

# Attacks on Approximate Caches in Text-to-Image Diffusion Models

Desen Sun  
*University of Waterloo*

Shuncheng Jie  
*University of Waterloo*

Sihang Liu  
*University of Waterloo*

## Abstract

Diffusion models are a powerful class of generative models that produce images and other content from user prompts, but they are computationally intensive. To mitigate this cost, recent academic and industry work has adopted approximate caching, which reuses intermediate states from similar prompts in a cache. While efficient, this optimization introduces new security risks by breaking isolation among users. This paper provides a comprehensive assessment of the security vulnerabilities introduced by approximate caching. First, we demonstrate a remote covert channel established with the approximate cache, where a sender injects prompts with special keywords into the cache system and a receiver can recover that even after days, to exchange information. Second, we introduce a prompt stealing attack using the approximate cache, where an attacker can recover existing cached prompts from hits. Finally, we introduce a poisoning attack that embeds the attacker’s logos into the previously stolen prompt, leading to unexpected logo rendering for the requests that hit the poisoned cache prompts. These attacks are all performed remotely through the serving system, demonstrating severe security vulnerabilities in approximate caching. The code for this work is available.<sup>1</sup>

## 1 Introduction

Over recent years, generative models have developed rapidly. Among them, text-to-image diffusion models dominate image generation in commercial systems, such as those from Google [53], Adobe [1] and OpenAI [44]. Thanks to their remarkable ability in generating high-quality images, users leverage them for scene and character designs [6, 7, 13, 16, 22, 35, 61, 72, 77], artwork construction [68], and advertisement [12]. Users only need to provide their prompts that describe the task, and the diffusion model can generate the image as specified.

Although diffusion models are powerful, they suffer from a high computational overhead. It takes seconds to generate a

single image. Such overhead mainly comes from the computation pattern, where a sequence of denoising steps are applied to an initial noise to convert it to the final image. Therefore, reducing the number of steps is a key approach to saving computation. Caching is a promising technique that has attracted attention from both academia and industry [2, 48, 76, 85]. For instance, Pinecone [48] and Zilliz [85] use semantic caches to reuse existing results if a previous prompt aligns with the current one. Approximate cache is another type of optimization [2, 76]. Instead of directly reusing the prior generations, it reuses intermediate states from similar prompts in the diffusion execution, and resumes the denoising steps to save computation while achieving better text–image alignment. For instance, NIRVANA [2] from Adobe is an approximate cache for diffusion models.

With the widespread use of text-to-image diffusion models, adversaries also exploit these models for their malicious purposes. Some studies take advantage of the diffusion model as a secret channel, embedding private messages and transmitting the output images [8, 24, 37, 47, 79]. Another type of attack steals high-quality prompts to save the prompt design cost [10, 58, 75]. There are also attacks that aim to poison the diffusion model and inject specific objects or concepts into output images [11, 18, 21, 43, 46, 56, 69, 74].

However, existing attacks focus on the model, while vulnerabilities of the diffusion model serving system remain largely underexplored. Approximate cache is promising in improving the efficiency of diffusion models, but it introduces additional components to the image generation system, potentially widening the attack surface. The goal of this work is to comprehensively assess the security implications of approximate caching and exploit its vulnerabilities.

To analyze approximate cache, we take NIRVANA [2], the state-of-the-art approximate cache from Adobe by replicating their design, and deploy two widely used text-to-image diffusion models, FLUX [28] and Stable Diffusion 3 (SD3) [14], and two real-world prompt datasets, DiffusionDB [73] and Lexica [58]. The serving system is deployed on cloud GPUs to make the environment realistic. Similar to conventional

<sup>1</sup><https://doi.org/10.5281/zenodo.17957900>

caches, like those in CPUs or file systems, approximate cache reduces the image generation latency. Our evaluation shows that cache hit or miss latency can be clearly distinguished. On an H100 GPU, skipping 10 % of steps yields 0.92 s and 0.48 s lower latency for FLUX and SD3, respectively. This timing difference can be leveraged by an attacker to determine whether their prompt hits or misses the cached prompts, which we refer to as *Attack Primitive 1*.

However, an approximate cache system is different from conventional caches. Unlike a conventional cache, where every access hits a specific entry, whether a prompt hits an entry in an approximate cache depends on prompt similarity, which largely varies by prompts. Thus, even though an attacker may probe the cache and receive a cache hit, the output cannot be directly used to derive cached states. We find that generations hitting the same cached prompt have higher similarity, as they preserve part of the original content, such as structure and layout. Therefore, such similarity can be leveraged to determine whether two cache hits originate from the same cached prompt. We refer to this characteristic as *Attack Primitive 2*.

Based on these attack primitives, we present three attacks. In these attacks, we assume an attack model where the attacker can only access the serving system like normal users and does not have prior knowledge about any user prompts in the cache.

First, we demonstrate a remote covert channel, where a sender and a receiver exchange messages through a diffusion model service with approximate caching (Section 4). Using special keywords and markers, the sender injects special prompts to the cache. Afterward, the receiver probes the approximate cache to detect whether the sender’s prompts exist. The receiver uses a combination of generation timing (Attack Primitive 1) and image content detection (Attack Primitive 2) to confirm that the cache was injected by the sender. Cache hits and misses are encoded as 1s and 0s. Using a number of keywords, the sender can transmit a message with a 97.8 % accuracy under the FLUX model [28]. Using real-world prompt traces from DiffusionDB, we demonstrate that sender’s prompts stay in the cache for over 44 hours, making this channel stealthy.

Second, we perform a prompt stealing attack, CacheTransparency (Section 5). The attacker probes the approximate cache and applies Attack Primitives 1 and 2, leveraging both timing and structural similarity of generated images to identify which probing prompts map to the same cached prompt. These prompts are then used to recover the target prompt. We evaluate this attack on FLUX and SD3, and two datasets, DiffusionDB and Lexica, with real-world user prompts. The results indicate that the attacker’s stolen prompts have an average of 0.78 cosine similarity compared to the original ones.

Lastly, we demonstrate a CachePollution attack where an attacker can inject their content (i.e., logos in this attack) in the diffusion model’s cache, and poison other users’ generations (Section 6). The attacker first uses an embedding-space

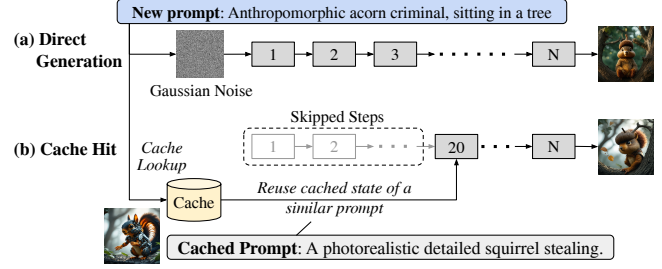


Figure 1: Diffusion model generation (a) directly from Gaussian noise and (b) from an approximate cache.

logo injection model to seamlessly embed the logo in stolen prompts, ensuring a high hit rate by other users. Then, if a user hits the attacker’s cached prompt, the output image will include the logo, even though it is not specified in the prompt.

We summarize the contributions as the following:

- To the best of our knowledge, this is the first work that exploits security vulnerabilities in the approximate cache for text-to-image diffusion models.
- We demonstrate a remote covert channel through an approximate caching system, leveraging images generated by special words to secretly exchange information.
- We design a prompt stealing attack, CacheTransparency. Without requiring users’ output images, the attacker can infer user prompts in the approximate cache.
- We introduce a poison attack, CachePollution. Without manipulating the model or training dataset, the attacker can poison the output of user prompts with specific logos.

## 2 Background

In this section, we introduce the architecture of text-to-image diffusion models and a key optimization to diffusion models using approximate caching.

### 2.1 Text-to-Image Diffusion Models

Diffusion model is a generative model with iterative computation [19]. During inference, a text-to-image diffusion model takes a Gaussian noise image as input, predicts and eliminates noise by a number of steps, and eventually generates a high-quality image. Figure 1a demonstrates how the diffusion model generates an image with a given prompt. The diffusion model processes the initial Gaussian noise for multiple denoising steps. In each step, it predicts the potential noise and eliminates such noise from the input. The prompt is used to guide the noise prediction in every step. After a number of denoising steps, the noise will eventually be converted to a high-quality image.

## 2.2 Approximate Cache Serving System

A major challenge of diffusion models is their substantial computational cost, primarily stemming from the iterative denoising process. Inspired by semantic caching in large language models (LLMs) [4, 17, 30, 39] and diffusion models [5, 48, 85], which enables reuse of outputs from prior prompts, recent work has introduced approximate caching that reuses intermediate states from previous generations [2, 60, 76], achieving a balance between quality and efficiency. The central insight of approximate caching is that similar prompts yield similar outputs. Thus, the intermediate state from a prior, similar prompt can serve as the starting point for a new prompt, allowing the system to skip already completed denoising steps. Typically, the number of skipped steps is determined by the *semantic similarity* between the new prompt and the cached prompt, where higher similarity allows the new prompt to skip more steps. Prior work demonstrates that up to 50 % of denoising steps can be reused without noticeable quality degradation [2], with every 10 % of steps cached to enable flexible reuse across varying similarity levels.

Figure 1b illustrates how an approximate cache works. When a new prompt arrives, the approximate caching system first converts the prompt to an embedding using the Contrastive Language-Image Pre-Training (CLIP) model [49] and calculates the cosine similarity between the new prompt and the existing cached prompts. If the similarity score exceeds a threshold, the system considers this as a hit and the request will reuse the corresponding cached state. Prior work has shown that a similarity over 0.65 [2] can be regarded as a hit. The new prompt will continue with denoising steps from the middle and skip the prior steps (20 steps in Figure 1b).

Moreover, cache management also plays a critical role in the effectiveness of approximate caching. In Adobe’s NIRVANA system [2], a prompt is inserted into the cache whenever no existing cache entry is hit. To evict stale entries, NIRVANA employs a Least Computationally Beneficial and Frequently Used (LCBFU) policy, which removes cache items that provide minimal computational savings and are infrequently reused. In contrast, more recent work adopts simpler strategies such as FIFO, ensuring that recently accessed prompts remain available in the cache [76].

## 3 Vulnerabilities of Diffusion Models

In this section, we discuss the existing attacks on diffusion models and the new security implications due to caching.

### 3.1 Attacks on Diffusion Models

Although powerful in generating content, recent work has shown that diffusion models have security concerns. One category of attacks notices that the diffusion model’s output inherently contains massive information, making it easy

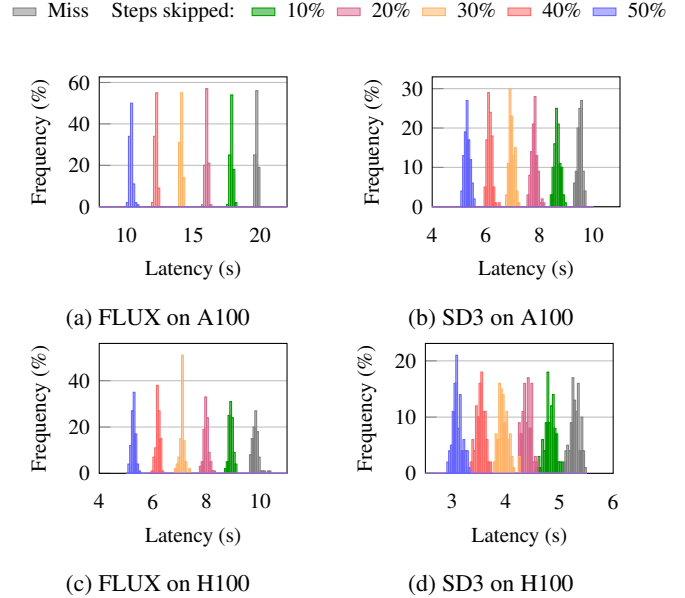


Figure 2: Approximate cache latency distribution ( $n = 100$ ).

for steganography. Previous studies have demonstrated attack techniques that embed secret messages into images [8, 24, 37, 47, 79]. These attacks usually require an attacker-controlled model to manipulate generated images. Another category of attacks aims at recovering prompts that generated a certain image, as the engineering of prompts is critical in generation. These attacks convert the generated images back to prompts [58] by taking publicly available generated images (e.g., those posted on the internet) as input and training a model to enable recovery. Some attacks also attempt to manipulate the generated content, such as inserting the attacker’s brand information or bias to the model to guide the generation process [11, 18, 21, 43, 46, 69]. Users will receive images with such an injection. Typically, attackers enable such attacks by polluting the training data [8, 23, 43].

### 3.2 New Vulnerabilities from Caching

Although approximate caching is a promising optimization approach, it introduces an additional component to the diffusion model serving system, which stores and reuses prior prompts, potentially extending the attack surface. Therefore, the goal of this work is to analyze and assess the security risks associated with approximate cache on diffusion models.

#### 3.2.1 Timing of Approximate Cache

Similar to caches in file systems or processors, approximate caching for diffusion models also aims at reducing execution latency. We first analyze its latency to better understand its security implications. We set up a text-to-image diffusion serving system on a remote server using the Runpod

cloud [51]. The server is over 600 km away from our client, ensuring a realistic cloud serving connection. We implement NIRVANA [2], the state-of-the-art approximate cache from Adobe. We follow its configuration that caches every 10 % of the denoising steps until 50 %. We evaluate two popular commercial open-sourced diffusion models, Stable Diffusion 3 Median (SD3) [14] and FLUX [28, 29] with two types of GPU, A100 and H100 (both have 80 GB of memory). Both diffusion models have 30 denoising steps.

For each diffusion model and GPU type, we randomly select 100 prompts and send requests from our local PC to reflect the impact of network fluctuation. Each request is evaluated with different numbers of skipped steps. In comparison, the deviation of H100 results is more significant than A100, owing to its faster generation, amplifying the impact of network fluctuation. Nonetheless, on both platforms, skipping even just 10 % of the steps yields a clear latency reduction, indicating the feasibility of a timing channel. Moreover, the latency differences between each level of skipped steps are also distinguishable on both platforms. As introduced in Section 2.2, the number of skipped steps is correlated with the similarity between the new prompt and the cached prompt. In the rest of this paper, we use an H100 for the experiments as it is a more challenging platform for timing channels.

#### Attack Primitive 1

Because an approximate cache reduces generation latency on cache hits, it enables attackers to determine whether their prompts hit the cache. In addition, the attacker can use the magnitude of the latency reduction to infer the similarity between their prompt and the cached prompt they hit.

### 3.2.2 Similarity of Image Generations

A cache hit reuses an intermediate result from a prior prompt. Therefore, such reuse likely retains information from a previous generation. According to previous studies, the diffusion model determines the image’s layout at an early stage [2, 76, 81], implying that reusing the same cached prompts reduces output diversity. Although the details may change after multiple denoising steps, the structure of the images remains similar to the cached state.

We evaluate such similarity by generating 100 images from different cached states and measuring their Structural Similarity Index Measure (SSIM), which is a common metric to measure the similarity between two images. We evaluated both SD3 and FLUX models. Figure 3 shows the distribution of SSIM scores between two images. If two prompts hit the same cached prompt, their SSIM score tends to be higher compared to those that hit different cached prompts. The difference is more prominent in FLUX, as it is a more powerful model that constructs the layout at very early stages.

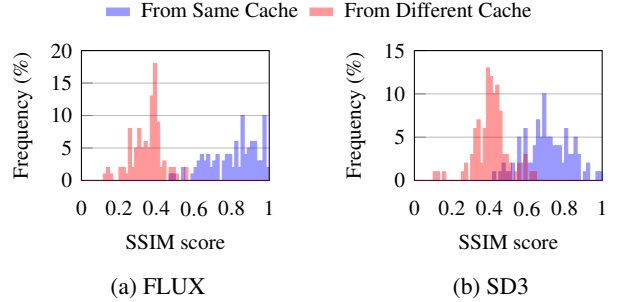


Figure 3: SSIM distribution ( $n = 100$ ).

#### Attack Primitive 2

Images generated from the same approximate cache have higher similarity. Attackers can use the generated image to infer the original prompt that their prompt hits.

## 4 Remote Covert Channel

A covert channel is a secret channel for two parties to exchange secret messages. In this section, we demonstrate that a sender and a receiver can establish a remote covert channel through the approximate cache of text-to-image diffusion models to asynchronously transmit messages. This is done by sending specially-crafted prompts to leave a message in the cache and retrieving it later. Compared to synchronous covert channels [3, 27, 33, 36, 54] that require both parties to simultaneously communicate, an asynchronous covert channel through text-to-image generation is highly stealthy.

### 4.1 Attack Model

We assume that the image generation service deploys the approximate caching technique for better efficiency. When a user sends a prompt, the service caches the prompt and intermediate states of the generation. We assume that the sender and the receiver do not have direct communication channels. Instead, they can only access the same remote diffusion-model-based image generation service through prompts. The sender and the receiver also do not have any knowledge about the existing cached prompts.

### 4.2 Covert Channel Design

Establishing an asynchronous covert channel, through which the sender leaves a message and the receiver retrieves it at a later time, requires accurate identification of whether the receiver’s prompt hits a cached prompt left by the sender. Attack Primitive 1 indicates that a prompt that hits a previous prompt can be identified through its image generation latency. As an approximate cache contains cached prompts from various users, it is difficult to determine whether the cached prompt



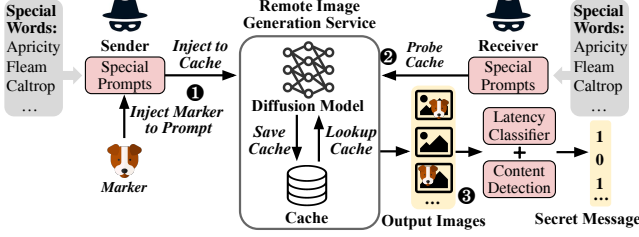


Figure 4: The setup of the remote covert channel, which is based on approximate cache in diffusion models.

that the receiver’s prompt hit was left by the sender. Therefore, we use a special keyword (e.g., uncommon words) to differentiate the sender’s prompt, which the receiver can use to retrieve the cached prompt. However, the approximate cache may treat a prompt as a hit if another prompt is similar to other parts of the receiver’s prompt, even if the sender did not inject such a prompt into the approximate cache. Attack Primitive 2 indicates that the output image can be used to infer whether the new prompt hits the original cached prompt, as they have higher similarity than other generated images. Based on both attack primitives, we additionally include a special marker. When leaving the message, the sender combines the marker with the special keyword in the prompt. Then, the receiver can probe the cache using the keyword and perform a two-level detection to confirm whether the prompt hits a cached prompt (using latency) and whether the hit is on the sender’s prompt (by detecting the marker in the output image).

Figure 4 demonstrates the covert channel process. First, the sender injects prompts to the approximate cache with special keywords (❶). Then, the receiver sends prompts with the same keywords (❷). Finally, the receiver uses the two-level detection to determine whether they hit the sender’s prompt (❸). A hit or a miss transmits a bit of 1 or 0, respectively. Specifically, the covert channel has the following components.

**Unique prompt generator.** We first use an LLM to generate a set of special, ancient words that are no longer used today, without any prior knowledge about the prompts in the test dataset. These special words are preknowledge shared by the sender and the receiver (e.g., shared offline before transmission). Then, both the sender and receiver use an LLM to construct prompts. On the sender side, the Llama model constructs a prompt for each special word with the marker. On the receiver side, the Llama model constructs a prompt for each special word to probe the cache.

**Latency classifier.** The receiver profiles the generation latency of the serving system and uses the average latency of hit and miss cases to build a classifier that determines whether their probing prompt hits any cached prompts.

**Content detector.** The receiver uses a content detection model to recognize the predefined marker in the output image. If recognized, the receiver’s prompt hits the sender’s prompt.

### 4.3 Setup

**Platform.** We use the approximate cache system and cloud platform introduced in Section 3.2.1.

**Model and Dataset.** We select the state-of-the-art text-to-image diffusion model, FLUX [28], as the primary model for evaluation. We additionally evaluate a smaller model, Stable Diffusion 3 Medium (SD3) [14]. We use DiffusionDB as the main dataset which contains real-world user prompts and use Lexica as a secondary dataset which contains a smaller number of prompts but in different styles. While we only choose prompts in English, in practice, other languages can also be used for this covert channel. We configure 100 GB cache size for DiffusionDB and 1 GB for Lexica due to their number of prompts and deploy the same cache replacement policy as NIRVANA [2] as default.

**Correctness Metric.** The success rate depends on two factors:

- **Insertion success rate** measures the rate of successful cache insertion by the sender. If the sender posts a request but hits the cache, the cache system will not insert a new cache, leading to incorrect message transmission.
- **Detection success rate** measures the receiver’s rate of successful retrieval of prompts with special words and the associated detection of the marker, once the sender has injected the special prompts into the cache successfully.

**Sender and Receiver Setup.** We use a Llama-3 70B model as the LLM to construct 10 special keywords and the corresponding unique prompts. Figure 5 illustrates these keywords and images generated by FLUX for message transmission. These extremely uncommon words increase the chance that the receiver’s prompts hit the sender’s cached prompts. We use “dog” as the marker for FLUX (this example) and “McDonald’s” for SD3. This is because FLUX is a more powerful model that can render complicated objects from the cached states compared to SD3. If the receiver does not hit the sender’s prompts, the output images resemble those in the first row; otherwise, the receiver obtains outputs like those in the second row. DINOv2 [45] is used to detect the marker in the receiver’s generated images, which is the same method of object detection in Silent Branding [23].

**Baseline.** We introduce a baseline that only uses generation latency of the prompt with special words to determine cache hit or miss, without using any marker.

### 4.4 Results

This section presents the evaluation results.

#### 4.4.1 Overall covert channel accuracy

We evaluate covert channel 100 times on both FLUX and SD3. Both sender and receiver send requests to the remote cloud. We assume that the cache system has all the unique prompts from DiffusionDB-2M. Table 1 shows that the covert channel achieves over 97.8 % and 95.8 % accuracy in FLUX

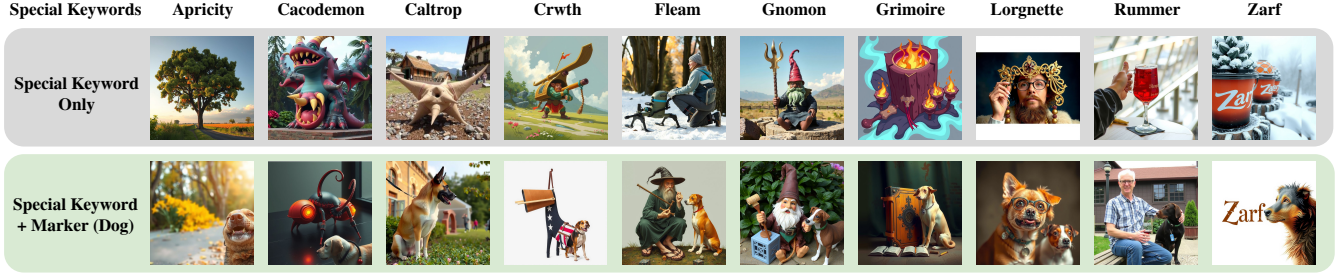


Figure 5: Covert channel examples (image generated by FLUX).

Table 1: Accuracy breakdown ( $n = 100$ ).

Model	Overall Accuracy (Latency + Content Classifier)	Latency-only Classifier
FLUX	97.8 %, $\sigma=2.5$ %	94.6 %, $\sigma=13.0$ %
SD3	95.8 %, $\sigma=3.6$ %	90.8 %, $\sigma=16.1$ %

and SD3, respectively. FLUX achieves a higher and more stable accuracy than SD3. This is because FLUX is a more powerful model, capable of generating clearer objects even in early denoising steps. Thus, the cached intermediate states in FLUX are more likely to preserve these objects.

We further explore the accuracy breakdown. Incorrect transmission can potentially come from two sources. First, the sender’s prompt may hit an existing cached prompt, without being cached in the serving system. Consequently, the receiver always receives a bit of 0. Our experiment shows a 100 % cache insertion success rate because the sender’s prompts are not similar to either Lexica or DiffusionDB-2M. Second, the *latency classifier* and *content detector* in two-level detection process can also introduce inaccuracies. Table 1 shows the *latency classifier*’s average accuracy, which is high (94.6% and 90.8% for FLUX and SD3, respectively) but varies by keyword. Misclassifications occur most often when the sender omits a prompt for a keyword (to transmit a 0), where the receiver may hit other cached prompts and cause false positives. Figure 6 presents the *latency classifier*’s accuracy for all 10 keywords. It achieves less than 60 % accuracy for some keywords (e.g., *Apricity*), likely because prompts with these keywords have high similarity scores with normal prompts. In contrast, including the *content classifier* ensures a more consistent accuracy in both models. In a few cases, the *content classifier* slightly lowers the accuracy because the model fails to render the marker clearly. This is more prominent in the weaker model, SD3 (e.g., *Fleam*).

#### 4.4.2 Lifetime of Sender’s Cache

We evaluate the lifetime of the sender’s cache entries, i.e., how long an injected prompt remains cached before eviction. We follow the same setup as NIRVANA [2], where a prompt

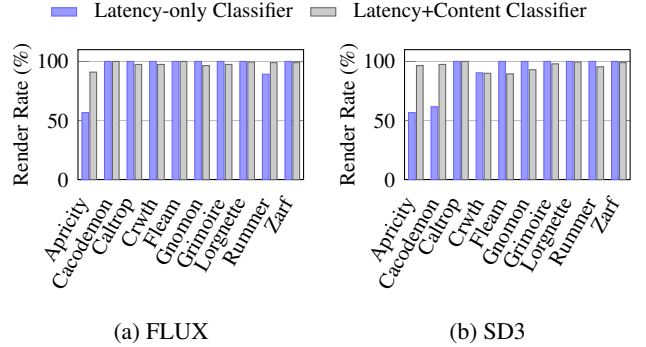


Figure 6: Render success rate of each keyword ( $n = 100$ ).

is injected only if it does not hit any cached prompt. We replay the trace in DiffusionDB-Large with 14M prompts according to the timestamps and use FLUX as the image generation model. We insert the sender’s prompts once the approximate cache is full, and count the time and number of requests the service received until eviction.

Figure 7a shows the lifetime under different cache sizes. As the cache size increases, the lifetime of injected cached prompts increases significantly. Figure 7b shows the lifetime under three replacement policies: LCBFU and FIFO are the default replacement policies in prior approximate caching systems [2, 76]; LRU is a popular replacement policy. We observe that LCBFU retains the sender’s prompts in the cache for the longest time because it manages caches in a finer granularity, effectively allowing for more cache entries. LRU evicts the sender’s prompt earliest, as these keywords barely receive hits from normal users. Overall, the sender’s prompts last in the cache for a long time (up to 44 hours), making the channel stealthy.

#### 4.4.3 Time and Resource Consumptions

We further conduct an experiment to measure the resource consumption of the covert channel. Table 2 shows the results when running the models on an H100. Because every image represents 1 bit, sending and receiving 1 bit both take 1 prompt. In our setup, each image has 16384 tokens due

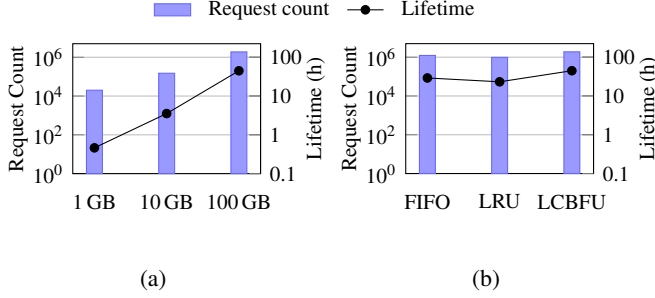


Figure 7: Sender’s cache lifetime under (a) different cache sizes (LCBFU) and (b) replacement policies (100 GB cache).

Table 2: Time and resource consumptions per bit on H100.

Model	FLUX	SD3
# Prompts (Sending/Receiving)	1	1
# Tokens (Sending/Receiving)	16384	16384
Sending Time (s)	9.8	5.3
Receiving Time (s)	8.2	4.3

to the  $8\times$  downsample ratio from the  $1024 \times 1024$  output resolution in both diffusion models. Therefore, sending and receiving 1 bit both consume 16384 tokens. We also evaluate the time for sending and receiving 1 bit. Sending 1 bit takes  $1.20\times$  and  $1.23\times$  more time compared to receiving one bit in FLUX and SD3, respectively. This difference is because sending incurs cache misses, while receiving benefits from cache hits. Although the bandwidth is lower than synchronous covert channels [27, 33], it is comparable to other asynchronous covert channels [55].

## 4.5 Discussions

Compared to prior attacks on diffusion models that transmits secret messages [8, 24, 37, 47, 79], this covert channel does not modify or train the diffusion model. Moreover, instead of using the timing channel alone, like remote covert channels on conventional caches [3, 27, 33, 36, 54], this covert channel analyzes the generation output to achieve a higher success rate. As discussed in Section 4.4.3, this covert channel requires a total of 2 prompts when sending and receiving 1 bit, leading to a lower bandwidth than some synchronous covert channels [27, 33] and higher resource consumptions. However, its asynchronous property allows the sender’s message to remain in the approximate cache for days, enabling the receiver to obtain the message at a later time. This enhances the stealthiness of this channel and makes it harder to be detected. Moreover, in case of unstable networking and delayed response, the *content classifier* is still effective as it can still check the marker in the output image without relying on latency measurements.

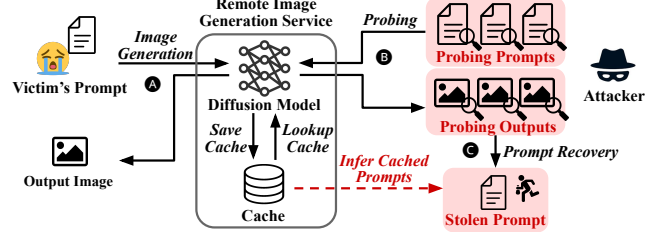


Figure 8: The setup and overview of CacheTransparency.

## 5 CacheTransparency: Prompt Stealing Attack

As prior work has shown, generating high-quality images requires prompt engineering and careful design of modifiers [10, 58]. In this section, we introduce CacheTransparency, a prompt stealing attack, where the attacker’s goal is to steal other users’ prompts (e.g., for commercial usage) from the approximate cache to reproduce their image generation.

### 5.1 Attack Model

We assume the same image generation serving system as Section 4.1. Similarly, we assume the attacker has no additional privileges than other normal users, i.e., zero knowledge of other users’ prompts or generated images and they can only send requests to those generation services to get images. The attacker is also unaware of the cache size, but only identifies which probing prompts hit the same cached prompt and recovers the corresponding prompt.

### 5.2 Attack Design

Figure 8 illustrates an overview CacheTransparency attack. The victim sends a prompt to the image generation service and the prompt is cached (A). The attacker later sends probing prompts to the service (B) and recovers the victim’s prompt by analyzing the probing prompts (C).

#### 5.2.1 Challenges

The attacker can distinguish a probing prompt’s hit/miss through latency (Attack Primitive 1). However, the similarity between the probing prompt and the target prompt can be low (e.g., only 0.65). Thus, a single probing prompt is insufficient for recovery. Using multiple probing prompts should improve the accuracy but two challenges need to be solved. First, it is difficult to determine which cached prompt a probing prompt hits. Approximate caching retrieves prompts by similarity, which introduces uncertainties. A misclassification on the target prompt degrades the recovery accuracy. Second, the embedding space does not directly map to words. Therefore,

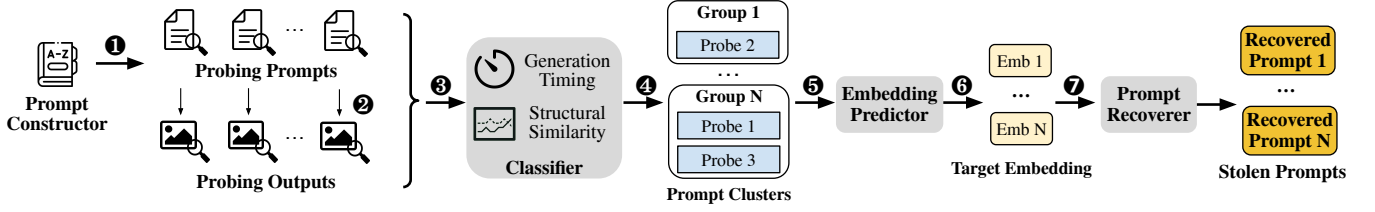


Figure 9: Design details of CacheTransparency.

even with an accurate classification of hits, converting multiple probing prompts that are similar in the embedding space back to the original prompt remains challenging.

### 5.2.2 Solution

To address these challenges, CacheTransparency follows the approach in Figure 9. First, we design a *prompt constructor* to construct probing prompts (①) and get corresponding images (②). Once the attacker has collected enough probing data, a two-level *classifier* (③) clusters these prompt-image pairs into multiple groups, where probing prompts in the same group hit the same target prompt (④). After that, the attacker uses an *embedding predictor* (⑤) to guess the cache embedding that every group hits (⑥). The created embedding maintains high similarity to every prompt in the group. We consider this embedding as the approximation of the cached prompt’s embedding and recover it back to the prompt with a *prompt recoverer* (⑦). The recovered prompt is the stolen prompt. The attacker sends these prompts back to the same generation application to obtain the images. We next discuss these components in detail.

**Prompt Constructor:** The *prompt constructor* generates a batch of prompts by sampling a variable number of modifiers from a predefined modifier collection file. We use the same modifier pool as a prior study [58]. For each attack trial, the *prompt constructor* starts from a subject and randomly samples modifiers from the pool. The number of modifiers per probing prompt varies. After constructing a prompt, the attacker sends it to the image generation service and exploits the latency to determine whether this prompt is a cache hit. Once a hit is detected, the attacker collects the prompts for the following processing. The *prompt constructor* also leverages a filter to prevent the constructed prompts from being too similar (keeping semantic similarity below 0.6 in our experiment) to the hit prompts. By increasing the diversity of hit prompts, this approach prevents overfitting when training the *embedding predictor*.

**Classifier.** CacheTransparency’s classifier consists of two components: a *timing classifier* that determines if a prompt is a cache hit based on its generation latency and a *structural classifier* that further determines which probing prompts hit the same cached prompt. The attacker sends the probing

prompts generated by the *prompt constructor* to the image generation service and measures the response latency. The *timing classifier* places prompts with response time within the cache hit latency threshold (9.5 s for FLUX and 5.06 s for SD3 on an H100) in a *hit set*. According to Attack Primitive 2, generated images tend to be more similar if they hit the same cached prompts. Therefore, to further increase the classifier’s accuracy, the *structural classifier* examines the prompts’ CLIP similarity to avoid false positives. It employs a 3-layer MLP, where the input is the CLIP similarity of two prompts and the SSIM scores of the corresponding images, and the output is whether two prompts hit the same cached prompts.

**Embedding Predictor.** Once the classifier has grouped all probing prompts, the attacker can then recover each group back to the original cached prompt that they hit. The *embedding predictor* is an embedding training process with the Stochastic Gradient Descent (SGD) algorithm. It first creates a random embedding  $E$  and computes the similarity scores as a vector  $S_E$  with each prompt from the group. We denote the similarity scores between the cached prompt and the prompts in the group as a vector  $S_C$ . Since the attacker can only infer the number of skipped steps based on the generation latency (Attack Primitive 1) instead of an accurate similarity score, we assume that the number of skipped steps represents the worst-case similarity. The *embedding predictor* takes the Mean Squared Error (MSE) between  $S_E$  and  $S_C$  as the loss function, and iteratively updates the embedding  $E$  based on SGD to make it similar to the original cached prompt.

**Prompt Recoverer.** The next step is to convert the embedding to prompts. Inspired by prior studies [40], we design a generative model named *prompt recoverer* to convert embeddings back to prompts. It first maps an embedding from the CLIP embedding space to the GPT-2 space with an MLP-based model. Then, it uses a 124M-parameter GPT-2 [50] to reconstruct the prompt word by word. When training, we do not freeze the parameters of GPT-2 to enhance the alignment between the output and normal users’ prompt style.

## 5.3 Attack Setup

**Platform.** Like before, we use the approximate cache system in Section 3.2.1.



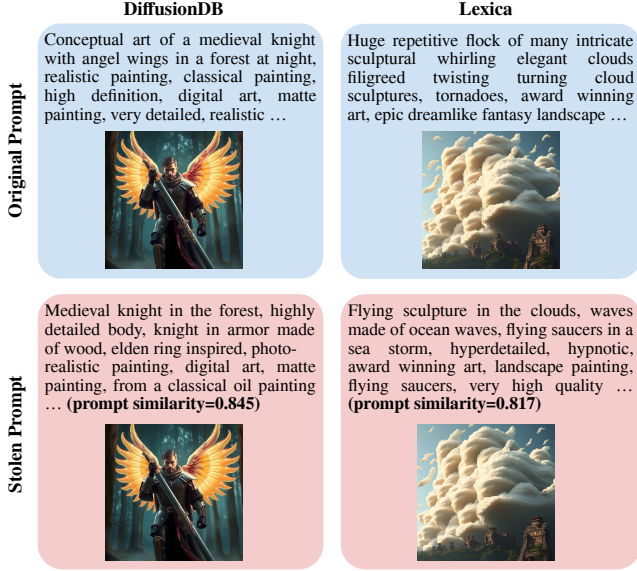


Figure 10: Examples of CacheTransparency.

**Model and Dataset.** We follow the same diffusion models and datasets as the covert channel, as described in Section 4.3. The attacker is unaffected by replacement, as they only probe the approximate cache. Therefore, we evaluate this attack using a fixed number of cache entries. Due to differences in dataset size, the approximate cache contains 100k entries for DiffusionDB and 10k entries for Lexica.

**CacheTransparency Training.** CacheTransparency consists of four components as described in Section 5.2. The *prompt recoverer* and *classifier* need to be trained. We randomly select 20 % prompts in DiffusionDB to train the two models, and evaluate CacheTransparency on the other 80 % prompts and the *unseen* dataset Lexica. Specifically, we select 200 unique prompts in the 20 % training set as cached prompts, and use other prompts that are able to hit these cached prompts to generate images. Using these prompt-image pairs, we train the *classifier* based on their structural and CLIP embedding similarities. *Prompt recoverer* takes the CLIP embedding as the input and the original text as the target output.

**CacheTransparency Probing.** The probing process takes two stages: the first stage constructs the prompts randomly and exploits the latency classifier to collect the hit prompts. Once the hits exceed a certain number (35 in our evaluation), probing moves to the second stage, where embeddings whose similarity to the hit prompts falls within an interval (0.5–0.6 in our evaluation) are sampled. This increases the likelihood of hitting the cached prompt while maintaining prompt diversity.

**Baseline.** As our attack model assumes that the attacker has no access to the victim’s generated images, previous prompt stealing attacks [58] on diffusion models do not work. Therefore, we use a naive side-channel attack method as the baseline, that

only uses the *prompt constructor* to generate similar prompts and a simple *timing classifier* to determine hit/miss, which has been used in prior prompt stealing attacks on LLMs [59, 84]. We refer to this method as *Naive Probing*.

**Accuracy Metrics.** We evaluate the similarity of stolen prompts and their generated images with the victim’s prompts and images using the metrics below:

- **Prompt semantic similarity.** The stolen prompt should describe similar content as the target prompt. We first evaluate the semantic similarity using cosine similarity in the CLIP embedding space [10, 58]. This metric is also what *Prompt Recoverer* is optimized for.
- **Prompt word-level similarity.** In addition to the semantic similarity, we also evaluate their word-level similarities using the metrics below:
  - Bilingual Evaluation Understudy (BLEU) [10, 63] is a metric that considers both the word count and the n-gram word sequence count, but does not consider the semantic similarity or synonyms. Specifically, we use the BLEU-1 score to reflect the word-level success rate.
  - Named Entity Recognition Recall (NER) [71] measures the success rate at the entity level. It counts the correct entity numbers in the candidate text compared to the reference text and calculates the recall rate.
  - BERTScore [63] captures the meaning of words by employing a pretrained BERT model to align words between candidate and reference texts, thus considering synonyms. We use BERTScore F1 as our metric.
- **Image similarity.** The image generated by the stolen prompt should also be similar to the original generation. We evaluate image similarity using the metrics below:
  - Contrastive Language-Image Pre-training (CLIP) [10, 58] encodes images to embeddings. The cosine similarity between two embeddings reflects the semantic similarity between two images.
  - Peak Signal-to-Noise Ratio (PSNR) [14, 23, 79] is a pixel-wise image similarity metric. We employ PSNR to quantify the differences between two images.
  - Structural Similarity Index Measure (SSIM) is the metric used in Section 3.2.2, which captures the structural similarities between images.

## 5.4 Results

Figure 10 demonstrates two examples of CacheTransparency from DiffusionDB and Lexica. The first row shows user prompts and the generated images. The second row shows CacheTransparency’s stolen prompts and the reproduced images. The stolen prompts are also similar to the user’s prompts. Even though there exist word-level differences, from a model’s perspective, the two prompts are highly similar. Thus, the generated images are almost identical to the original.

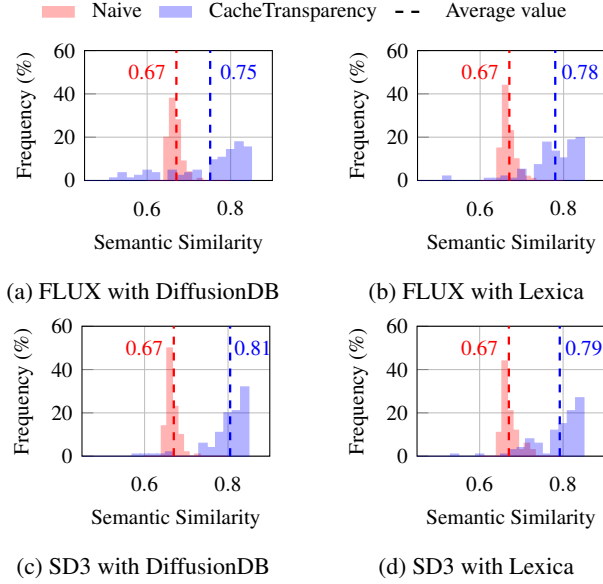


Figure 11: Semantic similarity distribution of recovered prompts ( $n = 100$ ).

Table 3: Word-level prompt recovery quality.

Dataset	Model	Method	BLEU	NERR	BERT-Score
DiffusionDB	FLUX	Naive Probing	0.12	0.01	0.83
		CacheTransparency	<b>0.22</b>	<b>0.17</b>	<b>0.85</b>
	SD3	Naive Probing	0.12	0.06	0.80
		CacheTransparency	<b>0.25</b>	<b>0.18</b>	<b>0.86</b>
Lexica	FLUX	Naive Probing	0.11	0.01	0.83
		CacheTransparency	<b>0.20</b>	<b>0.14</b>	<b>0.85</b>
	SD3	Naive Probing	0.11	0.02	0.83
		CacheTransparency	<b>0.22</b>	<b>0.13</b>	<b>0.85</b>

#### 5.4.1 Overall Success Rate

We first conduct an experiment to show the prompt and image similarity on both models and both datasets, using the metrics in Section 5.3. We process 100 rounds for each configuration and try to recover at least one prompt for each round.

**Prompt semantic similarity.** Figure 11 shows the distribution of the CLIP semantic similarity between the target prompts and the recovered prompts. On average, prompts recovered by CacheTransparency achieve 0.75–0.81 similarity scores, much higher than the naive baseline which is around 0.67. According to prior studies, such high prompt similarity can be considered successful [10, 58]. A few prompts recovered by CacheTransparency has a similarity score lower than 0.65 due to false positives from our *classifier* in those specific cases. We will discuss the impact of the false positives in Section 5.4.3.

Table 4: Image recovery quality.

Dataset	Model	Method	CLIP	PSNR	SSIM
DiffusionDB	FLUX	Naive Probing	0.86	20.89	0.74
		CacheTransparency	<b>0.90</b>	<b>24.95</b>	<b>0.82</b>
	SD3	Naive Probing	0.74	15.02	0.55
		CacheTransparency	<b>0.85</b>	<b>19.92</b>	<b>0.75</b>
Lexica	FLUX	Naive Probing	0.88	20.11	0.72
		CacheTransparency	<b>0.95</b>	<b>25.62</b>	<b>0.85</b>
	SD3	Naive Probing	0.75	15.39	0.531
		CacheTransparency	<b>0.84</b>	<b>19.72</b>	<b>0.71</b>

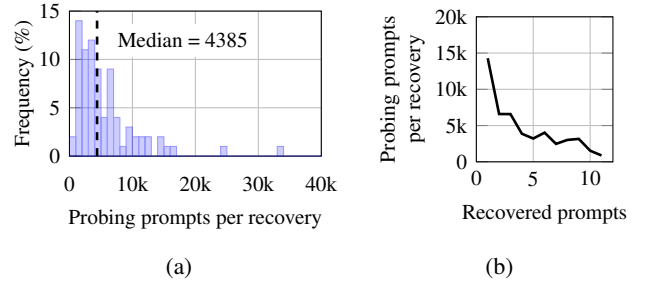


Figure 12: (a) Distribution of probing prompts and (b) amortized probing number over recovered prompts.

**Prompt word-level similarity.** Table 3 displays the success rate of CacheTransparency under word-level similarity metrics. For both BLEU and NERR, CacheTransparency performs much higher accuracy scores than Naive Probing. The reason is that Naive Probing only considers the semantic similarity due to the approximate caching mechanism. In contrast, CacheTransparency exploits a 124M-parameter GPT-2 model to summarize a cluster of probing prompts that hit the same cached prompt, achieving high accuracy. While BERTScore’s consideration of synonyms narrows the margin, CacheTransparency still consistently outperforms Naive Probing in BERTScore.

**Image similarity.** Table 4 presents the image similarity compared to the target image. CacheTransparency outperforms the baseline in all three metrics. Specifically, the PSNR score can exceed 25 and achieve over 19 for both datasets and models, indicating a negligible difference compared to the target image [15]. For both the baseline and CacheTransparency, FLUX has better similarity scores than SD3 across all metrics. This is because FLUX’s early cached states contain clearer content than SD3, resulting in more similar output.

#### 5.4.2 Number of Probing Prompts

To steal a prompt, the attacker needs to send a large number of probing prompts before collecting a good number of hits for

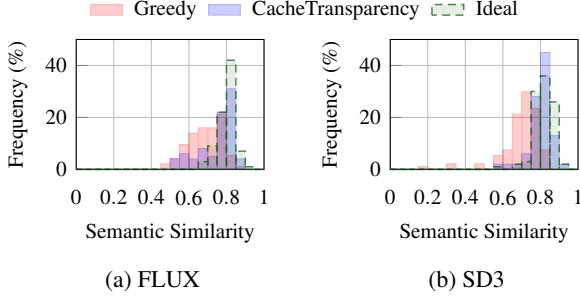


Figure 13: The effectiveness of *classifier* ( $n = 100$ ).

recovery. Figure 12a shows the distribution of the number of probing prompts per recovery (stolen prompts). Despite a long tail, the median is 4385. The high number is mainly due to the first stage of probing. After finding the initial hits, the *prompt constructor* can generate more specific probing prompts in the second stage. Figure 12b shows the median number of probing prompts per recovery over different numbers of recovered prompts after each recovery execution. The number of probing prompts is amortized, as the number of recovered prompts in a round increases (as low as 874 when 11 prompts are recovered in a round).

#### 5.4.3 Ablation Study on Classifier

We evaluate the effectiveness of the *classifier*. Because the classifier takes both the prompt and the image as input to determine structural similarity, we evaluate both FLUX and SD3 using the main dataset, DiffusionDB. We include two additional methods as comparison points: (a) A *greedy* method that uses all prompts that hit any cached prompts for recovery, without grouping them by their structural similarity. (b) An *ideal* scenario that classifies the probing prompts 100% correct. The prompt constructor generates the same probing prompts for CacheTransparency and these methods. Figure 13 shows that CacheTransparency is only 3.01% lower than *ideal* on average, following similar distributions. In comparison, without considering structural similarity, recovered prompts by the *greedy* method have a lower similarity (0.69 on average).

A false positive occurs when a probing prompt hits a different cached prompt but is mistakenly classified as hitting the target prompt in the cache. In our experiment, SD3 and FLUX have 0.36 and 1.63 false positives on average. We further evaluate its impact by randomly inserting variable numbers of false positives into the ideal scenario. Figure 14 shows that the similarity declines with more false positives. The experiment also indicates that the similarity drops significantly with only 1 false positive, which highlights the importance of an accurate classifier.

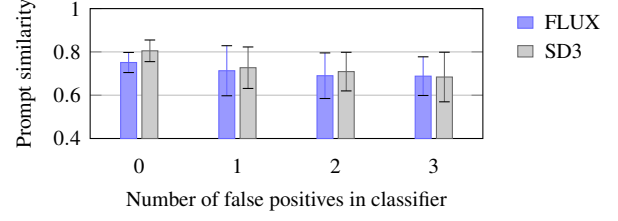


Figure 14: Sensitivity to the false positive in classifier (prompts from DiffusionDB).

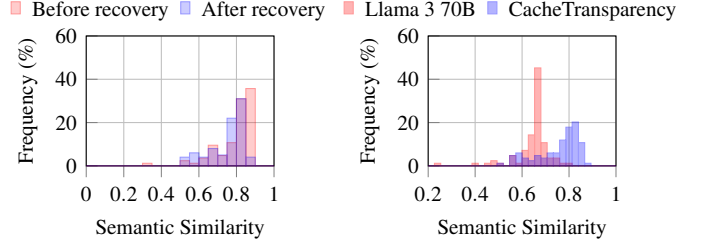


Figure 15: The effectiveness of *prompt recoverer* (FLUX vs. Llama-3 70B (FLUX with DiffusionDB,  $n = 100$ )).

#### 5.4.4 Ablation Study on Prompt Recoverer

The prompt recoverer component converts embeddings back to prompts. We evaluate its effectiveness by measuring the similarity loss during the conversion. Because it does not take images as input, we only evaluate FLUX using DiffusionDB. We compare the embedding of the target cached prompt directly with the *embedding predictor*'s output (before recovery), as well as the embedding after conversion back to the prompt (after recovery). Figure 15 presents the distribution of similarity scores. Compared to the embedding before recovery, *prompt recoverer* only incurs 4.4% similarity loss on average, preserving the similarity.

We also compare our prompt recovery technique to an LLM-based method. We compare the similarity score of prompts recovered by the combination of *Embedding Predictor* and *Prompt Recover* in CacheTransparency with those generated by a Llama-3 70B model [38]. As Figure 16 illustrated, CacheTransparency achieves 10.4% higher similarity scores than Llama. It is worth noting that the recovery models in CacheTransparency are lightweight compared to a 70B Llama-3, being able to execute on local devices (e.g., a gaming GPU). This low hardware requirement further enhances the stealthiness of CacheTransparency.

#### 5.4.5 Sensitivity Study on Hit Count

We analyze the impact of hit count, a key factor in the prompt recovery process, using the primary model, FLUX, and the

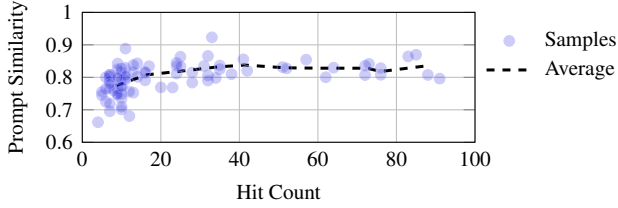


Figure 17: Sensitivity to hit count (FLUX with DiffusionDB).

DiffusionDB dataset. We evaluate 100 ideal experiments where the *classifier* is 100% correct and group the experiments by the number of prompts that hit the target cached prompt. Figure 17 illustrates the relationship between semantic similarity and the number of hits, where achieving a high similarity score (over 0.8) requires more than 17 hits. When the hit count increases over 26, the recovery similarity plateaus, indicating that the attacker can stop probing the image generation service once the classifier has collected 26 prompts that hit the same cached prompt.

## 5.5 Discussions

To the best of our knowledge, CacheTransparency is the first prompt stealing attack for text-to-image diffusion models via the approximate cache. Compared to prior works [10, 58, 75], CacheTransparency can steal prompts without requiring users to share their output image to the public. This enhances the capability of the prompt-stealing attack. CacheTransparency also constructs multiple probing prompts and exploits a timing classifier to determine the hit situation of those prompts, like cache side-channel attacks [20, 26, 32, 34, 64, 66, 67, 78, 80]. Differently, this attack deals with similarity-based cache retrieval, and uses a *structural classifier* and an *embedding predictor* to recover the target prompt from a set of probing prompts.

Like the covert channel (Section 4.5), CacheTransparency also works without cache timing. Without timing information, the *structural classifier* can directly cluster prompts by the cache they hit based on the output images. However, this is more costly as the classifier needs to compare each pair of the probing prompts (14k). In contrast, the *latency classifier* significantly narrows the search space.

## 6 CachePollution: Image Poisoning Attack

If a prompt hits the approximate cache, the output image resembles the cached one when it is similar with the cache prompt. Therefore, attackers can inject prompts with their preferred information (e.g., logos) into the cached states, which will later be reused by victims. In this section, we present an image poisoning attack, CachePollution.

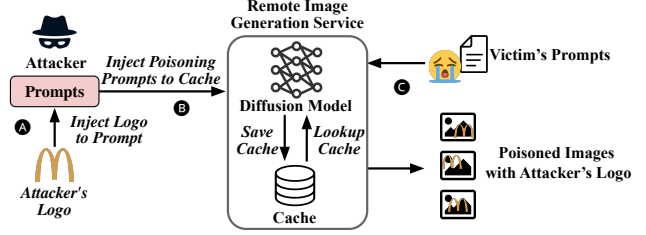


Figure 18: The setup and overview of CachePollution.

### 6.1 Attack Model

Figure 18 depicts the setup of this attack. We assume that an image generation service is the same as the previous covert channel (Section 4.1) and CacheTransparency attack (Section 5.1). Likewise, we assume the attacker can only access the image generation service via prompts. The attack’s goal is to first inject prompts with information under their control and leave such information in user generations. The attacker has no prior knowledge about the existing caches in the cache system. Thus they have to steal the prompts first and then embed extra information into those prompts. In this attack, we use logos to demonstrate the attacker’s poisoning capabilities. The injected logos can be used for advertisement purposes.

### 6.2 Attack Design

Figure 18 illustrates the overview of CachePollution. The attacker first injects the logo into prompts (A) that were stolen using CacheTransparency and then sends them to the approximate cache (B). When a victim hits poisoned prompts in the approximate cache, the output will display the same logo (according to Attack Primitive 2), even if the victim did not mention it (C). Because CacheTransparency constructs probing prompts with commonly used words, the CachePollution attack that is based on these stolen prompts enables cache hits but does not guarantee the degree of popularity of the poisoned prompts. Our evaluation shows that CachePollution pollutes a substantial number of user prompts even though these prompts can be less popular (discussed in Section 6.4.1.)

#### 6.2.1 Challenge

To inject a cache that contains a logo, the logo’s text description needs to be first included in the prompt and then cached. However, directly appending the logo to an arbitrary prompt is less likely to be hit by user prompts.

#### 6.2.2 Solution

Figure 19 depicts the design. First, the attacker steals cached prompts using the CacheTransparency attack (1). These prompts are good representations of other user prompts and



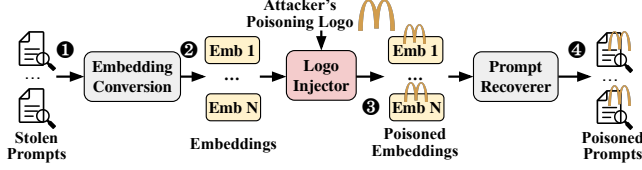


Figure 19: Design of CachePollution.



Figure 20: Examples of CachePollution (generated by FLUX).

are more likely to be hit. Then, the attacker converts these prompts to embeddings (2) and uses the *logo injector* to embed logo descriptions into the embeddings (3). Afterward, the attacker converts the embedding to a prompt with a similar model as the *prompt recoverer* in CacheTransparency (4). This prompt contains the logo but remains similar to the stolen prompt.

**Logo injector.** It is the core of this attack, which has two subcomponents: a model for *logo insertion* and another for *embedding prediction*. The *logo insertion* model is a small attention-based model that combines normal prompts with the attacker’s logos. It takes the prompt embedding and the logo, and generates an embedding that contains both. This is an effective way to insert logos, but the output may have low similarity with the original prompt, making it less likely to be hit by other users. Therefore, we incorporate another *embedding prediction model* to convert the injected prompts to be more similar to the original one. The *embedding prediction model* is similar to the one in CacheTransparency, except that it includes the logo information. It first generates an embedding  $E$  and uses the *logo insertion* model to guarantee that  $E$  contains the logo information. We note the embedding with logo information as  $E'$ . To ensure that  $E'$  preserves the semantics of both the original prompt and the logo, the model calculates two similarities:  $S_{E'}$  for the similarity between  $E'$  and the original prompt and  $S_{\text{logo}}$  for the similarity between  $E'$  and the logo, and uses  $(1 - S_{E'})^2 + (1 - S_{\text{logo}})^2$  as the loss function.  $E'$  is optimized using SGD until the loss is below  $10^{-4}$ .

Table 5: Poison effectiveness.

Method	FLUX				SD3			
	DiffusionDB		Lexica		DiffusionDB		Lexica	
	Hit	Render	Hit	Render	Hit	Render	Hit	Render
Direct Inject	2624	1580	1059	744	3408	883	632	139
CachePollution	<b>3646</b>	<b>2104</b>	<b>1226</b>	<b>863</b>	<b>4931</b>	<b>1360</b>	<b>838</b>	<b>180</b>

### 6.3 Attack Setup

**Platform.** We use the same system in Section 3.2.1.

**Model and Dataset.** Similar to the Convert Channel, we also set FLUX and DiffusionDB as the main model and dataset, and SD3 and Lexica as an extension. To evaluate the poisoning success rate, we send 1M prompts in DiffusionDB-Large by their timestamps and the whole Lexica randomly by its default order.

**Logos.** We evaluate this attack with 6 logos, including 4 well-known logos (“Nike”, “McDonald’s”, “Apple”, “Chanel”) and 2 customized logos (“Triangle”, “Blue Moon”), similar to the methodology in prior work [23]. We choose 50 target prompts stolen by CacheTransparency, as described in Section 6.2. Thus, each logo has 50 poisoned prompts.

**CachePollution Training.** The *logo injector* model contains a 2-layer MLP and an attention layer. To train this model, we use a training set based on 10 % of DiffusionDB-2M, We randomly insert the logo descriptions into these prompts. The training objective is to maximize the cosine similarity between the model’s predicted embedding and the embedding of logo-inserted prompts. To convert the poisoned embedding back to text, we exploit the same model as the *prompt recoverer model* in CacheTransparency. We retrain it with the new dataset with the added logo descriptions to ensure correct generation of the logo text.

**Baseline.** We take the naive implementation of the poison attack that randomly injects the logo text into the stolen prompts and inserts them into the cache system as a baseline.

**Metrics.** We use the following metrics to evaluate this attack:

- **Hit number** indicates the number of user prompts that hit the attack’s poisoned prompts in the approximate cache.
- **Render rate** is the rate of user prompts that hit the cached prompts and contain a visible logo in the output images. The logo is not always rendered successfully by diffusion models, especially when the number of skipped steps is too small or the logo is complicated.

### 6.4 Results

Figure 20 is an example of the poisoned output generated by FLUX. The first row presents the logos, and the second and third rows show the generated images with and without hitting the poisoned prompts. When hitting a poisoned prompt, the logo embeds into the generated image.

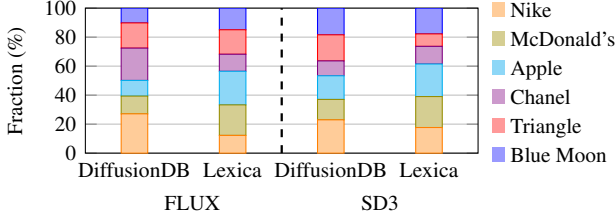


Figure 21: Breakdown of hits by logos.

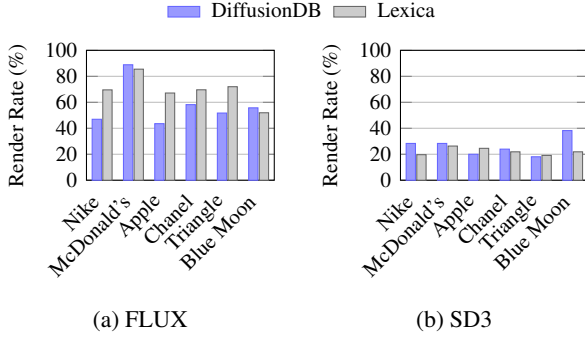


Figure 22: Render success rate for different models.

#### 6.4.1 Poison Success Rate

We first evaluate the hit number and render success rate. We simulate user prompts using datasets as described in Section 6.3. In parallel, the attacker sends poisoned prompts periodically to determine whether the prompt was successfully inserted into the approximate cache based on the generation latency. If a user prompt hits any poisoned cached state, we save the generated images and detect whether it contains the logo. The detection model is DINOv2 [45], similar to the method in prior work [23].

As Table 5 illustrates, CachePollution receives more hits than the direct injection baseline in all scenarios, due to the effective *logo injector*. Consequently, the success rate of CachePollution is also higher. Figure 21 details the breakdown of hits by logos. Because we use the same target prompts for all 6 logos, the variation among logos indicates how well a logo can be blended into the prompt. All 6 logos contribute to the total hit, indicating the generalization of this attack.

We also explore the render success rates among 6 logos. Figure 22 demonstrates that FLUX achieves a higher success rate. In contrast, SD3 struggles to preserve such visual content when reusing the cached states. The main reason is that SD3 (the median version) is less powerful than FLUX, resulting in weaker text-image alignment. Even when the logo text is explicitly included in the prompt, SD3 often fails to generate the corresponding logo. Figure 23 illustrates that, when a logo is embedded directly into the prompt, FLUX produces a clear logo, whereas SD3 does not. Logo complexity also sig-

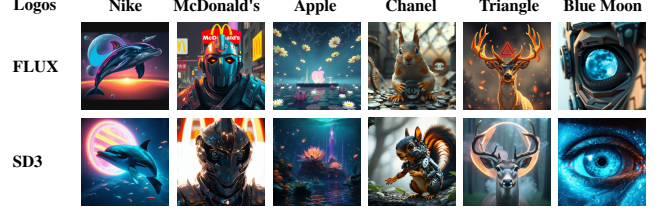


Figure 23: Generation comparison between FLUX and SD3 (Median) when the logo is directly embedded into the prompt.

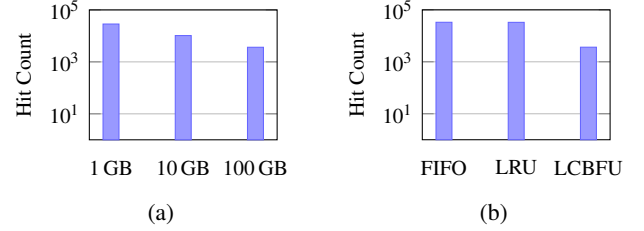


Figure 24: Poison effectiveness under (a) different cache sizes (LCBFU) and (b) replacement policies (100 GB cache).

nificantly impacts the success rate. For instance, Figure 22b shows that “Triangle” exhibits the lowest success rate with SD3, as its complicated lines can vanish after multiple denoising steps, while “Blue Moon” achieves a high success rate due to its simpler structure.

#### 6.4.2 Sensitivity Study

We finally explore CachePollution’s effectiveness under different cache configurations, like those studied in Section 4.4.2. Figure 24a shows that the hit count is higher when the cache size is smaller, as the cached prompt that the poisoned one will replace gets evicted earlier under a smaller cache, allowing more user prompts to hit the attacker’s poisoned cache. With the same cache size, Figure 24b shows the hit count is higher under FIFO and LRU than LCBFU because the target prompts in these schemes get evicted from the cache earlier. In LCBFU, cached prompts that were frequently hit in the past are harder to evict, leading to a lower hit count.

### 6.5 Discussion

Unlike previous poison attacks that pollute the training dataset [18, 23, 46, 57, 69], CachePollution poisons a serving system through prompts, without accessing or manipulating the training data. Therefore, this attack assumes a more realistic environment. Moreover, CachePollution can work in combination with other poisoning attacks, further increasing the render success rate of the attacker’s content.

CachePollution can also operate without the timing channel, which is only used for injecting poisoned prompts. With-

out it, the attacker can analyze the generation to determine whether their poisoned prompt was processed from scratch or a cached prompt, e.g., comparing it with the output from a separate system running the same model.

## 7 Potential Defense Mechanisms

**Random cache selection.** The approximate caching selects the cache of the highest similarity with the incoming prompt [2, 76], which allows the sender’s prompt with the same special word to be chosen. The defense mechanism can randomly choose from a number of potential cached prompts. This randomization makes it significantly harder for a receiver to hit a specific entry, significantly decreasing the success rate of the covert channel. Likewise, this defense also makes CacheTransparency more costly, as more probing prompts are needed to collect the same number of hits for each target. For the poisoning attack, fewer prompts will hit the poisoned prompt in the approximate cache, thus reducing the spread of the attacker’s content.

**Content filter.** Similar to filters in generative models [31, 62, 65, 70, 83] that defend against not-suitable-for-work (NSFW) content, filters can also be specific to removing the attacker’s content from the approximate cache. For example, to prevent the poisoning attack in this work, the service provider can incorporate a logo filter that detects logo-like objects in the image and potential logo descriptions in the prompt, to make sure both the cached prompts and the generated images do not contain logos.

**Malicious behavior detector.** Stealing prompts from an approximate cache takes a large number of probing prompts as shown in Section 5.4.2. A malicious behavior detector can monitor user’s activities [9, 25, 41, 42, 52, 82]. When a user appears to abuse the generation system, such as flooding the system with prompts, the service provider can slow down or disable the user’s generation.

## 8 Conclusions

Approximate caching improves the performance of diffusion models, but it also introduces significant security risks. We demonstrated three such attacks: a covert channel that transmits messages through the approximate cache, a prompt-stealing attack that reveals cached prompts, and a poisoning attack that embeds the attacker’s content into user’s generations. These findings demonstrate that approximate caching introduces new security vulnerabilities which must be addressed before widespread adoption.

## Acknowledgment

We thank the anonymous reviewers and the shepherd for their valuable feedback. This work is supported by a Discovery

Grant from the Natural Sciences and Engineering Research Council of Canada (NSERC).

## Ethical Considerations

**Decision to Conduct the Research.** Text-to-image diffusion models have been widely studied in academia and extensively used for creative generation in the industry. To alleviate the heavy computation overhead, approximate caching has been proposed and widely studied. There are many industrial deployment guides and academic studies about using approximate caching [2, 4, 60, 76]. The goal of this work is to identify potential risks early and alert the diffusion community and startups, as some startups may simply follow these guides and open-source code, overlooking the security risks.

**Stakeholders.** The attacks we identified pose potential threats to image generation service providers and their users, and prompt providers who design high-quality prompts.

**Impacts.** Our paper identifies the potential risks in approximate caching, especially when such systems are deployed in production for public use: First, an attacker may use the image generation service as a secret channel to transmit secret (and potentially illegal) messages. Second, the prompt provider’s well-designed prompts may be stolen by the attackers. Finally, service users may receive images with undesired patterns/logos, potentially containing attacker-controlled malicious information, in their generated images.

**Mitigation.** We propose three methods to mitigate the vulnerabilities of caching for diffusion models. First, we propose random cache selection techniques to decrease the possibility that the receiver hits the sender’s cached prompt, making approximate cache infeasible as a covert channel. Second, we propose to monitor the user behaviors to detect the potential malicious attackers in advance [9, 25, 41, 42, 52, 82]. This method identifies the probing operation in advance, protecting well-designed prompts by limiting the number of probing prompts, which leads to low-quality recovery for attackers. Finally, we propose to use content filters as in previous studies to filter the output images with unexpected logos [31, 62, 65, 70, 83]. By doing so, the normal users will not receive images with unexpected content in them. We have informed the authors and developers of NIRVANA, our reference system, about the risks and mitigation solutions.

**Attacks on Real Products.** We conducted our experiments in our test systems, as our attacks aim to steal users’ prompts and pollute the cache system of diffusion service. No real-world users are affected by our experiences. The test system, however, strictly follows the same assumptions and implementation of existing publications [2, 60, 76], especially NIRVANA, the caching system developed by Adobe.

## Open Science

Our study adheres to open science principles. We open the code for our implementation of NIRVANA approximate cache from Adobe [2], as well as code for all three attacks at the following link: <https://doi.org/10.5281/zenodo.17957900>. This repository also contains necessary scripts to reproduce the key results.

## References

- [1] Adobe. Create with adobe firefly generative AI. <https://www.adobe.com/products/firefly.html>, 2023.
- [2] Shubham Agarwal, Subrata Mitra, Sarthak Chakraborty, Srikrishna Karanam, Koyel Mukherjee, and Shiv Kumar Saini. Approximate caching for efficiently serving Text-to-Image diffusion models. In *21st USENIX Symposium on Networked Systems Design and Implementation (NSDI 24)*, pages 1173–1189, Santa Clara, CA, April 2024. USENIX Association.
- [3] Andrei Bacs, Saidgani Musaev, Kaveh Razavi, Cristiano Giuffrida, and Herbert Bos. DUPEFS: Leaking data over the network with filesystem deduplication side channels. In *20th USENIX Conference on File and Storage Technologies (FAST 22)*, pages 281–296, Santa Clara, CA, February 2022. USENIX Association.
- [4] Fu Bang. GPTCache: An open-source semantic cache for LLM applications enabling faster answers and cost savings. In Liling Tan, Dmitrijs Milajevs, Geeticka Chauhan, Jeremy Gwinnup, and Elijah Rippeth, editors, *Proceedings of the 3rd Workshop for Natural Language Processing Open Source Software (NLP-OSS 2023)*, pages 212–218, Singapore, December 2023. Association for Computational Linguistics.
- [5] Romain Beaumont. Clip retrieval: Easily compute clip embeddings and build a clip retrieval system with them. <https://github.com/rom1504/clip-retrieval>, 2022.
- [6] Aleksey Bokhovkin, Quan Meng, Shubham Tulsiani, and Angela Dai. SceneFactor: Factored latent 3D diffusion for controllable 3D scene generation. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, pages 628–639, June 2025.
- [7] Haoyu Chen, Xiaojie Xu, Wenbo Li, Jingjing Ren, Tian Ye, Songhua Liu, Ying-Cong Chen, Lei Zhu, and Xinchao Wang. POSTA: A go-to framework for customized artistic poster generation. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, pages 28694–28704, June 2025.
- [8] Jiahao Chen, Yu Pan, Yi Du, Chunkai Wu, and Lin Wang. Parasite: A steganography-based backdoor attack framework for diffusion models, 2025.
- [9] Marco Chiappetta, Erkey Savas, and Cemal Yilmaz. Real time detection of cache-based side-channel attacks using hardware performance counters. *Applied Soft Computing*, 49:1162–1174, 2016.
- [10] Ye Dayong, Zhu Tianqing, He Feng, Liu Bo, Xue Minhui, and Zhou Wanlei. Cross-modal prompt inversion: Unifying threats to text and image generative AI models. In *34th USENIX Security Symposium (USENIX Security 25)*. USENIX Association, July 2025.
- [11] Wenxin Ding, Cathy Y. Li, Shawn Shan, Ben Y. Zhao, and Haitao Zheng. Understanding implosion in text-to-image generative models. In *Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security, CCS ’24*, page 1211–1225, New York, NY, USA, 2024. Association for Computing Machinery.
- [12] Zhenbang Du, Wei Feng, Haohan Wang, Yaoyu Li, Jingsen Wang, Jian Li, Zheng Zhang, Jingjing Lv, Xin Zhu, Junsheng Jin, Junjie Shen, Zhangang Lin, and Jingping Shao. Towards reliable advertising image generation using human feedback. In Aleš Leonardis, Elisa Ricci, Stefan Roth, Olga Russakovsky, Torsten Sattler, and Gül Varol, editors, *Computer Vision – ECCV 2024*, pages 399–415, Cham, 2025. Springer Nature Switzerland.
- [13] Abdelrahman Eldesokey and Peter Wonka. Build-a-scene: Interactive 3d layout control for diffusion-based image generation. In *The Thirteenth International Conference on Learning Representations*, 2025.
- [14] Patrick Esser, Sumith Kulal, Andreas Blattmann, Rahim Entezari, Jonas Müller, Harry Saini, Yam Levi, Dominik Lorenz, Axel Sauer, Frederic Boesel, Dustin Podell, Tim Dockhorn, Zion English, Kyle Lacey, Alex Goodwin, Yannik Marek, and Robin Rombach. Scaling rectified flow transformers for high-resolution image synthesis, 2024.
- [15] Fernando A. Fardo, Victor H. Conforto, Francisco C. de Oliveira, and Paulo S. Rodrigues. A formal evaluation of psnr as quality measurement parameter for image segmentation algorithms, 2016.
- [16] Yifan Gao, Zihang Lin, Chuanbin Liu, Min Zhou, Tiezheng Ge, Bo Zheng, and Hongtao Xie. Postermaker: Towards high-quality product poster generation with accurate text rendering. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, pages 8083–8093, June 2025.



- [17] Waris Gill, Mohamed Elidrisi, Pallavi Kalapatapu, Ammar Ahmed, Ali Anwar, and Muhammad Ali Gulzar. MeanCache: User-centric semantic caching for LLM web services, 2025.
- [18] Chongye Guo, Jinhu Fu, Junfeng Fang, Kun Wang, and Guorui Feng. Redediting: Relationship-driven precise backdoor poisoning on text-to-image diffusion models, 2025.
- [19] Jonathan Ho, Ajay Jain, and Pieter Abbeel. Denoising diffusion probabilistic models. In *Proceedings of the 34th International Conference on Neural Information Processing Systems, NIPS '20*, Red Hook, NY, USA, 2020. Curran Associates Inc.
- [20] Gal Horowitz, Eyal Ronen, and Yuval Yarom. Spec-o-Scope: Cache probing at cache speed. In *Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security, CCS '24*, page 109–123, New York, NY, USA, 2024. Association for Computing Machinery.
- [21] Huayang Huang, Xiangye Jin, Jiaxu Miao, and Yu Wu. Implicit bias injection attacks against text-to-image diffusion models, 2025.
- [22] Zehuan Huang, Yuan-Chen Guo, Xingqiao An, Yunhan Yang, Yangguang Li, Zi-Xin Zou, Ding Liang, Xihui Liu, Yan-Pei Cao, and Lu Sheng. Midi: Multi-instance diffusion for single image to 3d scene generation. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, pages 23646–23657, June 2025.
- [23] Sangwon Jang, June Suk Choi, Jaehyeong Jo, Kimin Lee, and Sung Ju Hwang. Silent branding attack: Trigger-free data poisoning attack on text-to-image diffusion models. *arXiv preprint arXiv:2503.09669*, 2025.
- [24] Tushar M. Jois, Gabrielle Beck, and Gabriel Kaptchuk. Pulsar: Secure steganography for diffusion models. In *Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security, CCS '24*, page 4703–4717, New York, NY, USA, 2024. Association for Computing Machinery.
- [25] Tejal Joshi, Aarya Kawalay, Anvi Jamkhane, and Amit Joshi. Hybrid deep learning model for multiple cache side channel attacks detection: A comparative analysis, 2025.
- [26] Mehmet Kayaalp, Nael Abu-Ghazaleh, Dmitry Ponomarev, and Aamer Jaleel. A high-resolution side-channel attack on last-level cache. In *Proceedings of the 53rd Annual Design Automation Conference, DAC '16*, New York, NY, USA, 2016. Association for Computing Machinery.
- [27] Michael Kurth, Ben Gras, Dennis Andriesse, Cristiano Giuffrida, Herbert Bos, and Kaveh Razavi. NetCAT: Practical cache attacks from the network. In *2020 IEEE Symposium on Security and Privacy (SP)*, pages 20–38, 2020.
- [28] Black Forest Labs. Flux. <https://github.com/black-forest-labs/flux>, 2024.
- [29] Black Forest Labs, Stephen Batifol, Andreas Blattmann, Frederic Boesel, Saksham Consul, Cyril Diagne, Tim Dockhorn, Jack English, Zion English, Patrick Esser, Sumith Kulal, Kyle Lacey, Yam Levi, Cheng Li, Dominik Lorenz, Jonas Müller, Dustin Podell, Robin Rombach, Harry Saini, Axel Sauer, and Luke Smith. Flux.1 kontext: Flow matching for in-context image generation and editing in latent space, 2025.
- [30] Jiaxing Li, Chi Xu, Feng Wang, Isaac M von Riedemann, Cong Zhang, and Jiangchuan Liu. Scalm: Towards semantic caching for automated chat services with large language models, 2024.
- [31] Xinfeng Li, Yuchen Yang, Jiangyi Deng, Chen Yan, Yanjiao Chen, Xiaoyu Ji, and Wenyuan Xu. SafeGen: Mitigating sexually explicit content generation in text-to-image models. In *Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security, CCS '24*, page 4807–4821, New York, NY, USA, 2024. Association for Computing Machinery.
- [32] Fangfei Liu, Yuval Yarom, Qian Ge, Gernot Heiser, and Ruby B. Lee. Last-level cache side-channel attacks are practical. In *2015 IEEE Symposium on Security and Privacy*, pages 605–622, 2015.
- [33] Sihang Liu, Suraaj Kanniwadi, Martin Schwarzl, Andreas Kogler, Daniel Gruss, and Samira Khan. Side-Channel attacks on optane persistent memory. In *32nd USENIX Security Symposium (USENIX Security 23)*, pages 6807–6824, Anaheim, CA, August 2023. USENIX Association.
- [34] Zhibo Liu, Yuanyuan Yuan, Yanzuo Chen, Sihang Hu, Tianxiang Li, and Shuai Wang. Deepcache: Revisiting cache side-channel attacks in deep neural networks executables. In *Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security, CCS '24*, page 4495–4508, New York, NY, USA, 2024. Association for Computing Machinery.
- [35] Jian Ma, Yonglin Deng, Chen Chen, Nanyang Du, Haonan Lu, and Zhenyu Yang. GlyphDraw2: Automatic generation of complex glyph posters with diffusion models and large language models. *Proceedings of the AAAI Conference on Artificial Intelligence*, 39(6):5955–5963, Apr. 2025.

- [36] Lukas Maar, Jonas Juffinger, Thomas Steinbauer, Daniel Gruss, and Stefan Mangard. Kernelsnitch: Side-channel attacks on kernel data structures. In *Network and Distributed System Security Symposium (NDSS) 2025*, February 2025. Network and Distributed System Security Symposium 2025 : NDSS 2025, NDSS 2025 ; Conference date: 23-02-2025 Through 28-02-2025.
- [37] Aqib Mahfuz, Georgia Channing, Mark van der Wilk, Philip Torr, Fabio Pizzati, and Christian Schroeder de Witt. Psyduck: Training-free steganography for latent diffusion, 2025.
- [38] Meta. Introducing Meta Llama 3: The most capable openly available LLM to date. <https://ai.meta.com/blog/meta-llama-3/>, 2024.
- [39] Ramaswami Mohandoss. Context-based semantic caching for llm applications. In *2024 IEEE Conference on Artificial Intelligence (CAI)*, pages 371–376, 2024.
- [40] Ron Mokady, Amir Hertz, and Amit H. Bermano. Clipcap: Clip prefix for image captioning, 2021.
- [41] Maria Mushtaq, Ayaz Akram, Muhammad Khurram Bhatti, Maham Chaudhry, Vianney Lapotre, and Guy Gogniat. NIGHTs-WATCH: a cache-based side-channel intrusion detector using hardware performance counters. In *Proceedings of the 7th International Workshop on Hardware and Architectural Support for Security and Privacy, HASP '18*, New York, NY, USA, 2018. Association for Computing Machinery.
- [42] Maria Mushtaq, Ayaz Akram, Muhammad Khurram Bhatti, Maham Chaudhry, Muneeb Yousaf, Umer Farooq, Vianney Lapotre, and Guy Gogniat. Machine learning for security: The case of side-channel attack detection at run-time. In *2018 25th IEEE International Conference on Electronics, Circuits and Systems (ICECS)*, pages 485–488, 2018.
- [43] Ali Naseh, Jaechul Roh, Eugene Bagdasarian, and Amir Houmansadr. Backdooring bias ( $b^2$ ) into stable diffusion models. In *34nd USENIX Security Symposium (USENIX Security 25)*. USENIX Association, July 2025.
- [44] OpenAI. Dalle 3 system card. [https://cdn.openai.com/papers/\\$DALLE\\_3\\_System\\_Card\\$.pdf](https://cdn.openai.com/papers/$DALLE_3_System_Card$.pdf), 2023.
- [45] Maxime Oquab, Timothée Darcet, Theo Moutakanni, Huy V. Vo, Marc Szafraniec, Vasil Khalidov, Pierre Fernandez, Daniel Haziza, Francisco Massa, Alaaeldin El-Nouby, Russell Howes, Po-Yao Huang, Hu Xu, Vasu Sharma, Shang-Wen Li, Wojciech Galuba, Mike Rabbat, Mido Assran, Nicolas Ballas, Gabriel Synnaeve, Ishan Misra, Herve Jegou, Julien Mairal, Patrick Labatut, Armand Joulin, and Piotr Bojanowski. DINOv2: Learning robust visual features without supervision, 2023.
- [46] Zhuoshi Pan, Yuguang Yao, Gaowen Liu, Bingquan Shen, H. Vicky Zhao, Ramana Rao Kompella, and Sijia Liu. From trojan horses to castle walls: Unveiling bilateral data poisoning effects in diffusion models. In A. Globerson, L. Mackey, D. Belgrave, A. Fan, U. Paquet, J. Tomczak, and C. Zhang, editors, *Advances in Neural Information Processing Systems*, volume 37, pages 82265–82295. Curran Associates, Inc., 2024.
- [47] Yinyin Peng, Yaofei Wang, Donghui Hu, Kejiang Chen, Xianjin Rong, and Weiming Zhang. Ldstega: Practical and robust generative image steganography based on latent diffusion models. In *Proceedings of the 32nd ACM International Conference on Multimedia, MM '24*, page 3001–3009, New York, NY, USA, 2024. Association for Computing Machinery.
- [48] Pinecone. Making stable diffusion faster with intelligent caching. <https://www.pinecone.io/learn/faster-stable-diffusion/>, 2023.
- [49] Alec Radford, Jong Wook Kim, Chris Hallacy, Aditya Ramesh, Gabriel Goh, Sandhini Agarwal, Girish Sastry, Amanda Askell, Pamela Mishkin, Jack Clark, Gretchen Krueger, and Ilya Sutskever. Learning transferable visual models from natural language supervision. In Marina Meila and Tong Zhang, editors, *Proceedings of the 38th International Conference on Machine Learning*, volume 139 of *Proceedings of Machine Learning Research*, pages 8748–8763. PMLR, 18–24 Jul 2021.
- [50] Alec Radford, Jeff Wu, Rewon Child, David Luan, Dario Amodei, and Ilya Sutskever. Language models are unsupervised multitask learners. In *OpenAI*, 2019.
- [51] Runpod. Runpod: The cloud built for AI. <https://www.runpod.io/>, 2025.
- [52] Majid Sabbagh, Yunsi Fei, Thomas Wahl, and A. Adam Ding. SCADET: a side-channel attack detection tool for tracking prime+probe. In *Proceedings of the International Conference on Computer-Aided Design, ICCAD '18*, New York, NY, USA, 2018. Association for Computing Machinery.
- [53] Chitwan Saharia, William Chan, Saurabh Saxena, Lala Li, Jay Whang, Emily L Denton, Kamyar Ghasemipour, Raphael Gontijo Lopes, Burcu Karagol Ayan, Tim Salimans, Jonathan Ho, David J Fleet, and Mohammad Norouzi. Photorealistic text-to-image diffusion models with deep language understanding. In S. Koyejo, S. Mohamed, A. Agarwal, D. Belgrave, K. Cho, and

- A. Oh, editors, *Advances in Neural Information Processing Systems*, volume 35, pages 36479–36494. Curran Associates, Inc., 2022.
- [54] Michael Schwarzl, Martin Schwarzl, Moritz Lipp, Jon Masters, and Daniel Gruss. NetSpectre: Read arbitrary memory over network. In *Computer Security – ESORICS 2019: 24th European Symposium on Research in Computer Security, Luxembourg, September 23–27, 2019, Proceedings, Part I*, page 279–299, Berlin, Heidelberg, 2019. Springer-Verlag.
  - [55] Martin Schwarzl, Erik Kraft, Moritz Lipp, and Daniel Gruss. Remote memory-deduplication attacks. In *29th Annual Network and Distributed System Security Symposium (NDSS)*. The Internet Society, 2022.
  - [56] Shawn Shan, Wenxin Ding, Josephine Passananti, Stanley Wu, Haitao Zheng, and Ben Y. Zhao. Nightshade: Prompt-specific poisoning attacks on text-to-image generative models. In *2024 IEEE Symposium on Security and Privacy (SP)*, pages 807–825, 2024.
  - [57] Shawn Shan, Wenxin Ding, Josephine Passananti, Stanley Wu, Haitao Zheng, and Ben Y. Zhao. Nightshade: Prompt-specific poisoning attacks on text-to-image generative models. In *2024 IEEE Symposium on Security and Privacy (SP)*, pages 807–825, 2024.
  - [58] Xinyue Shen, Yiting Qu, Michael Backes, and Yang Zhang. Prompt stealing attacks against Text-to-Image generation models. In *33rd USENIX Security Symposium (USENIX Security 24)*, pages 5823–5840, Philadelphia, PA, August 2024. USENIX Association.
  - [59] Linke Song, Zixuan Pang, Wenhao Wang, Zihao Wang, XiaoFeng Wang, Hongbo Chen, Wei Song, Yier Jin, Dan Meng, and Rui Hou. The early bird catches the leak: Unveiling timing side channels in llm serving systems. *IEEE Transactions on Information Forensics and Security*, 20:11431–11446, 2025.
  - [60] Desen Sun, Henry Tian, Tim Lu, and Sihang Liu. Flex-cache: Flexible approximate cache system for video diffusion, 2024.
  - [61] Mingze Sun, Junhao Chen, Junting Dong, Yurun Chen, Xinyu Jiang, Shiwei Mao, Puhua Jiang, Jingbo Wang, Bo Dai, and Ruqi Huang. Drive: Diffusion-based rigging empowers generation of versatile and expressive characters. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, pages 21170–21180, June 2025.
  - [62] Zekun Sun, Zijian Liu, Shouling Ji, Chenhao Lin, and Na Ruan. Pretender: Universal active defense against diffusion finetuning attacks. In *The 34th USENIX Security Symposium*, 2025.
  - [63] Yicong Tan, Xinyue Shen, Yun Shen, Michael Backes, and Yang Zhang. On the effectiveness of prompt stealing attacks on in-the-wild prompts. In *2025 IEEE Symposium on Security and Privacy (SP)*, pages 392–410, 2025.
  - [64] Mohammadkazem Taram, Ashish Venkat, and Dean Tullsen. Packet chasing: Spying on network packets over a cache side-channel. In *2020 ACM/IEEE 47th Annual International Symposium on Computer Architecture (ISCA)*, pages 721–734, 2020.
  - [65] Corban Villa, Shujaat Mirza, and Christina Pöpper. Exposing the guardrails: Reverse-engineering and jail-breaking safety filters in dall· e text-to-image pipelines. In *34nd USENIX Security Symposium (USENIX Security 25)*. USENIX Association, July 2025.
  - [66] Junpeng Wan, Yanxiang Bi, Zhe Zhou, and Zhou Li. Meshup: Stateless cache side-channel attack on cpu mesh. In *2022 IEEE Symposium on Security and Privacy (SP)*, pages 1506–1524, 2022.
  - [67] Alan Wang, Boru Chen, Yingchen Wang, Christopher W. Fletcher, Daniel Genkin, David Kohlbrenner, and Riccardo Paccagnella. Peek-a-walk: Leaking secrets via page walk side channels. In *2025 IEEE Symposium on Security and Privacy (SP)*, pages 3534–3548, 2025.
  - [68] Bingyuan Wang, Qifeng Chen, and Zeyu Wang. Diffusion-based visual art creation: A survey and new perspectives. *ACM Comput. Surv.*, 57(10), May 2025.
  - [69] Haonan Wang, Qianli Shen, Yao Tong, Yang Zhang, and Kenji Kawaguchi. The stronger the diffusion model, the easier the backdoor: Data poisoning to induce copyright breaches without adjusting finetuning pipeline. In *Forty-first International Conference on Machine Learning*, 2024.
  - [70] Peiran Wang, Qiyu Li, Longxuan Yu, Ziyao Wang, Ang Li, and Haojian Jin. Moderator: Moderating text-to-image diffusion models through fine-grained context-based policies. In *Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security, CCS ’24*, page 1181–1195, New York, NY, USA, 2024. Association for Computing Machinery.
  - [71] Xiaochen Wang and Yue Wang. Sentence-level resampling for named entity recognition. In Marine Carpuat, Marie-Catherine de Marneffe, and Ivan Vladimir Meza Ruiz, editors, *Proceedings of the 2022 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies*, pages 2151–2165, Seattle, United States, July 2022. Association for Computational Linguistics.

- [72] Xiyu Wang, Yufei Wang, Satoshi Tsutsui, Weisi Lin, Bihan Wen, and Alex Kot. Evolving storytelling: Benchmarks and methods for new character customization with diffusion models. In *Proceedings of the 32nd ACM International Conference on Multimedia, MM '24*, page 3751–3760, New York, NY, USA, 2024. Association for Computing Machinery.
- [73] Zijie J. Wang, Evan Montoya, David Munechika, Haoyang Yang, Benjamin Hoover, and Duen Horng Chau. DiffusionDB: A large-scale prompt gallery dataset for text-to-image generative models. In Anna Rogers, Jordan Boyd-Graber, and Naoaki Okazaki, editors, *Proceedings of the 61st Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers)*, pages 893–911, Toronto, Canada, July 2023. Association for Computational Linguistics.
- [74] Yixin Wu, Ning Yu, Michael Backes, Yun Shen, and Yang Zhang. On the proactive generation of unsafe images from text-to-image models using benign prompts. *arXiv preprint arXiv:2310.16613*, 2023.
- [75] Yurong Wu, Fangwen Mu, Qiuhong Zhang, Jinjing Zhao, Xinrun Xu, Lingrui Mei, Yang Wu, Lin Shi, Junjie Wang, Zhiming Ding, and Yiwei Wang. Vulnerability of text-to-image models to prompt template stealing: A differential evolution approach. In Wanxiang Che, Joyce Nabende, Ekaterina Shutova, and Mohammad Taher Pilehvar, editors, *Findings of the Association for Computational Linguistics: ACL 2025*, pages 16903–16916, Vienna, Austria, July 2025. Association for Computational Linguistics.
- [76] Yuchen Xia, Divyam Sharma, Yichao Yuan, Souvik Kundu, and Nishil Talati. MoDM: Efficient serving for image generation via mixture-of-diffusion models. In *Proceedings of the 31st ACM International Conference on Architectural Support for Programming Languages and Operating Systems, Volume 1 (ASPLOS '26)*, Pittsburgh, PA, USA, March 2026. Association for Computing Machinery.
- [77] Yuanbo Yang, Jiahao Shao, Xinyang Li, Yujun Shen, Andreas Geiger, and Yiyi Liao. Prometheus: 3D-aware latent diffusion models for feed-forward text-to-3D scene generation. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, pages 2857–2869, June 2025.
- [78] Yuval Yarom and Katrina Falkner. FLUSH+RELOAD: A high resolution, low noise, L3 cache side-channel attack. In *23rd USENIX Security Symposium (USENIX Security 14)*, pages 719–732, San Diego, CA, August 2014. USENIX Association.
- [79] Jiwen Yu, Xuanyu Zhang, Youmin Xu, and Jian Zhang. Cross: Diffusion model makes controllable, robust and secure image steganography. In A. Oh, T. Naumann, A. Globerson, K. Saenko, M. Hardt, and S. Levine, editors, *Advances in Neural Information Processing Systems*, volume 36, pages 80730–80743. Curran Associates, Inc., 2023.
- [80] Jiyong Yu, Aishani Dutta, Trent Jaeger, David Kohlbrenner, and Christopher W. Fletcher. Synchronization storage channels (S2C): Timer-less cache Side-Channel attacks on the apple m1 via hardware synchronization instructions. In *32nd USENIX Security Symposium (USENIX Security 23)*, pages 1973–1990, Anaheim, CA, August 2023. USENIX Association.
- [81] Zihao Yu, Haoyang Li, Fangcheng Fu, Xupeng Miao, and Bin Cui. Accelerating text-to-image editing via cache-enabled sparse diffusion inference. *Proceedings of the AAAI Conference on Artificial Intelligence*, 38(15):16605–16613, Mar. 2024.
- [82] Tianwei Zhang, Yinqian Zhang, and Ruby B. Lee. CloudRadar: A real-time side-channel attack detection system in clouds. In Fabian Monrose, Marc Dacier, Gregory Blanc, and Joaquin Garcia-Alfaro, editors, *Research in Attacks, Intrusions, and Defenses*, pages 118–140, Cham, 2016. Springer International Publishing.
- [83] Yuyang Zhang, Jiahui Wen, Yihui Jin, Ziyu Liang, Run Wang, and Lina Wang. USD: NSFW content detection for text-to-image models via scene graph. In *The 34th USENIX Security Symposium*, 2025.
- [84] Xinyao Zheng, Husheng Han, Shangyi Shi, Qiyang Fang, Zidong Du, Xing Hu, and Qi Guo. Inputsntch: Stealing input in LLM services via timing side-channel attacks, 2024.
- [85] Zilliz. Semantic cache for LLMs. fully integrated with LangChain and llama\_index. <https://github.com/zilliztech/GPTCache>, 2023.