

Towards Highly Transferable Vision-Language Attack via Semantic-Augmented Dynamic Contrastive Interaction

Yuanbo Li¹, Tianyang Xu¹, Cong Hu¹, Tao Zhou¹, Xiao-Jun Wu^{1*}, Josef Kittler²

¹School of Artificial Intelligence and Computer Science, Jiangnan University

²Centre for Vision, Speech and Signal Processing (CVSSP), University of Surrey

liyuanbo12138@163.com, {tianyang.xu, conghu, taozhou.ai, wu_xiaojun}@jiangnan.edu.cn
 j.kittler@surrey.ac.uk

Abstract

With the rapid advancement and widespread application of vision-language pre-training (VLP) models, their vulnerability to adversarial attacks has become a critical concern. In general, the adversarial examples can typically be designed to exhibit transferable power, attacking not only different models but also across diverse tasks. However, existing attacks on language-vision models mainly rely on static cross-modal interactions and focus solely on disrupting positive image-text pairs, resulting in limited cross-modal disruption and poor transferability. To address this issue, we propose a Semantic-Augmented Dynamic Contrastive Attack (SADCA) that enhances adversarial transferability through progressive and semantically guided perturbation. SADCA progressively disrupts cross-modal alignment through dynamic interactions between adversarial images and texts. This is accomplished by SADCA establishing a contrastive learning mechanism involving adversarial, positive and negative samples, to reinforce the semantic inconsistency of the obtained perturbations. Moreover, we empirically find that input transformations commonly used in traditional transfer-based attacks also benefit VLPs, which motivates a semantic augmentation module that increases the diversity and generalization of adversarial examples. Extensive experiments on multiple datasets and models demonstrate that SADCA significantly improves adversarial transferability and consistently surpasses state-of-the-art methods. The code is released at <https://github.com/LiYuanBoJNU/SADCA>.

1. Introduction

Vision-language pre-training (VLP) models learn cross-modal semantic correlations through joint training on large-scale image-text pairs, providing superior feature represen-

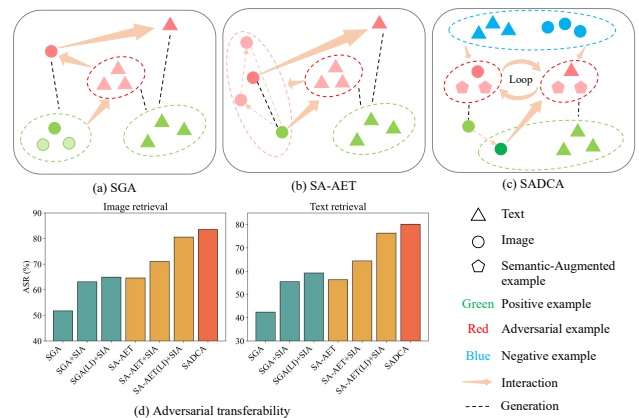


Figure 1. A comparison of our SADCA and existing frameworks. (a) and (b) illustrate the core concepts of SGA [18] and SA-AET [7], respectively, where only one or two static interactions are performed between the visual and textual modalities, with the interactions being limited solely to positive pairs. (c) illustrates the core idea of the proposed SADCA, which continuously disrupts cross-modal interactions through dynamic contrastive interactions with both positive and negative pairs. Additionally, it leverages a semantic augmentation strategy to enrich the data samples, thereby diversifying the semantic information. The arrow represents the interaction between the visual and textual modalities. The dotted lines represent the generation of adversarial examples from the original examples. (d) demonstrates the effectiveness of the input transformation [30] in enhancing the adversarial attack transferability. Furthermore, we observe that using large number of iterations (LI) to attack the image modality can further improve the attack performance.

tations and significantly enhancing performance across various tasks, such as image-text retrieval (ITR) [6, 8], image captioning (IC) [5, 39], and visual grounding (VG) [31, 41]. However, their robustness and reliability are of increasing concern, as numerous studies have demonstrated that VLP models are highly susceptible to adversarial attacks [9, 17,

*Corresponding Author

21, 35, 40, 43]. Investigating the generation of adversarial examples to attack VLP models is instrumental to the design of more robust VLP architectures, thus ensuring a secure deployment of foundational models.

Previous studies have primarily focused on generating adversarial examples for VLP models in white-box settings [40], where the attacker has access to internal model information such as parameters. However, in real-world scenarios, obtaining such detailed information is often infeasible, which limits the practicality of white-box attacks. This limitation has motivated increasing attention toward transfer-based attacks, which craft adversarial examples using known surrogate models and then transfer them to attack unseen black-box targets [32]. Several approaches have achieved certain success in improving the adversarial transferability to VLP models, such as SGA [18], DRA [2], and SA-AET [7]. Nevertheless, these approaches rely on static cross-modal interactions, generating adversarial examples solely from the original image-text pair, where the interaction between modalities occurs only once or twice. Such a design causes the generated adversarial examples to deviate from the semantic center along a fixed direction, lacking the ability to explore diverse directions within the semantic space. As a result, these methods struggle to disrupt the visual-textual alignment, which limits their generalization, as well as the cross-model transferability of the generated adversarial examples. Moreover, existing attacks typically involve only positive image-text pairs, neglecting the role of negative samples in shaping the semantic decision boundary. This one-sided optimization produces only a repulsive force that pushes examples away from their original semantic cluster but does not provide the complementary attractive force needed to pull them across semantic boundaries. Consequently, the adversarial examples remain inadequately separated from benign samples in the embedding space, thereby weakening their transferability. The reliance on static cross-modal interactions, coupled with the neglect of negative samples, significantly limits the transferability of existing vision-language adversarial attacks, as shown in Figure 1(a), (b), and (d).

Additionally, much like the efforts to enhance the generalization ability of deep neural networks (DNNs), increasing data diversity plays a crucial role in improving adversarial transferability [45]. Input transformations, as an effective strategy for enhancing data diversity, have been extensively studied and proven to improve the transferability of adversarial examples in traditional attack settings [27, 30] significantly. However, existing vision-language attacks largely overlook the importance of input transformations, often considering only limited scale-invariance within the image modality [18]. This lack of comprehensive data augmentation results in insufficient input diversity, thereby hindering the ability to achieve strong adversarial transferabil-

ity.

In this paper, to achieve highly transferable vision-language attacks, we propose a novel Semantic-Augmented Dynamic Contrastive Attack (SADCA) to improve the transferability of adversarial examples. Specifically, as illustrated in Figure 1(c), SADCA introduces a dynamic contrastive interaction mechanism that iteratively disrupts cross-modal semantic consistency by alternately updating adversarial images and texts. Simultaneously, it incorporates a contrastive learning strategy that maximizes similarity with negative samples while minimizing the alignment with positive samples. This effectively breaks the semantic matching relationships between images and texts, enhancing the capability of adversarial examples to be semantically misleading and improving their transferability. In addition, as shown in Figure 1(d), we empirically investigate the effectiveness of integrating existing input transformation strategies into vision-language attacks, and, in addition, propose a semantic augmentation module. This module performs local semantic enhancement on images and mixed semantic augmentation on texts to broaden the set of semantic views encountered during optimization. The resulting diversity yields richer semantic gradients and reduces overfitting to a single view, which together improve the generalization and cross-model transferability of the generated adversarial examples. Extensive experiments on multiple datasets and VLP models show that SADCA consistently outperforms state-of-the-art (SOTA) methods in adversarial transferability. Our contributions can be summarized as follows:

- We propose SADCA, a novel highly transferable vision-language attack method that iteratively disrupt image-text semantic consistency and amplify cross-modal misalignment by dynamic contrastive interaction.
- SADCA further introduces a semantic augmentation module to diversify the semantic information of adversarial examples, obtaining richer semantic gradients to further enhance adversarial transferability.
- Experimental results show that SADCA consistently outperforms SOTA approaches in cross-model and cross-task adversarial transferability.

2. Related Work

2.1. Vision-Language Pre-training Models

Vision-Language Pretraining (VLP) models are a class of multimodal learning frameworks designed to jointly model visual and textual modalities [1, 11, 24, 25, 28]. Their primary objective is to perform pretraining on large-scale image-text pair datasets to learn generalizable cross-modal representations, which can be effectively transferred to a variety of downstream tasks. Based on their architectural design, VLP models can be broadly classified into fusion-

based and alignment-based models. Fusion-based models (e.g., ALBEF [10], TCL [37]) typically use separate unimodal encoders to independently extract textual token embeddings and visual features. These are subsequently fused by a multimodal encoder to generate unified semantic representations. In contrast, alignment-based models (e.g., CLIP [22]) adopt two independent unimodal encoders for images and texts, aligning their embeddings within a shared semantic space through contrastive learning.

2.2. Transferable Adversarial Attacks

Transferable adversarial attacks [13, 14, 23, 34] aim to generate adversarial examples on a white-box (source) model that can successfully mislead an unseen black-box (target) model. Due to their black-box nature, such attacks are more applicable in real-world scenarios and are considered more valuable for research than white-box attacks. Input transformation is a widely adopted technique in image recognition to enhance the transferability of adversarial examples, with many methods having been proposed, such as Admix [29], SIA [30], and BSR [27]. Recently, studies have begun exploring transferable adversarial attacks in VLP models [3, 4, 26, 32, 42]. SGA [18] improves the transferability of multimodal adversarial examples by expanding a single image-text pair into a diverse set, thereby increasing adversarial diversity. DRA [2] exploits the intersection area of adversarial trajectories during optimization to enrich adversarial diversity and reduce the risk of overfitting. Furthermore, SA-AET [7] refines adversarial trajectories and generates adversarial examples in a contrastive space of semantic image-text features. However, these methods are constrained by static cross-modal interactions and the absence of guidance from negative pairs, making it difficult to fully disrupt the cross-modal alignment of adversarial examples. Additionally, their limited use of input transformations increases the risk of model overfitting and reduces the transferability of adversarial examples.

3. Methodology

3.1. Notations and Preliminaries

Let (v, t) denote the benign image-text pair extracted from a multimodal dataset D . For VLP model, the $F_I(\cdot)$ and $F_T(\cdot)$ represent the image encoder and text encoder, respectively. Vision-language attacks typically induce a semantic mismatch between the adversarial image and its corresponding adversarial text, while adhering to predefined perturbation constraints in both the visual and textual domains. Given a paired image and text input, the objective is to introduce subtle adversarial perturbations to both modalities such that the semantic similarity between the image and its associated text is significantly reduced. To achieve this, multimodal adversarial examples are generated by minimizing a feature

similarity loss function:

$$\begin{cases} \min J(F_I(v'), F_T(t')) \\ \text{s.t. } v' \in B[v, \epsilon_v], t' \in B[t, \epsilon_t] \end{cases} \quad (1)$$

where v' and t' denote the adversarial image-text pair within the image and text search spaces $B[v, \epsilon_v]$ and $B[t, \epsilon_t]$, ϵ_v and ϵ_t represent the maximum perturbation budgets for the image and text modalities, respectively. In this paper, we adopt cosine similarity $Cos(v', t') = \frac{F_I(v') \cdot F_T(t')}{\|F_I(v')\| \cdot \|F_T(t')\|}$ to measure the feature similarity of image-text pairs. For the adversarial image v' , the added perturbation should preserve visual similarity to the benign image v under the given constraints. For the adversarial text t' , modifications are made to the words in the benign text t without altering the original semantic meaning as perceived by humans.

3.2. SADCA

Despite recent progress in vision-language adversarial attacks, existing methods exhibit fundamental limitations that hinder transferability. They rely on static cross-modal interactions, generating adversarial examples in fixed semantic directions, and focus mainly on positive samples, neglecting negative samples that shape semantic boundaries. Consequently, adversarial examples experience limited separation from benign examples. Moreover, input diversity and data augmentation are underutilized, restricting coverage of the semantic space. These limitations motivate a more dynamic, contrastive, and semantically aware attack framework. To address this, we propose SADCA that aligns a benign image with multiple textual descriptions to obtain a semantically centered representation, then uses both positive and negative pairs in an iterative contrastive framework to induce continuous semantic misalignment. By pushing samples away from the semantic center and pulling them across negative samples, SADCA generates adversarial examples that are semantically more divergent and highly transferable across diverse VLP models and tasks.

Dynamic Contrastive Interaction. Since image feature embeddings often contain a substantial amount of information that is irrelevant to the corresponding text features, this redundant information can distort similarity computations and cause misalignment between visual and textual representations [7]. Using such biased original image-text pairs as positive samples directly may prevent adversarial examples from being displaced from the correct semantic center, thereby limiting their transferability. To address this, we first align the benign image and text representations within the semantic space to obtain a semantically centered aligned image, which is then used as the positive sample for subsequent image-text interactions. Specifically, we maximize the feature similarity between the benign image and the be-

nign text to obtain a semantically centered positive image:

$$v_p = \arg \max_{v_p \in B[v, \epsilon_v]} \sum_{m=1}^M \text{Cos}(v, t_m), \quad (2)$$

where $t_m \in T = \{t_1, t_2, \dots, t_M\}$ is the text caption paired with the benign image, and T represents the set of multiple text captions associated with the benign image. By aligning with multiple text features in the semantic space, a positive image v_p representation, that is closer to the semantic center, can be obtained. For the positive text set, the benign text set T is directly used as the positive text set $T_p = \{t_{p1}, t_{p2}, \dots, t_{pM}\}$.

For the selection of negative samples, we randomly choose K mismatched samples from the dataset to construct the negative image set $V_n = \{v_{n1}, v_{n2}, \dots, v_{nK}\}$ and the negative text set $T_n = \{t_{n1}, t_{n2}, \dots, t_{nK}\}$.

Leveraging the constructed positive and negative pairs, our objective is to guide the semantic deviation of adversarial examples away from the benign semantic center through a contrastive learning framework. By minimizing the similarity between adversarial examples and positive samples, while maximizing their similarity with negative samples in the semantic embedding space, we induce semantic-level shifts and ambiguity in the adversarial perturbations. This strategy enhances cross-modal adversarial transferability. Specifically, we minimize the feature similarity between adversarial samples and positive pairs while maximizing the feature similarity with negative pairs:

$$\min_{v'_i} \mathcal{L}(v'_i, T_p, T_n) = \sum_{m=1}^M \text{Cos}(v'_i, t_{pm}) - \lambda \sum_{k=1}^K \text{Cos}(v'_i, t_{nk}) \quad (3)$$

$$\min_{t'_i} \mathcal{L}(t'_i, v_p, V_n) = \text{Cos}(v_p, t'_i) - \lambda \sum_{k=1}^K \text{Cos}(v_{nk}, t'_i) \quad (4)$$

where v'_i and t'_i denote the adversarial image and adversarial text at the i -th iteration, λ is the weighting factor that controls the influence of negative samples in the guidance process, $\mathcal{L}(v'_i, T_p, T_n)$ and $\mathcal{L}(t'_i, v_p, V_n)$ denote the loss functions to optimize the adversarial image v'_i and the adversarial text t'_i , respectively.

Moreover, to thoroughly disrupt the cross-modal interactions of adversarial examples, we adopt a dynamic interaction mechanism that continuously perceives and disrupts the semantic alignment between adversarial images and texts during the attack process. Specifically, we minimize the feature similarity between the current adversarial image and adversarial text throughout the iterative process, thereby progressively weakening their semantic consistency:

$$\min_{v'_i} \mathcal{L}(v'_i, T'_i, T_n) = \sum_{m=1}^M \text{Cos}(v'_i, t'_{im}) - \lambda \sum_{k=1}^K \text{Cos}(v'_i, t_{nk}) \quad (5)$$

Algorithm 1 SADCA

Input: Image encoder F_I , Text encoder F_T , Dataset D , Image-text pair $\{v, t\}$, number of paired text M , iteration steps of adversarial image generation J , step size α , momentum factor μ , dynamic interaction steps I , number of negative samples K , weighting factor of negative samples λ , semantic augmentation number S .

Output: Adversarial image v' and adversarial text t' .

```

1: Build text set  $T = \{t_1, t_2, \dots, t_M\} \leftarrow D$ 
2: Build negative image set  $V_n$  and negative text set  $T_n$ 
3:  $v_p = \arg \max \sum_{m=1}^M \text{Cos}(v, t_m)$ 
4:  $v'_0 = v, T'_0 = T, g_0 = 0$ 
5: for  $i = 0$  to  $I - 1$  do
6:    $\mathcal{L}_t = \mathcal{L}(t'_{im}, v'_i, I_n) + \mathcal{L}(t'_{im}, v_p, I_n)$ 
7:    $T'_{i+1} = \{t'_{(i+1)m}\}_{m=1}^M = \arg \min \mathcal{L}_t$ 
8:   for  $j = 0$  to  $J - 1$  do
9:     Generate  $V'_{sa}$  from  $v'_{ij}$  by Eq. (7)
10:    Generate  $T'_{sa}$  from  $T'_{i+1}$  by Eq. (8)
11:     $\mathcal{L}_v = \mathcal{L}(V'_{sa}, T_p, T_n) + \mathcal{L}(V'_{sa}, T'_{sa}, T_n)$ 
12:     $g_{i(j+1)} = \mu \cdot g_{ij} + \frac{\nabla \mathcal{L}_v}{\|\nabla \mathcal{L}_v\|}$ 
13:     $v'_{i(j+1)} = \text{clip}_{v, \epsilon_v}(v'_{ij} + \alpha \cdot \text{sign}(g_{i(j+1)}))$ 
14:   end for
15: end for
16: return  $v' = v'_{IJ}, t' = t'_I$ 

```

$$\min_{t'_i} \mathcal{L}(t'_i, v'_i, V_n) = \text{Cos}(v'_i, t'_i) - \lambda \sum_{k=1}^K \text{Cos}(v_{nk}, t'_i) \quad (6)$$

where v'_i and t'_i denote the adversarial image and adversarial text at the i -th iteration.

The dynamic contrastive interaction operates on the current adversarial image and text at each iteration, meaning that the semantic representations of both modalities are continuously updated and the resulting gradient directions change accordingly. In each round of interaction, the degree of repulsion from positive samples and attraction toward negative samples is recalibrated, based on the latest semantic states, causing the adversarial examples to exhibit continuous semantic drift in the semantic space and to explore a broader range of potential attack directions. This iterative, dynamic adjustment not only enhances gradient diversity but also substantially improves transferability across models and tasks.

Semantic Augmentation Module. Although input transformation strategies originally developed for traditional image-based adversarial attacks have proven effective in improving the generalization of vision-language attacks, they primarily operate on the perceptual-level image features and overlook the cross-modal semantic alignment mechanisms that are unique to VLP models. As a result, these transformations struggle to disrupt the semantic matching process between image and text, leading to lim-

ited cross-modal transferability and weakened cross-modal attack effectiveness. To address this limitation, we propose the semantic augmentation module, which aims to enhance the diversity of semantic structures in the input, while preserving the semantic consistency of the original image-text labels. This approach enables more effective disruption of the alignment relationships within VLP models.

The semantic augmentation module consists of local semantic image augmentation and mixed semantic text augmentation. Specifically, local semantic image augmentation amplifies local semantic regions within the image, guiding the attack to focus on finer-grained semantic information. Given the adversarial image v' , we construct a set of locally semantic-augmented images V'_{sa} , where each image is generated by randomly cropping and resizing local regions. Additionally, a random image augmentation function $A \in \mathcal{A} = \{Rotate, Brightness, Flip...\}$ is applied to each image, selected from a set of diverse augmentation operations. The local semantic image augmentation process can be formalized as:

$$V'_{sa} = \{A_s(Resize(Crop(v'; r_s)))\}_{s=1}^S, \quad (7)$$

where $r_s \sim \mathcal{U}(0.4, 0.8)$ denotes the ratio factor, representing the area of the cropped region relative to the area of the original image. The mixed semantic text augmentation enhances semantic diversity by combining multiple textual descriptions to form broader semantic representations, thereby promoting inconsistency between image and text features in the semantic space. Specifically, it randomly selects and concatenates pairs of text samples from the adversarial text set T' , resulting in a new augmented text set T'_{sa} :

$$T'_{sa} = \{t_s = Concat(t'_i, t'_j) | t'_i, t'_j \in T', i \neq j\}_{s=1}^S. \quad (8)$$

The semantic augmentation module increases the diversity of semantic representation, while preserving overall semantic consistency, enabling the attack to disrupt cross-modal interactions within a broader semantic space. This helps to mitigate overfitting and enhances the transferability of adversarial examples. The overall procedure of the proposed SADCA is summarized in Algorithm 1.

4. Experiments

4.1. Experimental Setting

Dataset and VLP models. To evaluate the effectiveness of the proposed method, we select two widely used multimodal datasets, Flickr30K [20] and MSCOCO [15], to conduct experiments on the image-text retrieval task. In the cross-task transferability experiments, we use the RefCOCO+ [38] dataset for the visual grounding task and the MSCOCO dataset for the image captioning task. Following [18], we employ two popular types of VLP models:

fusion-based VLP and alignment-based VLP. For fusion-based VLP models, we consider ALBEF [10] and TCL [37]. For alignment-based VLP models, we select CLIP_{VIT} and CLIP_{CNN} [22] for evaluation.

Adversarial attack settings. Following [18], we adopt BERT-Attack [12], setting the text perturbation budget $\epsilon_t = 1$ and using a vocabulary W containing 10 candidate words for the text adversarial attack. For the image adversarial attack, we adopt the l_∞ norm constraint with a perturbation budget of $\epsilon_v = 8/255$. We compare the proposed SADCA with several SOTA methods, including PGD [19], Bert-Attack [12], Co-Attack [40], SGA [18], DRA [2], and SA-AET [7]. For the original versions of these methods, we follow their default settings, configuring the image adversarial attack with an iteration number $J = 10$. Furthermore, we construct enhanced variants of SGA and SA-AET by combining them with the input transformation method SIA [30], resulting in SGA(LI)+SIA and SA-AET(LI)+SIA. These enhanced versions use a larger number of iterations $J = 50$ to match the iteration budget of SADCA. For the proposed SADCA, we set the step size $\alpha = 2/255$, momentum factor $\mu = 1.0$, dynamic interaction iterations $I = 5$, image attack iterations $J = 10$, the number of negative samples $K = 20$, the weighting factor for negative samples $\lambda = 0.2$, and semantic-augmentation number $S = 10$. All experiments are conducted on a single NVIDIA RTX 3090 GPU.

Evaluation metrics. For image-text retrieval task, we use Attack Success Rate (ASR) at Rank-1 (R@1) as the evaluation metric for adversarial transferability. ASR represents the proportion of successfully attacked samples among all generated adversarial examples. A higher ASR indicates a more effective attack with greater transferability. For visual grounding and image captioning tasks, we compare the performance of target models before and after attacks.

4.2. Experimental Results

Cross-model adversarial transferability. We evaluate cross-model transferability on the ITR task using four representative VLP models: ALBEF, TCL, CLIP_{VIT}, and CLIP_{CNN}. Each model serves as the source model to generate adversarial examples, which are then transferred to the other three models. As shown in Table 5, SADCA achieves the highest average ASR in both TR and IR tasks, demonstrating strong generalization across architectures and training paradigms. For instance, when transferring from ALBEF to CLIP_{CNN}, SADCA surpasses SA-AET(LI)+SIA by 9.19% (TR) and 5.7% (IR). Similarly, from CLIP_{CNN} to CLIP_{VIT}, it outperforms the second-best method by 7.61% and 4.89%, respectively. This indicates that the dynamic contrastive interaction and semantic augmentation mechanisms effectively promote semantic divergence, enabling adversarial examples to explore a wider range of attack directions within the semantic space. Additional results on the

Table 1. A comparison of SADCA with SOTA methods on the image-text retrieval (ITR) task using the Flickr30K dataset. The "Source" column indicates the VLP model used to generate the multimodal adversarial examples. For both image retrieval (IR) and text retrieval (TR), we report the ASR (%) at Rank-1 (R@1). The "Average" represents the average ASR on the black-box VLP models.

Source	Attack	ALBEF		TCL		CLIP _{VIT}		CLIP _{CNN}		Average	
		TR R@1	IR R@1	TR R@1	IR R@1	TR R@1	IR R@1	TR R@1	IR R@1	TR R@1	IR R@1
ALBEF	PGD	93.74	94.43	24.03	27.90	10.67	15.82	14.05	19.11	16.25	20.94
	BERT-Attack	11.57	27.46	12.64	28.07	29.33	43.17	32.69	46.11	24.89	39.12
	Co-Attack	97.08	98.36	39.52	51.24	29.82	38.92	31.29	41.99	33.54	44.72
	SGA	99.90	99.93	87.88	88.05	36.69	46.78	39.59	49.78	54.72	61.54
	SGA(LI)+SIA	100	100	99.37	99.02	49.82	56.19	54.79	60.99	67.99	72.07
	DRA	99.90	99.93	91.57	91.36	46.26	56.80	49.55	59.01	62.46	69.06
	SA-AET	99.90	99.98	96.42	96.02	55.58	63.89	57.22	65.59	69.74	75.17
	SA-AET(LI)+SIA	100	100	99.58	99.38	75.71	78.58	76.25	80.41	83.85	86.12
	SADCA (ours)	100	100	98.52	97.83	81.10	82.83	85.44	86.11	88.35	88.92
TCL	PGD	35.77	41.67	99.37	99.33	10.18	16.30	14.81	21.10	20.25	26.36
	BERT-Attack	11.89	26.82	14.54	29.17	29.69	43.36	33.46	46.07	25.01	38.75
	Co-Attack	49.84	60.36	91.68	93.65	32.64	42.69	32.06	47.82	38.18	50.29
	SGA	92.40	92.77	100	100	36.81	46.97	41.89	51.53	57.70	63.76
	SGA(LI)+SIA	99.90	99.70	100	100	52.87	59.12	62.45	65.49	71.74	74.77
	DRA	95.20	95.58	100	100	47.24	57.28	52.23	62.23	64.89	71.70
	SA-AET	98.85	98.50	100	100	56.20	63.47	59.77	67.86	71.61	76.61
	SA-AET(LI)+SIA	99.95	99.93	100	100	77.04	81.48	80.20	84.05	85.73	88.49
	SADCA (ours)	99.58	99.56	100	100	78.28	83.18	86.46	88.71	88.11	90.48
CLIP _{VIT}	PGD	3.13	6.48	4.43	8.83	69.33	84.79	13.03	17.43	6.86	10.91
	BERT-Attack	9.59	22.64	11.80	25.07	28.34	39.00	30.40	37.43	17.26	28.38
	Co-Attack	8.55	20.18	10.01	21.29	78.53	87.50	29.50	38.49	16.02	26.65
	SGA	22.42	34.59	25.08	36.45	100	100	53.26	61.10	33.59	44.05
	SGA(LI)+SIA	54.33	60.20	57.43	62.60	100	100	89.02	89.24	66.93	70.68
	DRA	27.84	42.84	27.82	44.60	100	100	64.88	69.50	40.18	52.31
	SA-AET	36.60	50.44	39.20	51.10	100	100	71.01	74.10	48.94	58.55
	SA-AET(LI)+SIA	79.04	82.74	79.35	82.57	100	99.97	94.76	95.23	84.38	86.85
	SADCA (ours)	87.07	89.20	87.04	87.98	100	100	97.90	97.46	90.68	91.55
CLIP _{CNN}	PGD	2.29	6.15	4.53	8.88	5.40	12.08	89.78	93.04	4.07	9.04
	BERT-Attack	9.86	23.27	12.33	25.48	27.12	37.44	30.40	40.10	16.44	28.73
	Co-Attack	10.53	23.62	12.54	26.05	27.24	40.62	95.91	96.50	16.77	30.10
	SGA	15.64	28.06	18.02	33.07	39.92	51.45	99.87	99.90	24.53	37.53
	SGA(LI)+SIA	20.96	32.72	22.55	37.21	47.24	56.70	100	100	30.25	42.21
	DRA	19.50	34.59	21.60	37.88	48.47	59.12	99.87	99.90	29.86	43.86
	SA-AET	23.98	38.28	27.29	41.81	54.11	64.21	100	99.97	35.13	48.10
	SA-AET(LI)+SIA	38.69	51.80	44.89	56.33	69.57	74.68	100	100	51.05	60.94
	SADCA (ours)	49.43	60.55	55.53	63.19	77.18	79.57	100	100	60.71	67.77

MSCOCO dataset are provided in the supplementary material.

Cross-task adversarial transferability. In addition to evaluating the transferability of multimodal adversarial examples across different VLP models, we also conduct experiments to assess the effectiveness of the proposed SADCA in transferring across different vision-and-language (V+L) tasks. Specifically, we generate adversarial examples from the ITR task and evaluate their impact on the VG and IC tasks. For IC task, we use the ALBEF model pretrained on the ITR task to generate adversarial images.

These adversarial images are then fed into the BLIP [11] model to produce image captions. For VG task, we apply the ALBEF model pretrained on the ITR task to generate adversarial images. Meanwhile, we employ the same model pretrained on VG task to localize the image regions. As shown in the results of Table 2, the multimodal adversarial examples exhibit strong cross-task adversarial transferability, successfully affecting performance on both the VG and IC tasks. Compared to other SOTA methods, the adversarial examples generated by SADCA lead to significantly larger performance drops in VG and IC metrics. This

Table 2. Cross-task transferability. We use ALBEF model to generate multimodal adversarial examples and apply them to attack the Visual Grounding (VG) task on the RefCOCO+ dataset and the Image Captioning (IC) task on the MSCOCO dataset. The "Clean" denotes the performance of each task without any attack, where lower values indicate better effectiveness of the adversarial attack in both tasks.

Attack	ITR $\rightarrow$ VG			ITR $\rightarrow$ IC				
	Val $\downarrow$	TestA $\downarrow$	TestB $\downarrow$	B@4 $\downarrow$	METEOR $\downarrow$	ROUGE-L $\downarrow$	CIDEr $\downarrow$	SPICE $\downarrow$
Clean	58.46	65.89	46.25	39.7	31.0	60.0	133.3	23.8
SGA	50.56	57.42	40.66	28.0	24.6	51.2	91.4	17.7
DRA	49.70	56.32	40.54	27.2	24.2	50.7	88.3	17.2
SA-AET	47.44	53.27	38.58	21.0	20.5	45.2	65.7	13.6
SADCA (ours)	46.78	52.41	37.10	17.4	17.9	42.2	50.3	10.7

Table 3. Adversarial transferability on LVLMs. We use ALBEF model to generate multimodal adversarial examples and apply them to attack the LVLMs on the Flickr30K dataset.

Attack	LLaVA-1.5-7B	Qwen3-VL-8B	InternVL3-8B	Qwen2.5-VL-7B	GPT-5	GPT-4o-mini	Gemini-2.0	Claude-4.5
Clean	3.46	14.4	4.72	11.04	23.88	15.00	6.96	21.80
SGA	17.60	47.00	17.60	36.00	50.65	40.96	30.12	63.32
SGA(LI)+SIA	27.30	62.76	27.30	45.92	52.17	46.54	27.92	64.18
SA-AET	14.30	60.16	25.72	48.20	60.26	50.86	38.50	72.28
SA-AET(LI)+SIA	35.20	80.14	46.68	67.50	68.08	62.48	41.56	75.12
SADCA (ours)	40.34	86.34	69.06	82.82	78.61	79.12	52.06	79.02

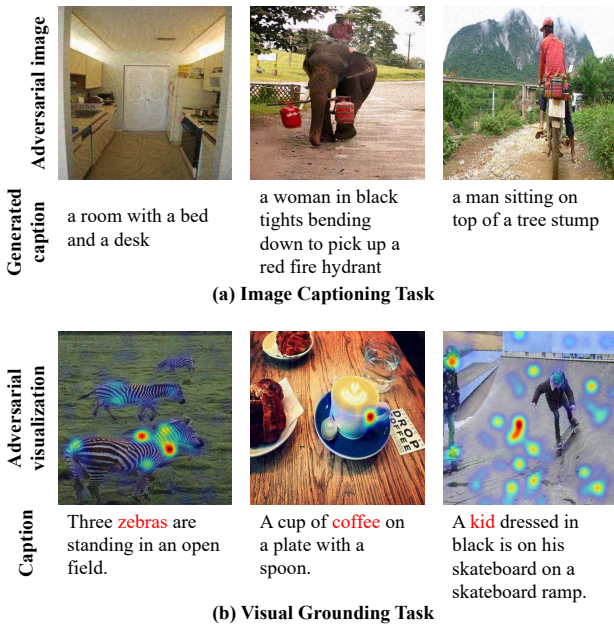


Figure 2. Visualization on Image Captioning and Visual Grounding Tasks.

demonstrates the superior effectiveness of SADCA in cross-task adversarial transferability, consistently outperforming all other methods. Figure 2 illustrates the results of image captioning and visual grounding on adversarial images generated by SADCA. As shown, both the generated captions and the localized regions deviate significantly from the ex-

pected outputs, indicating the effectiveness of SADCA.

Adversarial transferability on LVLMs. With the increasing scale of data and model parameters, Large Vision-Language Models (LVLMs) have become increasingly popular. Therefore, we evaluate the performance of SADCA on a range of LVLMs, including open-source models such as LLaVA [16], Qwen3-VL [36], InternVL3 [44], and Qwen2.5-VL [1], as well as closed-source models including GPT-5, GPT-4o-mini, Gemini-2.0, and Claude-4.5. Considering the differences between traditional VLP models and LVLm tasks, we redesign the experimental setup. Specifically, we employ a binary decision template (“Does the picture depict that ‘...’? Only answer Yes or No.”) to construct adversarial text prompts, which are combined with adversarial images as model inputs. The LVLMs are then prompted to make binary predictions under adversarial conditions. As shown in Table 3, SADCA consistently achieves the highest ASR across all models, revealing strong adversarial transferability. Both open-source and closed-source LVLMs exhibit poor robustness when confronted with multimodal adversarial examples. This observation highlights the importance of ensuring robustness against adversarial threats, which is as crucial as improving accuracy and overall performance in the development of LVLMs.

4.3. Parameter Analysis

We conduct parameter experiments on the hyperparameters of SADCA, including the number of dynamic interaction iteration I , the number of semantic augmentations S , the number of negative samples K , and the weighting factor

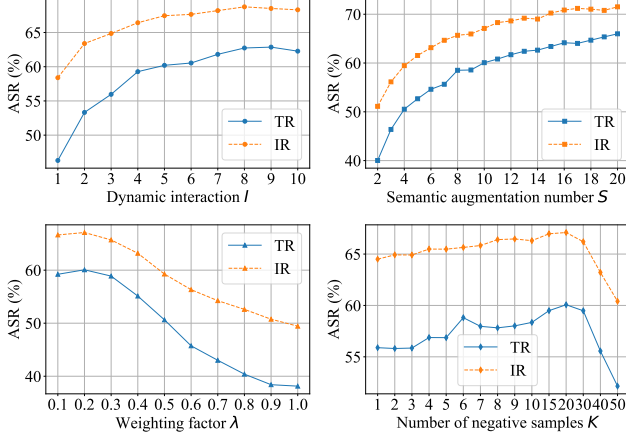


Figure 3. The ASR (%) with different parameters, including the dynamic interaction number I , the number of semantic augmentations S , the negative samples number K , and the weighting factor λ . The adversarial examples are generated on the Flickr30K dataset using CLIP_{CNN} as the source model and are evaluated on other black-box models.

Table 4. Ablation study for negative sample selection strategy. The adversarial examples are generated by CLIP_{CNN}.

	ALBEF		TCL		CLIPViT	
	TR R@1	IR R@1	TR R@1	IR R@1	TR R@1	IR R@1
Strategy (1)	44.00	56.13	49.43	59.33	74.11	77.51
Strategy (2)	41.81	54.58	47.84	58.17	73.13	76.80
Strategy (3)	44.53	58.40	50.16	60.38	75.58	79.22
Strategy (4)	45.15	57.48	51.42	60.43	75.71	79.06

λ for negative guidance. As shown in Figure 3, increasing the number of dynamic interaction leads to a more thorough disruption of cross-modal interactions, resulting in stronger attack performance, though the effect tends to plateau at higher values. A larger S improves transferability by enriching semantic diversity, with $S = 10$ offering a good trade-off between performance and efficiency. Regarding the weighting factor λ , since negative samples primarily serve as a repulsive force in guiding the adversarial direction, smaller values of λ tend to yield better performance. For K , a moderate value (e.g., $K = 20$) balances effective guidance and noise suppression.

4.4. Ablation Study

Impact of negative sample selection strategy. We explore several strategies for selecting negative samples: (1) selecting the K samples with the highest feature similarity to the positive sample; (2) selecting the K samples with the lowest feature similarity; and (3) selecting the K samples with intermediate similarity based on a ranked similarity list; (4) randomly selecting K negative samples. As shown in Table 4, random selection achieves the best performance due to its

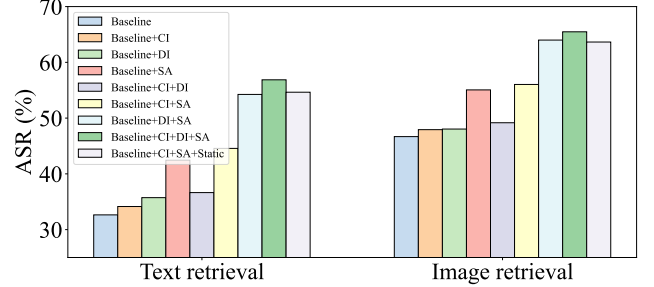


Figure 4. Ablation study for different modules of SADCA. The adversarial examples are generated on the Flickr30K dataset using CLIP_{CNN} as the source model and are evaluated on other black-box models.

higher sample diversity, which enhances generalization and transferability. In contrast, selecting the most similar negatives leads to overfitting to local decision boundaries, while the least similar ones provide weak gradients. Intermediate negatives strike a balance but still lack sufficient diversity for strong generalization.

Impact of different modules. We conduct ablation studies on the core components of SADCA, including Contrastive Interaction (CI), Dynamic Interaction (DI), and the Semantic Augmentation module (SA). As shown in Figure 4, each component individually contributes to improved attack performance, while the SADCA with all components achieves the best overall results. Additionally, we replace the dynamic interaction with a static interaction using the same iteration number. The observed performance drop under static interaction highlights the effectiveness of dynamic interaction in disrupting cross-modal alignment. Notably, when the dynamic interaction and semantic augmentation modules are combined, a significant performance boost is achieved, indicating that their synergy jointly expands the coverage and disruption depth of adversarial perturbations in the semantic space.

5. Conclusion

In this paper, we focus on highly transferable vision-language attacks and propose SADCA, a novel method designed to enhance the adversarial transferability of multi-modal adversarial examples. SADCA introduces a dynamic contrastive interaction mechanism to progressively disrupt cross-modal alignment and employs semantic-augmented transformations to increase the semantic diversity of adversarial examples. Extensive experiments conducted across various datasets and models demonstrate the effectiveness of SADCA, which consistently achieves superior transferability and outperforms SOTA methods.

6. Acknowledgement

This work was supported in part by the National Natural Science Foundation of China (62332008, 62576152, 62336004), the Basic Research Program of Jiangsu (BK20250104), the Fundamental Research Funds for the Central Universities (JUSRP202504007), and Leverhulme Trust Emeritus Fellowship EM-2025-06-09.

References

- [1] Shuai Bai, Keqin Chen, Xuejing Liu, Jialin Wang, Wenbin Ge, Sibao Song, Kai Dang, Peng Wang, Shijie Wang, Jun Tang, et al. Qwen2. 5-vl technical report. *arXiv preprint arXiv:2502.13923*, 2025. 2, 7
- [2] Sensen Gao, Xiaojun Jia, Xuhong Ren, Ivor Tsang, and Qing Guo. Boosting transferability in vision-language attacks via diversification along the intersection region of adversarial trajectory. In *European Conference on Computer Vision*, pages 442–460. Springer, 2024. 2, 3, 5
- [3] Dongchen Han, Xiaojun Jia, Yang Bai, Jindong Gu, Yang Liu, and Xiaochun Cao. Ot-attack: Enhancing adversarial transferability of vision-language models via optimal transport optimization. *arXiv preprint arXiv:2312.04403*, 2023. 3
- [4] Bangyan He, Xiaojun Jia, Siyuan Liang, Tianrui Lou, Yang Liu, and Xiaochun Cao. Sa-attack: Improving adversarial transferability of vision-language pre-training models via self-augmentation. *arXiv preprint arXiv:2312.04913*, 2023. 3
- [5] Hang Hua, Qing Liu, Lingzhi Zhang, Jing Shi, Soo Ye Kim, Zhifei Zhang, Yilin Wang, Jianming Zhang, Zhe Lin, and Jiebo Luo. Finecaption: Compositional image captioning focusing on wherever you want at any granularity. In *Proceedings of the Computer Vision and Pattern Recognition Conference*, pages 24763–24773, 2025. 1
- [6] Hailang Huang, Zhijie Nie, Ziqiao Wang, and Ziyu Shang. Cross-modal and uni-modal soft-label alignment for image-text retrieval. In *Proceedings of the AAAI Conference on Artificial Intelligence*, pages 18298–18306, 2024. 1
- [7] Xiaojun Jia, Sensen Gao, Qing Guo, Simeng Qin, Ke Ma, Yihao Huang, Yang Liu, Ivor Tsang, and Xiaochun Cao. Semantic-aligned adversarial evolution triangle for high-transferability vision-language attack. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 2025. 1, 2, 3, 5
- [8] Bin Kang, Bin Chen, Junjie Wang, Yulin Li, Junzhi Zhao, Junle Wang, and Zhuotao Tian. Calibclip: Contextual calibration of dominant semantics for text-driven image retrieval. In *Proceedings of the 33rd ACM International Conference on Multimedia*, pages 5140–5149, 2025. 1
- [9] Dehong Kong, Siyuan Liang, Xiaopeng Zhu, Yuansheng Zhong, and Wenqi Ren. Patch is enough: naturalistic adversarial patch against vision-language pre-training models. *Visual Intelligence*, 2(1):33, 2024. 1
- [10] Junnan Li, Ramprasaath Selvaraju, Akhilesh Gotmare, Shafiq Joty, Caiming Xiong, and Steven Chu Hong Hoi. Align before fuse: Vision and language representation learning with momentum distillation. *Advances in neural information processing systems*, 34:9694–9705, 2021. 3, 5
- [11] Junnan Li, Dongxu Li, Caiming Xiong, and Steven Hoi. Blip: Bootstrapping language-image pre-training for unified vision-language understanding and generation. In *International conference on machine learning*, pages 12888–12900. PMLR, 2022. 2, 6
- [12] Linyang Li, Ruotian Ma, Qipeng Guo, Xiangyang Xue, and Xipeng Qiu. Bert-attack: Adversarial attack against bert using bert. In *Proceedings of the 2020 Conference on Empirical Methods in Natural Language Processing (EMNLP)*, pages 6193–6202, 2020. 5
- [13] Yuanbo Li, Cong Hu, Rui Wang, and Xiaojun Wu. Hierarchical feature transformation attack: Generate transferable adversarial examples for face recognition. *Applied Soft Computing*, 172:112823, 2025. 3
- [14] Yuanbo Li, Cong Hu, and Xiao-Jun Wu. Transferable stealthy adversarial example generation via dual-latent adaptive diffusion for facial privacy protection. *IEEE Transactions on Information Forensics and Security*, 2025. 3
- [15] Tsung-Yi Lin, Michael Maire, Serge Belongie, James Hays, Pietro Perona, Deva Ramanan, Piotr Dollár, and C Lawrence Zitnick. Microsoft coco: Common objects in context. In *European conference on computer vision*, pages 740–755. Springer, 2014. 5
- [16] Haotian Liu, Chunyuan Li, Yuheng Li, and Yong Jae Lee. Improved baselines with visual instruction tuning. In *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*, pages 26296–26306, 2024. 7
- [17] Xiyao Liu, Jiaxin Hu, Qingying Yang, Ming Jiang, Jianbiao He, and Hui Fang. A divide-and-conquer reconstruction method for defending against adversarial example attacks. *Visual Intelligence*, 2(1):30, 2024. 1
- [18] Dong Lu, Zhiqiang Wang, Teng Wang, Weili Guan, Hongchang Gao, and Feng Zheng. Set-level guidance attack: Boosting adversarial transferability of vision-language pre-training models. In *Proceedings of the IEEE/CVF International Conference on Computer Vision*, pages 102–111, 2023. 1, 2, 3, 5
- [19] Aleksander Madry, Aleksandar Makelov, Ludwig Schmidt, Dimitris Tsipras, and Adrian Vladu. Towards deep learning models resistant to adversarial attacks. In *International Conference on Learning Representations*, 2018. 5
- [20] Bryan A Plummer, Liwei Wang, Chris M Cervantes, Juan C Caicedo, Julia Hockenmaier, and Svetlana Lazebnik. Flickr30k entities: Collecting region-to-phrase correspondences for richer image-to-sentence models. In *Proceedings of the IEEE international conference on computer vision*, pages 2641–2649, 2015. 5
- [21] Xiangyu Qi, Kaixuan Huang, Ashwinee Panda, Peter Henderson, Mengdi Wang, and Prateek Mittal. Visual adversarial examples jailbreak aligned large language models. In *Proceedings of the AAAI conference on artificial intelligence*, pages 21527–21536, 2024. 2
- [22] Alec Radford, Jong Wook Kim, Chris Hallacy, Aditya Ramesh, Gabriel Goh, Sandhini Agarwal, Girish Sastry, Amanda Askell, Pamela Mishkin, Jack Clark, et al. Learning

- transferable visual models from natural language supervision. In *International conference on machine learning*, pages 8748–8763. PmLR, 2021. 3, 5
- [23] Yuchen Ren, Zhengyu Zhao, Chenhao Lin, Bo Yang, Lu Zhou, Zhe Liu, and Chao Shen. Improving adversarial transferability on vision transformers via forward propagation refinement. In *Proceedings of the Computer Vision and Pattern Recognition Conference*, pages 25071–25080, 2025. 3
- [24] Quan Sun, Yuxin Fang, Ledell Wu, Xinlong Wang, and Yue Cao. Eva-clip: Improved training techniques for clip at scale. *arXiv preprint arXiv:2303.15389*, 2023. 2
- [25] Michael Tschanen, Alexey Gritsenko, Xiao Wang, Muhammad Ferjad Naeem, Ibrahim Alabdulmohsin, Nikhil Parthasarathy, Talfan Evans, Lucas Beyer, Ye Xia, Basil Mustafa, et al. Siglip 2: Multilingual vision-language encoders with improved semantic understanding, localization, and dense features. *arXiv preprint arXiv:2502.14786*, 2025. 2
- [26] Haodi Wang, Kai Dong, Zhilei Zhu, Haotong Qin, Aishan Liu, Xiaolin Fang, Jiakai Wang, and Xianglong Liu. Transferable multimodal attack on vision-language pre-training models. In *2024 IEEE Symposium on Security and Privacy (SP)*, pages 1722–1740. IEEE, 2024. 3
- [27] Kunyu Wang, Xuanran He, Wenxuan Wang, and Xiaosen Wang. Boosting adversarial transferability by block shuffle and rotation. In *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*, pages 24336–24346, 2024. 2, 3, 1
- [28] Weihang Wang, Qingsong Lv, Wenmeng Yu, Wenyi Hong, Ji Qi, Yan Wang, Junhui Ji, Zhuoyi Yang, Lei Zhao, Song XiXuan, et al. Cogvlm: Visual expert for pretrained language models. *Advances in Neural Information Processing Systems*, 37:121475–121499, 2024. 2
- [29] Xiaosen Wang, Xuanran He, Jingdong Wang, and Kun He. Admix: Enhancing the transferability of adversarial attacks. In *Proceedings of the IEEE/CVF international conference on computer vision*, pages 16158–16167, 2021. 3
- [30] Xiaosen Wang, Zeliang Zhang, and Jianping Zhang. Structure invariant transformation for better adversarial transferability. In *Proceedings of the IEEE/CVF International Conference on Computer Vision*, pages 4607–4619, 2023. 1, 2, 3, 5
- [31] Yeyuan Wang, Dehong Gao, Lei Yi, Linbo Jin, Jinxia Zhang, Libin Yang, and Xiaoyan Cai. Enhancing fine-grained vision-language pretraining with negative augmented samples. In *Proceedings of the AAAI Conference on Artificial Intelligence*, pages 8060–8068, 2025. 1
- [32] Youze Wang, Wenbo Hu, Yinpeng Dong, Hanwang Zhang, Hang Su, and Richang Hong. Exploring transferability of multimodal adversarial samples for vision-language pre-training models with contrastive learning. *IEEE Transactions on Multimedia*, 2025. 2, 3
- [33] Cihang Xie, Zhishuai Zhang, Yuyin Zhou, Song Bai, Jianyu Wang, Zhou Ren, and Alan L Yuille. Improving transferability of adversarial examples with input diversity. In *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*, pages 2730–2739, 2019. 1
- [34] Peng Xie, Yequan Bie, Jianda Mao, Yangqiu Song, Yang Wang, Hao Chen, and Kani Chen. Chain of attack: On the robustness of vision-language models against transfer-based adversarial attacks. In *Proceedings of the Computer Vision and Pattern Recognition Conference*, pages 14679–14689, 2025. 3
- [35] Wenzhuo Xu, Kai Chen, Ziyi Gao, Zhipeng Wei, Jingjing Chen, and Yu-Gang Jiang. Highly transferable diffusion-based unrestricted adversarial attack on pre-trained vision-language models. In *Proceedings of the 32nd ACM International Conference on Multimedia*, pages 748–757, 2024. 2
- [36] An Yang, Anfeng Li, Baosong Yang, Beichen Zhang, Binyuan Hui, Bo Zheng, Bowen Yu, Chang Gao, Chengen Huang, Chenxu Lv, et al. Qwen3 technical report. *arXiv preprint arXiv:2505.09388*, 2025. 7
- [37] Jinyu Yang, Jiali Duan, Son Tran, Yi Xu, Sampath Chanda, Liqun Chen, Belinda Zeng, Trishul Chilimbi, and Junzhou Huang. Vision-language pre-training with triple contrastive learning. In *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*, pages 15671–15680, 2022. 3, 5
- [38] Licheng Yu, Patrick Poirson, Shan Yang, Alexander C Berg, and Tamara L Berg. Modeling context in referring expressions. In *European conference on computer vision*, pages 69–85. Springer, 2016. 5
- [39] Zequn Zeng, Yan Xie, Hao Zhang, Chiyu Chen, Bo Chen, and Zhengjue Wang. Meacap: Memory-augmented zero-shot image captioning. In *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*, pages 14100–14110, 2024. 1
- [40] Jiaming Zhang, Qi Yi, and Jitao Sang. Towards adversarial attack on vision-language pre-training models. In *Proceedings of the 30th ACM International Conference on Multimedia*, pages 5005–5013, 2022. 2, 5
- [41] Jingyi Zhang, Jiaxing Huang, Sheng Jin, and Shijian Lu. Vision-language models for vision tasks: A survey. *IEEE transactions on pattern analysis and machine intelligence*, 46(8):5625–5644, 2024. 1
- [42] Peng-Fei Zhang, Guangdong Bai, and Zi Huang. Maa: Meticulous adversarial attack against vision-language pre-trained models. *arXiv preprint arXiv:2502.08079*, 2025. 3
- [43] Yunqing Zhao, Tianyu Pang, Chao Du, Xiao Yang, Chongxuan Li, Ngai-Man Man Cheung, and Min Lin. On evaluating adversarial robustness of large vision-language models. *Advances in Neural Information Processing Systems*, 36:54111–54138, 2023. 2
- [44] Jinguo Zhu, Weiyun Wang, Zhe Chen, Zhaoyang Liu, Shenglong Ye, Lixin Gu, Hao Tian, Yuchen Duan, Weijie Su, Jie Shao, et al. Internvl3: Exploring advanced training and test-time recipes for open-source multimodal models. *arXiv preprint arXiv:2504.10479*, 2025. 7
- [45] Yao Zhu, Yuefeng Chen, Xiaodan Li, Kejiang Chen, Yuan He, Xiang Tian, Bolun Zheng, Yaowu Chen, and Qingming Huang. Toward understanding and boosting adversarial transferability from a distribution perspective. *IEEE Transactions on Image Processing*, 31:6487–6501, 2022. 2