

Imperceptible but Forgeable: Practical Invisible Watermark Forgery via Diffusion Models

Ziping Dong¹ Chao Shuai¹ Zhongjie Ba¹ Peng Cheng¹ Zhan Qin¹ Qinglong Wang¹ Kui Ren¹

¹ The State Key Laboratory of Blockchain and Data Security, Zhejiang University, Hangzhou, China

Abstract

Invisible watermarking is critical for content provenance and accountability in Generative AI. Although commercial companies have increasingly committed to using watermarks, the robustness of existing watermarking schemes against forgery attacks is understudied. This paper proposes **DiffForge**, the first watermark forgery framework capable of forging imperceptible watermarks under a no-box setting. We estimate the watermark distribution using an unconditional diffusion model and introduce shallow inversion to inject the watermark into a non-watermarked image seamlessly. This approach facilitates watermark injection while preserving image quality by adaptively selecting the depth of inversion steps, leveraging our key insight that watermarks degrade with added noise during the early diffusion phases. Comprehensive evaluations show that DiffForge deceives open-source watermark detectors with a 96.38% success rate and misleads a commercial watermark system with over 97% success rate, achieving high confidence.¹ This work reveals fundamental security limitations in current watermarking paradigms. The experimental results and code are available at <https://anonymous.4open.science/r/PIFW-F6EA>.

1. Introduction

As generative models like DALL-E 3 (OpenAI, 2024), Stable Diffusion (Rombach et al., 2022), and Imagen 3 (Deepmind, 2024b) enable the creation of high-quality images from text prompts, they also raise concerns about the potential misuse of such technologies for generating misleading or fictitious imagery (Kayleen Devlin, 2024). To address these risks, watermarking techniques have become a key solution for embedding traceable information into generated

¹We have reported this to Amazon Artificial General Intelligence(AGI)'s Responsible AI team and discussed potential defense strategies. For more details, please refer to the Impact Statement.

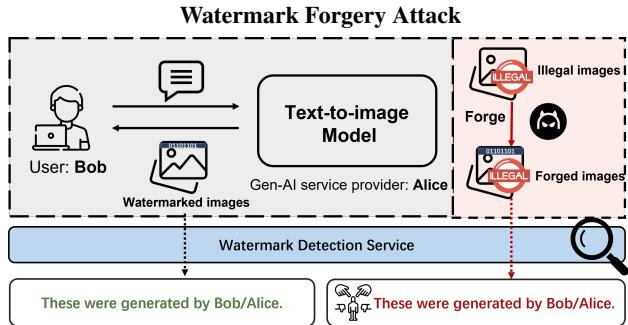


Figure 1. Bob utilizes the Gen-AI service provided by Alice, where Alice embeds watermark information into the images returned to Bob. This embedded watermark allows the image to be identified as having been generated either by Bob or Alice through a watermark detection service. By forging the watermark onto illegal or malicious content, the attacker can cause the image to be misidentified as having been generated by Bob or Alice, thereby damaging the reputation of legitimate users or service providers.

content, ensuring its authenticity and provenance (Jiang et al., 2024).

However, existing watermark systems are vulnerable to diverse adversarial attacks, including detection evasion (Jiang et al., 2023) and forgery. Forgery attacks (also known as spoofing attacks), where non-watermarked content is falsely detected as watermarked, have raised concerns. Such attacks can wrongly attribute maliciously watermarked content to innocent parties, such as Generative AI (Gen-AI) service providers, damaging the reputation of providers or legitimate users and undermining the credibility of watermarking systems, as shown in Fig. 1.

Research focus has been shifting to black-box and no-box scenarios as forgery attacks can be easily executed when the attacker has white-box access to the target watermarking scheme (Zhao et al., 2024). Recent work (Wang et al., 2021; Li et al., 2023) frames watermark forgery as an image translation task in a *black-box* setting, where the attacker can query the watermarking scheme to obtain paired datasets of watermarked and non-watermarked images. This allows the model to learn the transformation from non-watermarked to watermarked images. However, in practice, this scenario

is unrealistic, as attackers typically cannot query the watermarking algorithm to obtain paired data. To launch a *no-box* attack, Yang et al. (2024a) proposed a method for watermark pattern estimation, where only watermarked images are available. Their approach calculates the mean residual between watermarked and non-watermarked images and directly adds the estimated pattern at the pixel level. However, this method suffers from high estimation errors, leading to poor performance. Generally speaking, existing methods have significant limitations, primarily in terms of impractical assumption and they underperform in both forgery accuracy and image quality preservation. We argue that: 1) They fail to effectively estimate watermark information; 2) Embedding a watermark into clean images while preserving the image quality is particularly challenging without access to paired data and watermarking schemes (e.g., watermark detectors).

To tackle these challenges, we explore the use of diffusion models to estimate the watermark information in images, inspired by (Yu et al., 2021a; Zhao et al., 2023). Leveraging the power of diffusion models for modeling complex distributions, we train a diffusion model on watermarked images to accurately estimate and model their distribution. This allows us to generate watermarked images directly from random Gaussian noise. For watermark injection, we propose a novel approach that combines DDIM inversion with adaptive step selection during the forgery process. Specifically, shallow inversion involves inverting a non-watermarked image (i.e., the target clean image) into a shallow latent variable, minimizing the accumulation of errors in the DDIM inversion process to preserve most of the image content while leaving room for watermark injection in the denoising process. To further optimize watermark injection within the given image quality constraints, we propose *adaptive step selection* to dynamically adjust the inversion depth.

Building on these ideas, we propose **DiffForge**, a watermark forgery attack framework designed for practical attack scenarios. In this setting, the attacker has no prior knowledge of the Gen-AI service provider’s watermarking scheme and can only access watermarked content. We conduct extensive experiments on various watermark schemes, including real-world ones, to show the effectiveness of our method. Experimental results demonstrate that our attack achieves high success rates across multiple watermarking schemes while maintaining image quality. Notably, we apply our attack to a commercial watermark system, which is deployed in Amazon’s text-to-image model Titan (Amazon, 2024). The results show that our forged images are successfully recognized as Titan’s generated images, indicating our attack’s efficacy in real-world applications. Furthermore, we observe that our approach outperforms existing methods in the context of heterogeneous data, where the images used for extracting a watermark from and injecting a wa-

termark into come from different domains (e.g., different datasets or styles). This setting closely mimics real-world forgery attacks, a scenario overlooked by existing methods. Additionally, we investigate the robustness of the forged watermarks compared to genuine ones, providing valuable insights for potential defense strategies.

To summarize, our key contributions are as follows:

- We present **DiffForge** that leverages the capability of diffusion models, allowing watermark forgery without the need for prior knowledge of the watermarking scheme or paired data, offering a new perspective for considering the security of watermarking systems.
- We propose **shallow inversion**, a novel method that maximizes watermark embedding in non-watermarked images while preserving their visual integrity.
- We are the first to apply our watermark forgery attack in a commercial watermark system. All forged images successfully spoofed Amazon’s watermark detection API, confidently classified as watermarked. Compared to existing methods, our approach **improved the performance by 68%** while maintaining a **PSNR (Peak Signal-to-Noise Ratio) over 29.06dB**. This underscores the effectiveness and practicality of our attack in real-world applications.

2. Background

2.1. Image Watermarking

The invisible image watermarking process typically involves three stages: embedding, extraction, and verification. Given a host image x and a message m (typically a bit string), the embedding stage generates a watermarked image $x_w = E(x, m)$ using encoder E . During the extraction stage, the detector D extracts the watermark information from x_w , resulting in $m' = D(x_w)$. In the verification stage, the initially embedded watermark m is compared with the extracted watermark m' using a verification function V . This process is defined as $V(m, m', \rho)$, where ρ represents a threshold value. If the bit accuracy between m and m' exceeds ρ , the watermark verification is considered successful; otherwise, it fails. The value of ρ (e.g., the detection threshold) is determined based on the target false positive rate of the watermarking scheme. For instance, to achieve a false positive rate (FPR) below 0.05 for a 40-bit message, ρ should be set to 26, based on a Bernoulli distribution assumption (Lukas & Kerschbaum, 2023).

Image watermarking can be categorized into **Post-processing watermarking** and **In-processing watermarking**, depending on the stage at which the watermark is embedded. Both watermarking methods can be applied to

AI-generated content, and our forgery attack demonstrates the capability to effectively forge watermarks in both categories.

Post-processing Methods. These methods embed watermark messages into images post-generation. Non-neural network-based methods, such as embedding messages in the least significant bit of pixel values (Chopra et al., 2012) or using combinations of DWT and DCT (Al-Haj, 2007), often suffer from limited robustness to attacks like compression and noise, limiting their practical use. Neural network-based approaches have enhanced these methods by improving both robustness and visual quality, often utilizing encoder-decoder architectures (Tancik et al., 2020; Zhang et al., 2019; Zhu et al., 2018). Moreover, techniques such as adversarial training (Zhu et al., 2018) and invertible neural networks (Fang et al., 2023) have been employed to further improve the robustness and visual quality of watermarked images.

In-processing Methods. These methods involve embedding the message directly during the image generation process. Some approaches embed watermarks into training data or model weights (Yu et al., 2021a;b; Lukas & Kerschbaum, 2023). Others fine-tune specific components to embed the watermark message, such as fine-tuning the decoder of latent diffusion (Fernandez et al., 2023). In addition, semantic watermarking is a new technique that links the watermark with image semantics. Tree-Ring (Wen et al., 2023) embeds a ring pattern into the low-frequency components of Gaussian noise in the Fourier domain. Gaussian shading (Yang et al., 2024b) preserves the original distribution when sampling the initial noise and achieves watermark embedding with lossless performance. Semantic watermarking is still in its nascent stages and has not yet been deployed in practical applications. Therefore, we do not focus on semantic watermarking in this paper.

Real-World Deployment In line with commitments made to the White House, leading AI companies in the United States, providing generative AI services, are implementing watermarking systems to embed watermark information in content generated by their models before delivering it to users (Diane Bartz, 2024). OpenAI points out that invisible watermarking techniques are superior to the visible genre and metadata methods previously used in DALL-E 2 and DALL-E 3 (David, 2024), due to their imperceptibility and robust resistance to common image manipulations, such as screenshots, compression, and cropping. Google introduced Synthid (Deepmind, 2024c), which adds invisible watermarks to both Imagen 3 and Imagen 2 (Deepmind, 2024a). Amazon has deployed invisible watermarks on its Titan image generator (Amazon, 2024), and Microsoft has announced plans to incorporate invisible watermarks into AI-generated images in Bing (Mehdi, 2024).

2.2. AI-Generated Content Attribution.

AI-Generated Content Attribution based on invisible watermarks can be divided into two categories: **Model-Accountability** and **User-Accountability**.

Model-Accountability. In this category, the watermark message m embedded in the generated content is fixed and unrelated to the user. This watermark, embedded by the Gen-AI service provider, typically serves as a model identifier. For example, Stability AI uses the identifier 'StableDiffusionV1', which is converted into a bit string as the watermark message (StabilityAI, 2024). Similarly, Meta AI has proposed a method for identifying Stable Diffusion models by embedding unique watermarks during the generation process (MetaAI, 2023).

User-Accountability. refers to a more granular form of attribution, where, upon registration for a Gen-AI service, each user is assigned a unique watermark message m that gets stored in the database. Whenever the user generates content using the service, their specific watermark is embedded into the generated content (Jiang et al., 2024).

The main distinction between the two is the meaning of the embedded message. However, our framework focuses on forging the watermark message m , making our attack applicable to both types of attribution.

3. Threat Model

Watermark Forgery. A watermark forgery attack involves extracting the watermark from watermarked images and embedding it into non-watermarked images (e.g., harmful content). This manipulation disrupts the watermark detection process and can potentially harm the reputation of legitimate users or the Gen-AI service provider.

Attacker’s Objectives. The attacker aims to achieve two objectives: (1) a high watermark detection rate (bit accuracy) to ensure successful forgery and (2) a high visual quality of the forged image to make the forgery stealthy. These objectives ensure that the forged images are both effective in deceiving the detection system and visually indistinguishable from the genuine content.

Attacker’s Capability. In a no-box setting, the attacker can collect a certain percentage of the victim’s watermarked images from AI generation platforms, such as PromptHero (Pro, 2024b) and PromptBase (Pro, 2024a), as well as from social media, which can serve as an auxiliary data source. The attacker does not know the underlying watermarking scheme and the embedded message m , nor can they perform watermark embedding and decoding operations. Additionally, we conventionally assume that the Gen-AI service provider is unlikely to change their watermarking algorithm in the short term.

4. Watermark Forgery Attack

In this section, we present our watermark forgery attack framework, as illustrated in Fig. 2, which consists of two stages: (1) Watermark Estimation and (2) Shallow Inversion.

4.1. Watermark Estimation.

In the first stage, we collect a watermarked dataset \mathcal{D}_{aux} from the victim, with each sample containing the watermark message m . Unlike traditional approaches that treat watermark forgery as an image translation task and rely on the acquisition of paired dataset, we train a diffusion model to learn watermark information directly from the watermarked dataset \mathcal{D}_{aux} .

Diffusion models generate data by progressively adding noise in the forward process and then learning to recover the data from noise in the reverse process. Specifically, let x_0 represent the data from \mathcal{D}_{aux} , and let x_t denote the data at step t during the forward diffusion process. The forward diffusion process is modeled as a Markov chain, where at each step, Gaussian noise is added to the data. The conditional distribution of x_t given x_0 at each time step is described as:

$$q(x_t|x_0) = \mathcal{N}(x_t; \sqrt{\alpha_t}x_0, (1 - \alpha_t)\mathbb{I}) \quad (1)$$

where α_t is a schedule controlling the noise scale at each time step, and \mathbb{I} denotes the identity matrix. The reverse process is modeled by a neural network $\epsilon_\theta(x_t, t)$ predicting the noise added to x_0 , and the reverse process can be described as:

$$p_\theta(x_{t-1}|x_t) = \mathcal{N}(x_{t-1}; \mu_\theta(x_t, t), \Sigma_\theta(x_t, t)) \quad (2)$$

where $\mu_\theta(x_t, t)$ and $\Sigma_\theta(x_t, t)$ are the mean and covariance predicted by the neural network. We found that diffusion models can learn the embedded watermark information from a small number of samples without requiring explicit supervision or prior knowledge. After optimizing the diffusion model's original objective function (Ho et al., 2020):

$$\mathcal{L}_{\text{simple}} = \mathbb{E}_{t, \mathbf{x}_0, \epsilon} [\|\epsilon - \epsilon_\theta(\mathbf{x}_t, t)\|^2] \quad (3)$$

the attacker obtains a trained diffusion model \mathcal{M} , capable of generating spoofing images with the victim's watermark message m .

4.2. Shallow Inversion

After the first stage, we obtain a pre-trained diffusion model \mathcal{M} capable of generating watermarked images with a specific message m by denoising from a random Gaussian noise. However, a critical challenge arises: how to transform a non-watermarked image into a watermarked one while preserving its visual quality. To address this, we propose shallow inversion, an approach that combines DDIM

The watermark forgery attack framework

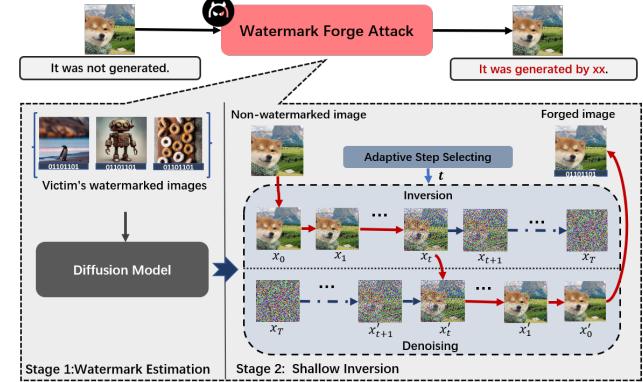


Figure 2. Our proposed watermark forgery attack consists of two stages, in the first stage a diffusion model is used to estimate the victim's watermark information, and in the second stage, the estimated watermark is added to the non-watermarked image via the shallow inversion and denoising. The red arrow indicates shallow inversion, and the blue dotted line represents the original DDIM inversion and denoising.

inversion (Dhariwal & Nichol, 2021; Nichol & Dhariwal, 2021) and *adaptive step selection*, achieving a practical balance between watermark information injection and image quality preservation.

In contrast to generating an image from Gaussian noise, DDIM Inversion reverses the process by using the learned model $\epsilon_\theta(x_t, t)$ to iteratively derive the noise x_T from a given image, following the equation::

$$x_{t+1} = \sqrt{\alpha_{t+1}}\hat{x}_0^t + \sqrt{1 - \alpha_{t+1}}\epsilon_\theta(x_t, t+1), \quad (4)$$

for $t \in \{0, 1, 2, \dots, T-1\}$.

Specifically, DDIM Inversion approximates the difference between consecutive steps in the sampling process. $x_{t-1} - x_t$, is approximately equal to the difference between the previous steps, $x_t - x_{t+1}$. This approximation allows for the replacement of the noise term $\epsilon_\theta(x_{t+1}, t+1)$ with $\epsilon_\theta(x_t, t+1)$, enabling the reversal of the sampling process. However, DDIM inversion of real images is unstable because each step relies on the local linearization approximation, leading to error accumulation and the loss of content from the original image (Lin et al., 2024; Zhang et al., 2024). We assume the error between $\epsilon_\theta(x_t, t+1)$ and $\epsilon_\theta(x_{t+1}, t+1)$ is Δ_t , we can then describe the error accumulation in the DDIM inversion for the estimate of the latent variable x_t as:

$$\delta_t = \sum_{u=0}^{t-1} C(u, t) \cdot \sqrt{1 - \alpha_u} \cdot \Delta_u, \quad (5)$$

$$\text{where } C(u, t) = \frac{\sqrt{\alpha_t} (\sqrt{\alpha_u} - \sqrt{\alpha_{u+1}})}{\sqrt{\alpha_u} \cdot \sqrt{\alpha_{u+1}}}.$$

It is evident that as the number of inversion iteration steps t increases, the error δ_t accumulates, leading to poor image

reconstruction quality. Our ablation studies further demonstrate this phenomenon (Sec. 5.3). The details of Eq. 5 are provided in App. B.

At this stage, we aim to find the latent variable of a non-watermarked image that maintains its fidelity and is suitable as the starting point for watermark injection. The issue of error accumulation suggests that too many inversion steps could lead to large reconstruction errors, which are detrimental to our goal. We further investigate the watermark reconstruction process.

During the training of the diffusion model \mathcal{M} , a watermarked image $x_{wm} \in \mathcal{D}_{aux}$ is progressively degraded by the addition of Gaussian noise. Crucially, the watermark information is destroyed in the earlier phases of the diffusion process, which we refer to as the *watermark degradation phase* (as illustrated in Fig. 3). Conversely, during the denoising process, the watermark is restored in the later stages. This observation suggests that performing the full T inversion steps of DDIM is unnecessary for watermark injection.

Therefore, we propose adaptive step selection, which is designed to balance watermark injection performance with image quality preservation. Since the watermark degradation phase may vary depending on the watermarking scheme, the attacker, without prior knowledge of the watermark, can select the appropriate step t based on a metric that evaluates forged image quality, e.g. Peak Signal-to-Noise Ratio (PSNR). Specifically, the attacker can search the largest t such that the metric exceeds a predefined lower bound κ . This ensures that the image quality remains high while allowing for deeper inversion, which facilitates greater watermark injection.

After the inversion step t is selected, the attacker applies an inversion process $I(x_0, t)$ to the non-watermarked image x_0 . This generates an intermediate latent variable x'_t that contains less noise and better preserves the original image content. The subsequent denoising process then reconstructs the image while simultaneously embedding the estimated watermark information.

The following equation in DDIM (Ho et al., 2020) defines the deterministic denoising process:

$$x'_{t-1} = \sqrt{\alpha_{t-1}} \hat{x}_0^t + \sqrt{1 - \alpha_{t-1}} \epsilon_\theta(x'_t, t) \quad (6)$$

$$\text{where } \hat{x}_0^t = \frac{x'_t - \sqrt{1 - \alpha_t} \epsilon_\theta(x'_t, t)}{\sqrt{\alpha_t}}$$

By iterating this equation, we obtain the forged image x'_0 . The pseudocode for shallow inversion is presented in Alg. A.

5. Experiments

In this section, we evaluate our proposed DiffForge framework for attacking both open-source watermarking schemes

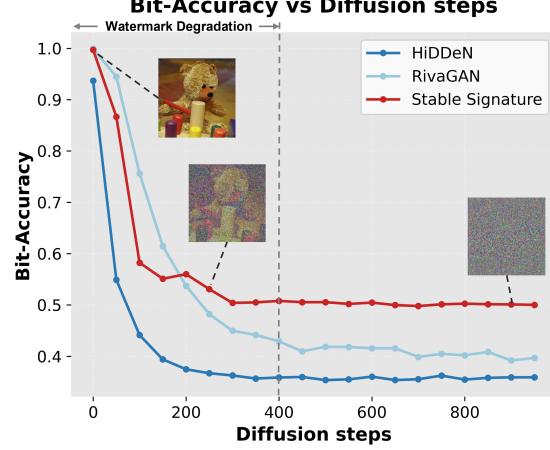


Figure 3. The watermark is degraded early in the diffusion process, with the watermark detection approaching the random, while the image content remains largely intact. The vertical axis represents the bit accuracy of the watermark for three watermarking schemes during the diffusion process.

and a commercial watermarking system. The experimental setup and results are as follows.

Datasets. To better align with the real-world scenario of watermark forgery attacks, where the target images (non-watermarked) for watermark injection follow a different distribution than the watermarked images (such as natural images and AI-generated images), we use a subset of DiffusionDB (Wang et al., 2022) as the victim’s dataset, which contains large-scale and diverse content generated by Stable diffusion (Rombach et al., 2022). For non-watermarked images, we used subsets of real-world datasets, including MS-COCO (Lin et al., 2014), ImageNet (Russakovsky et al., 2015), and Celeba-HQ (Huang et al., 2018), which are widely used in computer vision tasks. For each dataset, we randomly selected 1,000 images from its original validation set.

Watermarking Schemes. We targeted two post-processing watermarking schemes, HiDDeN (Zhu et al., 2018) and RivaGAN (Zhang et al., 2019), as well as an in-processing watermarking scheme, Stable Signature (Fernandez et al., 2023), and a real deployment watermark system, Amazon (Amazon, 2024). HiDDeN and RivaGAN can be adapted for two types of attribution by defining the meaning of the watermark message, while Stable Signature and Amazon are both part of the model accountability category, as mentioned in Sec. 2.2. Each scheme operates at fixed image resolutions: HiDDeN at 128×128 , RivaGAN at 256×256 , and both Stable Signature and Amazon at 512×512 .

Metrics. We evaluate the attack from two aspects. First, the visual quality of the forged images is assessed using the PSNR, where a higher PSNR indicates a better quality

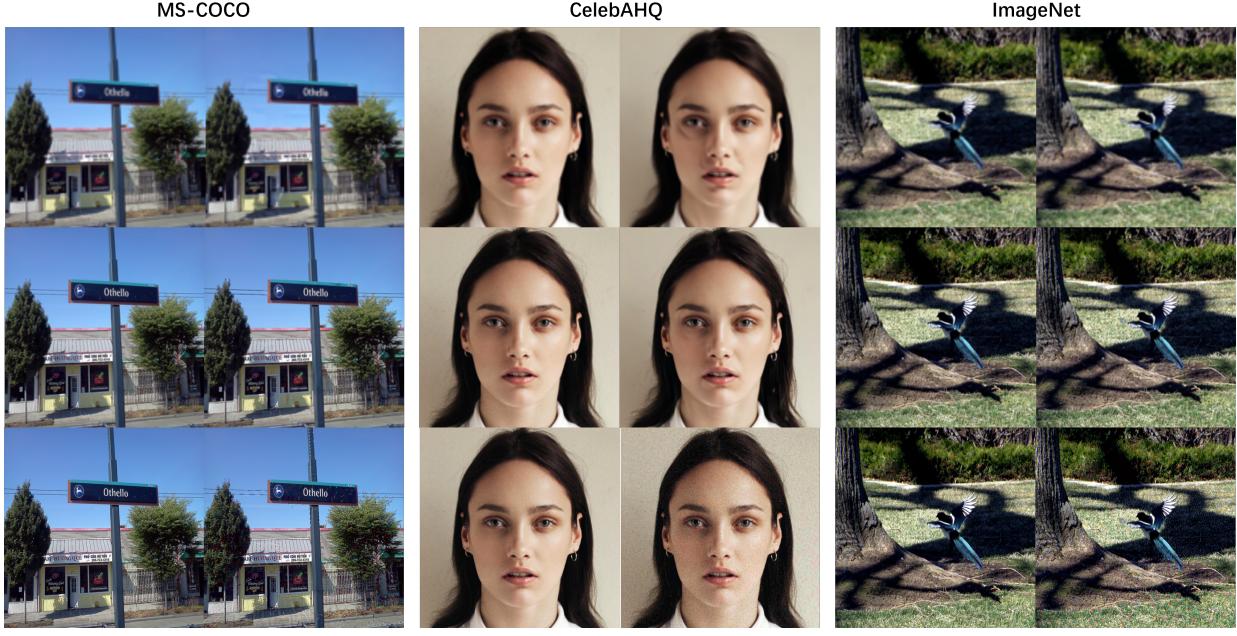


Figure 4. Comparison of forged watermark images and non-watermarked images for three different watermarking schemes: HiDDeN (first row), RivaGAN (second row), and Stable Signature (third row). The images on the left are non-watermarked, and the images on the right are the forged watermark images. The results are shown on three datasets: MS-COCO, CelebA-HQ, and ImageNet.

of the forged watermarked image. Second, we measure the attack’s effectiveness using the forged bit accuracy and false positive rate (FPR). Forged bit accuracy indicates the similarity between the watermark message extracted from the forged images and the victim’s genuine watermark message, while FPR represents the proportion of forged images incorrectly identified as watermarked during verification.

Attack parameters and Baseline. We use the accelerated sampling method of DDIM with $T = 100$ for inversion and denoising. The lower bound κ is set to PSNR = 28 unless otherwise specified. In addition, to provide a comparison with existing methods, we include (Yang et al., 2024a), which shares the same attacker’s capabilities with ours. and (Wang et al., 2021), which requires paired watermarked and non-watermarked images.

5.1. Watermark Forgery Attack

Attacks on open-source watermarking schemes. We compare the results of our method with those of the baseline methods. The attacker in (Yang et al., 2024a) has access to 10,000 watermarked images from the victim, while (Wang et al., 2021) has 20,000 images (10,000 watermarked images and their corresponding non-watermarked versions). The experimental results using a smaller number of watermarked images are provided in App. C.1.

As shown in Tab. 1, our method achieves competitive forged bit accuracy in most scenarios, even surpassing the paired-data-dependent approach. For RivaGAN, we achieve

98.90% bit accuracy on MS-COCO, surpassing (Yang et al., 2024a) by 48.14% and exceeding (Wang et al., 2021) (88.76%). Meanwhile, our FPR achieves 100.00% for Stable Signature compared to 93.60% of (Wang et al., 2021), whereas (Yang et al., 2024a) is close to 1%. In terms of PSNR, our method ensures all PSNR values remain above 28dB, preserving image quality. The image quality of forged examples are shown in Fig. 4.

Attacks on real-world watermarking system. We selected the Amazon watermark scheme² to further evaluate the effectiveness of our attack in real-world scenarios. The scheme detect whether an image is generated by the Titan model and provides a confidence level. We forged 300 images (100 images per dataset) and uploaded them to the API for verification. We define the Success Rate (SR) as the percentage of forged images that were incorrectly identified as generated by the Titan model. Additionally, we calculated the average confidence levels returned by the API for the forged images.

Tab. 2 reports the performance of our method and (Yang et al., 2024a) in attacking the Amazon watermark scheme. Our method consistently outperforms (Yang et al., 2024a) in both visual quality and attack success rate. Specifically, our method achieves an average PSNR above 30dB and an SR close to 100%, while (Yang et al., 2024a) shows significantly lower PSNR (below 25dB) and SR (ranging from

²Both the Titan model API and the watermark detection service API can be accessed via Amazon Bedrock (Amazon, 2025a).

Watermark Scheme	Dataset	(Wang et al., 2021) (Paired Data)			(Yang et al., 2024a)			Ours		
		PSNR↑	Forged bit accuracy↑	FPR@0.05↑	PSNR↑	Forged bit accuracy↑	FPR@0.05↑	PSNR↑	Forged bit accuracy↑	FPR@0.05↑
HiddeN (128×128)	MS-COCO	30.74	97.16%	99.90%	30.74	62.72%	10.50%	31.31	89.64%	96.90%
	CelebA-HQ	31.51	97.70%	100.00%	30.82	61.74%	5.20%	30.64	84.84%	97.70%
	ImageNet	30.68	95.74%	99.90%	30.71	62.36%	8.70%	32.12	85.07%	90.60%
RivaGAN (256×256)	MS-COCO	31.23	88.76%	100.00%	28.34	50.76%	0.80%	28.44	98.90%	100.00%
	CelebA-HQ	31.45	87.22%	98.80%	28.45	51.80%	1.00%	29.41	93.51%	96.50%
	ImageNet	31.42	84.59%	98.80%	28.32	50.87%	1.30%	30.63	88.09%	89.90%
Stable Signature (512×512)	MS-COCO	28.38	91.79%	97.70%	37.54	49.12%	1.00%	28.16	94.43%	99.70%
	CelebA-HQ	30.57	79.94%	93.60%	37.26	48.85%	0.10%	28.71	98.04%	100.00%
	ImageNet	31.01	86.04%	89.60%	37.48	47.40%	0.10%	28.86	89.85%	96.10%
Average		30.78	89.88%	97.59%	32.18	53.96%	3.19%	29.81	91.37%	96.38%

Table 1. Experimental results of the forge attack on three open-source watermarking methods compared with two baseline approaches. Bold numbers indicate the best performance under the same settings.

28% to 42%). Our method also achieves higher confidence levels in watermark detection, with values close to 3 (high confidence). Other details and forged examples are provided in the App. D.

believe this may provide a potential avenue for defending against our attack, and we discuss this further in App. E.

5.3. Ablation Study

In this section, we explore the relationship between the quality of forged images, watermark injection, and the inversion step t under three noise schedules: linear, cosine, and sigmoid. These schedules impact noise injection differently, influencing both watermark degradation and injection. As

Watermark Scheme	Attack	(Yang et al., 2024a)		Ours	
		Dataset	PSNR↑ SR↑/Confidence↑	PSNR↑ SR↑/Confidence↑	PSNR↑ SR↑/Confidence↑
Amazon WM	MS-COCO	24.18	32.0%/2	31.13	100.0%/2.89
	CelebA-HQ	24.10	42.0%/2	29.06	100.0%/2.99
	ImageNet	23.95	28.0%/2	30.90	97.0%/2.69

Table 2. Success rate(SR) and confidence of attacks on real-world deployed watermarking systems. The SR measures the proportion of images detected as watermarked, while the confidence levels—low (1), medium (2), and high (3)—reflect the API’s certainty in its detection.

5.2. Robustness of The Forged Watermark

To investigate the robustness of the forged watermark, we evaluated its performance variation under the interference of common distortions — Gaussian Noise, JPEG (Zhu et al., 2018), and Gaussian Blur (An et al., 2024). As shown in Tab. 3, the robustness of the replicated watermark is slightly lower than that of the real watermark, with an average decrease of 7.08% under Gaussian noise, 8.06% under JPEG compression and 13.19% under Gaussian blur. However, in a few cases, the robustness of the replicated watermark differs significantly from the real one, with a decline exceeding 20%, as indicated by the red downward arrows in the table. Particularly, under blurring, the replicated stable signature watermark is almost completely destroyed, with the bit accuracy dropping to around 50%. Therefore, we

Figure 5. Results illustrate the relationship between the selection of t , image quality (PSNR), and forged bit accuracy under linear, cosine, and sigmoid noise schedules. The lower bound κ is PSNR = 30 and the enlarged markers denote the optimal t from adaptive selection, with results based on the RivaGan watermarking scheme and CelebA-HQ dataset.

shown in Fig. 5(a), the quality of forged images decreases as t increases, consistent with error accumulation (see Sec. 4.2). The PSNR decline varies with different noise schedules: linear decreases uniformly, cosine and sigmoid drop slowly initially, with sigmoid showing a rapid mid-stage decline.

For watermark injection (Fig. 5(b)), the forged bit accuracy

Watermark Scheme	Distortion	Gaussian Noise		JPEG		Blur	
		Dataset	Original bit accuracy	Forged bit accuracy↑	Original bit accuracy	Forged bit accuracy↑	Original bit accuracy
HiddeN	MS-COCO	66.64%	60.21%	57.70%	56.63%	64.26%	62.32%
	CelebA-HQ	61.40%	59.36%	57.38%	56.91%	65.31%	62.38%
	ImageNet	66.31%	60.65%	57.07%	56.13%	66.40%	60.87%
RivaGAN	MS-COCO	99.16%	83.77%	98.89%	77.93% ↓20.96%	99.64%	88.19%
	CelebA-HQ	99.87%	93.19%	99.81%	89.18%	99.99%	97.14%
	ImageNet	97.61%	77.42% ↓20.19%	97.27%	72.61% ↓24.66%	98.85%	81.35%
Stable Signature	MS-COCO		81.89%		77.39%		53.62% ↓32.91%
	CelebA-HQ	88.95%	87.57%	90.04%	85.10%	86.53%	70.92%
	ImageNet		77.10%		73.28%		51.54% ↓34.99%
Average		82.85%	75.68% ↓7.11%	79.74%	71.68% ↓8.06%	83.00%	69.81% ↓13.19%

Table 3. Robustness evaluation of the original watermark scheme and the forged watermark under various image distortions. The robustness of both is represented by their bit accuracy. The green arrows indicate the decrease in bit accuracy for the forged watermark compared to the original, while the red arrows signify a drop of more than 20 percent. The Stable Signature method cannot embed watermarks in real images, so we use the results from generated images as a substitute. The distortion parameters are as follows: Gaussian Noise ($\sigma = 0.05$), JPEG (quality=80), and Blur (kernel size=5).

initially increases with t , peaks, and then decreases. This trend holds across all schedules, though sigmoid exhibits a sharper decline at higher t . Despite these variations, our adaptive step selection method consistently identifies the optimal t , marked by enlarged points in the figure. This ensures a forged bit accuracy over 87% while maintaining PSNR over 30, demonstrating robustness across different noise schedules. Additional results for other datasets are provided in App. C.2.

6. Related Work

In the field of watermark forgery, white-box attacks (Kinakh et al., 2024)—where attackers have full access to the watermarking algorithm—are of limited practical significance. Therefore, most existing forgery attacks focus on black-box and no-box settings. In a black-box setting, attackers can utilize the watermark embedding algorithm to insert watermarks. In contrast, in a no-box setting, attackers can only collect a limited number of watermarked images without any knowledge of the watermarking algorithm, nor can they use it to embed or extract watermarks.

In the black-box setting, Saberi et al. (2023) generate a watermarked noise image and add it to a real image to forge a watermark detector. However, this method is impractical in real-world situations, as attackers typically lack access to watermarked noise images. Wang et al. (2021) assume the attacker can access the non-watermarked version of the target watermarked image, which is unrealistic. Additionally, Li et al. (2023) use a denoising model to remove the watermark and approximate the non-watermarked image,

but it suffers from poor visual quality and limited performance at high resolutions.

In the no-box setting, Kutter et al. (2000) predict watermark patterns by calculating the mean and median of local regions of the watermarked image, adjusting invisibility using the noise visibility function (NVF). Yang et al. (2024a) estimate watermark patterns by averaging the residual between watermarked and non-watermarked images and then embed the pattern at the pixel level. Our parallel work Müller et al. (2024) has launched forgery attacks on semantic watermarking.

7. Discussion and Limitations

Although our proposed watermark forgery attack outperforms existing methods, differences in robustness between our forged and real watermarks provide valuable insights for potential defenses. We discuss possible defense strategies against our approach in App. E. Additionally, the computational and resource demands of model training may impose limitations on our method.

8. Conclusion

We present the first watermark forgery framework that requires neither access to the watermarking scheme nor paired data, achieving superior performance in real-world scenarios. Our experiments demonstrate that the attack success rate exceeds existing methods on both open-source and commercial watermarking systems, exposing their vulnerability and underscoring the need for more secure watermarking

techniques.

Impact Statement

Invisible watermarking plays a critical role in detecting and holding accountable AI-generated content, making it a solution of significant societal importance. Our research introduces a novel watermark forgery attack, revealing the vulnerabilities of current watermarking schemes to such attacks. Although our work involves the watermarking system deployed by Amazon, as responsible researchers, we have worked closely with Amazon’s Responsible AI team to develop a solution, which has now been deployed. The Amazon Responsible AI team has issued the following statement:

‘On March 28, 2025, we released an update that improves the watermark detection robustness of our image generation foundation models (Titan Image Generator and Amazon Nova Canvas). With this change, we have maintained our existing watermark detection accuracy. No customer action is required. We appreciate the researchers from the State Key Laboratory of Blockchain and Data Security at Zhejiang University for reporting this issue and collaborating with us.’

While our study highlights the potential risks of existing watermarking systems, we believe it plays a positive role in the early stages of their deployment. By providing valuable insights for improving current technologies, our work contributes to enhancing the security and robustness of watermarking systems, ultimately fostering more reliable solutions with a positive societal impact.

References

- Promptbase, 2024a. URL <https://promptbase.com/>.
- Promphero, 2024b. URL <https://promphero.com/midjourney-prompts>.
- Al-Haj, A. Combined dwt-dct digital image watermarking. *Journal of computer science*, 3(9):740–746, 2007.
- Amazon. Watermark detection for amazon titan image generator now available in amazon bedrock, 2024. URL <https://aws.amazon.com/cn/about-aws/wat-hats-new/2024/04/watermark-detection-amazon-titan-image-generator-bedrock/>.
- Amazon. Amazon titan image generator and watermark detection api are now available in amazon bedrock, 2025a. URL <https://aws.amazon.com/cn/blogs/aws/amazon-titan-image-generat-or-and-watermark-detection-api-are-now-available-in-amazon-bedrock/>.
- Amazon. Titan, 2025b. URL <https://aws.amazon.com/cn/bedrock/amazon-models/titan/>.
- An, B., Ding, M., Rabbani, T., Agrawal, A., Xu, Y., Deng, C., Zhu, S., Mohamed, A., Wen, Y., Goldstein, T., et al. Benchmarking the robustness of image watermarks. *arXiv preprint arXiv:2401.08573*, 2024.
- Chopra, D., Gupta, P., Sanjay, G., and Gupta, A. Lsb based digital image watermarking for gray scale image. *IOSR Journal of Computer Engineering*, 6(1):36–41, 2012.
- David, E. Openai is adding new watermarks to dall-e 3, 2024. URL <https://www.theverge.com/2024/2/6/24063954/ai-watermarks-dalle3-openai-content-credentials>.
- Deepmind, G. Imagen 2, 2024a. URL <https://deepmind.google/technologies/imagen-2/>.
- Deepmind, G. Imagen 3: Our highest quality text-to-image model, 2024b. URL <https://deepmind.google/technologies/imagen-3/>.
- Deepmind, G. Synthid: Identifying ai-generated content with synthid, 2024c. URL <https://deepmind.google/technologies/synthid/>.
- Dhariwal, P. and Nichol, A. Diffusion models beat gans on image synthesis. *Advances in neural information processing systems*, 34:8780–8794, 2021.
- Diane Bartz, K. H. Openai, google, others pledge to watermark ai content for safety, white house says, 2024. URL <https://www.reuters.com/technology/openai-google-others-pledge-watermark-ai-content-safety-white-house-2023-07-21/>.
- Fang, H., Qiu, Y., Chen, K., Zhang, J., Zhang, W., and Chang, E.-C. Flow-based robust watermarking with invertible noise layer for black-box distortions. In *Proceedings of the AAAI conference on artificial intelligence*, volume 37, pp. 5054–5061, 2023.
- Fernandez, P., Couairon, G., Jégou, H., Douze, M., and Furon, T. The stable signature: Rooting watermarks in latent diffusion models. In *Proceedings of the IEEE/CVF International Conference on Computer Vision*, pp. 22466–22477, 2023.
- Ho, J., Jain, A., and Abbeel, P. Denoising diffusion probabilistic models. *Advances in neural information processing systems*, 33:6840–6851, 2020.

- Huang, H., He, R., Sun, Z., Tan, T., et al. Introvae: Introspective variational autoencoders for photographic image synthesis. *Advances in neural information processing systems*, 31, 2018.
- Jiang, Z., Zhang, J., and Gong, N. Z. Evading watermark based detection of ai-generated content. In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security*, pp. 1168–1181, 2023.
- Jiang, Z., Guo, M., Hu, Y., and Gong, N. Z. Watermark-based detection and attribution of ai-generated content. *arXiv preprint arXiv:2404.04254*, 2024.
- Kayleen Devlin, J. C. Fake trump arrest photos: How to spot an ai-generated image, 2024. URL <https://www.bbc.com/news/world-us-canada-65069316>.
- Kinakh, V., Pulfer, B., Belousov, Y., Fernandez, P., Furon, T., and Voloshynovskiy, S. Evaluation of security of ml-based watermarking: Copy and removal attacks. *arXiv preprint arXiv:2409.18211*, 2024.
- Kutter, M., Voloshynovskiy, S. V., and Herrigel, A. Watermark copy attack. In *Security and Watermarking of Multimedia Contents II*, volume 3971, pp. 371–380. SPIE, 2000.
- Li, G., Chen, Y., Zhang, J., Li, J., Guo, S., and Zhang, T. Warfare: Breaking the watermark protection of ai-generated content. *arXiv e-prints*, pp. arXiv–2310, 2023.
- Lin, H., Wang, M., Wang, J., An, W., Chen, Y., Liu, Y., Tian, F., Dai, G., Wang, J., and Wang, Q. Schedule your edit: A simple yet effective diffusion noise schedule for image editing. *arXiv preprint arXiv:2410.18756*, 2024.
- Lin, T.-Y., Maire, M., Belongie, S., Hays, J., Perona, P., Ramanan, D., Dollár, P., and Zitnick, C. L. Microsoft coco: Common objects in context. In *Computer Vision–ECCV 2014: 13th European Conference, Zurich, Switzerland, September 6–12, 2014, Proceedings, Part V 13*, pp. 740–755. Springer, 2014.
- Lukas, N. and Kerschbaum, F. {PTW}: Pivotal tuning watermarking for {Pre-Trained} image generators. In *32nd USENIX Security Symposium (USENIX Security 23)*, pp. 2241–2258, 2023.
- Mehdi, Y. Announcing microsoft copilot, your everyday ai companion, 2024. URL <https://blogs.microsoft.com/blog/2023/09/21/announcing-microsoft-copilot-you-everyday-ai-companion/>.
- MetaAI. Stable signature: A new method for watermarking images created by open source generative ai, 2023. URL <https://ai.meta.com/blog/stable-signature-watermarking-generative-ai/>.
- Müller, A., Lukovnikov, D., Thietke, J., Fischer, A., and Quiring, E. Black-box forgery attacks on semantic watermarks for diffusion models. *arXiv preprint arXiv:2412.03283*, 2024.
- Nichol, A. Q. and Dhariwal, P. Improved denoising diffusion probabilistic models. In *International conference on machine learning*, pp. 8162–8171. PMLR, 2021.
- OpenAI. Dalle3, 2024. URL <https://openai.com/index/dall-e-3/>.
- Rombach, R., Blattmann, A., Lorenz, D., Esser, P., and Ommer, B. High-resolution image synthesis with latent diffusion models. In *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*, pp. 10684–10695, 2022.
- Russakovsky, O., Deng, J., Su, H., Krause, J., Satheesh, S., Ma, S., Huang, Z., Karpathy, A., Khosla, A., Bernstein, M., Berg, A. C., and Fei-Fei, L. ImageNet Large Scale Visual Recognition Challenge. *International Journal of Computer Vision (IJCV)*, 115(3):211–252, 2015. doi: 10.1007/s11263-015-0816-y.
- Saberi, M., Sadasivan, V. S., Rezaei, K., Kumar, A., Chegini, A., Wang, W., and Feizi, S. Robustness of ai-image detectors: Fundamental limits and practical attacks. *arXiv preprint arXiv:2310.00076*, 2023.
- StabilityAI, 2024. URL <https://github.com/Stability-AI/stablediffusion>.
- Tancik, M., Mildenhall, B., and Ng, R. Stegastamp: Invisible hyperlinks in physical photographs. In *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*, pp. 2117–2126, 2020.
- Wang, R., Lin, C., Zhao, Q., and Zhu, F. Watermark faker: towards forgery of digital image watermarking. In *2021 IEEE International Conference on Multimedia and Expo (ICME)*, pp. 1–6. IEEE, 2021.
- Wang, Z. J., Montoya, E., Munechika, D., Yang, H., Hoover, B., and Chau, D. H. Diffusiondb: A large-scale prompt gallery dataset for text-to-image generative models. *arXiv preprint arXiv:2210.14896*, 2022.
- Wen, Y., Kirchenbauer, J., Geiping, J., and Goldstein, T. Tree-ring watermarks: Fingerprints for diffusion images that are invisible and robust. *arXiv preprint arXiv:2305.20030*, 2023.
- Yang, P., Ci, H., Song, Y., and Shou, M. Z. Steganalysis on digital watermarking: Is your defense truly impervious? *arXiv preprint arXiv:2406.09026*, 2024a.

Yang, Z., Zeng, K., Chen, K., Fang, H., Zhang, W., and Yu, N. Gaussian Shading: Provable Performance-Lossless Image Watermarking for Diffusion Models, May 2024b. Comment: 17 pages, 11 figures, accepted by CVPR 2024.

Yu, N., Skripniuk, V., AbdeInabi, S., and Fritz, M. Artificial Fingerprinting for Generative Models: Rooting Deepfake Attribution in Training Data. In *2021 IEEE/CVF International Conference on Computer Vision (ICCV)*, pp. 14428–14437, Montreal, QC, Canada, October 2021a. IEEE. ISBN 978-1-66542-812-5. doi: 10.1109/ICCV48922.2021.01418.

Yu, N., Skripniuk, V., Chen, D., Davis, L. S., and Fritz, M. Responsible disclosure of generative models using scalable fingerprinting. In *International Conference on Learning Representations*, 2021b.

Zhang, K. A., Xu, L., Cuesta-Infante, A., and Veeramachaneni, K. Robust invisible video watermarking with attention. *arXiv preprint arXiv:1909.01285*, 2019.

Zhang, Z., Lin, M., Yan, S., and Ji, R. Easyinv: Toward fast and better ddim inversion. *arXiv preprint arXiv:2408.05159*, 2024.

Zhao, X., Gunn, S., Christ, M., Fairoze, J., Fabrega, A., Carlini, N., Garg, S., Hong, S., Nasr, M., Tramer, F., et al. Sok: Watermarking for ai-generated content. *arXiv preprint arXiv:2411.18479*, 2024.

Zhao, Y., Pang, T., Du, C., Yang, X., Cheung, N.-M., and Lin, M. A recipe for watermarking diffusion models. *arXiv preprint arXiv:2303.10137*, 2023.

Zhu, J., Kaplan, R., Johnson, J., and Fei-Fei, L. Hidden: Hiding data with deep networks. In *Proceedings of the European conference on computer vision (ECCV)*, pp. 657–672, 2018.

A. Shallow Inversion Algorithm

Algorithm 1 Shallow Inversion

Require: Non-watermarked image x_0 , pre-trained diffusion model \mathcal{M} , maximum inversion steps T , search step size s , image quality lower bound κ , image quality metric \mathcal{Q}

Ensure: Forged image x'_0 with embedded watermark while preserving image quality

Initialize: $t \leftarrow T$ {Start from the maximum inversion step}

while $t > 0$ **do**

- Inversion step:** Map x_0 to latent variable x'_t
 $x'_t \leftarrow I_{inversion}(x_0, t, \mathcal{M})$
- Denoising step:** Denoise x'_t to forged image x'_0
 $x'_0 \leftarrow D_{denoise}(x'_t, t, \mathcal{M})$
- if** $\mathcal{Q}(x_0, x'_0) \geq \kappa$ **then**
 - break** {Stop if the reconstructed image quality is sufficiently high}
- end if**
- Update step t :**
 $t \leftarrow t - s$

end while

Return: x'_0 {Return the forged image}

B. DDIM Inversion Error Accumulation.

Theorem B.1 (Error Accumulation in DDIM Inversion). *For the DDIM inversion process with noise schedule $\{\alpha_t\}$, the latent variable x_t can be expressed as:*

$$x_t = \frac{\sqrt{\alpha_t}}{\sqrt{\alpha_0}} x_0 + \sum_{u=0}^{t-1} \frac{\sqrt{\alpha_t}(\sqrt{\alpha_u} - \sqrt{\alpha_{u+1}})}{\sqrt{\alpha_u} \sqrt{\alpha_{u+1}}} \sqrt{1 - \alpha_u} \epsilon_u \quad (7)$$

where $\epsilon_u = \epsilon_\theta(x_{u+1}, u+1)$ represents the predicted noise at step u .

Proof. We prove this by mathematical induction.

Base Case ($t = 1$): Using the DDIM inversion formula:

$$\begin{aligned} x_1 &= \frac{\sqrt{\alpha_1}}{\sqrt{\alpha_0}} x_0 + \left(1 - \frac{\sqrt{\alpha_1}}{\sqrt{\alpha_0}}\right) \sqrt{1 - \alpha_0} \epsilon_0 \\ &= \frac{\sqrt{\alpha_1}}{\sqrt{\alpha_0}} x_0 + \frac{\sqrt{\alpha_1}(\sqrt{\alpha_0} - \sqrt{\alpha_1})}{\sqrt{\alpha_0} \sqrt{\alpha_1}} \sqrt{1 - \alpha_0} \epsilon_0. \end{aligned} \quad (8)$$

This matches the general form in Equation (7).

Inductive Hypothesis: Assume for $t = k$, the expression holds:

$$x_k = \frac{\sqrt{\alpha_k}}{\sqrt{\alpha_0}} x_0 + \sum_{u=0}^{k-1} \frac{\sqrt{\alpha_k}(\sqrt{\alpha_u} - \sqrt{\alpha_{u+1}})}{\sqrt{\alpha_u} \sqrt{\alpha_{u+1}}} \sqrt{1 - \alpha_u} \epsilon_u. \quad (9)$$

Inductive Step ($t = k + 1$): From the DDIM recurrence relation:

$$x_{k+1} = \frac{\sqrt{\alpha_{k+1}}}{\sqrt{\alpha_k}} x_k + \left(1 - \frac{\sqrt{\alpha_{k+1}}}{\sqrt{\alpha_k}}\right) \sqrt{1 - \alpha_k} \epsilon_k. \quad (10)$$

Substituting the inductive hypothesis into the recurrence:

$$x_{k+1} = \frac{\sqrt{\alpha_{k+1}}}{\sqrt{\alpha_k}} \left[\frac{\sqrt{\alpha_k}}{\sqrt{\alpha_0}} x_0 + \sum_{u=0}^{k-1} \frac{\sqrt{\alpha_k}(\sqrt{\alpha_u} - \sqrt{\alpha_{u+1}})}{\sqrt{\alpha_u} \sqrt{\alpha_{u+1}}} \sqrt{1-\alpha_u} \epsilon_u \right] \\ + \left(1 - \frac{\sqrt{\alpha_{k+1}}}{\sqrt{\alpha_k}} \right) \sqrt{1-\alpha_k} \epsilon_k \quad (11)$$

$$= \frac{\sqrt{\alpha_{k+1}}}{\sqrt{\alpha_0}} x_0 + \sum_{u=0}^{k-1} \frac{\sqrt{\alpha_{k+1}}(\sqrt{\alpha_u} - \sqrt{\alpha_{u+1}})}{\sqrt{\alpha_u} \sqrt{\alpha_{u+1}}} \sqrt{1-\alpha_u} \epsilon_u \\ + \frac{\sqrt{\alpha_{k+1}}(\sqrt{\alpha_k} - \sqrt{\alpha_{k+1}})}{\sqrt{\alpha_k} \sqrt{\alpha_{k+1}}} \sqrt{1-\alpha_k} \epsilon_k. \quad (12)$$

Combining the summation terms:

$$x_{k+1} = \frac{\sqrt{\alpha_{k+1}}}{\sqrt{\alpha_0}} x_0 + \sum_{u=0}^k \frac{\sqrt{\alpha_{k+1}}(\sqrt{\alpha_u} - \sqrt{\alpha_{u+1}})}{\sqrt{\alpha_u} \sqrt{\alpha_{u+1}}} \sqrt{1-\alpha_u} \epsilon_u. \quad (13)$$

This completes the inductive proof. \square

Remark B.2. Assume the error between $\epsilon_\theta(x_t, t+1)$ and $\epsilon_\theta(x_{t+1}, t+1)$ is Δ_t . the cumulative error δ_t grows with increasing inversion steps t :

$$\delta_t = \sum_{u=0}^{t-1} C(u, t) \sqrt{1-\alpha_u} \Delta_u, \quad (14)$$

where $C(u, t) = \frac{\sqrt{\alpha_t}(\sqrt{\alpha_u} - \sqrt{\alpha_{u+1}})}{\sqrt{\alpha_u} \sqrt{\alpha_{u+1}}}$.

C. Additional Experimental Results

C.1. Attack Performance with Fewer Number of Victim's Images

To further evaluate the advantages of our attack, we constrained the attacker's capabilities by reducing the number of victim images to 5,000, as shown in Tab. 4. For an extremely limited number of victim images, specifically restricted to 10,50 and 100, we considered that such a small dataset might cause the diffusion model training to fail or extremely overfit. Therefore, we utilized a pre-trained diffusion model and fine-tuned it to conduct our attack. The results are shown in Tab. 5.

C.2. Additional results of ablation study

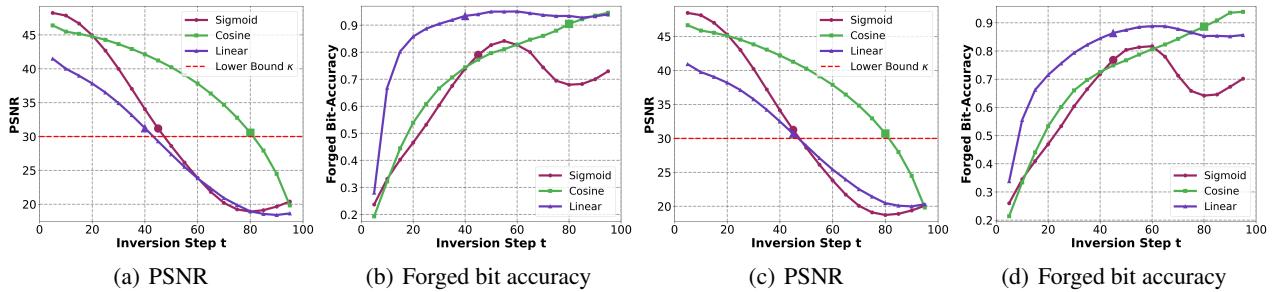


Figure 6. Results illustrate the relationship between the selection of t , image quality (PSNR), and Forged bit accuracy under linear, cosine, and sigmoid noise schedules. The lower bound κ is PSNR = 30 and the enlarged markers denote the optimal t from adaptive selection, with results based on the RivaGan watermarking scheme and MS-COCO dataset((a),(b)), ImageNet((c),(d)).

Attacks		(Wang et al., 2021) (Paired Data)			(Yang et al., 2024a)			Ours		
Watermark Scheme	Dataset	PSNR↑	Forged bit accuracy↑	FPR@0.05↑	PSNR↑	Forged bit accuracy↑	FPR@0.05↑	PSNR↑	Forged bit accuracy↑	FPR@0.05↑
HiddeN (128×128)	MS-COCO	31.02	80.56%	99.30%	31.97	62.81%	10.30%	31.99	89.48%	97.20%
	CelebA-HQ	31.57	82.28%	99.90%	32.02	62.00%	6.20%	31.99	85.29%	98.50%
	ImageNet	31.24	78.61%	95.00%	31.96	62.38%	9.50%	32.91	84.88%	91.10%
RivaGAN (256×256)	MS-COCO	32.94	93.26%	100.00%	30.05	50.30%	0.60%	32.15	96.00%	99.80%
	CelebA-HQ	32.64	93.67%	100.00%	30.11	51.19%	1.10%	32.19	87.08%	91.20%
	ImageNet	33.11	90.94%	99.60%	30.05	50.32%	0.80%	33.23	80.68%	77.50%
Stable Signature (512×512)	MS-COCO	28.87	91.68%	98.40%	31.55	50.88%	1.40%	30.36	87.96%	96.10%
	CelebA-HQ	32.33	79.90%	92.40%	31.27	51.33%	1.20%	28.49	95.59%	100.00%
	ImageNet	29.59	85.77%	89.90%	31.48	49.21%	0.80%	30.79	83.49%	89.30%
Average		31.48	86.30%	97.17%	31.16	54.49%	3.54%	31.57	87.83%	93.41%

Table 4. Comparison of attack performance on three open-source watermarking methods using a reduced number (5,000) of victim images.

(Yang et al., 2024a)						Ours	
Num	Dataset	PSNR↑	Forged bit-accuracy↑	FPR@0.05↑	PSNR↑	Forged bit accuracy↑	FPR@0.05↑
10	MS-COCO	18.47	48.93%	1.00%	34.62	65.88%	44.10%
	CelebAHQ	18.53	52.05%	1.80%	34.48	73.66%	77.90%
	ImageNet	18.50	49.30%	1.00%	34.53	65.83%	46.10%
50	MS-COCO	23.92	50.82%	1.30%	34.06	63.92%	36.30%
	CelebAHQ	24.54	53.49%	1.80%	34.14	71.06%	69.20%
	ImageNet	24.25	51.20%	0.70%	34.01	64.10%	38.90%
100	MS-COCO	27.81	51.46%	1.60%	33.41	73.12%	69.00%
	CelebAHQ	29.28	53.09%	1.80%	33.67	81.23%	93.50%
	ImageNet	27.65	52.30%	2.20%	33.32	73.35%	69.80%

Table 5. Comparison of attack performance on three open-source watermarking methods using a limited number(10,50,100) of victim images.

D. Attacking Amazon Watermarks

D.1. Omitted experimental details

Among the available options, most companies (e.g., Google, OpenAI, etc.) do not open their watermark detection mechanisms to users, making it impossible to evaluate the success of our attack. In contrast, Amazon provides access to its watermark detection for the Titan model (Amazon, 2025b), allowing us to directly measure the performance of our attack. Therefore, we chose Amazon’s watermarking scheme for our experiments.

Amazon’s watermarking scheme, referred to as Amazon WM, is designed for model accountability, ensuring that AI-generated content can be traced back to its source. The watermark detection API checks whether an image is generated by the Titan model and provides a confidence level for the detection. This confidence level reflects the likelihood that the image contains a valid watermark.

We generated 10,000 images using ten distinct prompts to train the diffusion model, selecting $t = 20$ based on adaptive step selection. For each dataset, we forged 100 images and submitted them to Amazon’s watermark detection API. Additionally, we tested images from non-public datasets, including human-captured photos and web-sourced images, which were also flagged as Titan-generated after forgery. Detection results from the API are illustrated in Fig. 7 and the forged examples are shown in 8 and D.1.

Results

To determine if an image was generated using a Titan Image Generator model, upload an image above and select analyze.



Watermark detected (Confidence: [High](#))

Bedrock detected a watermark generated by the [Titan Image Generator model](#) on this image.

Figure 7. Sample results from Amazon’s watermark detection API, showing detection outcomes, confidence levels, and content sources.

E. Potential Mitigations

As discussed in Sec. 5.2, forged and original watermarks exhibit differences in robustness, particularly under certain transformations. This discrepancy could potentially serve as a defensive strategy. Specifically, for widely deployed invisible watermark schemes, detection systems might mitigate forged watermarks by preprocessing uploaded images prior to detection, effectively removing the forged watermark while minimally impacting the original watermark.

Furthermore, semantic watermarking (Wen et al., 2023; Yang et al., 2024b) may offer resistance to our attack, as the watermark information is intrinsically linked with the image content, making it challenging to replicate the watermark on non-watermarked images using our approach. However, semantic watermarking remains in its early stages of development and has not yet been deployed, primarily due to unresolved challenges related to watermark capacity and traceability mechanisms. We encourage further research in this direction.



Figure 8. Examples of forged images for Amazon Watermark using 5,000 victim images.



Figure 9. Examples of forged images for Amazon Watermark using 10,000 victim images.