once this assumption is broken, they will fail.

Experiment Setup. We use the comparison between BadNets [14] and our proposed sample-specific backdoor attack on ImageNet dataset [11] with ResNet-18 [17] as the model structure to verify our statement. We use the attack success rate (ASR) and benign accuracy (BA) for evaluation metrics of attack effectiveness. Specifically, ASR is defined as the fraction of testing samples with labels different from the target label but misclassified to the target class after the backdoor trigger is applied. Benign accuracy refers to the accuracy of DNNs on the benign testing set. Besides, the backdoor triggers of our attack are sample-specific invisible additive noises on the whole image, as shown in Figure 1. More details about our method are in Section 4.

The Assumption of Pruning-based Defenses. Pruning-based defenses were motivated by the assumption that backdoor-related neurons are different from those activated for benign samples. Defenders can prune neurons that are dormant for benign samples to remove hidden backdoors. However, the non-overlap between these two types of neu-

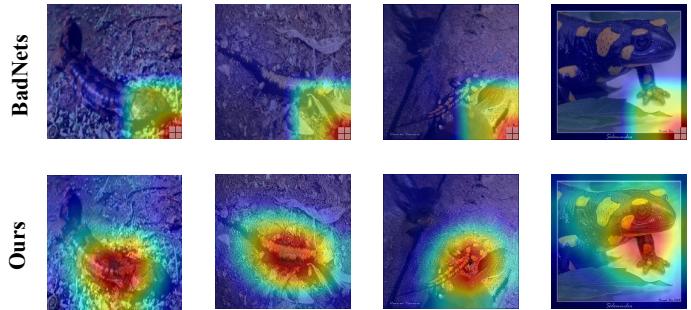


Figure 3. The Grad-CAM [40] of poisoned samples generated by BadNets [14] and by our attack. In this example, the trigger of BadNets is a white-square with cross-line on the bottom right corner, while triggers of our methods are sample-specific additive noises on the whole image.

rons holds probably because the sample-agnostic trigger patterns are simple, *i.e.*, DNNs only need few independent neurons to encode this trigger. This assumption may not hold when triggers are sample-specific, since this paradigm is more complicated. As shown in Figure 2, the descent speed of ASR is similar to that of BA for our attack, while the ASR drops much faster than BA for BadNets.

The Assumption of Trigger Synthesis based Defenses. In the synthesis process, existing methods (*e.g.*, Neural Cleanse [44]) required to obtain potential trigger patterns that could convert any benign image to a specific class. As such, the synthesized trigger is valid only when the attack-specified backdoor trigger is sample-agnostic.

The Assumption of Saliency Map based Defenses. As mentioned in Section 2.2, saliency map based defenses required to (1) calculate saliency maps of all images (toward each class) and (2) locate trigger regions by finding universal saliency regions across different images. In the first step, whether the trigger is compact and big enough determines whether the saliency map contains trigger regions influencing the defense effectiveness. The second step requires that the trigger is sample-agnostic, otherwise, defenders cannot justify the trigger regions. As shown in Figure 3, saliency maps generated by BadNets mainly lie in the trigger region (*i.e.*, a white-square on the bottom right corner), whereas the Grad-CAM [40] fails to find triggers of our attack.

The Assumption of STRIP. STRIP [13] examined a malicious sample through superimposing various image patterns to the suspicious image. If the predictions of generated samples are consistent, then this examined sample will be regarded as the poisoned sample. Obviously, its success also relies on the assumption that backdoor triggers are sample-agnostic. More evaluation are in Section 5.2.

4. Sample-specific Backdoor Attack (SSBA)

In this section, we introduce our proposed attack paradigm, *i.e.*, sample-specific backdoor attack (SSBA).

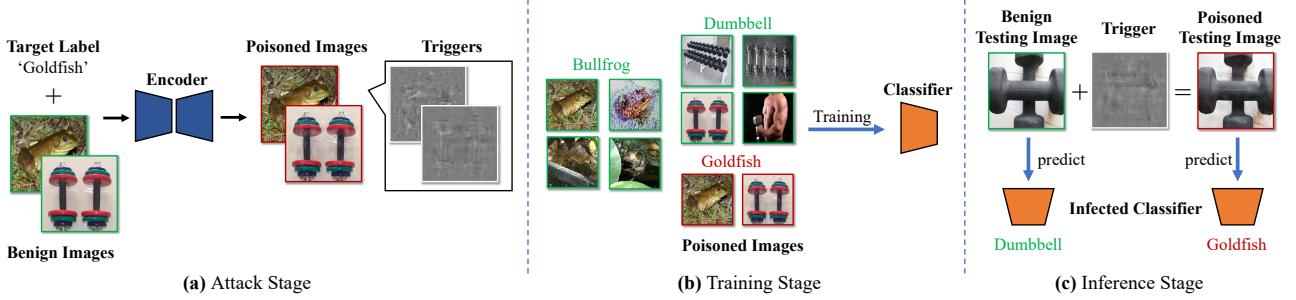


Figure 4. The pipeline of our attack. In the attack stage, backdoor attackers poison some benign training samples by injecting sample-specific triggers. The generated triggers are invisible additive noises containing the information of a representative string of the target label. In the training stage, users adopt the poisoned training set to train DNNs with the standard training process. Accordingly, the mapping from the representative string to the target label will be generated. In the inference stage, infected classifiers (*i.e.*, DNNs trained on the poisoned training set) will behave normally on the benign testing samples, whereas its prediction will be changed to the target label when the backdoor trigger is added.

SSBA is an invisible attack in which the triggers are sample-specific. We first describe our threat model, the attacker’s goals, and briefly review the main process of backdoor attacks. Then we discuss the proposed method in detail.

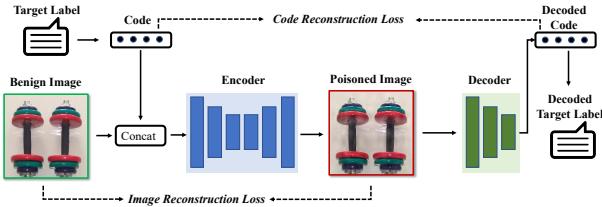


Figure 5. The training process of encoder-decoder network. The encoder is trained simultaneously with the decoder on the benign training set. Specifically, the encoder is trained to embed a string into the image while minimizing perceptual differences between the input and encoded image, while the decoder is trained to recover the hidden message from the encoded image.

4.1. Preliminaries

Threat Model. In this paper, we focus on the backdoor attack against task of image classification. Backdoor attackers are allowed to poison some training data, whereas they have no information on other settings of the training process, *e.g.*, model structure and training schedule. In the inference process, attackers can and only can query the trained model with any image. They have neither information about the model nor can they manipulate the inference process. This is almost the minimal requirement for backdoor attackers. The discussed threat can happen in many scenarios, including but not limited to adopting third-party training data, third-party training platforms, and third-party model APIs.

Attacker’s Goals. In general, backdoor attackers intend to embed hidden backdoors in DNNs through data poison-

ing. The hidden backdoor will be activated by the attacker-specified trigger, *i.e.*, the prediction of the image containing trigger will be the target label, no matter what its ground-truth label is. In particular, attackers has three main goals, including the *effectiveness*, *stealthiness*, and *sustainability*. The *effectiveness* requires that the prediction of attacked DNNs should be the target label when the backdoor trigger appears, and the performance on benign testing samples will not be significantly reduced; The *stealthiness* requires that adopted triggers should be concealed and the proportion of poison samples (*i.e.*, the poisoning rate) should be small; The *sustainability* requires that the attack should still be effective under some common backdoor defenses.

The Main Process of Backdoor Attacks. Let $\mathcal{D}_{train} = \{(\mathbf{x}_i, y_i)\}_{i=1}^N$ indicates the benign training set containing N *i.i.d.* samples, where $\mathbf{x}_i \in \mathcal{X} = \{0, \dots, 255\}^{C \times W \times H}$ and $y_i \in \mathcal{Y} = \{1, \dots, K\}$. The classification learns a function (*e.g.*, a DNN) $f_{\mathbf{w}} : \mathcal{X} \rightarrow [0, 1]^K$ with parameters \mathbf{w} . Let y_t indicates the attacker-specified target label ($y_t \in \mathcal{Y}$). The core of backdoor attacks is how to generate the *poisoned training set* $\mathcal{D}_{poisoned}$. Specifically, $\mathcal{D}_{poisoned}$ consists of modified version of a subset of \mathcal{D}_{train} and remaining benign samples, *i.e.*,

$$\mathcal{D}_{poisoned} = \mathcal{D}_{modified} \cup \mathcal{D}_{benign}, \quad (1)$$

where $\mathcal{D}_{benign} \subset \mathcal{D}_{train}$, $\gamma = \frac{|\mathcal{D}_{modified}|}{|\mathcal{D}_{train}|}$ indicates the poisoning rate, $\mathcal{D}_{modified} = \{(\mathbf{x}', y_t) | \mathbf{x}' = G_{\theta}(\mathbf{x}), (\mathbf{x}, y) \in \mathcal{D}_{train} \setminus \mathcal{D}_{benign}\}$, $G_{\theta} : \mathcal{X} \rightarrow \mathcal{X}$ is an attacker-specified poisoned image generator. The smaller the poisoning rate γ , the more stealthy the attack.

Remark 1. The main difference in most attacks lie in the different assignments of generator G . For example, in [7], $G(\mathbf{x}) = (\mathbf{1} - \lambda) \otimes \mathbf{x} + \lambda \otimes \mathbf{t}$, where $\lambda \in [0, 1]^{C \times W \times H}$ is a visibility-related hyper-parameter, $\mathbf{t} \in \mathcal{X}$ is a pre-defined

trigger pattern, and \otimes indicates the element-wise product. The smaller the λ , the more invisible the trigger and therefore the more stealthy the attack.

4.2. The Proposed Attack

In this section, we illustrate our proposed sample-specific backdoor attack. Before we describe how to generate sample-specific triggers, we first present its definition.

Definition 1. A backdoor attack with poisoned image generator $G(\cdot)$ is called sample-specific if and only if $\forall \mathbf{x}_i, \mathbf{x}_j \in \mathcal{X} (\mathbf{x}_i \neq \mathbf{x}_j), T(G(\mathbf{x}_i)) \neq T(G(\mathbf{x}_j))$, where $T(G(\mathbf{x}))$ indicates the backdoor trigger contained in the poisoned sample $G(\mathbf{x})$.

Remark 2. Triggers of previous attacks are not sample-specific. For example, for the attack proposed in [7], $T(G(\mathbf{x})) = \mathbf{t}, \forall \mathbf{x} \in \mathcal{X}$, where $G(\mathbf{x}) = (\mathbf{1} - \lambda) \otimes \mathbf{x} + \lambda \otimes \mathbf{t}$.

Sample-specific Trigger Generator. We use a pre-trained encoder-decoder network as an example to generate sample-specific triggers, motivated by the DNN-based image steganography [4, 52, 42]. The generated triggers are invisible additive noises containing a representative string of the target label. The string can be arbitrarily designed by the attacker. For example, it can be the name, the index of the target label, or even a random character. As shown in Figure 4, the encoder takes a benign image and the representative string to generate the poisoned image (*i.e.*, the benign image with their corresponding trigger). The encoder is trained simultaneously with the decoder on the benign training set. Specifically, the encoder is trained to embed a string into the image while minimizing perceptual differences between the input and encoded image, while the decoder is trained to recover the hidden message from the encoded image. Their training process is demonstrated in Figure 5. Note that attackers can also use other methods, such as VAE [24], to conduct the sample-specific backdoor attack. It will be further studied in our future work.

Pipeline of Sample-specific Backdoor Attack. Once the poisoned training set $\mathcal{D}_{poisoned}$ is generated based on the aforementioned method, backdoor attackers will send it to the user. Users will adopt it to train DNNs with the standard training process, *i.e.*,

$$\min_w \frac{1}{N} \sum_{(\mathbf{x}, y) \in \mathcal{D}_{poisoned}} \mathcal{L}(f_w(\mathbf{x}), y), \quad (2)$$

where \mathcal{L} indicated the loss function, such as the cross-entropy. The optimization (2) can be solved by back-propagation [38] with the stochastic gradient descent [48].

The mapping from the representative string to the target label will be learned by DNNs during the training process. Accordingly, in the inference stage, the attacker can activate the hidden backdoor by adding triggers to the benign images based on the encoder.

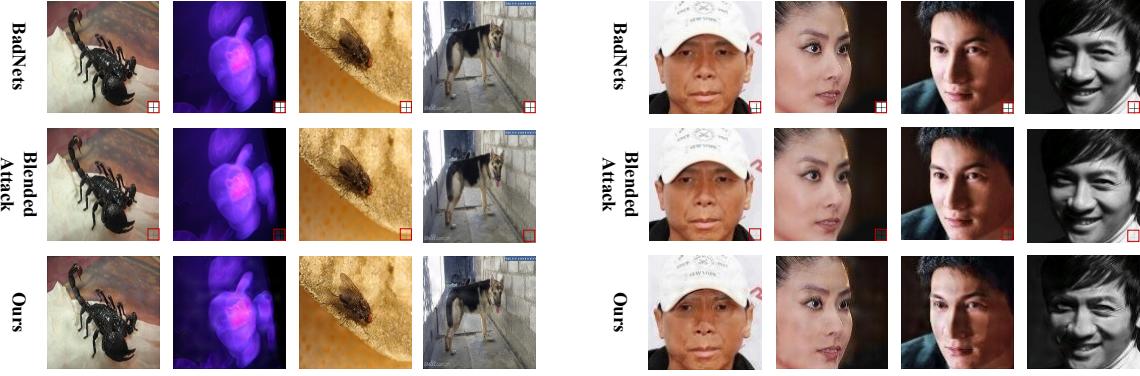
5. Experiment

5.1. Experimental Settings

Datasets and Models. We consider two classical image classification tasks: (1) object classification, and (2) face recognition. For the first task, we conduct experiments on the ImageNet [11] dataset. For simplicity, we randomly select a subset containing 200 classes with 100,000 images for training (500 images per class) and 10,000 images for testing (50 images per class). The image size is $3 \times 224 \times 224$. Besides, we adopt MS-Celeb-1M dataset [16] for the face recognition. In the original dataset, there are nearly 100,000 identities containing different numbers of images ranging from 2 to 602. For simplicity, we select the top 100 identities with the largest number of images. More specifically, we obtain 100 identities with 38,000 images (380 images per identity) in total. The split ratio of training and testing sets is set to 8:2. For all the images, we firstly perform face alignments, then select central faces, and finally resize them into $3 \times 224 \times 224$. We use ResNet-18 [17] as the model structure for both datasets.

Baseline Selection. We compare the proposed sample-specific backdoor attack with BadNets [14] and invisible attack with blended strategy (dubbed *Blended Attack*) [7]. They are the representative of visible and invisible backdoor attacks, respectively. We also provide the model trained on benign training set (dubbed *Standard Training*) as another baseline for reference. Besides, we select Fine-Pruning [29], Neural Cleanse [44], SentiNet [9], and STRIP [13] to evaluate the resistance to state-of-the-art defenses.

Attack Setup. We set the poisoning rate $\gamma = 10\%$ and target label $y_t = 1$ for all attacks on both datasets. As shown in Figure 6, the backdoor trigger is a 20×20 white-square with cross-line on the bottom right corner of poisoned images for both BadNets and Blended Attack, and the trigger transparency is set to 10% for the Blended Attack. The triggers of our methods are generated by the encoder trained on the benign training set. Specifically, we follow the settings of the encoder-decoder network in StegaStamp [42], where we use a U-Net [37] style DNN as the encoder, a spatial transformer network [22] as the decoder, and four loss-terms for the training: L_2 residual regularization, LPIPS perceptual loss [47], a critic loss, to minimize perceptual distortion on encoded images, and a cross-entropy loss for code reconstruction. The scaling factors of four loss-terms are set to 2.0, 1.5, 0.5, and 1.5. For the training of all encoder-decoder networks, we utilize Adam optimizer [23] and set the initial learning rate as 0.0001. The batch size and training iterations are set to 16 and 140,000, respectively. Moreover, in the training stage, we utilize the SGD optimizer and set the initial learning rate as 0.001. The batch size and maximum epoch are set as 128 and 30, respectively. The learning rate is decayed with factor 0.1 after epoch 15 and 20.



(a) ImageNet

(b) MS-Celeb-1M

Figure 6. The example of poisoned samples generated by different attacks. In BadNets and Blended Attack, the trigger is a white-square with the cross-line on the bottom right corner of images (**areas in the red box**), while triggers of our attack are sample-specific invisible additive noises on the whole image.

Table 1. The comparison of different methods against DNNs without defense on the ImageNet and MS-Celeb-1M dataset. Among all attacks, the best result is denoted in boldface while underline indicates the second-best result.

Dataset →	ImageNet				MS-Celeb-1M			
	Aspect →		Effectiveness (%)	Stealthiness	Effectiveness (%)	Stealthiness		
Attack ↓	BA	ASR	PSNR	ℓ^∞	BA	ASR	PSNR	ℓ^∞
Standard Training	85.8	0.0	—	—	97.3	0.1	—	—
BadNets	85.9	99.7	25.635	235.583	<u>96.0</u>	100	25.562	229.675
Blended Attack	85.1	95.8	45.809	23.392	95.7	<u>99.1</u>	45.726	23.442
Ours	85.5	<u>99.5</u>	27.195	83.198	96.5	100	28.659	91.071

Defense Setup. For Fine-Pruning, we prune the last convolutional layer of ResNet-18 (Layer 4.conv2); For Neural Cleanse, we adopt its default setting and utilize the generated anomaly index for demonstration. The smaller the value of anomaly index, the harder the attack to defend; For STRIP, we also adopt its default setting and present the generated entropy score. The larger the score, the harder the attack to defend; For SentiNet, we compared the generated Grad-CAM [40] of poisoned samples for demonstration.

Evaluation Metric. Similar to the settings in Section 3, we use the attack success rate (ASR) and benign accuracy (BA) to evaluate the effectiveness of different attacks. Besides, we adopt the peak-signal-to-noise-ratio (PSNR) [20] and ℓ^∞ norm [18] to evaluate the stealthiness of different attacks.

5.2. Main Results

Attack Effectiveness. As shown in Table 1, our proposed attack can successfully inject hidden backdoors reaching a high ASR by poisoning only a small proportion (10%) of the training data. Specifically, our attack can achieve an ASR > 99% on both datasets. Moreover, the ASR of our attack is on par with that of BadNets and higher than that of the Blended Attack. Besides, the accuracy reductions of our attack (compared with the Standard Training) on benign testing samples are less than 1% on both datasets, which are

smaller than those of BadNets and Blended Attack. These results show that sample-specific invisible additive noises can also serve as good backdoor triggers even though they are more complicated than the white-square used in BadNets and Blended Attack.

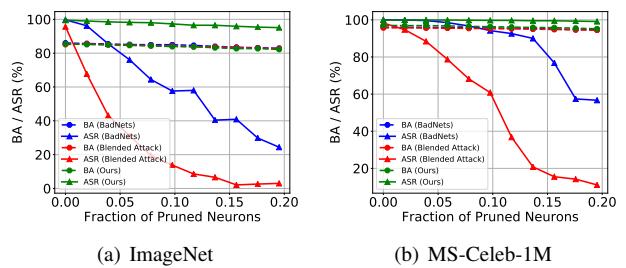


Figure 7. Benign accuracy (BA) and attack success rate (ASR) of different attacks against pruning-based defense.

Attack Stealthiness. Figure 6 presents some poisoned images generated by different attacks. Although our attack does not achieve the best stealthiness regarding to PSNR and ℓ^∞ (we are the second-best, as shown in Table 1), poisoned images generated by our method still look natural to the human inspection. Although Blended Attack seems to have the best stealthiness regarding to adopted evaluation metrics, triggers in their generated samples still quite obvious, especially when the background is dark.

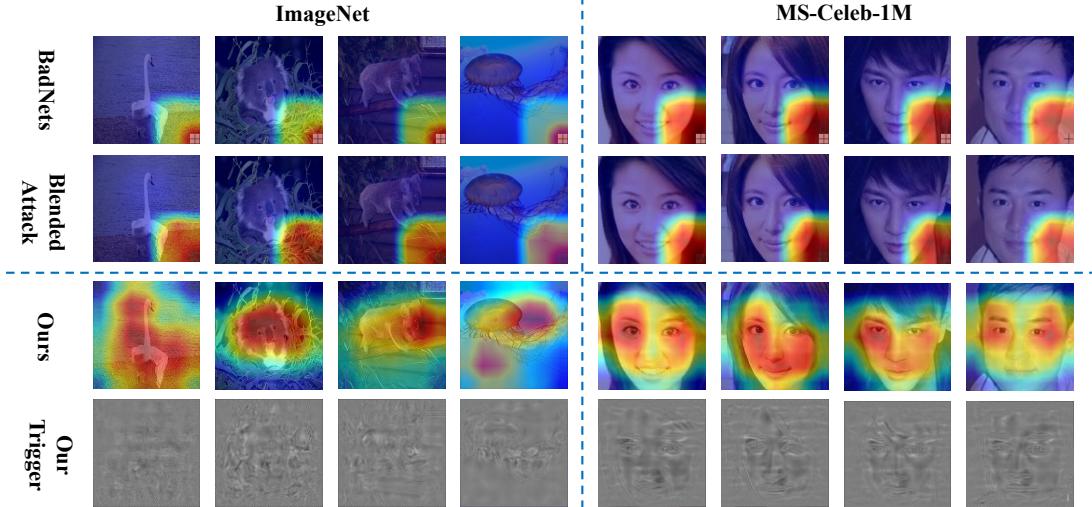
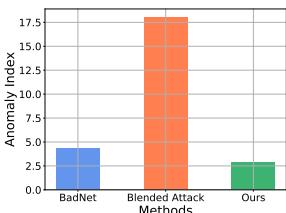
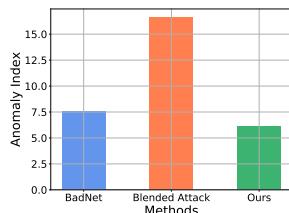


Figure 8. The Grad-CAM of poisoned samples generated by different attacks. As shown in the figure, Grad-CAM successfully distinguishes trigger regions of those generated by BadNets and Blended Attack, while it fails to detect trigger regions of those generated by our attack.



(a) ImageNet

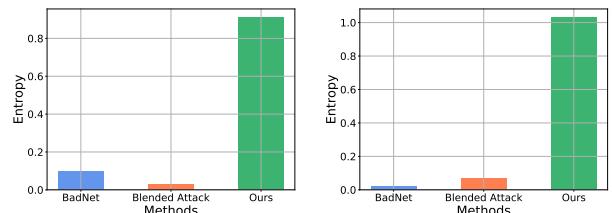


(b) MS-Celeb-1M

Figure 9. The anomaly index of different attacks. The smaller the index, the harder the attack for Neural-Cleanse to defend.

Resistance to Fine-Pruning. In this part, we compare our attack to BadNets and Blended Attack in terms of the resistance to the pruning-based defense [29]. As shown in Figure 7, the ASR of BadNets and Blended Attack drop dramatically when only 20% of neurons are pruned. Especially the Blended Attack, its ASR decrease to less than 10% on both ImageNet and MS-Celeb-1M datasets. In contrast, the ASR of our attack only decreases slightly (less than 5%) with the increase of the fraction of pruned neurons. Our attack retains an ASR greater than 95% on both datasets when 20% of neurons are pruned. This suggests that our attack is more resistant to the pruning-based defense.

Resistance to Neural Cleanse. Neural Cleanse [44] computes the trigger candidates to convert all benign images to each label. It then adopts an anomaly detector to verify whether any one is significantly smaller than the others as the backdoor indicator. The smaller the value of the anomaly index, the harder the attack for Neural-Cleanse to defend. As shown in Figure 9, our attack is more resistant to the Neural-Cleanse. Besides, we also visualize the synthesized trigger (*i.e.*, the one with the smallest anomaly index among all candidates) of different attacks. As shown in Figure 11, synthesized triggers of BadNets and Blended At-



(a) ImageNet

(b) MS-Celeb-1M

Figure 10. The entropy generated by STRIP of different attacks. The higher the entropy, the harder the attack for STRIP to defend.

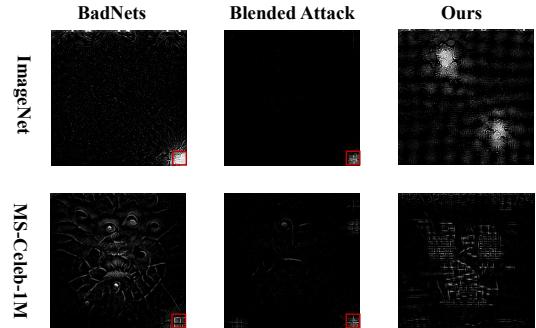


Figure 11. The synthesized triggers generated by Neural Cleanse. Red box in the figure indicates ground-truth trigger areas.

tack contain similar patterns to those used by attackers (*i.e.*, white-square on the bottom right corner), whereas those of our attack are meaningless.

Resistance to STRIP. STRIP [13] filters poisoned samples based on the prediction randomness of samples generated by imposing various image patterns on the suspicious image. The randomness is measured by the entropy of the average prediction of those samples. As such, the higher the entropy, the harder an attack for STRIP to defend. As shown

in Figure 10, our attack is more resistant to the STRIP compared with other attacks.

Resistance to SentiNet. SentiNet [9] identifies trigger regions based on the similarities of Grad-CAM of different samples. As shown in Figure 8, Grad-CAM successfully distinguishes trigger regions of those generated by BadNets and Blended Attack, while it fails to detect trigger regions of those generated by our attack. In other words, our attack is more resistant to SentiNet.

5.3. Discussion

In this section, unless otherwise specified, all settings are the same as those stated in Section 5.1.

Table 2. The ASR (%) of our attack with consistent (dubbed *Ours*) or inconsistent (dubbed *Ours (inconsistent)*) triggers. The inconsistent trigger is generated based on a different testing image.

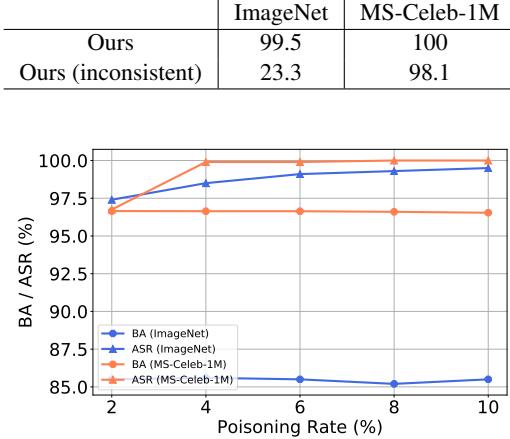


Figure 12. The effect of poisoning rate towards our attack.

The Effect of Poisoning Rate γ . In this part, we discuss the effect of the poisoning rate γ towards ASR and BA in our attack. As shown in Figure 12, our attack reaches a high ASR ($> 95\%$) on both datasets by poisoning only 2% training samples. Besides, the ASR increases with an increase of γ while the BA remains almost unchanged. In other words, there is almost no trade-off between the ASR and BA in our method. However, the increase of γ will also decrease the attack stealthiness. Attackers need to specify this parameter for their specific needs.

The Exclusiveness of Generated Triggers. In this part, we explore whether the generated sample-specific triggers are exclusive, *i.e.*, whether testing image with trigger generated based on another image can also activate the hidden backdoor of DNNs attacked by our method. Specifically, for each testing image x , we randomly select another testing image x' ($x' \neq x$). Now we query the attacked DNNs with $x + T(G(x'))$ (rather than with $x + T(G(x))$). As shown in Table 2, the ASR decreases sharply when inconsistent triggers (*i.e.*, triggers generated based on different images)

Table 3. Out-of-dataset generalization of our method in the attack stage. The experiments demonstrate that an encoder trained on a dataset can also be adapted to generate poisoned samples of different datasets for our attack.

Dataset for Classifier →	ImageNet		MS-Celeb-1M	
Dataset for Encoder ↓	BA	ASR	BA	ASR
ImageNet	85.5	99.5	95.6	99.5
MS-Celeb-1M	85.1	99.4	96.5	100

are adapted on the ImageNet dataset. However, on the MS-Celeb-1M dataset, attack with inconsistent triggers can still achieve a high ASR. This may probably because most of the facial features are similar and therefore the learned trigger has better generalization. We will further explore this interesting phenomenon in our future work.

Table 4. The ASR (%) of our method attacked with out-of-dataset testing samples. The experiments demonstrate that using out-of-dataset samples to generate poisoned samples can still successfully activate the hidden backdoor in DNNs attacked by our method.

Dataset for Training →	ImageNet		MS-Celeb-1M	
Dataset for Inference ↓	BA	ASR	BA	ASR
Microsoft COCO	100	99.9	100	99.9
Random Noise	100	99.9	100	99.9

Out-of-dataset Generalization in the Attack Stage. Recall that the encoder is trained on the benign version of the poisoned training set in previous experiments. In this part, we explore whether the one trained on another dataset can still be adapted for generating poisoned samples of a new dataset (without any fine-tuning) in our attack. As shown in Table 3, the effectiveness of attack with encoder trained on another dataset is on par with that of the one trained on the same dataset. In other words, attackers can reuse already trained encoders to generate poisoned samples, if their image size is the same. *This property will significantly reduce the computational cost of our attack.*

Out-of-dataset Generalization in the Inference Stage. In this part, we verify that whether out-of-dataset images (with triggers) can successfully attack DNNs attacked by our method. We select the Microsoft COCO dataset [28] and a synthetic noise dataset for the experiment. They are representative of nature images and synthetic images, respectively. Specifically, we randomly select 1,000 images from the Microsoft COCO and generate 1,000 synthetic images where each pixel value is uniformly and randomly selected from $\{0, \dots, 255\}$. All selected images are resized to $3 \times 224 \times 224$. As shown in Table 4, our attack with poisoned samples generated based on out-of-dataset images can also achieve nearly 100% ASR. *It indicates that attackers can activate the hidden backdoor in attacked DNNs with arbitrary images (not necessary with testing images).*

6. Conclusion

In this paper, we showed that existing backdoor attacks were easily alleviated by current backdoor defenses mostly because their backdoor trigger is sample-agnostic, *i.e.*, different poisoned samples contain the same trigger. Based on this understanding, we explored a new attack paradigm, the sample-specific backdoor attack (SSBA), where the backdoor trigger is sample-specific. Our attack breaks the fundamental assumption of defenses, therefore can bypass them. Specifically, we generate sample-specific invisible additive noises as backdoor triggers by encoding an attacker-specified string into benign images, motivated by the DNN-based image steganography. The mapping from the string to the target label will be learned when DNNs are trained on the poisoned dataset. Extensive experiments are conducted, which verify the effectiveness of our method in attacking models with or without defenses.

Appendix

Table 5. The BA (%) and ASR (%) of methods with VGG-16. Among all attacks, the best result is denoted in boldface while underline indicates the second-best result.

Dataset →	ImageNet		MS-Celeb-1M	
Attack ↓, Metric →	BA	ASR	BA	ASR
Standard Training	83.9	0	96.9	0.1
BadNets	84.6	100	<u>95.8</u>	100
Blended Attack	<u>84.3</u>	96.9	95.5	<u>99.2</u>
Ours	83.5	<u>98.6</u>	96.3	100

7. More Results of Methods with VGG-16

In the main manuscript, we used ResNet-18 [17] as the model structure for all experiments. To verify that our proposed attack is also effective towards other model structures, we provide additional results of methods with VGG-16 [41] in this section. Unless otherwise specified, all settings are the same as those used in the main manuscript.

7.1. Attack Effectiveness

Follow the settings adopted in the main manuscript, we compare the effectiveness of methods from the aspect of attack success rate (ASR) and benign accuracy (BA).

As shown in Table 5, our attack can also reach a high attack success rate and benign accuracy on both ImageNet and MS-Celeb-1M dataset with VGG-16 as the model structure. Specifically, our attack can achieve an ASR $> 98.5\%$ on both datasets. Moreover, the ASR of our attack is on par with that of BadNets and higher than that of the Blended Attack. These results verify that sample-specific invisible additive noises can also serve as good backdoor triggers even though they are more complicated than the white-square used in BadNets and Blended Attack.

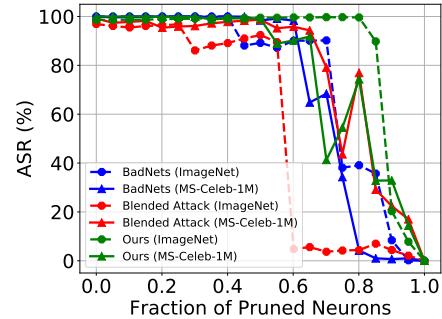


Figure 13. The ASR (%) of different attacks *w.r.t.* the fraction of pruned neurons on the ImageNet and MS-Celeb-1M dataset.

7.2. Resistance to Fine-Pruning

In this part, we also compare our attack with the BadNets and Blended Attack in terms of the resistance to the pruning-based defense [29]. As shown in Figure 13, curves of our attack are always above those of other attacks. In other words, our descent speed is slower although ASRs of all attacks decrease with the increase of the fraction of pruned neurons. For example, on the ImageNet dataset, the ASR of Blended Attack decrease to less than 10% when 60% neurons are pruned, whereas our attack still preserves a high ASR ($> 95\%$). This suggests that our attack is more resistant to the pruning-based defense.

7.3. Resistance to Neural Cleanse

In this part, we also compare our attack with the BadNets and Blended Attack in terms of the resistance to the Neural Cleanse [44]. Recall that there are two indispensable requirements for the success of Neural Cleanse, including (1) successful select one candidate (*i.e.*, the anomaly index is big enough) and (2) the selected candidate is close to the backdoor trigger.

As shown in Figure 15, the anomaly index of our attack is smaller than that of BadNets and Blended Attack on the ImageNet dataset. In other words, our attack is more resistant to the Neural Cleanse in this case. We also visualize the synthesized trigger (*i.e.*, the one with the smallest anomaly index among all candidates) of different attacks. As shown in Figure 16, although our attack reaches the highest anomaly index on the MS-Celeb-1M dataset, synthesized triggers of our attack are meaningless. In contrast, synthesized triggers of BadNets and Blended Attack contain similar patterns to the ones used by attackers. As such, our attack is still more resistant to the Neural Cleanse in this case.

7.4. Resistance to STRIP

STRIP [13] filters poisoned samples based on the prediction randomness of samples generated by imposing various image patterns on the suspicious image. The random-

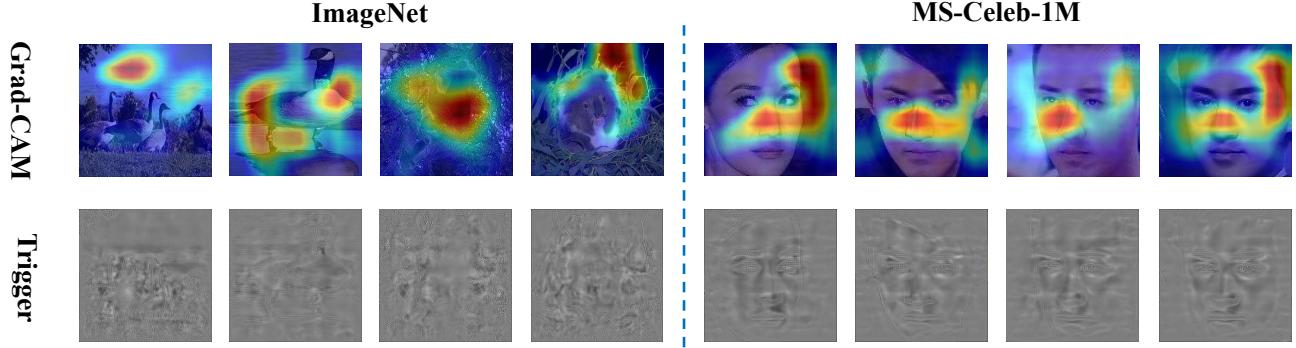
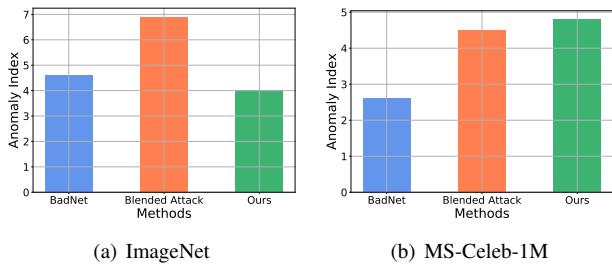


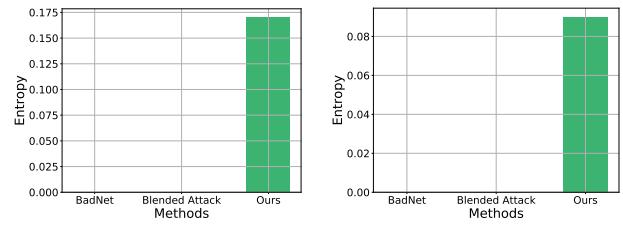
Figure 14. The Grad-CAM of poisoned samples and their corresponding triggers of our attack.



(a) ImageNet

(b) MS-Celeb-1M

Figure 15. The anomaly index of different attacks with VGG-16 on the ImageNet and MS-Celeb-1M dataset. The smaller the index, the harder the attack for Neural-Cleanse to defend.



(a) ImageNet

(b) MS-Celeb-1M

Figure 17. The entropy generated by STRIP of different attacks. The higher the entropy, the harder the attack for STRIP to defend.

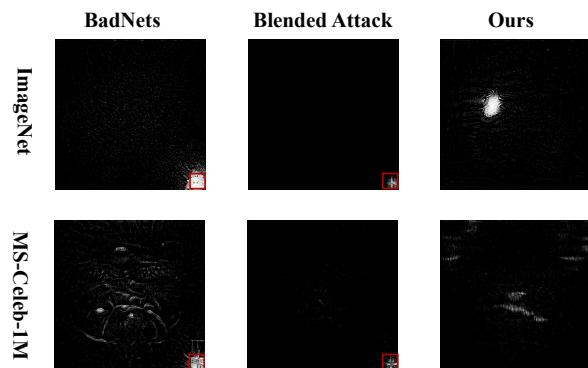


Figure 16. The synthesized triggers generated by Neural Cleanse. Red box in the figure indicates ground-truth trigger areas.

ness is measured by the entropy of the average prediction of those samples. As such, the higher the entropy, the harder an attack for STRIP to defend. As shown in Figure 17, our attack has a significantly higher entropy compared with other baseline methods on both ImageNet and MS-Celeb-1M datasets. In other words, our attack is more resistant to the STRIP compared with other attacks.

7.5. Resistance to SentiNet

SentiNet [9] identifies trigger regions based on the similarities of Grad-CAM of different samples. As shown in Figure 14, Grad-CAM fails to detect trigger regions of images generated by our attack. Besides, the Grad-CAM of different poisoned samples has a significant difference. As such, our attack can bypass the SentiNet.

8. The Connection to Related Areas

Backdoor attack is closely related to *adversarial attack* and *data poisoning*. In this section, we discuss the similarities and differences between our proposed backdoor attack and adversarial attacks, data poisoning, respectively.

8.1. Backdoor Attack and Adversarial Attack

Adversarial attack, especially black-box adversarial attack [21, 12, 6] has certain similarities compared with backdoor attack. Firstly, both of them do not require to know any information about the deployed DNNs in the inference stage. Secondly, they all require modifying the image in the inference stage and the perturbations are all sample-specific², except for universal adversarial attacks

²As we mentioned, we use our proposed backdoor attack for the comparison. Most existing backdoor attacks have a sample-agnostic attack

(e.g., [33, 34, 43]). As such, researchers who are not familiar with the backdoor attack might question its research significance.

Although adversarial attacks and backdoor attacks share certain similarities, they have essential differences [26]. Firstly, the perturbation is known (*i.e.*, non-optimized) by the backdoor attacker whereas the adversarial attacker needs to obtain it through the optimization process based on the output of the model. Such optimization in adversarial attacks requires multiple queries and therefore may probably be detected. Secondly, their mechanism has essential differences. Specifically, backdoor attackers take advantage of the excessive learning ability towards ‘non-robust’ features (such as textures) of DNNs, while the adversarial vulnerability results from the differences in behaviors of DNNs and humans. In conclusion, backdoor attacks study on the security threats in the training process and adversarial attacks focus on the security threats in the inference process. They are equally important and worth further exploration.

8.2. Backdoor Attack and Data Poisoning

Data poisoning [46, 1, 31] and backdoor attacks share certain similarities in the training stage. They all try to maliciously manipulate DNNs by introducing poisoned samples during the training process. However, they still have significant differences.

Firstly, they have different attacker’s goals. Specifically, data poisoning aims at degrading the performance in predicting benign testing samples. In contrast, backdoor attacks preserve the performance on benign testing samples, similar to the benign model, while changing the prediction of poisoned samples to the target label. Data poisoning can be regarded as the ‘non-targeted poisoning-based backdoor attack’ with transparent triggers to some extent. Secondly, backdoor attacks are more stealthy compared to data poisoning. Defenders can detect data poisoning by simply evaluating the model performance on a small local verification set, while this approach has limited benefits in detecting backdoor attacks.

References

- [1] Scott Alfeld, Xiaojin Zhu, and Paul Barford. Data poisoning attacks against autoregressive models. In *AAAI*, 2016. 11
- [2] Eugene Bagdasaryan and Vitaly Shmatikov. Blind backdoors in deep learning models. *arXiv preprint arXiv:2005.03823*, 2020. 11
- [3] Eugene Bagdasaryan, Andreas Veit, Yiqing Hua, Deborah Estrin, and Vitaly Shmatikov. How to backdoor federated learning. In *AISTATS*, 2020. 1, 11
- [4] Shumeet Baluja. Hiding images in plain sight: Deep steganography. In *NeurIPS*, 2017. 2, 5
- [5] Huili Chen, Cheng Fu, Jishen Zhao, and Farinaz Koushanfar. Deepinspect: A black-box trojan detection and mitigation framework for deep neural networks. In *IJCAI*, 2019. 2
- [6] Weilun Chen, Zhaoxiang Zhang, Xiaolin Hu, and Baoyuan Wu. Boosting decision-based black-box adversarial attacks with random sign flip. In *ECCV*, 2020. 10
- [7] Xinyun Chen, Chang Liu, Bo Li, Kimberly Lu, and Dawn Song. Targeted backdoor attacks on deep learning systems using data poisoning. *arXiv preprint arXiv:1712.05526*, 2017. 1, 2, 4, 5
- [8] Hao Cheng, Kaidi Xu, Sijia Liu, Pin-Yu Chen, Pu Zhao, and Xue Lin. Defending against backdoor attack on deep neural networks. In *KDD Workshop*, 2020. 2
- [9] Edward Chou, Florian Tramer, and Giancarlo Pellegrino. Sentinel: Detecting localized universal attack against deep learning systems. In *IEEE S&P Workshop*, 2020. 2, 5, 8, 10
- [10] Jiazhui Dai, Chuanshuai Chen, and Yufeng Li. A backdoor attack against lstm-based text classification systems. *IEEE Access*, 7:138872–138878, 2019. 1
- [11] Jia Deng, Wei Dong, Richard Socher, Li-Jia Li, Kai Li, and Li Fei-Fei. Imagenet: A large-scale hierarchical image database. In *CVPR*, 2009. 3, 5
- [12] Yinpeng Dong, Hang Su, Baoyuan Wu, Zhifeng Li, Wei Liu, Tong Zhang, and Jun Zhu. Efficient decision-based black-box adversarial attacks on face recognition. In *CVPR*, 2019. 10
- [13] Yansong Gao, Change Xu, Derui Wang, Shiping Chen, Damith C Ranasinghe, and Surya Nepal. Strip: A defence against trojan attacks on deep neural networks. In *ACSAC*, 2019. 2, 3, 5, 7, 9
- [14] Tianyu Gu, Kang Liu, Brendan Dolan-Gavitt, and Siddharth Garg. Badnets: Evaluating backdooring attacks on deep neural networks. *IEEE Access*, 7:47230–47244, 2019. 1, 2, 3, 5, 11
- [15] Wenbo Guo, Lun Wang, Yan Xu, Xinyu Xing, Min Du, and Dawn Song. Towards inspecting and eliminating trojan backdoors in deep neural networks. In *ICDM*, 2020. 2
- [16] Yandong Guo, Lei Zhang, Yuxiao Hu, Xiaodong He, and Jianfeng Gao. Ms-celeb-1m: A dataset and benchmark for large-scale face recognition. In *ECCV*, 2016. 5
- [17] Kaiming He, Xiangyu Zhang, Shaoqing Ren, and Jian Sun. Deep residual learning for image recognition. In *CVPR*, 2016. 3, 5, 9
- [18] Robert V Hogg, Joseph McKean, and Allen T Craig. *Introduction to mathematical statistics*. Pearson Education, 2005. 6
- [19] Xijie Huang, Moustafa Alzantot, and Mani Srivastava. Neuroninspect: Detecting backdoors in neural networks via output explanations. *arXiv preprint arXiv:1911.07399*, 2019. 3
- [20] Quan Huynh-Thu and Mohammed Ghanbari. Scope of validity of psnr in image/video quality assessment. *Electronics letters*, 44(13):800–801, 2008. 6
- [21] Andrew Ilyas, Logan Engstrom, Anish Athalye, and Jessy Lin. Black-box adversarial attacks with limited queries and information. In *International Conference on Machine Learning*, 2018. 10

paradigm [14, 27, 3], while the backdoor trigger could be semantic [3, 2] in which the attacker does not need to modify the testing image.

- [22] Max Jaderberg, Karen Simonyan, Andrew Zisserman, et al. Spatial transformer networks. In *NeurIPS*, 2015. 5
- [23] Diederik P Kingma and Jimmy Ba. Adam: A method for stochastic optimization. In *ICLR*, 2015. 5
- [24] Diederik P Kingma and Max Welling. Auto-encoding variational bayes. In *ICLR*, 2014. 5
- [25] Ang Li, Shanshan Zhao, Xingjun Ma, Mingming Gong, Jianzhong Qi, Rui Zhang, Dacheng Tao, and Ramamohanarao Kotagiri. Short-term and long-term context aggregation network for video inpainting. In *ECCV*, 2020. 1
- [26] Yiming Li, Baoyuan Wu, Yong Jiang, Zhifeng Li, and Shutao Xia. Backdoor learning: A survey. *arXiv preprint arXiv:2007.08745*, 2020. 1, 11
- [27] Yiming Li, Tongqing Zhai, Baoyuan Wu, Yong Jiang, Zhifeng Li, and Shutao Xia. Rethinking the trigger of backdoor attack. *arXiv preprint arXiv:2004.04692*, 2020. 11
- [28] Tsung-Yi Lin, Michael Maire, Serge Belongie, James Hays, Pietro Perona, Deva Ramanan, Piotr Dollár, and C Lawrence Zitnick. Microsoft coco: Common objects in context. In *ECCV*, 2014. 8
- [29] Kang Liu, Brendan Dolan-Gavitt, and Siddharth Garg. Fine-pruning: Defending against backdooring attacks on deep neural networks. In *RAID*, 2018. 2, 3, 5, 7, 9
- [30] Li Liu, Gang Feng, Denis Beaurempas, and Xiao-Ping Zhang. Re-synchronization using the hand preceding model for multi-modal fusion in automatic continuous cued speech recognition. *IEEE Transactions on Multimedia*, 2020. 1
- [31] Xuanqing Liu, Si Si, Jerry Zhu, Yang Li, and Cho-Jui Hsieh. A unified framework for data poisoning attack to graph-based semi-supervised learning. In *NeurIPS*, 2019. 11
- [32] Yuntao Liu, Ankit Mondal, Abhishek Chakraborty, Michael Zuzak, Nina Jacobsen, Daniel Xing, and Ankur Srivastava. A survey on neural trojans. In *ISQED*, 2020. 1
- [33] Seyed-Mohsen Moosavi-Dezfooli, Alhussein Fawzi, Omar Fawzi, and Pascal Frossard. Universal adversarial perturbations. In *CVPR*, 2017. 11
- [34] Konda Reddy Mopuri, Aditya Ganeshan, and R Venkatesh Babu. Generalizable data-free objective for crafting universal adversarial perturbations. *IEEE transactions on pattern analysis and machine intelligence*, 41(10):2452–2465, 2018. 11
- [35] Ximing Qiao, Yukun Yang, and Hai Li. Defending neural backdoors via generative distribution modeling. In *NeurIPS*, 2019. 2
- [36] Erwin Quiring and Konrad Rieck. Backdooring and poisoning neural networks with image-scaling attacks. In *IEEE S&P Workshop*, 2020. 2
- [37] Olaf Ronneberger, Philipp Fischer, and Thomas Brox. U-net: Convolutional networks for biomedical image segmentation. In *MICCAI*, 2015. 5
- [38] D.E. Rumelhart, G.E. Hinton, and R.J. Williams. Learning internal representations by error propagation. *Nature*, 323(2):318–362, 1986. 5
- [39] Aniruddha Saha, Akshayvarun Subramanya, and Hamed Pirsiavash. Hidden trigger backdoor attacks. In *AAAI*, 2020. 1, 2
- [40] Ramprasaath R Selvaraju, Michael Cogswell, Abhishek Das, Ramakrishna Vedantam, Devi Parikh, and Dhruv Batra. Grad-cam: Visual explanations from deep networks via gradient-based localization. In *ICCV*, 2017. 3, 6
- [41] Karen Simonyan and Andrew Zisserman. Very deep convolutional networks for large-scale image recognition. In *ICLR*, 2015. 9
- [42] Matthew Tancik, Ben Mildenhall, and Ren Ng. Stegastamp: Invisible hyperlinks in physical photographs. In *CVPR*, 2020. 2, 5
- [43] Simen Thys, Wiebe Van Ranst, and Toon Goedemé. Fooling automated surveillance cameras: adversarial patches to attack person detection. In *CVPR Workshop*, 2019. 11
- [44] Bolun Wang, Yuanshun Yao, Shawn Shan, Huiying Li, Bimal Viswanath, Haitao Zheng, and Ben Y Zhao. Neural cleanse: Identifying and mitigating backdoor attacks in neural networks. In *IEEE S&P*, 2019. 2, 3, 5, 7, 9
- [45] Shuo Wang, Surya Nepal, Carsten Rudolph, Marthie Grobler, Shangyu Chen, and Tianle Chen. Backdoor attacks against transfer learning with pre-trained deep learning models. *IEEE Transactions on Services Computing*, 2020. 1
- [46] Huang Xiao, Battista Biggio, Gavin Brown, Giorgio Fumera, Claudia Eckert, and Fabio Roli. Is feature selection secure against training data poisoning? In *ICML*, 2015. 11
- [47] Richard Zhang, Phillip Isola, Alexei A Efros, Eli Shechtman, and Oliver Wang. The unreasonable effectiveness of deep features as a perceptual metric. In *CVPR*, 2018. 5
- [48] Tong Zhang. Solving large scale linear prediction problems using stochastic gradient descent algorithms. In *ICML*, 2004. 5
- [49] Yuyang Zhang, Shubiao Xu, Baoyuan Wu, Jian Shi, Weiliang Meng, and Xiaopeng Zhang. Unsupervised multi-view constrained convolutional network for accurate depth estimation. *IEEE Transactions on Image Processing*, 29:7019–7031, 2020. 1
- [50] Shihao Zhao, Xingjun Ma, Xiang Zheng, James Bailey, Jingjing Chen, and Yu-Gang Jiang. Clean-label backdoor attacks on video recognition models. In *CVPR*, 2020. 2
- [51] Haotu Zhong, Cong Liao, Anna Cinzia Squicciarini, Sencun Zhu, and David Miller. Backdoor embedding in convolutional neural network models via invisible perturbation. In *ACM CODASPY*, 2020. 1
- [52] Jiren Zhu, Russell Kaplan, Justin Johnson, and Li Fei-Fei. Hidden: Hiding data with deep networks. In *ECCV*, 2018. 2, 5
- [53] Liwan Zhu, Rui Ning, Cong Wang, Chunsheng Xin, and Hongyi Wu. Gangsweep: Sweep out neural backdoors by gan. In *ACM MM*, 2020. 2