

Unlearning Concepts in Diffusion Model via Concept Domain Correction and Concept Preserving Gradient

Yongliang Wu*
yongliang0223@gmail.com
Southeast University

Shiji Zhou*†
zhoushiji00@gmail.com
Tsinghua University

Mingzhuo Yang
118020068@link.cuhk.edu.cn
The Chinese University of Hong Kong, Shenzhen

Liangzhe Wang
wanglianze@gmail.com
Tsinghua University

Wenbo Zhu
wenbo_zhu@berkeley.edu
University of California, Berkeley

Heng Chang
changh17@tsinghua.org.cn
Tsinghua University

Xiao Zhou
xzhou@tsinghua.edu.cn
Tsinghua University

Xu Yang
xuyang_palm@seu.edu.cn
Southeast University

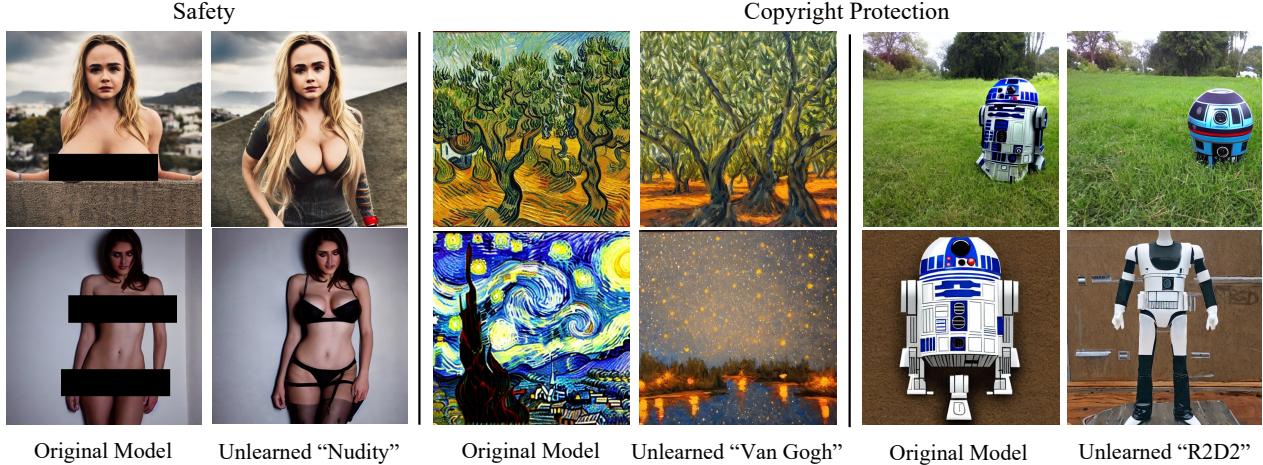


Figure 1: The social impact of incorporating unlearning concepts in diffusion models are significant. Safety: This involves preventing the generation of inappropriate content. Copyright protection: It includes avoiding the replication of styles associated with copyrighted artists and the depiction of specific objects, such as the style of Van Gogh or the R2D2 droid that appears in the "Star Wars" films.

ABSTRACT

Current text-to-image diffusion models have achieved groundbreaking results in image generation tasks. However, the unavoidable inclusion of sensitive information during pre-training introduces

*Both authors contributed equally to this research.

†Corresponding author.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

ACM MM, 2024, Melbourne, Australia

© 2024 Copyright held by the owner/author(s). Publication rights licensed to ACM.

ACM ISBN 978-x-xxxx-xxxx-x/YY/MM

<https://doi.org/10.1145/nnnnnnn.nnnnnnn>

significant risks such as copyright infringement and privacy violations in the generated images. Machine Unlearning (MU) provides an effective way to remove sensitive concepts captured by the model, but has been shown to be a promising approach to addressing these issues. Nonetheless, existing MU methods for concept erasure encounter two primary bottlenecks: 1) generalization issues, where concept erasure is effective only for the data within the unlearn set, and prompts outside the unlearn set often still result in the generation of sensitive concepts; and 2) utility drop, where erasing target concepts significantly degrades the model's performance. To this end, this paper first proposes a concept domain correction framework for unlearning concepts in diffusion models. By aligning the output domains of sensitive concepts and anchor concepts through adversarial training, we enhance the generalizability of the unlearning results. Secondly, we devise a concept-preserving scheme based on gradient surgery. This approach alleviates the

parts of the unlearning gradient that contradict the relearning gradient, ensuring that the process of unlearning minimally disrupts the model's performance. Finally, extensive experiments validate the effectiveness of our model, demonstrating our method's capability to address the challenges of concept unlearning in diffusion models while preserving model utility.

CCS CONCEPTS

- Security and privacy → Social aspects of security and privacy;
- Computing methodologies → Artificial intelligence.

KEYWORDS

Diffusion Model, Machine Unlearning, Gradient Surgery

1 INTRODUCTION

The development of diffusion models for text-to-image synthesis has advanced rapidly, demonstrating a remarkable ability to generate photorealistic images, leading to the creation of applications such as Stable Diffusion [18] and Midjourney [2]. Unfortunately, the pre-training datasets often consist of copyrighted materials, personal photos [3], and unsafe information [21], causing the generative images having copyright, privacy, and safety issues. This situation raises significant risks of sensitive data leakage [25], directly conflicting with the growing legislative emphasis on the "right to be forgotten" [19].

A naive approach is to filter out sensitive information and then retrain the entire model from scratch [17, 18]. However, given that these generative models are typically trained on large-scale datasets [22], this method can be very costly in terms of computing resources. Another strategy involves using a Safety Checker to detect the presence of inappropriate content in generated images [18]. However, this approach relies heavily on the performance of the detector and is limited by its inherent biases.

In response to these challenges, machine unlearning [26] has emerged as a potentially promising solution. Fundamentally, machine unlearning is a method that enables models to forget the memory of sensitive information contained within their training datasets, thus preventing the generation of images involving sensitive concepts through crafted prompts. As illustrated in Figure 1, by applying unlearning operation to text-to-image generative models, we can enhance safety (left, where "Nudity" has been unlearned) and copyright protection (right, by unlearning the "Van Gogh" style and "R2D2" instance). Recently, a series of studies have been introduced focusing on the unlearning of concepts in diffusion models [4, 5, 11, 12, 28]. For example, ConAbl [11] suggests linking a target concept to a predefined anchor concept by minimizing the L2 distance between the predicted noises for these two concepts. ESD [4] fine-tunes the model to predict in the opposite direction of classifier-free guidance, effectively aligning the targeted concept with that of an empty string. SPM [12] employs a Latent Anchor approach to eliminate concepts and uses a similarity-based retention loss to preferentially weight surrogate concepts, thereby preserving non-target concepts.

However, when applying machine unlearning for concept erasure, two primary issues arise. First, there is the challenge of generalizability: how to ensure that a model completely unlearns a target

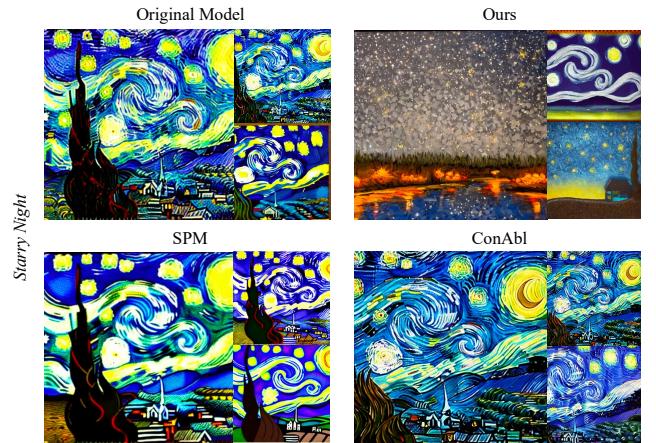


Figure 2: The generalization of implicit content through distribution alignment: after the unlearning of the style of Van Gogh, our method is also capable of erasing the associated prompt of "Starry Night," a case that previous methods fail to accomplish.

concept with only a limited number of training samples. Second, there is the need for concept preservation: ensuring that while forgetting target concepts, the model performance on other concepts remains unaffected. Existing methods have not fully resolved these issues. Specifically, for unlearning generalization, some approaches focus on reducing the distance between sample pairs generated from the target and anchor concepts [11], or minimize the value and key in the cross-attention layers between target text embedding and anchor text embeddings [5], resulting in effectiveness limited to sampled or related prompts and failing to achieve complete concept elimination. As shown in Figure 2, these methods frequently struggle with generalizing to prompts that fall outside their training scope, or to those that are implicitly related, such as "Starry Night," which is among Van Gogh's most renowned works. For concept preservation, some methods [5, 11, 12], incorporate regularization strategies that, while attempting to retain other concepts, overlook the inherent contradiction between unlearning and utility preservation, thus failing to maintain effectiveness.

To address these challenges, we first introduce a concept domain correction framework that employs a discriminator to simulate a membership inference attack (MIA) [23], distinguishing between the output domains of target and anchor concepts. Through adversarial training against MIA, we align these output domains, thereby aiming for the complete elimination of the target concept in a distributional sense. To our knowledge, we are the first to focus on the generalizability of unlearning concepts in text-to-image diffusion models using adversarial training. Through such operations, our methods demonstrate superior generalization performance on the target concept, as illustrated in Figure 2. Remarkably, our approach can even successfully unlearn "Starry Night," achieving this in the absence of any mention of the content within the train set. To tackle the issue of concept preservation, we propose a concept preserving gradient approach that trims conflicting parts of the unlearning gradient with utility regularization, ensuring that each optimization iteration does not compromise the model's utility, thereby

achieving both concept unlearning and preservation. Through comprehensive experiments across a wide range of instances, styles, and offensive concepts, we verify that our method is capable of effectively unlearning targeted concepts while having a minimal impact on closely related surrounding concepts that ought to be preserved.

Our Contributions are summarized as follows: (1) We formulate a concept domain correction framework for unlearning concepts in diffusion models. This is achieved by employing a distribution classifier in an adversarial manner to align the output domains of the to-be-forgotten target concepts with those of the anchor concepts, thereby enhancing the generalizability of the unlearning effect. (2) We propose a concept-preserving gradient surgery method. By trimming the contradictory parts between the unlearning gradient and the retraining gradient, our method strives to optimize the unlearning objectives while minimally affecting the model's performance on other concepts. (3) Extensive experiments show that our method can successfully unlearn specific concepts with minimal effect on related concepts compared to state-of-the-art methods.

2 RELATED WORK

Text-to-image diffusion models [14, 18, 20] have recently demonstrated impressive potential in generating high-quality images, typically trained on large-scale web-crawled datasets like LAION-5B [22]. However, these uncurated datasets are likely to contain harmful or copyrighted content, which could lead the model to generate sensitive or Not Safe For Work (NSFW) content. The existing community has already initiated efforts to address this issue, which can generally be classified into three main categories: dataset filtering, model fine-tuning, and post-generation classification.

Dataset Filtering. Dataset filtering involves excluding specific images from the training dataset. For example, Adobe Firefly uses licensed and public-domain materials to guarantee its suitability for commercial use [17]. In a similar vein, Stable Diffusion v2.0 [18] employs an NSFW filter to eliminate inappropriate content from the LAION-5B dataset. While this approach has demonstrated some level of effectiveness, it presents notable challenges. On one side, it can lead to considerable operational burdens, as it might necessitate retraining the model from scratch. On the other side, the accuracy and inherent biases of these filtering systems can lead to unreliable exclusion of sensitive content. Additionally, detecting abstract copyright elements, such as an artist's unique style, proves challenging for standard detection methods.

Model Fine-tuning. Model fine-tuning method focus on fine-tuning the model's weights to prevent the generation of harmful content. The performance of these methods is typically evaluated based on two critical considerations: the ability to unlearn target concepts and to preserve non-target concepts. ESD [4] proposes the alignment of the probability distributions of the targeted concept with that of a empty string. Nevertheless, this technique may trigger a collapse problem owing to the absence of explicit control over the training dynamics. Forget-Me-Not [28] employs attention re-steering to pinpoint and address attention maps linked to specific concepts within the cross-attention layers of the diffusion U-Net architecture. This approach enables the progressive unlearning of

the selected concept during image synthesis by diminishing the attention weights associated with that concept. However, both of the aforementioned methods lack a mechanism for preserving the integrity of other non-target concepts. UCE [5] employs a closed-form solution for modifying cross-attention weights. This technique recalibrates the attention weights to induce deliberate changes in the keys and values tied to particular text embeddings for a set of concepts to be edited. Simultaneously, it aims to limit the impact on a separate set of concepts that are to be retained. ConAbl [11] suggests associating a target concept with a predefined anchor concept by minimizing the L2 distance between the predicted noises for these two concepts. Additionally, it introduces a regularization loss to preserve the integrity of the anchor concept. However, these approaches do not entirely resolve the tension between the objectives of unlearning and retention, potentially impacting the optimization efficiency of both goals. SPM [12] introduces a novel Latent Anchoring fine-tuning strategy accompanied by a similarity-based retention loss to differentially weight surrogate concepts that are distant in the latent space. While this approach can alleviate the contradictions between two objectives, it does not directly resolve their conflicts. Our method directly employs a gradient surgery technique to manipulate the gradients of the two conflicting objective functions. Furthermore, previous approaches heavily depend on the configuration of the training set, for instance, by forming pairs of anchor and target concepts or directly manipulating concepts, which could lead to a decrease in generalization performance when applied beyond the training scope. In contrast, our method directly modifies the concept at the distribution level, effectively mitigating this issue.

Post-generation Classification. Post-generation classification methods focus on employing a safety checker [18] to analyze images after they have been generated, in order to determine whether any harmful content has been produced. This approach shares a similar drawback with the first category, in that it heavily relies on the performance of the classifier and may be affected by biases, thereby impacting the effectiveness of content filtering. On the other hand, it struggles to adequately protect against copyright-protected content, which requires specially designed and trained detectors and cannot cover all content types.

3 METHOD

In this section, we first briefly review the Diffusion Model in Section 3.1. Then, we define the formulation of the goal for concept unlearning in text-to-image models in Section 3.2. In Section 3.3, we present our adversarial training framework for concept domain correction. Finally, in Section 3.4, we introduce a concept preserving gradient strategy designed to address the conflicts between unlearning and retraining objectives.

3.1 Diffusion Models

Diffusion Models consist of two distinct Markov chains: the forward chain, which incrementally converts the original data into a noisy state, and the reverse chain, which meticulously reconstructs the original data from this noisy state [10, 24]. In the forward process of diffusion models, noise ϵ is progressively added to the input image across multiple timesteps $t \in [0, T]$. The noisy image at timestep t

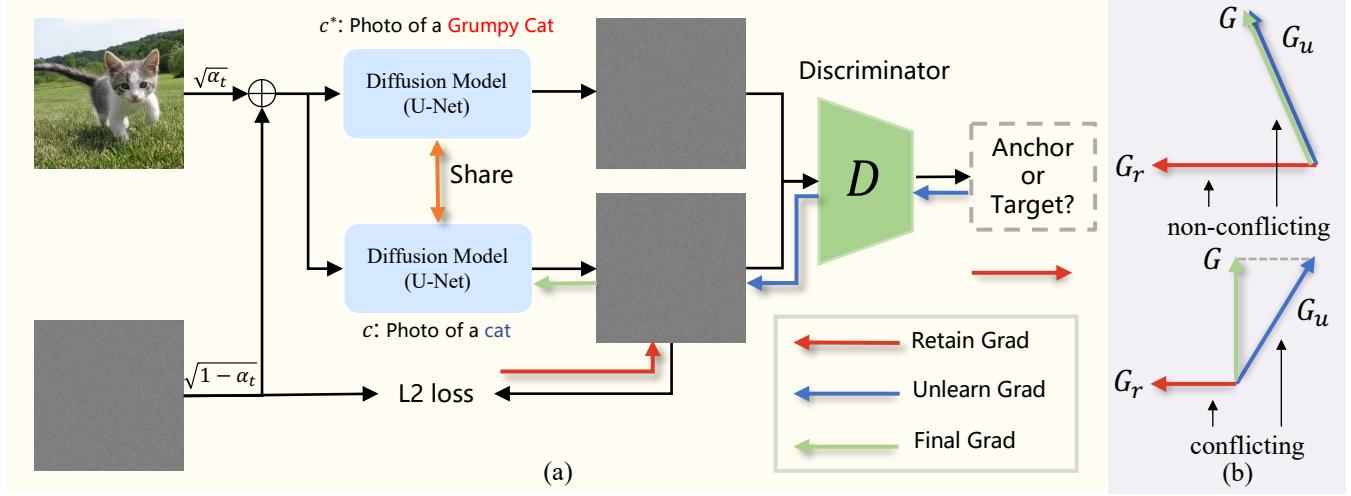


Figure 3: (a) The overall architecture of our proposed method, which updates the parameters of model through an adversarial training process. This process compels the diffusion model (acting as the generator) to predict noise that the discriminator cannot reliably classify as being associated with the target concept, such as "Grumpy Cat", or the anchor concept, such as "Cat". Consequently, this aligns the distributions between the target and anchor concepts. (b) If the unlearning gradient G_u does not conflict with the retraining gradient G_r , we update the parameter in the direction of G_u . if G_u is conflict with G_r , we mitigate the contradictory gradient between them.

can be generated according to the following equation:

$$x_t = \sqrt{\alpha_t}x_0 + \sqrt{1 - \alpha_t}\epsilon, \quad (1)$$

where x_0 represents the original clean image and α_t modulates the noise level.

The denoising network $\epsilon_\theta(x_t, c, t)$ is adeptly trained to reverse the noise addition, reconstructing the image at timestep $t - 1$ from the noisy image at timestep t . This network can also incorporate conditions from other modalities, such as a caption c , to guide the denoising process [18]. This process can be formulated as follows:

$$p_\theta(x_0, \dots, x_T) = p(x_T) \prod_{t=1}^T p_\theta(x_{t-1}|x_t), \quad (2)$$

where $p(x_T)$ is the distribution of the data after adding noise over T timesteps, and $p_\theta(x_{t-1}|x_t)$ represents the conditional probability of recovering the data at the previous timestep $t - 1$ from the noisy data at timestep t , parameterized by θ .

3.2 Concept Unlearning Formulation

Following the definitions provided by previous methods [4, 5, 11], we define concept unlearning as the task of preventing the generation of images associated with a given target concept c^* that need to be unlearned.

We define the process of unlearning concepts as the removal of a specific concept c^* from the pre-trained model M_{init} . Assuming an unlearning algorithm \mathcal{U} that eliminates c^* from M_{init} , the parameters of M_{init} will be altered as a result of this operation. The modified model is denoted as \hat{M} , and the process can be represented by the following formula:

$$\mathcal{U}(M_{init}, c^*) = \hat{M}. \quad (3)$$

Previous methods [4, 11, 12] typically align the target concept c^* explicitly with an anchor concept c (which could also be an empty string), which can be mathematically expressed as:

$$\min_{\hat{M}} dis(\hat{M}(c^*), M_{init}(c)) = 0. \quad (4)$$

Since previous methods optimize the above problem by minimizing the loss between training prompts with target concept c^* and anchor concept c , this strategy often heavily depends on the design of the training prompt and lack the ability to generalize beyond the specific prompt template used during training.

Ideally, we seek to achieve an alignment of distributions rather than minimizing the distance on a specific training prompt template. This unlearning objective can be formulated as:

$$\min_{\hat{M}} dis(P(\hat{M}(c^*)), P(M_{init}(c))). \quad (5)$$

At the same time, we wish to maintain the distribution of the original anchor and other unrelated concepts unchanged, so the following retaining objective should be satisfied:

$$P(\hat{M}(c)) \sim P(M_{init}(c)). \quad (6)$$

Therefore, Equation 5 can also be approximated as:

$$dis(P(\hat{M}(c^*)), P(\hat{M}(c))) \approx 0. \quad (7)$$

We assume that an ideal unlearning algorithm for diffusion models should satisfy the aforementioned Equation 5 and 7 at same time.

3.3 Concept Domain Correction

To address the first optimization objective outlined in Equation 5, which is focused on unlearning the target concept, we propose a Concept Domain Correction framework based on adversarial



Figure 4: Visualization examples of single instance concept unlearning. The prompts for image generation are displayed on the left, with the concept targeted for unlearning indicated at the top. It is observable that our method, after effectively unlearning a specific instance, maintains a good preservation of the other concepts.

training [7]. The goal is to align the target concept domain to the anchor concept domain.

An intuitive idea is to fine-tune the pre-trained diffusion model $\hat{M} = M_{init}$, which can be considered as a *generator*, and to train a *discriminator* D alternately until the *discriminator* can no longer distinguish the difference between $\hat{M}(c)$ and $\hat{M}(c^*)$.

However, the Markov chain nature of Diffusion Models makes direct manipulation of the generated images quite challenging, and existing diffusion models typically perform denoising operations in the latent space to reduce the complexity of the noise prediction process [18]. Therefore, we propose to align the noise distribution directly within the latent space. By adopting this approach, the task of the Discriminator shifts from assessing the "authenticity" of images [7] to determining the source text condition of the currently predicted noise.

As shown in Figure 3 (a), assuming we have a target concept c^* that we wish to unlearn and an anchor target c . We can generate samples x by drawing from the distribution $p(x|c)$, where x represents an image generated by the pre-trained diffusion model M_{init} , utilizing the anchor target c as condition. Following this, the noised sample $\{x_i\}_{i=0}^t$ is obtained by applying the process outlined in Equation 1.

The denoising network, represented as ϵ_θ , is tasked with estimating the noise at a specific timestep t , conditioned on two distinct conceptual concept conditions, c^* and c . We then construct a discriminator, denoted as D , to simulate a membership inference attack (MIA) [25], with the goal of distinguishing between the noise distributions associated with these two types of concepts. The parameters of the denoising network are fine-tuned to ensure that the discriminator cannot discern which concept the noise is conditioned on at any

given diffusion step t . We iteratively update the parameters of both the generator and the discriminator. Thus, the training process can be formulated as a min-max game objective:

$$\min_{\epsilon_\theta} \max_D V(\epsilon_\theta, D) = \mathbb{E}_{x \sim p(x|c)} [\log(D(\epsilon_\theta(x_t, c, t)))] + \mathbb{E}_{x \sim p(x|c)} [\log(1 - D(\epsilon_\theta(x_t, c^*, t)))]. \quad (8)$$

Theoretically, the framework of adversarial training ensures alignment between the target concept domain and the anchor concept domain [6], a process we describe as concept domain correction. Since this alignment is achieved at the domain level without directly manipulating the target and anchor concepts, it is anticipated that the generalization capability of concept unlearning will exceed that of prior approaches.

3.4 Concept Preserving Gradient

Ensuring the retention of non-target concepts after a specific concept has been unlearned is a crucial evaluation metric for unlearning methods [4, 11, 13]. This forms the second optimization objective, as illustrated in Equation 6.

Previous methods concentrate on utilizing a relearning strategy, which involves adding the standard diffusion loss to anchor concepts or creating a preservation set to ensure retention [5, 11]. Although this approach has been proven partly feasible, due to the similarity between the anchor and target concepts, it can lead to a conflict between the objectives of unlearning and retaining, thereby impacting the efficiency of the learning process. Thus, SPM [12] proposes a strategy to assigning different weights to the retain losses for various preserved concepts, based on their CLIP similarity with target concept [16]. Nonetheless, this method still does not address the training dynamics to balance the dual objectives of unlearning and retaining in a explicit manner.

In our method, we adopt an effective and efficient gradient surgery paradigm [27, 29] to directly mitigate the gradient conflicts between the unlearning objective and the retaining objective. As illustrated in Figure 3 (b), we formally define the gradients of the unlearning and retaining objectives as G_u and G_r , respectively. The training process presents two distinct cases: (1) If the angle between G_u and G_r is less than 90° , this signifies that the direction of optimization for the unlearning loss aligns with that of the retaining objective. In this case, we adjust the updated gradient direction G to align with G_u . (2) On the other hand, if the angle surpasses 90° , this signifies a conflict between the unlearning loss and the objective of retaining. In such cases, optimizing in the direction of G_u would interfere the original utility of non-target concepts. To address this, we project G_u onto the orthogonal direction of G_r for optimization, effectively resolving the gradient conflict and preventing interference with the retaining goal. This concept preserving gradient approach can be succinctly expressed through mathematical formulation as follows:

$$G = \begin{cases} G_u, & \text{if } G_u \cdot G_r \geq 0 \\ G_u - \lambda \cdot \frac{G_u \cdot G_r}{\|G_r\|^2} G_r, & \text{otherwise.} \end{cases} \quad (9)$$

Where λ is a hyper-parameter used to control the extent of gradient surgery, which we set to a default value of 1 during training.

Through the approach described above, the conflict part of the unlearning gradient will be eliminated. Hence, the optimization

Table 1: Quantitative Evaluation of Instance Concepts Unlearning. The top-performing results are highlighted in bold, and the second-best results are underlined. Our method achieves a favorable trade-off between the unlearning and retraining objectives.

	Snoopy			Mickey			Spongebob			Pikachu		
	CS	CA	FID	CS	CA	FID	CS	CA	FID	CS	CA	FID
SD v1.4	74.29	93.01	-	72.07	93.25	-	72.80	90.38	-	72.48	94.76	-
<i>Erasing Snoopy</i>												
	CS↓	CA↓	FID↑	CS↑	CA↑	FID↓	CS↑	CA↑	FID↓	CS↓	CA↑	FID↓
ESD	45.12	15.62	<u>179.04</u>	52.79	30.62	141.35	56.15	38.62	132.60	64.76	73.12	71.70
ConAbl	63.47	74.87	88.79	69.23	83.37	51.77	70.12	86.37	58.08	70.14	83.62	61.97
SPM	55.15	40.25	110.22	71.63	92.12	26.45	72.53	81.00	31.22	72.27	94.75	18.53
Ours	49.29	36.00	209.92	<u>69.86</u>	<u>84.00</u>	<u>48.17</u>	<u>70.52</u>	<u>82.00</u>	<u>56.55</u>	<u>70.75</u>	<u>86.75</u>	<u>52.27</u>
<i>Erasing Snoopy and Mickey</i>												
	CS↓	CA↓	FID↑	CS↓	CA↓	FID↑	CS↑	CA↑	FID↓	CS↑	CA↑	FID↓
ESD	44.30	47.12	195.93	43.66	27.25	208.22	51.12	8.75	168.84	56.39	47.37	120.42
ConAbl	61.64	71.25	106.92	62.29	63.87	106.27	69.78	80.37	69.00	70.83	86.12	57.61
SPM	54.75	39.50	111.07	54.00	<u>28.87</u>	129.97	72.10	88.37	37.81	71.92	94.50	26.99
Ours	47.72	37.25	221.98	<u>55.02</u>	35.75	<u>203.27</u>	<u>69.97</u>	<u>81.25</u>	<u>61.36</u>	69.91	<u>87.50</u>	<u>53.23</u>
<i>Erasing Snoopy, Mickey and Spongebob</i>												
	CS↓	CA↓	FID↑	CS↓	CA↓	FID↑	CS↓	CA↓	FID↑	CS↓	CA↑	FID↓
ESD	43.50	41.00	<u>211.12</u>	43.50	28.75	216.38	41.16	12.37	228.74	47.01	20.50	169.28
ConAbl	61.42	69.87	107.11	62.12	63.75	106.01	68.47	78.62	61.14	68.64	<u>89.62</u>	61.37
SPM	54.61	40.50	112.33	54.12	<u>29.75</u>	128.80	52.36	<u>23.12</u>	152.16	71.72	<u>93.37</u>	<u>30.28</u>
Ours	48.33	<u>34.75</u>	<u>206.20</u>	<u>54.03</u>	30.50	<u>201.79</u>	<u>51.63</u>	30.75	<u>197.38</u>	69.38	81.50	<u>55.87</u>

direction will not impair the utility of model, then we can efficiently unlearn concepts while avoiding damage to other content.

4 EXPERIMENTS

4.1 Implement Details

Training. We train our model for 1,000 iterations, using a batch size of 8 and a learning rate of 4e-6. During the initial 200 iterations, we employ a warm-up strategy that updates only the parameters of the discriminator to prevent an overly strong generator from diminishing its learning performance. The optimization is conducted using the Adam optimizer. For the discriminator, we utilize a PatchGAN architecture [30], which is composed of 5 convolutional layers. Each layer employs 4×4 convolutional kernels with a stride of 2. All experiments are carried out on two A100 GPUs, with the implementation of the code in the PyTorch framework.

Style. We utilize generic painting styles as a anchor concept during the process of removing a style. Initially, clip-retrieval [1] is employed to acquire a collection of text prompts $\{c\}$ that are proximate to the term “painting” in the CLIP latent space. Subsequently, 1000 images are generated using 200 prompts from the original model. The suffix “in the style of {target style}” is appended to $\{c\}$ to derive the target prompts $\{c^*\}$.

Instance. We employ ChatGPT [15] to create 200 prompts $\{c\}$ containing the anchor concept, such as “Dog”. Following a similar process to the style pipeline, we generate 1000 images using the pre-trained diffusion model and obtain the target text prompts $\{c^*\}$ by substituting the word “Dog” with “Snoopy”.

4.2 Evaluation metrics

To evaluate the unlearning performance of our model, we utilize the CLIP Score (CS), CLIP Accuracy (CA), and the Fréchet Inception Distance (FID) [8, 9, 11]. The CLIP Score calculates the similarity between the image generated and the given prompt. CLIP Accuracy is determined by performing a binary classification to distinguish

Table 2: Quantitative Evaluation of Artistic Style Unlearning.
Our method demonstrates superior performance in unlearning the target style while preserving the non-target style generation.

	Van Gogh		Picasso		Rembrandt		Andy Warhol		Caravaggio	
	CS	FID	CS	FID	CS	FID	CS	FID	CS	FID
SD v1.4	74.31	-	69.67	-	72.46	-	69.09	-	72.60	-
<i>Erasing Van Gogh</i>										
	CS↓	FID↑	CS↑	FID↓	CS↑	FID↓	CS↑	FID↓	CS↑	FID↓
ESD	50.64	195.76	63.48	94.88	65.10	93.35	61.63	124.43	65.18	90.54
ConAbl	54.60	180.47	62.83	95.93	65.96	87.54	65.46	101.18	64.54	91.22
SPM	51.80	198.65	68.96	35.39	70.53	56.12	70.45	60.71	72.06	62.20
Ours	49.58	223.88	65.67	73.65	71.06	63.58	65.82	107.00	69.97	83.39
<i>Erasing Picasso</i>										
	CS↑	FID↓	CS↓	FID↑	CS↑	FID↓	CS↑	FID↓	CS↑	FID↓
ESD	67.65	94.43	57.45	170.59	69.00	81.24	60.88	126.48	68.64	85.80
ConAbl	66.70	119.26	55.45	210.29	69.85	82.06	62.30	133.67	65.32	96.24
SPM	73.55	43.70	49.22	269.58	71.22	53.89	70.52	62.73	71.98	61.70
Ours	71.89	52.53	52.73	311.34	72.85	42.38	68.59	75.65	72.18	57.71
<i>Erasing Rembrandt</i>										
	CS↑	FID↓	CS↑	FID↓	CS↓	FID↑	CS↑	FID↓	CS↑	FID↓
ESD	64.83	95.26	66.14	66.74	34.48	220.91	64.46	98.32	57.60	118.70
ConAbl	65.02	101.18	65.81	62.75	53.53	133.64	66.66	89.04	57.88	118.35
SPM	73.13	46.89	69.26	34.26	32.69	275.29	70.66	58.68	70.31	68.65
Ours	71.76	56.16	67.30	70.68	43.01	241.49	70.53	56.54	69.07	85.86

between the concept that has been unlearned and the anchor concept, analyzing their respective distances in the latent space in relation to the prompt. The FID assesses the divergence between the distribution of images generated post-unlearning and the distribution from the original model. We utilize 80 templates proposed in CLIP [16] as prompts for evaluation.

4.3 Main Results

Removal of Single Instance. To illustrate the effectiveness of our approach in unlearning specific instances, we employ several iconic subjects as examples, similar to those previously utilized in other studies [11, 12]. These subjects include "Grumpy Cat", "Snoopy", "Mickey Mouse", "R2-D2", and "SpongeBob".

As shown in Figure 4, our method successfully removes the targeted concept from the generated content without compromising the coherence or integrity of other elements within the scene. This capability extends to scenarios where input prompts are expanded into complex and detailed descriptions. The method ensures that while the specific target concept is eliminated, other described elements and scene characteristics in the prompt remain intact and unaffected.

To further quantify the effectiveness of our method in comparison to previous methods, we employ the concept of "Snoopy" as an example to provide quantitative experimental results for our method's efficacy. Similar to prior approach [12], in order to demonstrate the proficiency of our method in preserving non-target concepts while simultaneously unlearning concept, we utilize the dictionary of the CLIP text tokenizer to identify concepts that exhibit the highest level of relatedness, as determined by cosine similarity. Specifically, we select the concepts with the strongest connections: "Mickey", "SpongeBob", and "Pikachu". As illustrated in Table 1, the results indicate that ESD stands out for its superior unlearning capabilities, yet it underperforms in preserving non-target concepts. This limitation is likely due to its unrestricted training approach,

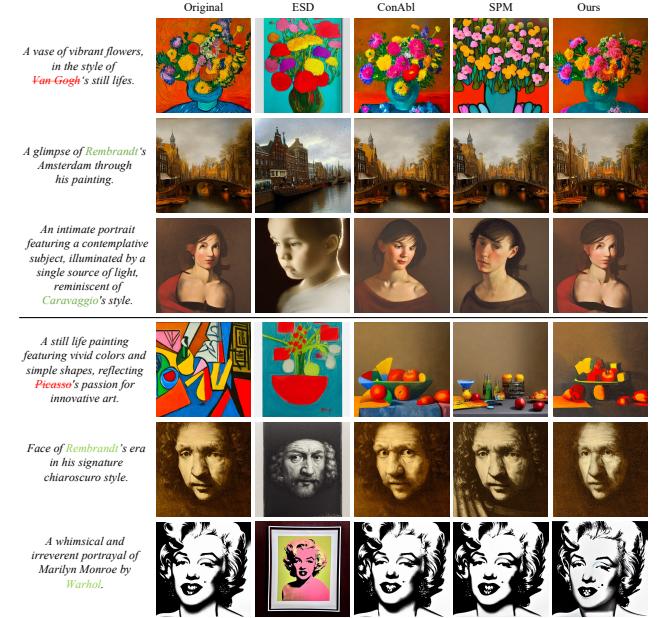


Figure 5: Visualization examples of artistic styles unlearning.
Upper: "Van Gogh". lower: "Picasso". Our approach demonstrates the unlearning of the target concept while maintaining the integrity of other non-target concepts.

which unintentionally compromises the integrity of these non-target concepts. SPM, on the other hand, excels in maintaining non-target concepts but is less effective in unlearning compared to our methods. ConAbl shows moderate performance, which can be attributed to its straightforward implementation of the L2 loss, creating a tension between unlearning and retaining objectives. In contrast, our method strikes a more balanced compromise between these two critical aspects.

Removal of Multiple Instances. In practical applications, the ability to unlearn multiple target concepts holds significant importance. Building upon the single instance removal experiment, we extend our methodology to include the unlearning of two additional concepts, as shown in Table 1. As we increase the number of concepts to be unlearned, the impact on non-target concepts by the ESD method becomes markedly pronounced, revealing its inadequacy in effectively meeting the objective of selective retraining. In contrast, methods such as ConAbl, SPM, and our own, demonstrate the ability to preserve commendable performance on other unrelated concepts, even as the number of concepts to be forgotten grows. Echoing the conclusion from single concept removal, our approach directly tackles the inherent conflict between retaining knowledge and facilitating unlearning, thereby delivering superior performance in both dimensions.

Removal of Styles. To validate the performance of our model in unlearning styles, we choose several representative artists including "Van Gogh", "Picasso", "Rembrandt", "Andy Warhol", and "Caravaggio", and focus on unlearning the styles of the first three. As detailed in Table 2, we provide the numerical outcomes using

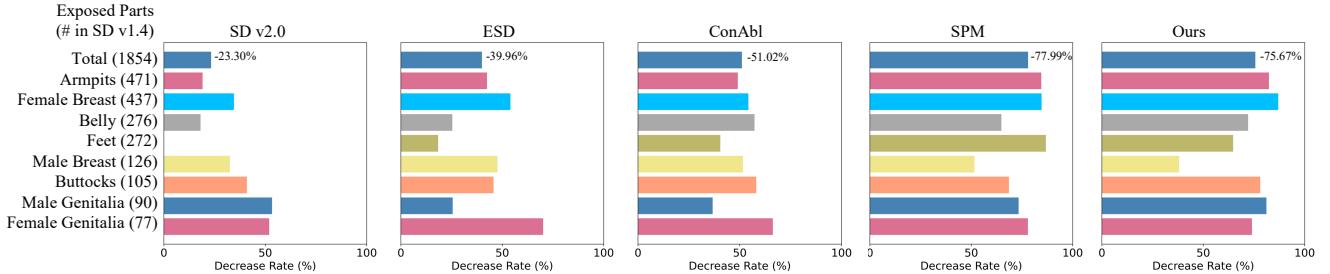


Figure 6: The I2P benchmark results using NudeNet Detection. We use the generations produced by Stable Diffusion v1.4 as baseline. The bin plots illustrate the reduction in explicit content through various unlearning methods for the nudity concept. Our approach demonstrates superior performance, effectively purging explicit content across a spectrum of exposed body categories compared to previous methods.

Table 3: Ablation study on assessing the impact of L2 loss (L2) versus concept preserving gradient (CP).

L2 CP	Snoopy			Mickey			Spongebob			Pikachu		
	CS ↓	CA ↓	FID ↑	CS ↑	CA ↑	FID ↓	CS ↑	CA ↑	FID ↓	CS ↑	CA ↑	FID ↓
SD v1.4	74.29	93.01	-	72.07	93.25	-	72.80	90.38	-	72.48	94.76	-
	52.27	31.50	146.53	66.96	77.25	107.59	69.43	81.50	85.19	72.90	90.00	64.03
✓	56.68	60.25	187.30	70.25	92.00	47.54	71.16	86.75	45.55	72.55	90.25	56.26
✓ ✓	49.29	36.00	209.92	69.86	84.00	48.17	70.52	82.00	56.55	70.75	86.75	52.27

the CS and FID metrics for the target style concept as well as for other non-target style concepts.

Based on the data presented in the table, it can be deduced that our approach effectively accomplishes unlearning across the three distinct styles, as demonstrated by the reduction in CS and the elevation in FID scores for the specified target styles. Moreover, our method continues to exhibit strong performance on artistic styles that are not targeted for unlearning, maintaining high CS values and low FID scores. This suggests that our method is capable of selectively unlearning the learned patterns associated with the target style while retaining the content integrity of other styles.

To further demonstrate the effectiveness of our method in practical examples compared to previous methods, we showcase several examples as illustrated in Figure 5. We observe that both ESD and SPM exhibit excessive unlearning in the case of Van Gogh, resulting in generated images that lack aesthetic appeal. In contrast, our method produces images that appear more natural and visually coherent. And when it comes to maintaining other styles, ESD consistently underperforms across all cases. Our approach, along with SPM and ConAbl, shows comparable results in the unlearning of Picasso's style. Yet, our approach stands out in its ability to maintain the content of Caravaggio's style after the process of unlearning Van Gogh.

Removal of Inappropriate Content. Avoiding the generation of inappropriate content is a critical application of machine unlearning. We adopt the I2P benchmark [21], which consists of 4,703 risky prompts for evaluation. A lightweight nudity detection model, NudeNet¹, is applied to quantify the number of nude body parts in these generated images.

¹<https://github.com/notAI-tech/NudeNet/tree/v3>

As depicted in Figure 6, retraining methods that filter out inappropriate content, such as SD v2.0, are only able to reduce a portion of the exposed body parts by 23.30%. However, the other two methods, ESD and ConAbl, are capable of achieving more effective unlearning. Our method manages to achieve a total reduction of 75.67%, and although it falls short of the total number reduction achieved by SPM, it holds an advantage in mitigating exposure of sensitive body parts such as the "female breast" and "buttocks".

4.4 Ablation Study

To further demonstrate the effectiveness of the concept-preserving gradient, we use the unlearning of instance concepts as a case study and compare it against a baseline that employs regularization loss (L2 Loss) as well as a baseline without any retaining operations. As shown in Table 3, from the perspective of the unlearning effect, our method, along with methods that do not incorporate any form of retaining loss, demonstrates superior capability in unlearning the desired concept. Conversely, the straightforward use of L2 loss falls short in effectively facilitating the unlearning goal. This observation points to a fundamental clash between the objectives of unlearning and retaining, thereby compromising the efficiency of the unlearning process. From the perspective of retaining, approach that omit any form of retention loss perform the worst, indicating the inefficiency in preserving non-target concepts. The utilization of L2 loss does offer a certain level of retention, yet the enhancement is slight compared to approaches that utilize a concept-preserving gradient. In some instances, the outcomes from using L2 loss are even inferior to those achieved by our method. Thus, the employing of concept-preserving gradients enables effective unlearning while maintaining the utility of the model.

5 CONCLUSION AND LIMITATIONS

This paper aims to address the issues of generalization and utility drop in concept unlearning. Firstly, we introduce an approach based on adversarial training for concept domain correction. This method achieves the purpose of generalized unlearning of the target concept by adjusting the output domains of both the target and anchor concepts. Secondly, we propose a concept-preserving gradient method based on gradient surgery. This method eliminates

the conflicting parts between the unlearning gradient and the retaining gradient, ensuring that the process of unlearning minimally impacts the model's utility. Through extensive experimentation, we have verified the proposed methods. The results conclusively demonstrate our ability to achieve more generalized concept unlearning while maintaining the generative performance of other concepts.

Limitations. The primary limitation of our work lies in our continued reliance on an anchor-based approach as our baseline workflow. This method necessitates a certain amount of time for data preparation, leading to significant computational overhead. A potential avenue for improvement could involve adopting the Latent Anchor method from SPM [12], which presents an optimization or circumvention of this data preparation process. We consider the refinement or avoidance of this preparatory stage an important direction for our future research.

REFERENCES

- [1] Romain Beaumont. 2022. Clip Retrieval: Easily compute clip embeddings and build a clip retrieval system with them. <https://github.com/rom1504/clip-retrieval>.
- [2] Ali Borji. 2022. Generated faces in the wild: Quantitative comparison of stable diffusion, midjourney and dall-e 2. *arXiv preprint arXiv:2210.00586* (2022).
- [3] Nicolas Carlini, Jamie Hayes, Milad Nasr, Matthew Jagielski, Vikash Sehwag, Florian Tramer, Borja Balle, Daphne Ippolito, and Eric Wallace. 2023. Extracting training data from diffusion models. In *32nd USENIX Security Symposium (USENIX Security 23)*. 5253–5270.
- [4] Rohit Gandikota, Joanna Materzyńska, Jaden Fiotto-Kaufman, and David Bau. 2023. Erasing concepts from diffusion models. In *Proceedings of the IEEE/CVF International Conference on Computer Vision*. 2426–2436.
- [5] Rohit Gandikota, Hadas Orgad, Yonatan Belinkov, Joanna Materzyńska, and David Bau. 2024. Unified concept editing in diffusion models. In *Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision*. 5111–5120.
- [6] Yaroslav Ganin, Evgeniya Ustinova, Hana Ajakan, Pascal Germain, Hugo Larochelle, François Laviolette, Mario March, and Victor Lempitsky. 2016. Domain-adversarial training of neural networks. *Journal of machine learning research* 17, 59 (2016), 1–35.
- [7] Ian Goodfellow, Jean Pouget-Abadie, Mehdi Mirza, Bing Xu, David Warde-Farley, Sherjil Ozair, Aaron Courville, and Yoshua Bengio. 2020. Generative adversarial networks. *Commun. ACM* 63, 11 (2020), 139–144.
- [8] Jack Hessel, Ari Holtzman, Maxwell Forbes, Ronan Le Bras, and Yejin Choi. 2021. Clipscore: A reference-free evaluation metric for image captioning. *arXiv preprint arXiv:2104.08718* (2021).
- [9] Martin Heusel, Hubert Ramsauer, Thomas Unterthiner, Bernhard Nessler, and Sepp Hochreiter. 2017. Gans trained by a two time-scale update rule converge to a local nash equilibrium. *Advances in neural information processing systems* 30 (2017).
- [10] Jonathan Ho, Ajay Jain, and Pieter Abbeel. 2020. Denoising diffusion probabilistic models. *Advances in neural information processing systems* 33 (2020), 6840–6851.
- [11] Nupur Kumari, Bingliang Zhang, Sheng-Yu Wang, Eli Shechtman, Richard Zhang, and Jun-Yan Zhu. 2023. Ablating concepts in text-to-image diffusion models. In *Proceedings of the IEEE/CVF International Conference on Computer Vision*. 22691–22702.
- [12] Mengyao Lyu, Yuhong Yang, Haiwen Hong, Hui Chen, Xuan Jin, Yuan He, Hui Xue, Jungong Han, and Guiguang Ding. 2023. One-dimensional Adapter to Rule Them All: Concepts, Diffusion Models and Erasing Applications. *arXiv preprint arXiv:2312.16145* (2023).
- [13] Thanh Tam Nguyen, Thanh Trung Huynh, Phi Le Nguyen, Alan Wee-Chung Liew, Hongzhi Yin, and Quoc Viet Hung Nguyen. 2022. A survey of machine unlearning. *arXiv preprint arXiv:2209.02299* (2022).
- [14] Alexander Quinn Nichol, Prafulla Dhariwal, Aditya Ramesh, Pranav Shyam, Pamela Mishkin, Bob McGrew, Ilya Sutskever, and Mark Chen. 2022. GLIDE: Towards Photorealistic Image Generation and Editing with Text-Guided Diffusion Models. In *International Conference on Machine Learning*. PMLR, 16784–16804.
- [15] OpenAI. 2021. ChatGPT. <https://openai.com/research/chatgpt>.
- [16] Alec Radford, Jong Wook Kim, Chris Hallacy, Aditya Ramesh, Gabriel Goh, Sandhini Agarwal, Girish Sastry, Amanda Askell, Pamela Mishkin, Jack Clark, et al. 2021. Learning transferable visual models from natural language supervision. In *International conference on machine learning*. PMLR, 8748–8763.
- [17] Dana Rao. 2023. Responsible Innovation in the Age of Generative AI. Blog post.
- [18] Robin Rombach, Andreas Blattmann, Dominik Lorenz, Patrick Esser, and Björn Ommer. 2022. High-resolution image synthesis with latent diffusion models. In *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*. 10684–10695.
- [19] Jeffrey Rosen. 2011. The right to be forgotten. *Stan. L. Rev. Online* 64 (2011), 88.
- [20] Chitwan Saharia, William Chan, Saurabh Saxena, Lala Li, Jay Whang, Emily L Denton, Kamyar Ghasemipour, Raphael Gontijo Lopes, Burcu Karagol Ayan, Tim Salimans, et al. 2022. Photorealistic text-to-image diffusion models with deep language understanding. *Advances in neural information processing systems* 35 (2022), 36479–36494.
- [21] Patrick Schramowski, Manuel Brack, Björn Deiseroth, and Kristian Kersting. 2023. Safe latent diffusion: Mitigating inappropriate degeneration in diffusion models. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*. 22522–22531.
- [22] Christoph Schuhmann, Romain Beaumont, Richard Vencu, Cade Gordon, Ross Wightman, Mehdi Cherti, Theo Coombes, Aarush Katta, Clayton Mullis, Mitchell Wortsman, et al. 2022. Laion-5b: An open large-scale dataset for training next generation image-text models. *Advances in Neural Information Processing Systems* 35 (2022), 25278–25294.
- [23] Reza Shokri, Marco Stronati, Congzheng Song, and Vitaly Shmatikov. 2017. Membership inference attacks against machine learning models. In *2017 IEEE symposium on security and privacy (SP)*. IEEE, 3–18.
- [24] Jiaming Song, Chenlin Meng, and Stefano Ermon. 2020. Denoising Diffusion Implicit Models. In *International Conference on Learning Representations*.
- [25] Yixin Wu, Ning Yu, Zheng Li, Michael Backes, and Yang Zhang. 2022. Membership inference attacks against text-to-image generation models. *arXiv preprint arXiv:2210.00968* (2022).
- [26] Heng Xu, Tianqiang Zhu, Lefeng Zhang, Wanlei Zhou, and Philip S Yu. 2023. Machine unlearning: A survey. *Comput. Surveys* 56, 1 (2023), 1–36.
- [27] Tianhe Yu, Saurabh Kumar, Abhishek Gupta, Sergey Levine, Karol Hausman, and Chelsea Finn. 2020. Gradient surgery for multi-task learning. *Advances in Neural Information Processing Systems* 33 (2020), 5824–5836.
- [28] Eric Zhang, Kai Wang, Xingqian Xu, Zhangyang Wang, and Humphrey Shi. 2023. Forget-me-not: Learning to forget in text-to-image diffusion models. *arXiv preprint arXiv:2303.17591* (2023).
- [29] Beier Zhu, Yulei Niu, Yucheng Han, Yue Wu, and Hanwang Zhang. 2023. Prompt-aligned gradient for prompt tuning. In *Proceedings of the IEEE/CVF International Conference on Computer Vision*. 15659–15669.
- [30] Jun-Yan Zhu, Taesung Park, Phillip Isola, and Alexei A Efros. 2017. Unpaired image-to-image translation using cycle-consistent adversarial networks. In *Proceedings of the IEEE international conference on computer vision*. 2223–2232.

Supplementary Materials: Unlearning Concepts in Diffusion Model via Concept Domain Correction and Concept Preserving Gradient

We organize the supplemental materials as follows. In Section 1, we present the user study results on style unlearning comparison. In Section 2, we showcase the visual comparison results for the elimination of multiple concepts. In Section 3, we demonstrate the visual outcomes under various preservation strategies.

1 USER STUDY OF STYLE UNLEARNING

To evaluate how effectively the style unlearning process is perceived by humans, we conduct a user study. We utilize Google Image Search to identify the highest-ranked works of each artist and collected the four most representative paintings by those artists. For each artist, we formulate five generic text prompts intended to evoke the artist's style. These prompts are as follows: "An image in the style of [artist]", "Art by [artist]", "A famous painting of [artist]", "A reproduction of the famous art of [artist]", and "An artwork reflecting the influence of [artist]". Using three different seeds for each prompt, we generate images for testing. We first showcase the real paintings that were collected earlier, followed by asking participants to evaluate, on a five-point Likert scale, the extent to which the style of the generated images matches that of the collected images. Our study involves a total of 21 participants, resulting in 225 responses per participant.

In Figure 1, we observe that the original Stable Diffusion model exhibited the highest similarity. The other four unlearning methods have all been proven effective. Compared to these, the elimination by ConAbl is the weakest, with an average score of 2.38, while the method by SPM is the strongest, reaching 1.76. Our approach achieves a score of 1.79, closely trailing behind the SPM method. Although our numerical performance does not exceed that of SPM, as illustrated in Figures 4, 5, and 6, the SPM method consistently produces disorganized outputs that are challenging to interpret. This inconsistency is observed across various artistic styles. Meanwhile, the methods by ESD and ConAbl still occasionally reveal outcomes retaining the artist's style. In contrast, our method yields more natural and effective results in unlearning.

2 VISUALIZATION OF MULTIPLE CONCEPT UNLEARNING

We provide visual results for the unlearning of multiple concepts as shown in 2. On the left, we display the case of Mickey before and after unlearning. Compared to other methods, ESD exhibits the most significant change after unlearning Snoopy, with our method maintaining the best consistency. However, after proceeding to unlearn Mickey in the second step, both ESD and ConAbl still display Mickey in the images. We attribute this to the use of overly long and complex prompt phrases, which further validates our previous analysis that it relies on the design of prompt templates in the training set and lacks effective generalization and transferability, leading to suboptimal results. Finally, upon further unlearning SpongeBob, our method and SPM show no changes, whereas ESD

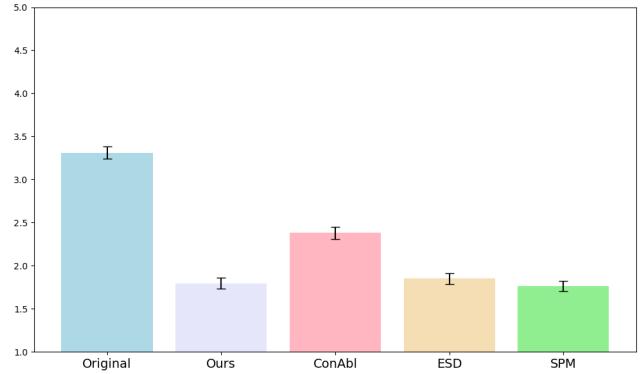


Figure 1: User study evaluations indicate that our approach is capable of effectively unlearning the targeted style concept, delivering results that are on par with the latest state-of-the-art methods.

is further impacted. On the right, we present an example of an image, Pikachu, that undergoes a process of unlearning. With each step of unlearning, ESD is significantly affected, eventually rendering Pikachu unrecognizable. In contrast, the impact on the other three methods is minimal, with ConAbl performing the best which is attributed to the use of L2 loss as regularization. Compared to SPM, our method demonstrates better preservation of color and maintains the visual style (realistic style) more effectively.

3 VISUALIZATION OF CONCEPT PRESERVATION GRADIENT

We visualize some cases comparing a baseline without any preservation loss to a baseline using L2 loss, as illustrated in Figure 3. It is evident that the method without any preservation loss performs best in terms of unlearning, completely removing the concept of Snoopy. On the other hand, the method employing L2 loss, while also partially unlearning Snoopy, still allows for the discernment of Snoopy's features in the images. Our approach not only forgets Snoopy but also preserves the other elements of the scene described in the prompt. In terms of preserving other concepts, our method achieves near-optimal performance across all examples. For instance, in the R2D2 case, our method successfully maintains the position of the foot. In the Mickey Mouse case, the method without preservation performs the worst, with L2 loss being slightly better. In the Pikachu example, neither method excels at preservation, but L2 loss manages to retain some of the yellow color of Pikachu's ears. In the case of Grumpy Cat, while the main instance is retained in both, our method excels in preserving background elements and the cat's posture.

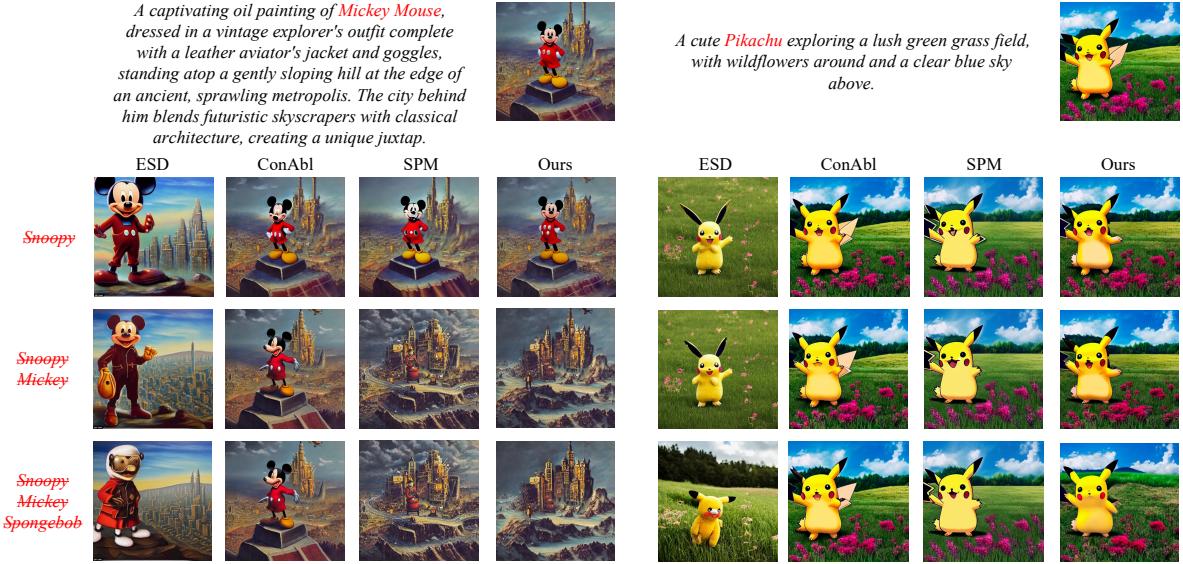


Figure 2: The visualization results of multiple concepts unlearning. Our approach demonstrates optimal performance, both in terms of retaining concepts not targeted for unlearning after the targeted concept has been forgotten, and in not affecting previously unlearned concepts when subsequently unlearning other concepts.

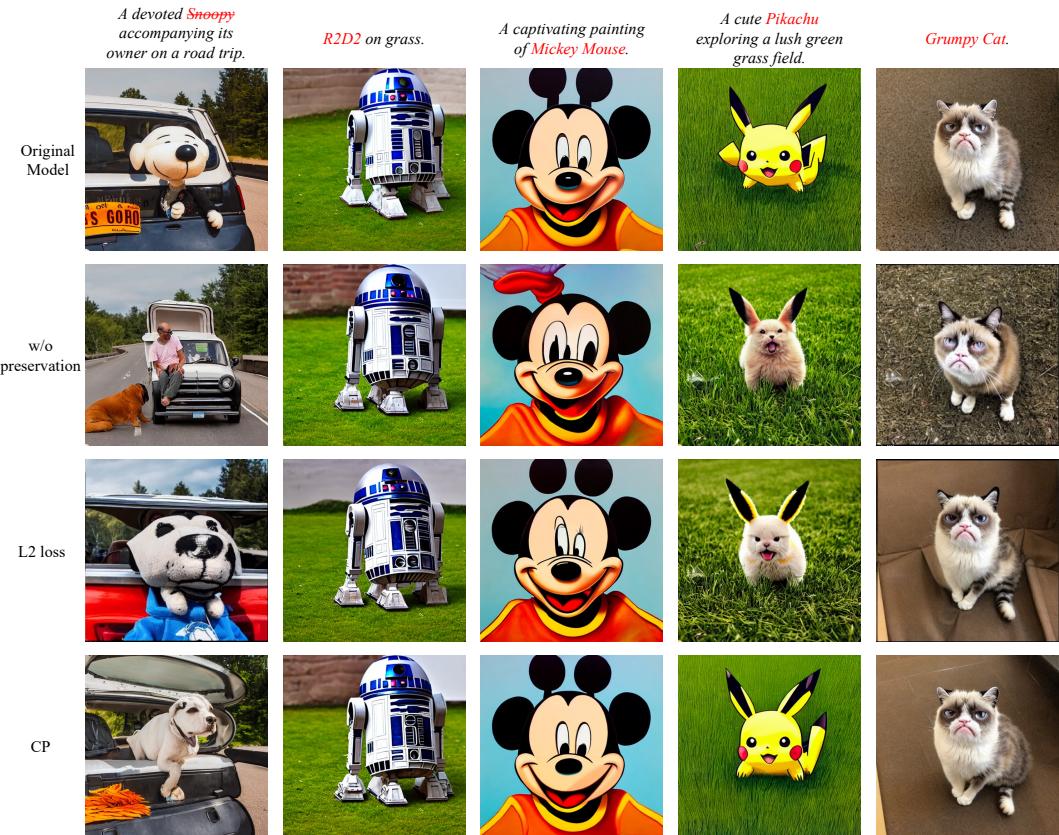


Figure 3: Visual results Compared to without any preservation loss (w/o preservation) and those utilizing an L2 loss, our method (Concept Preservation Gradient, CP) achieves an optimal trade-off between unlearning and maintaining.

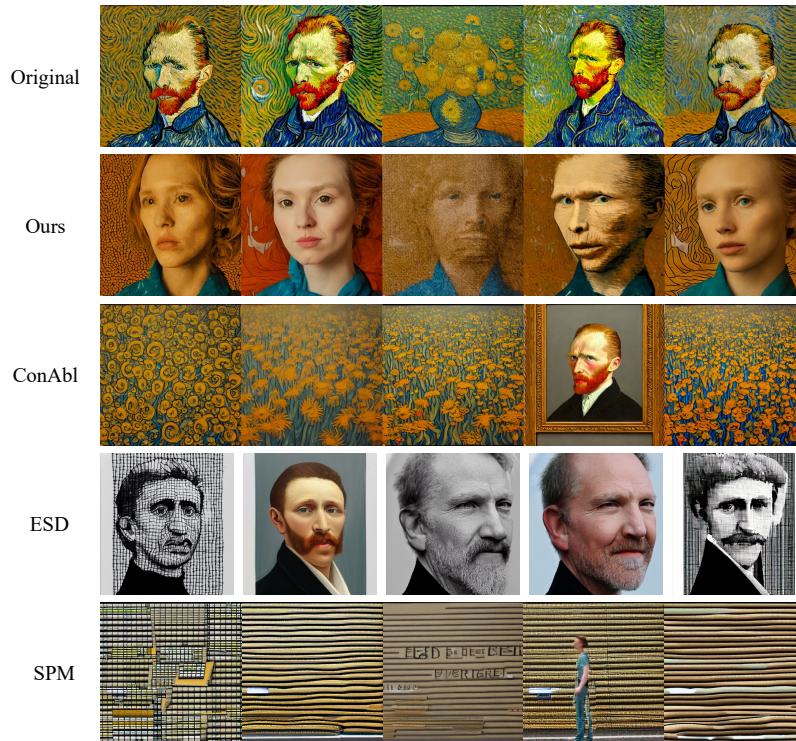


Figure 4: Additional Visualization Results of Unlearning Van Gogh Style.

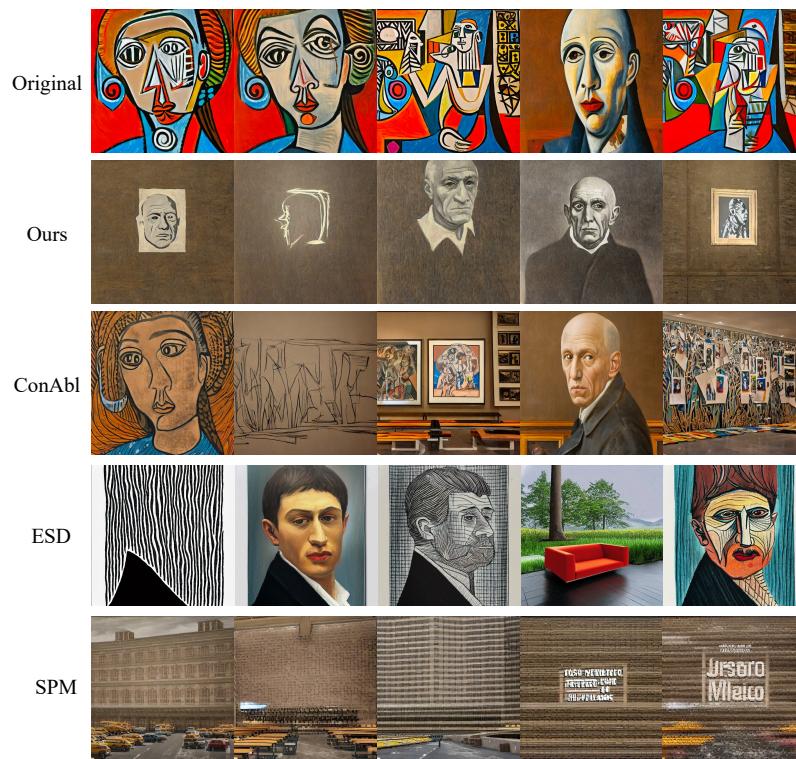


Figure 5: Additional Visualization Results of Unlearning Picasso Style.

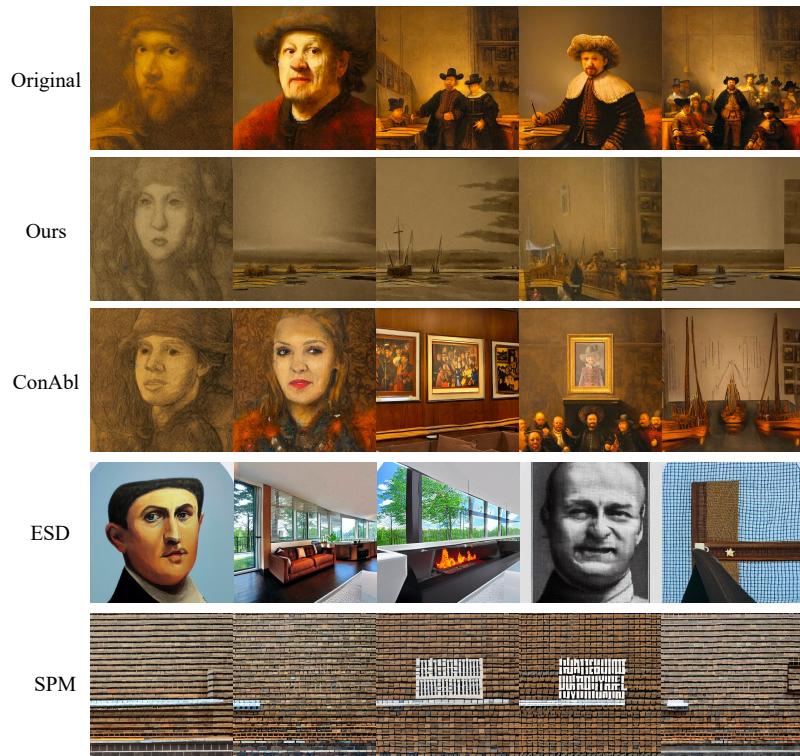


Figure 6: Additional Visualization Results of Unlearning Rembrandt Style.