Exploring the Transferability of Visual Prompting for Multimodal Large Language Models

Supplementary Material

A. Detailed Experimental Settings

Here we describe the detailed experimental settings to guarantee the reproducibility. All experiments are conducted on NVIDIA A100-80GB GPUs.

A.1. Datasets

In this work, we adopt 10 datasets in total to validate the effectiveness of the proposed TVP. We categorize them into 4 visual or multimodal tasks and we will introduce them respectively.

Object Recognition. Following [2, 9], we take closeended evaluation for recognition, restricting the vocabulary to the category names of the datasets. To be specific, The prompt given to the models is "*This is a photo of a*" and the target for text completion will be the ground-truth label in text. We concatenate each candidate category after the prompt and select the one with maximum log-likelihood as the prediction. The description for TSE is in the template of "*This is a photo of a {ground-truth label*}".

We take 7 datasets for this task, including CIFAR-10, CIFAR-100 [31], ImageNette [19] (a subset of ImageNet), which are commonly used for image classification, and SVHN [42], Oxford Pets [23], FGVCAircraft [41] (manufacturer level), Food101 [6], which are popular datasets for fine-grained classification in specific domains. By default, we take the train split for training, val split for validation and test split for testing as provided in the dataset. If val split is not provided, we sample a certain proportion for validation.

Object Counting. We take CLEVR [25] as an example. Unlike recognition, we take an open-ended evaluation for object counting. We ask the models "*How many objects are there in this image? Answer with a single number.*" and generate the response with do_sample set False and other parameters as default. We evaluate the response as correct or not by checking whether the answer of number appears in it. The corresponding description for TSE is "*There are* {*number*} *objects in this image*". We take the train split for training and sample 10% and 20% out of val split for validation and testing respectively.

Multimodal Reasoning. We take Hatefulmemes [29] for multimodal reasoning, which ask the models to decide whether the text on the meme and the visual content combined together convey hatred. Following [9], the prompt is *"This is an image with "{}" written on it. Is it hateful?"*, and we take the ranking method used for recognition here with "Yes" and "No" as labels. We use the normalized log-

likelihood to calculate ROC AUC score. The description for TSE is "*This is (not) hateful*". We take 90% of train split for training, the rest 10% for validation and dev split for testing.

Hallucination Correction. We take POPE [35], which ask the models whether there is a certain object in the image or not to evaluate their hallucination. The prompt given to the model is consistent with the default setting in official code, as "Is there a "{}" in the image?" and we also take "Yes" and "No" as labels. The description for TSE is in the template of "There are {object list} in the image." based on the annotations from MSCOCO [36]. We take the public release split (3000 samples) for testing and generate another dataset of 12000 samples for training and validation with 90%-10% random split. In this work, we only adopt datasets built with adversarial negative sampling strategy to challenge the models at utmost.

A.2. Models

We select 6 modern MLLMs for experiments. These models have different implementations, for instance BLIVA [21] uses two projection layers to better address visual-text alignment and VPGTrans [63] introduces the concept of visual prompt generator to transfer pre-trained visual encoder across different LLMs. We clone the official codebase of different models and unify the interface for training and inference to better incorporate different models.

The detailed configuration for them mainly involves the the choices of LLMs. We take Vicuna-7B-v0 [8] for MiniGPT-4 [69], BLIVA and VPGTrans, Vicuna-7B-v1.1 for InstructBLIP [9], Flan-T5-XL [55] for BLIP2 [34], and ChatGLM-6B [61] for VisualGLM-6B [1]. For visual encoders, these MLLMs share the structure of ViT-G/14, but with different projection layers and training paradigms, which guarantee the model diversity. These models can be deployed conveniently following the official instructions provided in the repositories.

As for the CLIP's visual encoder for TSE, we use ViT-B/32, a lightweight and popular version for studying CLIP. Since TSE is to introduce extra task knowledge, it does not need to have the same visual encoder as MLLMs.

A.3. Hyperparameters

We introduce the setting of hyperparameters in this work. The design of visual prompts has been introduced in Sec. 3.1. The batch size for training is 16. The learning rate γ in Eq. (7) is 10 by default. The maximal number of

training epochs is 10 with cosine scheduler following [56].

For the weights for the proposed FCA and TSE loss terms, we set them optimal by searching within {0.0005, 0.001, 0.003, 0.005, 0.008} and {0.0001, 0.0005, 0.001} respectively on validation set, while keeping other hyperparameters consistent with baselines.

B. Additional Results

B.1. Results on Other Datasets

Besides the 6 datasets displayed in the main paper, we also validate the effectiveness of our method on 4 commonly used classification datasets and demonstrate the results in Tab. 6.

Apart from the coarse-grained classification dataset CIFAR-100, the zero-shot performance of modern MLLMs on these fine-grained datasets in specific domains is far from satisfactory, further emphasizing the necessities for adapting MLLMs to downstream tasks.

The observations and conclusions in Sec. 4.2 remain consistent. We can see that visual prompts generated by TVP on a single model (MiniGPT-4 or InstructBLIP) bring the most significant improvements to 6 models. Moreover, by ensembling two models for training visual prompts, the performance is further boosted to higher levels.

B.2. Results on Corrupted Datasets

Robustness has been a crucial issue for deep neural network, concerning the stability of model in applications. It is natural to evaluate the robustness of visual prompts to image common corruptions [17]. We examine the performance of visual prompts generated by MiniGPT-4 on corrupted datasets like CIFAR-10-C and ImageNette-C. We set the severity level as 3 and test with 15 corruptions. We use the official release of CIFAR-10-C and the official code¹ to generate corresponding corrupted dataset for ImageNette.

The results are shown in Tab. 9. Visual prompts generated by VP and EVP cannot effectively improve the 6 models on average under the corruptions imposed to CIFAR-10, while TVP can still bring 2.30% and 3.09% on CIFAR-10-C and ImageNette-C respectively. The results indicate that the consolidation of task-agnostic representations and enhancement of task-related semantics by TVP effectively strengthen the robustness of learned visual prompts to common image corruptions.

B.3. Detailed Results for Ablations and Analyses

Due to space limit, we only report the average performance or average delta in performance for ablation studies in Sec. 4.4 and in-depth analyses in Sec. 4.5. Here, we display the results for each setting and each model in detail. Detailed results for Tab. 2 are in Tab. 10, those for Tab. 3 are in Tab. 7, those for Fig. 5 are in Tab. 11 and those for Tab. 4 are in Tab. 8.

C. Discussion on Computational Efficiency

As we target on efficient adaptation for diverse MLLMs rather than fine-tuning each of them respectively, we here discuss the computational efficiency of the proposed TVP.

C.1. Comparison with Fine-tuning Methods

We conduct additional experiments on an A100-80G GPU with half precision and the same batch size as TVP. If the training exceeds GPU memory (e.g., BLIVA), we adopt gradient accumulation. Here we use CIFAR-10 and the prompts trained on InstructBLIP to compare with full fine-tuning and LoRA. Results are displayed in Tab. 5. Though FFT and LoRA have moderately higher accuracy than TVP due to much larger numbers of trainable parameters (\geq 4B for FFT, \geq 8M for LoRA and \sim 70K for TVP), TVP has the minimal computation overhead, which is reflected in the smallest memory demand and the shortest average training time. When the computation resources are limited to fine-tuning, off-the-shelf visual prompts trained by TVP are expected to achieve black-box adaptation with no cost. This supports the motivation of our method.

	Ins	structBl	LIP		BLIP2		M	iniGPT	-4	BLIVA		
	FFT	LoRA	TVP	FFT	LoRA	TVP	FFT	LoRA	TVP	FFT	LoRA	TVP
Acc (%)	99.16	98.78	98.07	99.09	98.08	96.02	99.27	95.18	91.69	99.07	98.14	97.78
Mem. (GB)	63.5	33.8	31.1	36.9	21.8	9.2†	62.4	35.6	18.3†	66.5	55.2	18.5^{\dagger}
Time (min)	30	26	27	28	26	0	29	25	0	118	92	0

Table 5. Comparison of performance, memory costs and training time with fine-tuning methods. gray for black-box models, † for inference mode, since they need no training for TVP.

C.2. Comparison with Baseline Visual Prompting

Compared to the baselines, VP and EVP, TVP demands additional forward passes through vision encoders. Taking MiniGPT-4 for example, VP and EVP need one forward pass in each iteration and take around 820GFLOPs. For TVP, the combination of FCA and TSE demands an extra forward pass through the MLLM's visual encoder (~260GFLOPs, FCA) and another forward pass through CLIP (~7GFLOPs, TSE). While extra computation for TSE is negligible, FCA brings around 32% more computation overloads, with a similar increase in training time. However, the original visual features only need to be computed once, thus the cost for FCA can be distributed to each epoch and will only bring around 3% extra computations when trained for 10 epochs, which is acceptable. The computation overheads can be further alleviated in the future.

¹https://github.com/hendrycks/robustness

Recognition:	CIFAR-100	MiniGPT-4	InstructBLIP	BLIP2	VPGTrans	BLIVA	VisualGLM	Avg. Δ
	Clean	61.85	58.41	60.65	58.00	56.34	12.71	0.00
MiniGPT-4	VP [3] EVP [56] TVP (ours)	63.54* 71.05* 75.36 *	44.40 48.91 65.10	60.05 56.43 64.15	59.93 59.23 57.84	53.36 56.44 53.58	12.15 20.10 21.34	-2.42 +0.70 +4.90
InstructBLIP	VP [3] EVP [56] TVP (ours)	60.65 62.24 63.92	76.16* 78.68 * 77.92*	58.60 61.66 63.72	58.32 57.37 62.62	58.40 59.86 56.09	9.47 12.13 12.97	+2.27 +4.00 +4.88
Ensemble	VP [3] EVP [56] TVP (ours)	65.48* 70.13* 73.33*	71.77* 74.89* 77.62*	63.48 62.40 64.19	60.25 62.07 62.79	55.04 60.76 62.18	9.15 14.96 13.26	+2.87 +6.21 +7.57
Recognitio	on: Pet37	MiniGPT-4	InstructBLIP	BLIP2	VPGTrans	BLIVA	VisualGLM	Avg. Δ
	Clean	30.50	27.23	11.53	16.52	22.21	31.07	0.00
MiniGPT-4	VP [3] EVP [56] TVP (ours)	42.38* 56.67* 59.53 *	33.69 30.44 39.00	11.80 13.22 16.57	23.14 22.40 25.27	25.81 27.91 30.53	29.46 28.37 29.35	+4.54 +6.66 +10.20
InstructBLIP	VP [3] EVP [56] TVP (ours)	40.23 40.83 41.05	37.80* 65.25* 66.86 *	13.27 12.16 14.28	17.83 17.63 22.27	29.71 31.70 42.95	29.54 30.36 30.44	+4.89 +9.81 +13.13
Ensemble	VP [3] EVP [56] TVP (ours)	46.77* 56.99* 51.35*	43.80* 66.31* 61.60*	15.10 13.55 13.87	22.13 15.10 26.30	32.73 32.76 48.11	30.69 29.60 28.02	+8.69 +12.54 +15.03
Recognition	n: Aircraft	MiniGPT-4	InstructBLIP	BLIP2	VPGTrans	BLIVA	VisualGLM	Avg. Δ
Recognition	n: Aircraft	MiniGPT-4	InstructBLIP 10.26	6.54	VPGTrans 14.34	BLIVA 8.19	VisualGLM 4.05	Avg .Δ
Recognition	Clean VP [3] EVP [56] TVP (ours)	<pre> FLdDiul 8.55 30.15* 32.52* 33.99* </pre>	II.26 8.67 9.36 9.81	6.54 6.93 6.42 7.41	support 14.34 14.97 17.64 20.76	8.19 11.13 11.25 7.20	VisualGTW 4.05 4.02 4.02	Avg.∆ 0.00 +3.99 +4.88 +5.21
Recognition MiniGPT-4 InstructBLIP	Clean VP [3] EVP [56] TVP (ours) VP [3] EVP [56] TVP (ours)	*La 900 8.55 30.15* 32.52* 33.99* 12.90 22.92 30.48	All Transmission 10.26 8.67 9.36 9.81 16.92* 31.35* 36.03 *	6.54 6.93 6.42 7.41 4.59 5.28 4.02	sureLLDA 14.34 14.97 17.64 20.76 12.18 23.97 20.76	8.19 11.13 11.25 7.20 8.97 11.04 11.85	WIDIPURITY 4.02 4.02 4.02 4.02 4.02 4.02 4.02	Avg.Δ 0.00 +3.99 +4.88 +5.21 +1.27 +7.78 +9.21
Recognition MiniGPT-4 InstructBLIP Ensemble	Clean VP [3] EVP [56] TVP (ours) VP [3] EVP [56] TVP (ours) VP [3] EVP [56] TVP (ours)	*La 50 8.55 30.15* 32.52* 33.99* 12.90 22.92 30.48 28.68* 26.76* 30.27*	Al TIR TID.26 8.67 9.36 9.81 16.92* 31.35* 36.03* 25.50* 26.34* 24.84*	6.54 6.93 6.42 7.41 4.59 5.28 4.02 7.29 6.45 4.02	supplication of the second state of the second	8.19 11.13 11.25 7.20 8.97 11.04 11.85 11.52 12.22 24.00	WTBJINIA 4.05 4.02 4.02 4.02 4.02 4.02 4.02 4.02 4.02	Avg. Δ 0.00 +3.99 +4.88 +5.21 +1.27 +7.78 +9.21 +6.35 +6.83 +9.82
Recognition MiniGPT-4 InstructBLIP Ensemble Recognition	 Aircraft Clean VP [3] EVP [56] TVP (ours) VP [3] EVP [56] TVP (ours) VP [3] EVP [56] TVP (ours) 	** ** 0:115* 30.15* 32.52* 33.99* 12.90 22.92 30.48 26.76* 30.27* **	LID 26 10.26 8.67 9.36 9.81 16.92* 31.35* 36.03* 25.50* 26.34* 24.84* LID 25 25.50* 26.34* 24.84*	Carrier 6.54 6.93 6.42 7.41 4.59 5.28 4.02 7.29 6.45 4.02 Carrier Carrier	sue_LDdA 14.34 14.97 17.64 20.76 12.18 23.97 20.76 13.02 17.13 23.10	 KAI19 8.19 11.13 11.25 7.20 8.97 11.04 11.85 11.52 12.22 24.00 VATIE 	Algorithm Algorithm A.02 4.02 4.03 4.02 4.04 4.05 4.05 4.02 4.05 4.02 4.05 4.02 4.05 4.02 4.05 4.02 <	Avg.Δ 0.00 +3.99 +4.88 +5.21 +1.27 +7.78 +9.21 +6.35 +6.83 +9.82 Avg.Δ
Recognition MiniGPT-4 InstructBLIP Ensemble Recognition	 Aircraft Clean VP [3] EVP [56] TVP (ours) VP [3] EVP [56] TVP (ours) VP [3] EVP [56] TVP (ours) 	************************************	LITER 10.26 8.67 9.36 9.81 16.92* 31.35* 36.03* 25.50* 26.34* 24.84* LITER 28.99	6.54 6.93 6.42 7.41 4.59 5.28 4.02 7.29 6.45 4.02 7.29 6.45 4.02 7.29 6.45 4.02	sur_LDdA 14.34 14.97 17.64 20.76 12.18 23.97 20.76 13.02 17.13 23.10 sur_LDdA 30.42	VITB 8.19 11.13 11.25 7.20 8.97 11.04 11.52 12.22 24.00 VITB 36.08	WT01 A.05 A.02 A.03 A.05 A.02 A.03 A.04 A.05 A.05 <th< td=""><td>Avg.Δ 0.00 +3.99 +4.88 +5.21 +1.27 +7.78 +9.21 +6.35 +6.83 +9.82 Avg.Δ 0.00</td></th<>	Avg.Δ 0.00 +3.99 +4.88 +5.21 +1.27 +7.78 +9.21 +6.35 +6.83 +9.82 Avg.Δ 0.00
Recognition MiniGPT-4 InstructBLIP Ensemble Recognition MiniGPT-4	Lean VP [3] EVP [56] TVP (ours) VP [3] EVP [56] TVP (ours) VP [3] EVP [56] TVP (ours) Image: Clean VP [3] EVP [56] TVP (ours)	*** *** *** ***	LITER 10.26 8.67 9.36 9.81 16.92* 31.35* 36.03* 25.50* 26.34* 24.84* LITER 28.99 32.08 30.93 37.66	Carring 6.54 6.93 6.42 7.41 4.59 5.28 4.02 7.29 6.45 4.02 7.29 6.45 4.02 7.29 6.45 4.02 7.29 6.45 4.02 7.29 6.45 4.02 7.20 7.20 7.20 7.20 7.21 7.20 7.20 7.20 7.20 7.20 7.20 7.20 7.20	Suppl Su	Exercise 3 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	WT0IensiA 4.05 4.02 4.02 4.02 4.02 4.02 4.02 4.02 4.02	Avg. \triangle 0.00 +3.99 +4.88 +5.21 +1.27 +7.78 +9.21 +6.35 +6.83 +9.82 Avg. \triangle 0.00 -0.88 +3.95 +6.74
Recognition MiniGPT-4 InstructBLIP Ensemble Recognition MiniGPT-4 InstructBLIP	 Aircraft Clean VP [3] EVP [56] TVP (ours) VP [3] EVP [56] TVP (ours) VP [3] EVP [56] TVP (ours) Clean VP [3] EVP [56] TVP (ours) VP [3] EVP [56] TVP (ours) 	** ** 8.55 30.15* 32.52* 33.99* 12.90 22.92 30.48 26.76* 30.27* ** ** 4.66* 32.99 ** ** 50.14* 63.72* 64.16* 19.68 37.47 38.49 **	All TIRD DUB Sector 25, 2014 10,26 8,67 9,36 9,81 16,92* 31,35* 36,03* 25,50* 26,34* 24,84* All TIRD DUB 28,99 32,08 30,93 37,66 41,23* 64,95* 68,51*	Carring 6.54 6.93 6.42 7.41 4.59 5.28 4.02 7.29 6.45 4.02 7.29 6.45 4.02 7.29 6.45 4.02 7.29 6.45 4.02 7.29 6.45 4.02 7.41 8 4.729 334.10 45.43 33.70 48.95 33.70	Support 14.34 14.34 14.97 17.64 20.76 12.18 23.97 20.76 13.02 17.13 23.10 30.42 23.49 27.64 29.43 20.485 31.25 31.13	Exprime 8.19 11.13 11.25 7.20 8.97 11.04 11.85 11.52 22.22 24.00 36.08 31.92 33.74 36.36 36.38 43.37 44.75	W10JensiA 4.05 4.02 4.02 4.02 4.02 4.02 4.02 4.02 4.02	Avg. \triangle 0.00 +3.99 +4.88 +5.21 +1.27 +7.78 +9.21 +6.35 +6.83 +9.82 Avg. \triangle 0.00 -0.88 +3.95 +6.74 +8.01 +9.46

Table 6. Results on 4 more datasets of object recognition. Visual prompts are trained on MiniGPT-4, InstructBLIP and their ensemble with different methods, and further tested on 6 modern MLLMs. Top-1 accuracy (%) is reported.

Trained on	Prompt Wid.	MiniGPT-4	InstructBLIP	BLIP2	VPGTrans	BLIVA	VisualGLM	Avg. Δ
	5	94.29	84.17	89.40	91.60	90.94	90.15	+2.84
	10	96.00	84.03	93.17	91.82	92.73	85.17	+3.23
MiniGPT 4	20	96.82	91.26	86.68	88.49	93.71	90.39	+3.97
WIIIIOI I-4	40	95.70	89.44	88.49	87.68	89.69	88.78	+2.71
	50	96.77	87.29	87.62	88.26	88.05	87.15	+1.93
	80	94.21	78.21	86.41	84.02	85.91	76.62	-3.03
	5	89.73	96.41	85.08	91.95	93.64	88.97	+3.71
	10	88.03	97.06	92.47	91.89	94.90	91.72	+5.42
Instruct DI ID	20	88.04	98.04	82.78	93.96	97.95	93.13	+5.06
IIISUUCIDLIP	40	85.16	98.24	86.37	89.21	89.88	93.55	+3.15
	50	84.52	97.81	93.58	87.33	91.50	86.28	+2.91
	80	82.38	94.75	83.15	81.85	88.31	80.39	-2.12
	5	91.64	94.53	94.72	88.97	94.71	86.94	+4.66
	10	95.08	95.65	92.73	87.58	94.00	78.77	+3.38
Encomble	20	95.19	96.55	93.37	90.59	96.23	84.33	+5.45
Liisemble	40	97.73	97.41	84.59	91.52	97.17	90.34	+5.87
	50	96.60	97.31	88.85	88.20	95.02	88.31	+5.12
	80	92.01	95.99	84.14	81.64	94.14	91.62	+2.67

Table 7. Detaile results for the ablation study about the impact of prompt width on the performance of TVP on CIFAR-10 in Tab. 3.

Datasets	Model	MiniGPT-4	InstructBLIP	BLIP2	VPGTrans	BLIVA	VisualGLM	Avg. Δ
CIFAR-10	VP [3]	87.97	94.20	82.59	88.64	89.13	90.47	+1.57
	EVP [56]	81.89	89.44	82.19	90.11	84.15	95.14	-0.11
	TVP (ours)	88.80	94.38	89.92	91.53	89.91	93.63	+4.10
ImageNette	VP [3]	84.25	74.70	92.00	81.50	84.59	72.79	+1.24
	EVP [56]	83.18	77.38	87.39	83.31	79.82	72.18	+0.14
	TVP (ours)	88.36	77.20	94.01	82.78	80.15	73.86	+2.33
SVHN	VP [3]	39.42	30.00	32.87	33.57	27.49	21.62	-0.29
	EVP [56]	35.34	24.27	33.20	34.63	21.97	20.24	-2.84
	TVP (ours)	41.98	30.02	26.88	39.49	31.55	26.23	+1.57
Pet37	VP [3]	34.15	33.01	14.64	20.82	25.40	28.26	+2.87
	EVP [56]	33.39	31.34	9.46	16.54	29.35	26.25	+1.21
	TVP (ours)	38.05	30.01	14.99	23.58	28.56	27.12	+3.87
Aircraft	VP [3]	16.50	7.74	5.88	13.08	10.56	4.02	+0.97
	EVP [56]	19.05	9.24	4.05	11.01	9.09	4.02	+0.75
	TVP (ours)	15.15	11.58	4.05	10.68	8.58	4.02	+0.35
Food101	VP [3]	31.45	27.33	40.48	29.19	41.70	5.31	-1.04
	EVP [56]	33.03	33.27	37.90	26.85	40.24	4.08	-1.05
	TVP (ours)	37.47	43.84	38.89	28.95	38.93	4.95	+1.89

Table 8. Detailed results for the analysis on the generalization of TVP using ensemble across diverse recognition datasets in Tab. 4.

Corruption Types	Fog	JPEG Compression	Zoom Blur	Glass Blur	Shot Noise	Defocus Blur	Elastic Transform	Frost	Brightness	Snow	Gaussian noise	Motion Blur	Contrast	Impulse Noise	Pixelate	Avg. Δ
Clean VP [3] EVP [56] TVP (ours)	85.73 81.96 85.31 89.46	69.41 55.36 57.10 68.65	82.87 79.68 82.51 87.46	70.72 58.69 58.49 67.95	71.13 60.05 63.76 71.92	85.93 82.67 85.93 89.95	82.87 80.42 83.90 87.85	83.12 77.66 80.46 85.58	86.69 83.59 86.78 90.82	82.69 78.71 82.33 86.76	65.85 52.67 56.20 66.12	80.24 74.12 76.57 83.01	86.72 82.86 85.96 90.02	79.38 71.06 75.04 80.71	81.75 76.26 76.67 83.34	0.00 -6.62 -3.87 +2.30
	a) Aver	age performan	ce unde	er diffe	rent co	mmon co	rruptions at	level	3 on CIFAR	-10 wi	th visual p	rompts g	enerated of	on MiniC	PT-4.	
(a Corruption Types	a) Aver	age performan JPEG Compression	ce unde Zoom Blur	er diffe Glass Blur	Shot Noise	Defocus Blur	Elastic Transform	Frost	3 on CIFAR Brightness	-10 wit	th visual p Gaussian noise	Motion Blur	contrast	on MiniC Impulse Noise	PT-4.	Avg. Δ

(b) Average performance under different common corruptions at level 3 on ImageNette with visual prompts generated on MiniGPT-4.

Table 9. Average performance under common corruptions [17] of different methods on CIFAR-10 and ImageNette. Visual prompts generated by the proposed TVP still lead to the most significant improvements, showing better robustness to common corruptions.

FCA	TSE	MiniGPT-4	InstructBLIP	BLIP2	VPGTrans	BLIVA	VisualGLM	Avg. Δ	FCA	TSE	MiniGPT-4	InstructBLIP	BLIP2	VPGTrans	BLIVA	VisualGLM	Avg. Δ
×	X	97.97	84.57	83.39	86.93	86.45	85.92	0.28	×	X	96.79	68.15	91.36	79.08	75.82	76.05	0.81
\checkmark	X	97.95	86.97	90.58	90.94	92.18	87.82	3.82	\checkmark	X	95.87	75.87	96.51	82.24	78.19	70.11	2.73
X	\checkmark	97.94	86.93	85.74	90.32	92.78	81.30	1.91	×	\checkmark	97.81	67.59	91.64	78.35	84.23	82.93	3.36
\checkmark	\checkmark	98.33	92.82	91.68	88.70	87.48	87.53	3.83	\checkmark	\checkmark	97.71	78.34	94.98	86.34	84.51	75.34	5.80
	(a) CIFAR-10											(b) Imagel	Nette			
FCA	TSE	MiniGPT-4	InstructBLIP	BLIP2	VPGTrans	BLIVA	VisualGLM	Avg. Δ	FCA	TSE	MiniGPT-4	InstructBLIP	BLIP2	VPGTrans	BLIVA	VisualGLM	Avg.Δ
X	X	74.24	41.59	48.87	57.61	36.11	33.12	17.48	×	X	52.17	39.03	20.17	8.00	34.23	13.60	8.64
\checkmark	X	74.81	56.69	52.98	51.96	50.35	24.93	20.84	\checkmark	X	50.57	36.03	22.30	20.93	32.53	18.03	10.83
X	\checkmark	81.39	53.41	50.99	59.46	56.60	32.91	24.68	×	\checkmark	54.07	31.33	16.60	20.33	32.87	21.07	10.15
\checkmark	\checkmark	75.17	54.32	61.95	51.10	60.28	32.17	24.72	\checkmark	\checkmark	51.00	42.90	22.07	19.50	36.00	13.00	11.51
				(c) SVH	IN				(d) CLEVR								
FCA	TSE	MiniGPT-4	InstructBLIP	BLIP2	VPGTrans	BLIVA	VisualGLM	Avg. Δ	FCA	TSE	MiniGPT-4	InstructBLIP	BLIP2	VPGTrans	BLIVA	VisualGLM	Avg.Δ
×	×	57.58	60.66	55.34	56.87	60.64	57.27	0.09	×	×	68.06	69.80	50.00	61.07	71.33	69.40	0.90
\checkmark	X	56.99	63.24	54.15	58.82	63.00	57.52	0.99	\checkmark	X	69.60	74.00	50.13	59.47	74.80	70.27	2.33
X	\checkmark	58.31	61.65	55.20	56.43	61.66	56.40	0.31	×	\checkmark	69.00	75.13	49.93	61.27	72.40	69.47	2.15
\checkmark	\checkmark	56.93	62.38	56.20	60.19	64.09	58.15	1.69	\checkmark	\checkmark	68.73	75.13	51.40	64.47	72.67	71.00	3.19
			(e)	Hatefulr	nemes								(f) POF	Έ			

Table 10. Detailed results for the ablation study on different combinations of FCA and TSE in Tab. 2.

Model	l	MiniGPT-4	InstructBLIP	BLIP2	VPGTrans	BLIVA	VisualGLM	Avg.	Model	l	MiniGPT-4	InstructBLIP	BLIP2	VPGTrans	BLIVA	VisualGLM	Avg.	
			CII	FAR-10					ImageNette									
VP [3]	1% 5% 10% 25% 50%	83.08 82.06 84.29 90.97 90.53	74.95 76.07 77.58 80.35 81.14	79.80 79.20 80.00 82.42 77.45	80.35 80.97 80.99 81.34 83.29	81.67 80.07 81.96 84.63 84.31	75.28 77.98 73.38 77.28 79.84	79.19 79.39 79.70 82.83 82.76	VP [3]	1% 5% 10% 25% 50%	77.58 81.91 78.22 82.42 82.01	64.08 64.28 65.17 60.25 62.14	93.50 91.80 95.13 93.12 92.64	77.73 81.40 77.12 79.29 76.66	73.53 80.48 67.52 71.41 77.83	72.25 73.45 72.43 76.10 76.94	76.45 78.89 75.93 77.10 78.04	
EVP [56]	1% 5% 10% 25% 50%	97.11 97.85 97.93 98.24 98.00	86.67 85.56 83.15 85.16 84.07	83.74 83.06 83.00 82.29 83.86	87.06 86.64 88.81 87.53 87.39	89.23 87.92 84.78 85.71 86.66	82.60 86.49 86.49 85.72 86.01	87.74 87.92 87.36 87.44 87.67	EVP [56]	1% 5% 10% 25% 50%	93.01 97.61 98.00 97.44 97.40	62.00 62.80 71.87 76.08 62.06	94.96 89.10 90.37 89.15 85.12	74.07 77.10 72.97 63.99 74.70	83.38 79.88 76.05 84.58 82.52	80.57 80.25 75.85 74.24 86.57	81.33 81.12 80.85 80.91 81.39	
TVP (ours)	1% 5% 10% 25% 50%	97.80 97.24 97.85 98.23 97.68	86.04 87.79 87.69 84.86 87.59	85.27 88.32 90.82 89.20 93.57	87.90 87.28 87.36 87.61 86.33	88.65 90.09 91.97 89.96 88.12	89.69 89.14 87.87 86.34 85.25	89.23 89.98 90.59 89.37 89.76	TVP (ours)	1% 5% 10% 25% 50%	96.13 97.61 97.20 97.63 98.09	72.08 62.70 72.25 72.48 73.99	89.30 91.80 94.70 89.86 90.29	79.06 76.87 83.21 85.96 84.66	90.78 83.46 82.93 80.46 86.09	70.45 91.95 74.68 73.71 75.03	82.97 84.07 84.16 83.35 84.69	
			S	VHN								CI	LEVR					
VP [3]	1% 5% 10% 25% 50%	67.63 66.96 81.06 58.26 73.98	47.78 38.52 35.09 41.86 50.65	43.42 47.80 21.37 50.85 46.92	36.19 44.07 40.87 58.74 45.37	38.35 33.59 32.99 35.33 43.52	26.21 34.96 20.47 29.64 20.82	43.26 44.32 38.64 45.78 46.88	VP [3]	1% 5% 10% 25% 50%	33.17 38.37 40.13 39.81 39.30	31.57 27.57 36.00 26.44 28.80	12.73 12.83 23.33 12.95 12.77	12.73 21.63 10.97 12.50 12.00	32.87 19.23 28.67 21.84 28.63	12.87 12.57 12.63 13.77 12.83	22.66 22.03 25.29 21.22 22.39	
EVP [56]	1% 5% 10% 25% 50%	75.05 77.55 80.57 76.78 75.98	31.80 44.95 42.22 44.75 41.35	52.44 48.97 61.53 51.18 47.41	42.97 57.99 53.69 59.47 55.47	44.37 39.28 53.69 46.58 34.93	27.53 36.55 22.24 33.14 30.37	45.69 50.88 52.32 51.98 47.59	EVP [56]	1% 5% 10% 25% 50%	47.03 25.07 49.80 44.70 53.70	35.53 35.97 34.57 32.43 42.60	15.47 27.93 16.43 20.67 20.10	11.37 9.77 15.60 16.40 7.47	31.80 34.60 32.40 35.57 33.87	13.03 14.30 13.10 12.90 12.90	25.71 24.61 26.98 27.11 28.44	
TVP (ours)	1% 5% 10% 25% 50%	79.68 85.53 80.52 80.70 82.58	38.39 48.70 47.70 51.20 51.23	56.55 64.67 61.37 62.89 65.77	46.34 58.15 56.63 59.59 59.79	48.16 48.28 45.20 59.93 53.57	33.36 39.79 35.24 35.20 35.91	50.41 57.52 54.44 58.25 58.14	TVP (ours)	1% 5% 10% 25% 50%	45.60 43.10 48.77 47.13 47.37	37.70 17.50 45.93 42.77 42.37	15.13 26.60 14.53 19.80 24.43	25.50 15.03 20.60 21.13 15.70	34.70 41.80 37.67 34.53 35.27	12.77 23.17 13.40 12.87 13.30	28.57 27.87 30.15 29.71 29.74	
			Hatef	ulmeme	es							Р	OPE					
VP [3]	1% 5% 10% 25% 50%	57.04 57.08 57.50 60.16 57.27	56.22 56.44 55.73 58.05 55.97	60.26 54.53 57.94 57.49 53.82	51.79 53.84 55.40 55.54 54.38	49.67 54.68 53.38 53.21 54.70	56.58 54.31 48.88 48.01 55.34	55.26 55.15 54.81 55.41 55.25	VP [3]	1% 5% 10% 25% 50%	54.67 51.53 52.73 53.93 51.00	68.13 66.87 70.67 70.73 71.27	49.87 50.00 50.00 49.87 50.00	58.07 62.87 59.07 59.27 63.07	72.53 73.73 73.00 73.27 73.93	69.67 71.53 69.13 71.60 69.33	62.16 62.76 62.43 63.11 63.10	
EVP [56]	1% 5% 10% 25% 50%	48.33 54.29 55.02 58.26 57.42	60.13 62.50 62.45 59.88 61.64	55.84 52.35 50.84 54.90 57.07	61.23 55.90 57.80 54.60 52.98	59.54 61.70 63.04 62.16 61.64	56.94 57.02 57.31 58.92 57.64	57.00 57.29 57.74 58.12 58.07	EVP [56]	1% 5% 10% 25% 50%	51.60 60.73 64.73 58.73 61.36	74.00 67.60 65.33 73.93 72.13	50.00 50.04 50.00 50.00 49.95	58.67 61.24 59.67 60.67 61.27	72.53 74.77 71.67 74.20 72.69	68.13 69.47 70.47 69.47 69.98	62.49 63.97 63.65 64.50 64.56	
TVP (ours)	1% 5% 10% 25% 50%	51.60 53.65 54.75 59.83 55.34	61.32 62.68 61.40 61.81 62.45	55.06 53.30 54.52 53.86 53.51	59.24 58.00 59.10 57.17 59.42	61.36 62.48 62.53 62.88 64.65	57.80 58.22 58.02 57.45 58.06	57.73 58.06 58.39 58.83 58.91	TVP (ours)	1% 5% 10% 25% 50%	61.00 62.73 59.87 71.13 70.47	71.47 69.47 75.47 69.93 68.67	50.13 50.00 49.87 49.60 49.87	59.00 65.20 65.13 60.60 61.00	75.00 72.47 74.27 72.67 75.47	69.80 70.53 70.67 70.40 70.33	64.40 65.07 65.88 65.72 65.97	

Table 11. Detailed results for the analysis on the impact from different training data scales in Fig. 5.

References

- [1] Visualghm-6b. https://github.com/THUDM/ VisualGLM-6B/, 2023. 5, 7, 1
- [2] Jean-Baptiste Alayrac, Jeff Donahue, Pauline Luc, Antoine Miech, Iain Barr, Yana Hasson, Karel Lenc, Arthur Mensch, Katherine Millican, Malcolm Reynolds, et al. Flamingo: a visual language model for few-shot learning. In Advances in Neural Information Processing Systems, pages 23716– 23736, 2022. 1, 2
- [3] Hyojin Bahng, Ali Jahanian, Swami Sankaranarayanan, and Phillip Isola. Exploring visual prompts for adapting largescale models. *arXiv preprint arXiv:2203.17274*, 2022. 1, 2, 3, 4, 6, 5
- [4] Yijun Bian and Huanhuan Chen. When does diversity help generalization in classification ensembles? *IEEE Transactions on Cybernetics*, 52(9):9059–9075, 2021. 7
- [5] Rishi Bommasani, Drew A Hudson, Ehsan Adeli, Russ Altman, Simran Arora, Sydney von Arx, Michael S Bernstein, Jeannette Bohg, Antoine Bosselut, Emma Brunskill, et al. On the opportunities and risks of foundation models. *arXiv* preprint arXiv:2108.07258, 2021. 1
- [6] Lukas Bossard, Matthieu Guillaumin, and Luc Van Gool. Food-101 – mining discriminative components with random forests. In *Computer Vision – ECCV 2014*, pages 446–461, 2014. 7, 1
- [7] Huanran Chen, Yichi Zhang, Yinpeng Dong, and Jun Zhu. Rethinking model ensemble in transfer-based adversarial attacks. arXiv preprint arXiv:2303.09105, 2023. 7
- [8] Wei-Lin Chiang, Zhuohan Li, Zi Lin, Ying Sheng, Zhanghao Wu, Hao Zhang, Lianmin Zheng, Siyuan Zhuang, Yonghao Zhuang, Joseph E. Gonzalez, Ion Stoica, and Eric P. Xing. Vicuna: An open-source chatbot impressing gpt-4 with 90%* chatgpt quality, 2023. 1
- [9] Wenliang Dai, Junnan Li, Dongxu Li, Anthony Meng Huat Tiong, Junqi Zhao, Weisheng Wang, Boyang Li, Pascale Fung, and Steven C. H. Hoi. Instructblip: Towards generalpurpose vision-language models with instruction tuning. *arXiv preprint arXiv:2305.06500*, 2023. 1, 2, 3, 4, 5, 6, 7
- [10] Yinpeng Dong, Fangzhou Liao, Tianyu Pang, Hang Su, Jun Zhu, Xiaolin Hu, and Jianguo Li. Boosting adversarial attacks with momentum. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition* (*CVPR*), pages 9185–9193, 2018. 3, 7
- [11] Yinpeng Dong, Tianyu Pang, Hang Su, and Jun Zhu. Evading defenses to transferable adversarial examples by translation-invariant attacks. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, pages 4312–4321, 2019. 2
- [12] Yinpeng Dong, Huanran Chen, Jiawei Chen, Zhengwei Fang, Xiao Yang, Yichi Zhang, Yu Tian, Hang Su, and Jun Zhu. How robust is google's bard to adversarial image attacks? arXiv preprint arXiv:2309.11751, 2023. 7
- [13] Zhengxiao Du, Yujie Qian, Xiao Liu, Ming Ding, Jiezhong Qiu, Zhilin Yang, and Jie Tang. GLM: General language model pretraining with autoregressive blank infilling. In Proceedings of the 60th Annual Meeting of the Association for

Computational Linguistics (Volume 1: Long Papers), pages 320–335, 2022. 7

- [14] Gamaleldin F. Elsayed, Ian Goodfellow, and Jascha Sohl-Dickstein. Adversarial reprogramming of neural networks. In *International Conference on Learning Representations*, 2019. 3, 4
- [15] Chaoyou Fu, Peixian Chen, Yunhang Shen, Yulei Qin, Mengdan Zhang, Xu Lin, Zhenyu Qiu, Wei Lin, Jinrui Yang, Xiawu Zheng, et al. Mme: A comprehensive evaluation benchmark for multimodal large language models. arXiv preprint arXiv:2306.13394, 2023. 1, 2, 5
- [16] Anisha Gunjal, Jihan Yin, and Erhan Bas. Detecting and preventing hallucinations in large vision language models. arXiv preprint arXiv:2308.06394, 2023. 2
- [17] Dan Hendrycks and Thomas Dietterich. Benchmarking neural network robustness to common corruptions and perturbations. In *International Conference on Learning Representations*, 2019. 8, 2, 4
- [18] Neil Houlsby, Andrei Giurgiu, Stanislaw Jastrzebski, Bruna Morrone, Quentin De Laroussilhe, Andrea Gesmundo, Mona Attariyan, and Sylvain Gelly. Parameter-efficient transfer learning for nlp. In *Proceedings of the 36th International Conference on Machine Learning*, pages 2790–2799, 2019. 2, 3
- [19] Jeremy Howard. imagenette. "https://github.com/ fastai/imagenette/". 5, 1
- [20] Edward J Hu, Yelong Shen, Phillip Wallis, Zeyuan Allen-Zhu, Yuanzhi Li, Shean Wang, Lu Wang, and Weizhu Chen. Lora: Low-rank adaptation of large language models. arXiv preprint arXiv:2106.09685, 2021. 2, 3
- [21] Wenbo Hu, Yifan Xu, Y Li, W Li, Z Chen, and Z Tu. Bliva: A simple multimodal llm for better handling of text-rich visual questions. arXiv preprint arXiv:2308.09936, 2023. 1, 3, 5
- [22] Qidong Huang, Xiaoyi Dong, Dongdong Chen, Weiming Zhang, Feifei Wang, Gang Hua, and Nenghai Yu. Diversity-aware meta visual prompting. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), pages 10878–10887, 2023. 3
- [23] C. V. Jawahar, A. Zisserman, A. Vedaldi, and O. M. Parkhi. Cats and dogs. In 2012 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), pages 3498–3505, 2012. 7, 1
- [24] Menglin Jia, Luming Tang, Bor-Chun Chen, Claire Cardie, Serge Belongie, Bharath Hariharan, and Ser-Nam Lim. Visual prompt tuning. In *Computer Vision – ECCV 2022*, pages 709–727, 2022. 2, 3, 6, 8
- [25] Justin Johnson, Bharath Hariharan, Laurens Van Der Maaten, Li Fei-Fei, C Lawrence Zitnick, and Ross Girshick. Clevr: A diagnostic dataset for compositional language and elementary visual reasoning. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), pages 2901–2910, 2017. 5, 1
- [26] Apoorv Khandelwal, Luca Weihs, Roozbeh Mottaghi, and Aniruddha Kembhavi. Simple but effective: Clip embeddings for embodied ai. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), pages 14829–14838, 2022. 5

- [27] Muhammad Uzair Khattak, Hanoona Rasheed, Muhammad Maaz, Salman Khan, and Fahad Shahbaz Khan. Maple: Multi-modal prompt learning. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, pages 19113–19122, 2023. 3, 8
- [28] Muhammad Uzair Khattak, Syed Talal Wasim, Muzammal Naseer, Salman Khan, Ming-Hsuan Yang, and Fahad Shahbaz Khan. Self-regulating prompts: Foundational model adaptation without forgetting. In *Proceedings of the IEEE/CVF International Conference on Computer Vision* (*ICCV*), pages 15190–15200, 2023. 3, 5
- [29] Douwe Kiela, Hamed Firooz, Aravind Mohan, Vedanuj Goswami, Amanpreet Singh, Pratik Ringshia, and Davide Testuggine. The hateful memes challenge: Detecting hate speech in multimodal memes. In Advances in Neural Information Processing Systems, pages 2611–2624, 2020. 5, 1
- [30] Daehee Kim, Youngjun Yoo, Seunghyun Park, Jinkyu Kim, and Jaekoo Lee. Selfreg: Self-supervised contrastive regularization for domain generalization. In *Proceedings of the IEEE/CVF International Conference on Computer Vision* (*ICCV*), pages 9619–9628, 2021. 5
- [31] Alex Krizhevsky, Geoffrey Hinton, et al. Learning multiple layers of features from tiny images. 2009. 5, 7, 1
- [32] Bohao Li, Rui Wang, Guangzhi Wang, Yuying Ge, Yixiao Ge, and Ying Shan. Seed-bench: Benchmarking multimodal llms with generative comprehension. arXiv preprint arXiv:2307.16125, 2023. 1, 2
- [33] Chunyuan Li, Cliff Wong, Sheng Zhang, Naoto Usuyama, Haotian Liu, Jianwei Yang, Tristan Naumann, Hoifung Poon, and Jianfeng Gao. Llava-med: Training a large languageand-vision assistant for biomedicine in one day. arXiv preprint arXiv:2306.00890, 2023. 2
- [34] Junnan Li, Dongxu Li, Silvio Savarese, and Steven Hoi. Blip-2: Bootstrapping language-image pre-training with frozen image encoders and large language models. arXiv preprint arXiv:2301.12597, 2023. 1, 2, 5
- [35] Yifan Li, Yifan Du, Kun Zhou, Jinpeng Wang, Wayne Xin Zhao, and Ji-Rong Wen. Evaluating object hallucination in large vision-language models. arXiv preprint arXiv:2305.10355, 2023. 2, 5, 1
- [36] 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 *Computer Vision – ECCV 2014*, pages 740–755, 2014. 1
- [37] Haotian Liu, Chunyuan Li, Qingyang Wu, and Yong Jae Lee. Visual instruction tuning. In Advances in Neural Information Processing Systems, 2023. 1, 2, 4
- [38] Xiao Liu, Kaixuan Ji, Yicheng Fu, Weng Tam, Zhengxiao Du, Zhilin Yang, and Jie Tang. P-tuning: Prompt tuning can be comparable to fine-tuning across scales and tasks. In *Proceedings of the 60th Annual Meeting of the Association for Computational Linguistics (Volume 2: Short Papers)*, pages 61–68, 2022. 2, 3
- [39] Yang Liu, Yuanshun Yao, Jean-Francois Ton, Xiaoying Zhang, Ruocheng Guo Hao Cheng, Yegor Klochkov, Muhammad Faaiz Taufiq, and Hang Li. Trustworthy llms: a survey and guideline for evaluating large language models' alignment. arXiv preprint arXiv:2308.05374, 2023. 2

- [40] Gen Luo, Yiyi Zhou, Tianhe Ren, Shengxin Chen, Xiaoshuai Sun, and Rongrong Ji. Cheap and quick: Efficient visionlanguage instruction tuning for large language models. In Advances in Neural Information Processing Systems, pages 29615–29627, 2023. 3
- [41] S. Maji, J. Kannala, E. Rahtu, M. Blaschko, and A. Vedaldi. Fine-grained visual classification of aircraft. Technical report, 2013. 7, 1
- [42] Yuval Netzer, Tao Wang, Adam Coates, Alessandro Bissacco, Bo Wu, and Andrew Y. Ng. Reading digits in natural images with unsupervised feature learning. In NIPS Workshop on Deep Learning and Unsupervised Feature Learning 2011, 2011. 1, 5
- [43] Changdae Oh, Hyeji Hwang, Hee-young Lee, YongTaek Lim, Geunyoung Jung, Jiyoung Jung, Hosik Choi, and Kyungwoo Song. Blackvip: Black-box visual prompting for robust transfer learning. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), pages 24224–24235, 2023. 4, 6
- [44] 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 *Proceedings of the 38th International Conference* on Machine Learning, pages 8748–8763, 2021. 2, 3, 5
- [45] Konstantinos I Roumeliotis and Nikolaos D Tselikas. Chatgpt and open-ai models: A preliminary review. *Future Internet*, 15(6):192, 2023. 1
- [46] Ramprasaath R. Selvaraju, Michael Cogswell, Abhishek Das, Ramakrishna Vedantam, Devi Parikh, and Dhruv Batra. Grad-cam: Visual explanations from deep networks via gradient-based localization. In *Proceedings of the IEEE International Conference on Computer Vision (ICCV)*, 2017.
- [47] Sheng Shen, Liunian Harold Li, Hao Tan, Mohit Bansal, Anna Rohrbach, Kai-Wei Chang, Zhewei Yao, and Kurt Keutzer. How much can clip benefit vision-and-language tasks? In *International Conference on Learning Representations*, 2022. 5
- [48] Yixuan Su, Tian Lan, Huayang Li, Jialu Xu, Yan Wang, and Deng Cai. Pandagpt: One model to instruction-follow them all. arXiv preprint arXiv:2305.16355, 2023. 2
- [49] Hugo Touvron, Thibaut Lavril, Gautier Izacard, Xavier Martinet, Marie-Anne Lachaux, Timothée Lacroix, Baptiste Rozière, Naman Goyal, Eric Hambro, Faisal Azhar, et al. Llama: Open and efficient foundation language models. arXiv preprint arXiv:2302.13971, 2023. 1, 3, 7
- [50] Hugo Touvron, Louis Martin, Kevin Stone, Peter Albert, Amjad Almahairi, Yasmine Babaei, Nikolay Bashlykov, Soumya Batra, Prajjwal Bhargava, Shruti Bhosale, et al. Llama 2: Open foundation and fine-tuned chat models. arXiv preprint arXiv:2307.09288, 2023. 1
- [51] Yun-Yun Tsai, Pin-Yu Chen, and Tsung-Yi Ho. Transfer learning without knowing: Reprogramming black-box machine learning models with scarce data and limited resources. In *Proceedings of the 37th International Conference on Machine Learning*, pages 9614–9624, 2020. 3

- [52] Naonori Ueda and Ryohei Nakano. Generalization error of ensemble estimators. In *Proceedings of International Conference on Neural Networks (ICNN'96)*, pages 90–95. IEEE, 1996. 7
- [53] Laurens Van der Maaten and Geoffrey Hinton. Visualizing data using t-sne. *Journal of machine learning research*, 9 (11), 2008. 4
- [54] Twan Van Laarhoven. L2 regularization versus batch and weight normalization. arXiv preprint arXiv:1706.05350, 2017. 5
- [55] Jason Wei, Maarten Bosma, Vincent Zhao, Kelvin Guu, Adams Wei Yu, Brian Lester, Nan Du, Andrew M Dai, and Quoc V Le. Finetuned language models are zero-shot learners. In *International Conference on Learning Representations*, 2022. 1
- [56] Junyang Wu, Xianhang Li, Chen Wei, Huiyu Wang, Alan Yuille, Yuyin Zhou, and Cihang Xie. Unleashing the power of visual prompting at the pixel level. arXiv preprint arXiv:2212.10556, 2022. 1, 2, 3, 4, 5, 6, 7, 8
- [57] Qiong Wu, Wei Yu, Yiyi Zhou, Shubin Huang, Xiaoshuai Sun, and Rongrong Ji. Parameter and computation efficient transfer learning for vision-language pre-trained models. In Advances in Neural Information Processing Systems, pages 41034–41050, 2023. 3
- [58] Yixin Wu, Rui Wen, Michael Backes, Pascal Berrang, Mathias Humbert, Yun Shen, and Yang Zhang. Quantifying privacy risks of prompts in visual prompt learning. arXiv preprint arXiv:2310.11970, 2023. 2, 3
- [59] Peng Xu, Wenqi Shao, Kaipeng Zhang, Peng Gao, Shuo Liu, Meng Lei, Fanqing Meng, Siyuan Huang, Yu Qiao, and Ping Luo. Lvlm-ehub: A comprehensive evaluation benchmark for large vision-language models. *arXiv preprint arXiv:2306.09265*, 2023. 1, 2
- [60] Shukang Yin, Chaoyou Fu, Sirui Zhao, Ke Li, Xing Sun, Tong Xu, and Enhong Chen. A survey on multimodal large language models. arXiv preprint arXiv:2306.13549, 2023. 2
- [61] Aohan Zeng, Xiao Liu, Zhengxiao Du, Zihan Wang, Hanyu Lai, Ming Ding, Zhuoyi Yang, Yifan Xu, Wendi Zheng, Xiao Xia, et al. Glm-130b: An open bilingual pre-trained model. arXiv preprint arXiv:2210.02414, 2022. 1
- [62] Yuexiang Zhai, Shengbang Tong, Xiao Li, Mu Cai, Qing Qu, Yong Jae Lee, and Yi Ma. Investigating the catastrophic forgetting in multimodal large language models. arXiv preprint arXiv:2309.10313, 2023. 1
- [63] Ao Zhang, Hao Fei, Yuan Yao, Wei Ji, Li Li, Zhiyuan Liu, and Tat-Seng Chua. Transfer visual prompt generator across llms. In Advances in Neural Information Processing Systems, 2023. 2, 5, 7, 1
- [64] Haozhe Zhao, Zefan Cai, Shuzheng Si, Xiaojian Ma, Kaikai An, Liang Chen, Zixuan Liu, Sheng Wang, Wenjuan Han, and Baobao Chang. Mmicl: Empowering vision-language model with multi-modal in-context learning. arXiv preprint arXiv:2309.07915, 2023. 2
- [65] Kaiyang Zhou, Jingkang Yang, Chen Change Loy, and Ziwei Liu. Conditional prompt learning for vision-language models. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), pages 16816– 16825, 2022. 3, 8

- [66] Kaiyang Zhou, Jingkang Yang, Chen Change Loy, and Ziwei Liu. Learning to prompt for vision-language models. *International Journal of Computer Vision*, 130(9):2337–2348, 2022. 3
- [67] Kaiyang Zhou, Ziwei Liu, Yu Qiao, Tao Xiang, and Chen Change Loy. Domain generalization: A survey. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 45(4):4396–4415, 2023. 5
- [68] Wen Zhou, Xin Hou, Yongjun Chen, Mengyun Tang, Xiangqi Huang, Xiang Gan, and Yong Yang. Transferable adversarial perturbations. In *Computer Vision – ECCV 2018*, pages 452–467, 2018. 2, 3, 4
- [69] Deyao Zhu, Jun Chen, Xiaoqian Shen, Xiang Li, and Mohamed Elhoseiny. Minigpt-4: Enhancing vision-language understanding with advanced large language models. arXiv preprint arXiv:2304.10592, 2023. 1, 2, 3, 4, 5, 6, 7