

# Unbridled Icarus: A Survey of the Potential Perils of Image Inputs in Multimodal Large Language Model Security

Yihe Fan, Yuxin Cao, Ziyu Zhao, Ziyao Liu, Shaofeng Li

**Abstract**—Multimodal Large Language Models (MLLMs) demonstrate remarkable capabilities that increasingly influence various aspects of our daily lives, constantly defining the new boundary of Artificial General Intelligence (AGI). Image modalities, enriched with profound semantic information and a more continuous mathematical nature compared to other modalities, greatly enhance the functionalities of MLLMs when integrated. However, this integration serves as a double-edged sword, providing attackers with expansive vulnerabilities to exploit for highly covert and harmful attacks. The pursuit of reliable AI systems like powerful MLLMs has emerged as a pivotal area of contemporary research. In this paper, we endeavor to demonstrate the multifaceted risks associated with the incorporation of image modalities into MLLMs. Initially, we delineate the foundational components and training processes of MLLMs. Subsequently, we construct a threat model, outlining the security vulnerabilities intrinsic to MLLMs. Moreover, we analyze and summarize existing scholarly discourses on MLLMs' attack and defense mechanisms, culminating in suggestions for the future research on MLLM security. Through this comprehensive analysis, we aim to deepen the academic understanding of MLLM security challenges and propel forward the development of trustworthy MLLM systems.

## I. INTRODUCTION

Multimodal Large Language Models (MLLMs) have achieved remarkable success in recent years, extending the capabilities of Large Language Models (LLMs) to comprehend and process both textual and visual information. Notably, models such as GPT-4 and LLaVA, when fine-tuned with human feedback and instructions, have not only enhanced interaction with human users by supporting visual inputs but also demonstrated potential in recommendation systems and other safety-sensitive applications [1].

Incorporating multimodal data, especially images, into LLMs raises significant security issues due to the **richer semantics and more continuous nature of visual data** compared to other multimodal data such as text and audio. While images broaden the applications of LLMs and enhance their functionality, they also open up new vulnerabilities for exploitation by attackers [2]–[5]. The concern around image hijacks stems from their automatic generation, imperceptibility to humans, and the potential for arbitrary control over a model's output, presenting a significant security challenge.

Yihe Fan is with School of Electronics and Information Engineering, Tongji University, China. Yuxin Cao is with School of Computing, National University of Singapore, Singapore. Ziyu Zhao is with Fan Gongxiu Honors College, Beijing University of Technology, China. Ziyao Liu is with Nanyang Technological University, Singapore. Shaofeng Li is with School of Computer Science and Engineering, Southeast University, China. E-mail: 2152045@tongji.edu.cn, yuxincao@comp.nus.edu.sg, ziyu.zhao.zzy@gmail.com, liuziyao@ntu.edu.sg, shaofengli2013@gmail.com.

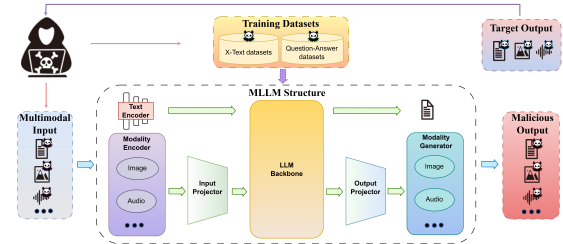


Fig. 1: The general model architecture of MLLMs and the vulnerabilities that attackers may exploit to manipulate the model to generate malicious output.

Ignoring the risks introduced by incorporating images could lead to unpredictable and potentially dire consequences.

While there are plentiful significant researches focused on the security of LLMs [6]–[8], the study of MLLM security is still in its infancy. We innovatively conduct a study on MLLM security, specifically focusing on the threats, attacks, and defensive strategies associated with the integration of the image modality. Following extensive research, we have identified several security risks associated with incorporating image modality, including: (1) cross-modal training that weakens traditional security alignments, (2) the rapid, efficient, and covert nature of attacking MLLMs by optimizing images to control their outputs, and (3) the difficulty in detecting malicious information concealed within images. To deepen the understanding of security issues in MLLMs, we conduct a comprehensive investigation into the current state of security research for MLLMs. Particularly, we focus on the offensive and defensive strategies that arise with the introduction of image modality data. Our contributions are summarized as follows.

- We meticulously construct a specific threat model for MLLMs, categorizing the diverse vulnerabilities and potential attacks in different attack scenarios.
- We conduct a comprehensive review of the current state-of-the-art attacks and defenses for MLLM security.
- We propose several possible directions for future research of MLLMs' security, providing some inspiration for other researchers.

## II. BACKGROUND

In this section, we delve into the foundational architecture and training process of current MLLMs [9], as shown in Figure 1. Our exploration aims to set the stage for a comprehensive review focused on the security topics of MLLMs. This foundational understanding help us understand the origins of security issues associated with MLLMs.

### A. Model Structure

The structure of MLLMs encompasses a sophisticated framework designed to process, interpret, and generate content across different modalities. 1) *Modality Encoders*: The Modality Encoders are tasked with encoding input data from various modalities (e.g., images, videos and audio) into a unified high-dimensional feature representation. This process typically utilizes Convolutional Neural Networks or Transformer models for images, and specifically designed neural networks for audio. 2) *Input Projector*: The Input Projector aligns the encoded features from different modalities with the textual feature space, transforming them into formats that LLM Backbone can process. 3) *LLM Backbone*: Acting as the core component, the LLM Backbone handles representations from various modalities for semantic understanding, inference, and decision-making. The backbone generates textual outputs or signal tokens that guide modality generators in producing multimodal content. 4) *Output Projector*: The Output Projector maps the LLM backbone's signal tokens back to the feature space of the original modality, enabling modality generators to comprehend these instructions. This step typically involves converting textual representations into feature representations specific to various modalities. 5) *Modality Generators*: The Modality Generators generate specific multimodal outputs based on the instructions from the LLM backbone and output projector, including models for image, video, or audio generation.

### B. Training Process

1) *Multimodal Pre-training*: This stage involves pre-training on X-Text (e.g., Image-Text, Audio-Text) datasets to learn to integrate information from different modalities (e.g., text, images, audio). This is crucial for capturing the intrinsic connections between modalities, laying the groundwork for future task-specific fine-tuning.

2) *Multimodal Instruction Tuning*: Building on the multimodal pre-training foundation, the model is further fine-tuned through multimodal instruction tuning. This comprises supervised fine-tuning using Question-Answer datasets and Reinforcement Learning from Human Feedback [10]. Multimodal instruction tuning enhances the model's responsiveness to specific instructions, aiming to improve performance on cross-modal tasks based on natural language instructions.

## III. THREAT MODEL

The threat model for attacking MLLMs encompasses a range of vulnerabilities, attack scenarios and attack objectives. Below is an expanded framework focusing on the unique aspects of attacking MLLMs.

### A. Vulnerabilities

When exploring the vulnerabilities within MLLMs, attackers exploit several weaknesses to achieve their goals. These vulnerabilities span both the training phase by utilizing data for pre-training and fine-tuning on multimodal instructions, and the inference phase, where multimodal data inputs meticulously designed by attackers are processed to control the MLLMs' behavior.

1) *Training Datasets*: A significant vulnerability resides within the training data. Attackers employ data poisoning techniques, inserting malicious data into the training datasets to undermine the model during the training phase. Training with the poisoned data can lead to models learning incorrect associations or biases, which attackers exploit to manipulate the model's outputs or decision-making processes.

2) *Multimodal Input*: The complexity of processing inputs from different modalities presents additional vulnerabilities. Attackers meticulously craft inputs in one or more modalities to exploit how MLLMs integrate and interpret the multimodal information. For instance, an image with subtly manipulated features might be paired with text to mislead the model into generating an erroneous or malicious output.

### B. Attack Scenarios

After identifying the vulnerabilities to be attacked, the attackers carry out their attacks based on various assumptions which can be classified into white-box, black-box and grey-box scenarios:

1) *White-box Attacks*: In this scenario, attackers have comprehensive access to the model, including its weights, architecture, and potentially the training data. This access enables them to exploit gradient information and conduct sophisticated attacks that might target the nuanced ways in which MLLMs integrate information from different modalities. The profound understanding of the model's inner workings allows for the crafting of attacks that are precisely tuned to exploit specific vulnerabilities.

2) *Black-box Attacks*: Contrary to the white-box scenario, black-box attackers have very limited information and no knowledge of the model's internal structure, parameters, or training data. For attacks during the training phase, attackers can only rely on their experience to construct poisoned data; while for attacks during the inference phase, attackers can only interact with (query) the model through an API without direct access to its internals. Despite this limitation, they can still probe the model with a variety of inputs to discern its behavior and identify weaknesses. These attacks focus on discovering vulnerabilities in how the model processes and integrates multimodal data, relying on available outputs to guide the attack strategy.

3) *Gray-box Attacks*: In gray-box attacks, attackers possess knowledge that lies between that of white-box and black-box attacks. In the context of attacks on MLLMs, gray-box attackers might only have access to one of the following: gradient information of the MLLMs' pretrained encoder, or a surrogate model with the similar structure and function as the attacked model. Attackers rely on these structures to construct potential poisoned data during the training phase or create adversarial samples during the inference phase. Gray-box attacks on MLLMs depend on the transferability of the pretrained encoder to downstream tasks and the transferability between different MLLMs.

### C. Attack Objectives

1) *Cognitive Bias*: Cognitive Bias is reflected by the model's output that is close to a target specified by an

attacker (targeted) or simply deviate from the original content (untargeted), resulting in false or uncertain information.

2) *Specific String Output*: Specific String Output concentrates on manipulating the output of the model as a preset string, which is stricter than the targeted Cognitive Bias.

3) *Jailbreak*: Jailbreak refers to a behavior that exploits vulnerabilities in MLLMs to bypass model's safety alignment, which aims to prevent inappropriate or dangerous outputs. Unlike other attack goals focusing on errors, jailbreak aims to uncover and allow the generation of unsafe outputs.

4) *Prompt Injection*: Similar to injection attacks in the traditional field of computer security, Prompt Injection also involves attackers carefully controlling inputs to make the model mistakenly treat data as instructions. By manipulating inputs with hidden instructions, attackers can subtly influence the model to deliver misleading or harmful results.

5) *Backdoor Implantation*: Backdoor Implantation embeds a hidden mechanism in the model that activates a specific response when triggered by a certain input. These backdoor triggers, often with subtle changes in the input data, allow the model to function normally until activated.

6) *Privacy Breach*: In the context of security on MLLMs, Privacy Breach refers to the result that the attacker extracts or infers confidential data about users or the model itself. Attackers might induce the model to leak sensitive information stored in its training data or runtime conversation information by using carefully crafted images or other multimodal inputs.

## IV. ATTACK

This section reviews three primary attack categories in existing research on MLLM security. Table I provides a comparative overview of different attacks against MLLMs.

### A. Structure-based Attack

Operating often in the black-box attack scenario, structure-based attacks employ simple typography or text-to-image tools to manually design the multimodal inputs of MLLMs. These attacks involve transferring the harmfulness of text into images, using inducing textual prompts to direct MLLMs to focus on malicious content within the images, thereby circumventing safety checks to achieve the attack's aim. A basic strategy [30] entails the direct incorporation of raw text into images, either as commands or erroneous statements, thereby challenging MLLMs to accurately differentiate between genuine data and embedded instructions, thus achieving visual prompt injection. Qraitem *et al.* [20] introduced a novel self-generated typographic attack tailored for MLLMs, demonstrating MLLMs' susceptibility to such attacks by compelling the model to produce misleading text, thereby reducing its classification accuracy. Shayegani *et al.* [2] employed text-to-image tools to transfer malicious information from text to images and crafted four triggers that contain malicious information and directly integrated them into images, using inducing prompts such as "How to create the object in the image" to facilitate jailbreak attacks. Gong *et al.* [4] positioned harmful information within a series of

images, akin to assembling a puzzle, successfully breaching the defenses of several open-source MLLMs.

### B. Perturbation-based Attack

Attacks of this category involve introducing adversarial perturbations into the input data, often in a way that is imperceptible to humans. These perturbations are designed to exploit the vulnerabilities in the model's processing of input data, causing the model to output incorrect or harmful responses. Initial efforts focused on attacks against visual pre-training models [25], [31]–[36], assessing their robustness across different downstream tasks. These studies explored adversarial attacks that simultaneously perturb images and texts, alongside employing various data augmentation techniques to enhance transferability to other pre-trained models, laying a solid foundation for attacking the entire MLLM.

In white-box scenarios, attacks leverage the gradient information from various components of MLLMs to optimize images to achieve various objectives. Schlarmann and Hein [11] utilized adversarial images to directly control the output of the OpenFlamingo model, signifying the first demonstration of MLLMs' vulnerability to adversarial images. Subsequently, Qi *et al.* [12] conducted adversarial optimizations for both text and image modalities employing a custom corpus alongside few-shot learning methodologies. They observed that the inherent continuity of images not only facilitated a more rapid optimization process for attacks—approximately 12 times faster than that for text—but also ensured greater stealthiness. Luo *et al.* [13] employed a cross-prompt optimization strategy, proving for the first time that a single adversarial image could execute attacks across multiple prompts. Bailey *et al.* [14] presented a study on Image Hijacks, a method whereby subtle alterations to images can influence the output of models during inference. Through a technique named Behaviour Matching, the research indicates a significant ability to direct model responses, highlighting potential security vulnerabilities. Further explorations into white-box scenarios using adversarial images to control MLLM behaviors include Bagdasaryan *et al.* [15]'s use of images and audio for invisible prompt injection and Wang *et al.* [16]'s investigation into the impact of adversarial samples on MLLMs' chain-of-thought (CoT) reasoning. Additionally, a recent attack on MLLM agents by Gu *et al.* [18] highlighted a profound safety concern in multi-agent environments, termed infectious jailbreak. Through their white-box optimization strategy, an infectious adversarial image was generated and input to a single agent called Agent Smith. Once introduced to an Agent Smith within an intelligence team, the likelihood of agents being infected rose exponentially with each chat round, emphasizing the severe harm that adversarial images pose to MLLM agent systems. Tan *et al.* [19] reached a similar conclusion that a single MLLM agent can be subtly influenced to generate prompts that induce other MLLM agents in the society to output malicious content. Lu *et al.* [17] developed AnyDoor, a novel test-time backdoor strategy for MLLMs that utilizes adversarial perturbations on test images to inject a backdoor

TABLE I: Comparison of different attacks. **Setting:** White-box (W), Black-box (B), Grey-box (G); **Vulnerability:** Multimodal input (I-*modality*), Instruction tuning in training datasets (T-IT); **Category:** Structure-based (S), Perturbation-based (P), Data poisoning-based (D); **Attack Objective:** Cognitive Bias (G1), Specific String Output (G2), Jailbreak (G3), Prompt Injection (G4), Backdoor Implantation (G5), Privacy Breach (G6); **Victim Model:** MLLMs without specifying exact versions.

Attack	Setting	Vulnerability	Category			Attack Objective						Victim Model	
			S	P	D	G1	G2	G3	G4	G5	G6		
Schlarman <i>et al.</i> [11]	W	I-image		✓		✓	✓						OpenFlamingo
Qi <i>et al.</i> [12]	W	I-image/text		✓				✓					InstructBLIP/LLaVA/MiniGPT
Luo <i>et al.</i> [13]	W	I-image		✓		✓	✓						BLIP-2/InstructBLIP/OpenFlamingo
Bailey <i>et al.</i> [14]	W	I-image		✓			✓	✓				✓	BLIP-2/InstructBLIP/LLaVA
Bagdasaryan <i>et al.</i> [15]	W	I-image/audio		✓						✓			PandaGPT/LLaVA
Wang <i>et al.</i> [16]	W	I-image		✓		✓							LLaVA/MiniGPT/OpenFlamingo
D.Lu <i>et al.</i> [17]	W	I-image		✓						✓			InstructBLIP/LLaVA/MiniGPT
Gu <i>et al.</i> [18]	W	I-image		✓				✓					LLaVA
Tan <i>et al.</i> [19]	W	I-image		✓				✓					LLaVA/PandaGPT
Qraitem <i>et al.</i> [20]	B	I-image	✓			✓							InstructBLIP/LLaVA/MiniGPT/GPT-4
Shayegani <i>et al.</i> [2]	B	I-image	✓					✓					MiniGPT/LLaVA
Gong <i>et al.</i> [4]	B	I-image	✓					✓					MiniGPT/CogVLM/LLaVA
Li <i>et al.</i> [3]	B	I-image		✓				✓					Gemini/GPT-4/LLaVA
Wu <i>et al.</i> [21]	B	I-text		✓				✓					GPT-4
Zhao <i>et al.</i> [5]	G	I-image		✓		✓							LLVA/MiniGPT/BLIP-2
Dong <i>et al.</i> [22]	G	I-image		✓		✓		✓					Bard/Bing Chat/GPT-4
Wang <i>et al.</i> [23]	G	I-image		✓		✓							InstructBLIP/MiniGPT/BLIP-2
Bagdasaryan <i>et al.</i> [24]	G	I-image/audio		✓		✓							BindDiffusion/PandaGPT
Han <i>et al.</i> [25]	G	I-image		✓		✓							Bing Chat/GPT-4
Niu <i>et al.</i> [26]	G	I-image		✓				✓					InstructBLIP/LLaVA/MiniGPT/mPLUGOwl2
Tao <i>et al.</i> [27]	B	T-IT			✓			✓					LLaVA
Xu <i>et al.</i> [28]	B	T-IT			✓	✓							LLaVA/MiniGPT
Liang <i>et al.</i> [29]	B	T-IT			✓					✓			OpenFlamingo

and use preset prompts as the trigger to activate the backdoor, eliminating the need to modify training data and enhancing the attack versatility and stealthiness.

In black-box scenarios, attacks impose a significant burden on LLM systems due to the substantial computational cost associated with model inference, leading to high cost and easy detection. Traditional non-gradient optimization methods require thousands of API queries to achieve success, with only Zhao *et al.* [5] conducting a basic exploration by iterating eight times using the Randomized Gradient-Free method [37]. Recent developments have seen LLMs themselves acting as attackers’ offensive tools to optimize adversarial samples. Chao *et al.* [38] employed an LLM agent to evaluate content harm and optimize text, achieving jailbreak at the prompt level within 20 queries. Inspired by this work, MLLM agents were used to optimize adversarial samples with fewer queries [3], [21].

In grey-box scenarios, transfer attacks are the prevalent means employed for generating adversarial examples. Zhao *et al.* [5] first utilized gradient information from a single pretrained visual encoder, guiding adversarial images in the embedding space to diverge from or converge to the embedding of the original or target text. Dong *et al.* [22] sought to enhance transferability by acquiring gradient information from multiple surrogate pretrained encoders and MLLMs, and successfully compromised mainstream commercial MLLMs. Wang *et al.* [23] proposed InstructTA to improve the robustness and transferability of the adversarial examples across different MLLMs. This enhancement is accomplished by augmenting an inferred instruction with paraphrased versions generated by an LLM. Bagdasaryan and Shmatikov [24] revealed that subtle, nearly impercep-

tible perturbations allow attackers to misalign inputs across modalities within the embedding space. They also explored the transferability of illusions across different embeddings. Han *et al.* [25] applied Optimal Transport Optimization to enhance the efficacy of transfer attacks against single pretrained encoders, showing its effectiveness and transferability on two closed-source MLLMs, GPT-4 and Bing Chat. Niu *et al.* [26] proposed an optimization method for image Jailbreaking Prompt, achieving strong data-universal properties and model transferability. Although transfer attacks have been shown to be effective, their explainability remains a challenge.

### C. Data Poisoning-based Attack

Data poisoning constitutes a strategy of contaminating the training dataset of a model by introducing maliciously engineered data, which can profoundly alter the model’s behavior. Data poisoning-based attacks are notably surreptitious, allowing the compromised model to function normally across a majority of inputs, yet manifest harmful or biased behaviors under specific conditions or in response to particular inputs. The primary objective of data poisoning often revolves around degrading the model’s overall performance or embedding backdoors for potential exploitation [39], [40].

Tao *et al.* [27] effectively achieved data poisoning by substituting original textual captions with Malicious Jailbreak Prompts (JBP) during the instruction tuning phase. In the subsequent inference phase, the introduction of images coupled with JBP and harmful query texts facilitates the jailbreaking goal. Xu *et al.* [28] implemented poisoned data within the multimodal pre-training, with the intention of prompting the MLLM to misclassify and disseminate incorrect information. Liang *et al.* [29] were the first to embed

TABLE II: Comparison of different defenses. **Branch:** Training-time defense (TD), Inference-time defense (ID).

Defense	Branch	Core Method
[41]	TD	Supervised fine-tuning with RTVLM
[42]	TD	Disrupt connections between poisoned image-caption pairs
[43]	TD	Introduce learnable robust text prompts
[44]	TD	Introduce learnable robust text prompts
[45]	TD	Natural language feedback
[46]	ID	Mutation-based framework to detect jailbreak
[47]	ID	MLLM-Protector as a plugin for LLM
[48]	ID	Leverage cross-model guidance for harmlessness alignment
[49]	ID	Employ adaptive defense prompts
[50]	ID	Transform unsafe image inputs into text

a backdoor within MLLMs by injecting poisoned samples containing triggers in either instructions or images during instruction tuning, thus enabling the malicious manipulation for outputs of the victim model via predetermined triggers. Their approach fostered the learning of image triggers via an isolation and clustering strategy, significantly boosting the potency of black-box attacks through an iterative, character-level text trigger generation technique.

Although data poison-based attacks demonstrate high effectiveness, they invariably require some level of model retraining, entailing substantial costs, particularly in light of the extensive parameter space characteristic of MLLMs.

## V. DEFENSE

In this section, we illustrate the current efforts towards the safety protection of MLLMs. We present the comparison of different defenses on MLLMs in Table II.

### A. Training-time Defense

The RTVLM dataset introduced by Li *et al.* [41] evaluates the robustness of MLLMs to challenging scenarios with both text and image inputs, revealing vulnerabilities in key areas such as faithfulness and privacy. This study suggests that supervised fine-tuning with RTVLM enhances the security of MLLMs. To fortify pretrained models against adversarial threats, [42] proposed ROCLIP, a robust contrastive learning framework tailored for large-scale vision-language models. ROCLIP involves disrupting the connections between poisoned image-caption pairs during the pretraining phase, notably diminishing the success rate of data poisoning and backdoor attacks. Moreover, the works done by Zhang *et al.* [43] and Li *et al.* [44] enhanced the adversarial robustness of pretrained vision-language models by introducing learnable robust text prompts. This technique, known as AdvPT, not only fortifies the models against white-box and black-box attacks, but, when combined with existing image processing defense techniques, significantly improves their defensive capabilities. Chen *et al.* [45] proposed DRESS, a novel MLLM that leverages Natural Language Feedback (NLF) from GPT-4 to enhance alignment with human preferences and improve multi-turn interaction capabilities, demonstrating superior response generation aligned with values of helpfulness, honesty, and harmlessness.

### B. Inference-time Defense

In the inference phase, various methods have been proposed to safeguard MLLMs against potential threats without compromising their performance and training cost. Zhang *et al.* [46] proposed JailGuard, which emerged as a pioneering mutation-based framework designed to detect multimodal jailbreaking attacks. By exploiting the inherent lack of robustness in attack queries, JailGuard generates variations of input queries and assesses the divergence in model responses to identify attacks. Pi *et al.* [47] proposed MLLM-Protector, a plugin that includes a harm detector to identify potential risks in model responses and a response detoxifier to correct them, enhancing MLLM safety without performance compromise. Wang *et al.* [48] proposed InferAligner that utilizes safety steering vectors from safety-aligned models to guide the target model's outputs in response to harmful prompts, ensuring safe responses to potentially damaging inputs. In parallel, Wang *et al.* [49] proposed AdaShield, which combines manually designed static prompts with an adaptive framework to defend MLLMs against structured jailbreaking attacks, resulting in a diverse prompt pool for various attack scenarios. Gou *et al.* [50] proposed ECSO (Eyes Closed, Safety On) to protect MLLMs from Jailbreak by converting harmful images into text, enhancing model safety without requiring manual annotation.

## VI. CONCLUSION

In our study, we conduct a comprehensive investigation on the security implications tied to MLLMs, with a special focus on the complexities introduced by integrating images. To aid in this endeavor, we build a threat model specific to MLLMs and systematically review current state-of-the-art attack and defense of MLLMs' safety, categorizing the diverse vulnerabilities and potential attacks in different attack scenarios. We also delve into the issues present in existing research and identify some promising directions for future development. With our work, MLLM practitioners can gain a deeper understanding of potential attacks and better implement effective defenses of MLLMs. We hope this survey can provide insights for researchers, contributing to the advancements in constructing trustworthy MLLM systems.

## REFERENCES

- [1] J. Fan, M. Xu, Z. Liu, H. Ye, C. Gu, D. Niyato, and K.-Y. Lam, "A learning-based incentive mechanism for mobile aigc service in decentralized internet of vehicles," in *2023 IEEE 98th Vehicular Technology Conference (VTC2023-Fall)*, pp. 1–5, IEEE, 2023.
- [2] E. Shayegani, Y. Dong, and N. Abu-Ghazaleh, "Jailbreak in pieces: Compositional adversarial attacks on multi-modal language models," in *The Twelfth International Conference on Learning Representations*, 2023.
- [3] Y. Li, H. Guo, K. Zhou, W. X. Zhao, and J.-R. Wen, "Images are achilles' heel of alignment: Exploiting visual vulnerabilities for jailbreaking multimodal large language models," *arXiv preprint arXiv:2403.09792*, 2024.
- [4] Y. Gong, D. Ran, J. Liu, C. Wang, T. Cong, A. Wang, S. Duan, and X. Wang, "Figstep: Jailbreaking large vision-language models via typographic visual prompts," *arXiv preprint arXiv:2311.05608*, 2023.
- [5] Y. Zhao, T. Pang, C. Du, X. Yang, C. Li, N.-M. M. Cheung, and M. Lin, "On evaluating adversarial robustness of large vision-language models," *Advances in Neural Information Processing Systems*, vol. 36, 2024.



- [6] E. Shayegani, M. Mamun, Y. Fu, P. Zaree, Y. Dong, and N. Abu-Ghazaleh, "Survey of vulnerabilities in large language models revealed by adversarial attacks. arxiv. doi: 10.48550,," *arXiv preprint arXiv:2310.10844*, 2023.
- [7] X. Huang, W. Ruan, W. Huang, G. Jin, Y. Dong, C. Wu, S. Bensalem, R. Mu, Y. Qi, X. Zhao, *et al.*, "A survey of safety and trustworthiness of large language models through the lens of verification and validation," *arXiv preprint arXiv:2305.11391*, 2023.
- [8] T. Cui, Y. Wang, C. Fu, Y. Xiao, S. Li, X. Deng, Y. Liu, Q. Zhang, Z. Qiu, P. Li, *et al.*, "Risk taxonomy, mitigation, and assessment benchmarks of large language model systems," *arXiv preprint arXiv:2401.05778*, 2024.
- [9] D. Zhang, Y. Yu, C. Li, J. Dong, D. Su, C. Chu, and D. Yu, "Mm-llms: Recent advances in multimodal large language models," *arXiv preprint arXiv:2401.13601*, 2024.
- [10] X. Wang, S. Duan, X. Yi, J. Yao, S. Zhou, Z. Wei, P. Zhang, D. Xu, M. Sun, and X. Xie, "On the essence and prospect: An investigation of alignment approaches for big models," *arXiv preprint arXiv:2403.04204*, 2024.
- [11] C. Schlarman and M. Hein, "On the adversarial robustness of multi-modal foundation models," in *Proceedings of the IEEE/CVF International Conference on Computer Vision*, pp. 3677–3685, 2023.
- [12] X. Qi, K. Huang, A. Panda, M. Wang, and P. Mittal, "Visual adversarial examples jailbreak aligned large language models," in *The Second Workshop on New Frontiers in Adversarial Machine Learning*, 2023.
- [13] H. Luo, J. Gu, F. Liu, and P. Torr, "An image is worth 1000 lies: Adversarial transferability across prompts on vision-language models," *arXiv preprint arXiv:2403.09766*, 2024.
- [14] L. Bailey, E. Ong, S. Russell, and S. Emmons, "Image hijacks: Adversarial images can control generative models at runtime," *arXiv preprint arXiv:2309.00236*, 2023.
- [15] E. Bagdasaryan, T.-Y. Hsieh, B. Nassi, and V. Shmatikov, "(ab) using images and sounds for indirect instruction injection in multi-modal llms," *arXiv preprint arXiv:2307.10490*, 2023.
- [16] Z. Wang, Z. Han, S. Chen, F. Xue, Z. Ding, X. Xiao, V. Tresp, P. Torr, and J. Gu, "Stop reasoning! when multimodal llms with chain-of-thought reasoning meets adversarial images," *arXiv preprint arXiv:2402.14899*, 2024.
- [17] D. Lu, T. Pang, C. Du, Q. Liu, X. Yang, and M. Lin, "Test-time backdoor attacks on multimodal large language models," *arXiv preprint arXiv:2402.08577*, 2024.
- [18] X. Gu, X. Zheng, T. Pang, C. Du, Q. Liu, Y. Wang, J. Jiang, and M. Lin, "Agent smith: A single image can jailbreak one million multimodal llm agents exponentially fast," *arXiv preprint arXiv:2402.08567*, 2024.
- [19] Z. Tan, C. Zhao, R. Moraffah, Y. Li, Y. Kong, T. Chen, and H. Liu, "The wolf within: Covert injection of malice into mllm societies via an mllm operative," *arXiv preprint arXiv:2402.14859*, 2024.
- [20] M. Qraitem, N. Tasnim, K. Saenko, and B. A. Plummer, "Vision-llms can fool themselves with self-generated typographic attacks," *arXiv preprint arXiv:2402.00626*, 2024.
- [21] Y. Wu, X. Li, Y. Liu, P. Zhou, and L. Sun, "Jailbreaking gpt-4v via self-adversarial attacks with system prompts," *arXiv preprint arXiv:2311.09127*, 2023.
- [22] Y. Dong, H. Chen, J. Chen, Z. Fang, X. Yang, Y. Zhang, Y. Tian, H. Su, and J. Zhu, "How robust is google's bard to adversarial image attacks?," *arXiv preprint arXiv:2309.11751*, 2023.
- [23] X. Wang, Z. Ji, P. Ma, Z. Li, and S. Wang, "Instructta: Instruction-tuned targeted attack for large vision-language models," *arXiv preprint arXiv:2312.01886*, 2023.
- [24] E. Bagdasaryan and V. Shmatikov, "Ceci n'est pas une pomme: Adversarial illusions in multi-modal embeddings," *arXiv preprint arXiv:2308.11804*, 2023.
- [25] D. Han, X. Jia, Y. Bai, J. Gu, Y. Liu, and X. Cao, "Ot-attack: Enhancing adversarial transferability of vision-language models via optimal transport optimization," *arXiv preprint arXiv:2312.04403*, 2023.
- [26] Z. Niu, H. Ren, X. Gao, G. Hua, and R. Jin, "Jailbreaking attack against multimodal large language model," *arXiv preprint arXiv:2402.02309*, 2024.
- [27] X. Tao, S. Zhong, L. Li, Q. Liu, and L. Kong, "Imgtrojan: Jailbreaking vision-language models with one image," *arXiv preprint arXiv:2403.02910*, 2024.
- [28] Y. Xu, J. Yao, M. Shu, Y. Sun, Z. Wu, N. Yu, T. Goldstein, and F. Huang, "Shadowcast: Stealthy data poisoning attacks against vision-language models," *arXiv preprint arXiv:2402.06659*, 2024.
- [29] J. Liang, S. Liang, M. Luo, A. Liu, D. Han, E.-C. Chang, and X. Cao, "VI-trojan: Multimodal instruction backdoor attacks against autoregressive visual language models," *arXiv preprint arXiv:2402.13851*, 2024.
- [30] J. Rehberger, "Image to prompt injection with google bard," <https://embracethered.com/blog/posts/2023/google-bard-image-to-prompt-injection/>, 2023.
- [31] J. Zhang, Q. Yi, and J. Sang, "Towards adversarial attack on vision-language pre-training models," in *Proceedings of the 30th ACM International Conference on Multimedia*, pp. 5005–5013, 2022.
- [32] D. Lu, Z. Wang, T. Wang, W. Guan, H. Gao, and F. 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*, pp. 102–111, 2023.
- [33] Z. Zhou, S. Hu, M. Li, H. Zhang, Y. Zhang, and H. Jin, "Advclip: Downstream-agnostic adversarial examples in multimodal contrastive learning," in *Proceedings of the 31st ACM International Conference on Multimedia*, pp. 6311–6320, 2023.
- [34] Z. Yin, M. Ye, T. Zhang, T. Du, J. Zhu, H. Liu, J. Chen, T. Wang, and F. Ma, "Vlattack: Multimodal adversarial attacks on vision-language tasks via pre-trained models," *arXiv preprint arXiv:2310.04655*, 2023.
- [35] Y. Wang, W. Hu, Y. Dong, and R. Hong, "Exploring transferability of multimodal adversarial samples for vision-language pre-training models with contrastive learning," *arXiv preprint arXiv:2308.12636*, 2023.
- [36] B. He, X. Jia, S. Liang, T. Lou, Y. Liu, and X. Cao, "Sa-attack: Improving adversarial transferability of vision-language pre-training models via self-augmentation," *arXiv preprint arXiv:2312.04913*, 2023.
- [37] Y. Nesterov and V. Spokoiny, "Random gradient-free minimization of convex functions," *Foundations of Computational Mathematics*, vol. 17, no. 2, pp. 527–566, 2017.
- [38] P. Chao, A. Robey, E. Dobriban, H. Hassani, G. J. Pappas, and E. Wong, "Jailbreaking black box large language models in twenty queries," *arXiv preprint arXiv:2310.08419*, 2023.
- [39] S. Li, M. Xue, B. Z. H. Zhao, H. Zhu, and X. Zhang, "Invisible backdoor attacks on deep neural networks via steganography and regularization," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 5, pp. 2088–2105, 2021.
- [40] S. Li, H. Liu, T. Dong, B. Z. H. Zhao, M. Xue, H. Zhu, and J. Lu, "Hidden backdoors in human-centric language models," in *Proceedings of ACM CCS*, 2021.
- [41] M. Li, L. Li, Y. Yin, M. Ahmed, Z. Liu, and Q. Liu, "Red teaming visual language models," *arXiv preprint arXiv:2401.12915*, 2024.
- [42] W. Yang, J. Gao, and B. Mirzasoleiman, "Robust contrastive language-image pretraining against data poisoning and backdoor attacks," *Advances in Neural Information Processing Systems*, vol. 36, 2024.
- [43] J. Zhang, X. Ma, X. Wang, L. Qiu, J. Wang, Y.-G. Jiang, and J. Sang, "Adversarial prompt tuning for vision-language models," *arXiv preprint arXiv:2311.11261*, 2023.
- [44] L. Li, H. Guan, J. Qiu, and M. Spratling, "One prompt word is enough to boost adversarial robustness for pre-trained vision-language models," *arXiv preprint arXiv:2403.01849*, 2024.
- [45] Y. Chen, K. Sikka, M. Cogswell, H. Ji, and A. Divakaran, "Dress: Instructing large vision-language models to align and interact with humans via natural language feedback," *arXiv preprint arXiv:2311.10081*, 2023.
- [46] X. Zhang, C. Zhang, T. Li, Y. Huang, X. Jia, X. Xie, Y. Liu, and C. Shen, "A mutation-based method for multi-modal jailbreaking attack detection," *arXiv preprint arXiv:2312.10766*, 2023.
- [47] R. Pi, T. Han, Y. Xie, R. Pan, Q. Lian, H. Dong, J. Zhang, and T. Zhang, "Mllm-protector: Ensuring mllm's safety without hurting performance," *arXiv preprint arXiv:2401.02906*, 2024.
- [48] P. Wang, D. Zhang, L. Li, C. Tan, X. Wang, K. Ren, B. Jiang, and X. Qiu, "Inferaligner: Inference-time alignment for harmlessness through cross-model guidance," *arXiv preprint arXiv:2401.11206*, 2024.
- [49] Y. Wang, X. Liu, Y. Li, M. Chen, and C. Xiao, "Adashield: Safeguarding multimodal large language models from structure-based attack via adaptive shield prompting," *arXiv preprint arXiv:2403.09513*, 2024.
- [50] J. Gou, K. Chen, Z. Liu, L. Hong, H. Xu, Z. Li, D.-Y. Yeung, Y. T. Kwok, and Y. Zhang, "Eyes closed, safety on: Protecting multimodal llms via image-to-text transformation," *arXiv preprint arXiv:2403.09572*, 2024.