Fallback-Enabled Closed-Set Classification: Cross-Modal Consistency in Vision-Language Models

Anonymous authors
Paper under double-blind review

Abstract

Vision-Language Models (VLMs) can describe and label images; however, this does not imply that they truly process what they are perceiving. Recent studies show that, despite their breadth of training, VLMs are surprisingly unreliable as classifiers, for either closed-world or open-world settings. In this work, we explore a deeper question: can a VLM recognize when an image falls outside the set of categories it is asked to choose from? Our results reveal a surprising failure mode: even when the notion of in-set versus out-of-set is explicitly defined, VLM models often assign plausible in-set labels to out-of-set images, violating the task's explicit constraint. Motivated by this, we propose a cross-modal consistency framework that reasons over both the visual and textual arms of the model and accepts an answer only when they agree. Experiments on three well-known datasets (DomainNet, VisDA and INaturalist-2021) demonstrate that this approach consistently improves balanced known *vs.* unknown detection over Source-Free Universal Domain Adaptation (SF-UniDA) baselines, showing that cross-modal consistency improves a VLM's ability to follow the task logic and distinguish when an image falls outside the intended label space. Our results suggest that, with strong VLMs, fallback behavior need not rely exclusively on specialized SF-UniDA adaptation pipelines: a lightweight cross-modal consistency decision rule can be competitive with representative SF-UniDA baselines on standard benchmarks.

1 Introduction

A long-standing challenge in (visual) recognition is to design systems that not only assign labels among known categories but also detect when an input does not belong to any of the known categories. This challenge has been studied under various names, such as open-world classification Ding & Pang (2024); Shu et al. (2017); Fei & Liu (2016), universal domain adaptation (UniDA). UniDA You et al. (2019b); Chang et al. (2022) aims to simultaneously address both domain and category shift, where the target label space may partially overlap with the source domain. UniDA methods Saito & Saenko (2021); Choe et al. (2025) must identify and classify shared classes while rejecting unknown target categories. Source-free universal domain adaptation (SF-UniDA) You et al. (2019a); Liang et al. (2021) further circumvents the dependency on source data, making adaptation feasible under privacy and efficiency constraints. This is so because it considers the case where one only has access to a pretrained model without access to source data and must adapt the model to a target domain.

The problem studied in these approaches has conceptual *and* practical implications. Epistemically, a system that "knows when it does not know" embodies a basic form of self-awareness long valued in philosophy, as Socrates taught, "wisdom begins by acknowledging the limits of one's knowledge". Practically, in safety-critical cases, for example, if a medical condition does not belong to the known set of conditions in the diagnostic label set, the medical imaging recognition system should be able to detect it to prevent risky diagnoses.

The rapid development of Vision-Language Models (VLMs) Bai et al. (2023); Achiam et al. (2023); Wei et al. (2022) has opened new possibilities to address this challenge Yin et al. (2023); Kapoor et al. (2024). However, large foundation models suffer from serious hallucination issues Kalai et al. (2025); Huang et al.

Figure 1: Illustration of the problem. From left to right, we showcase four scenarios, *i*) a known object gets wrongly recognized as unknown, *ii*) a known object gets recognized as known, *iii*) an unknown sample gets wrongly classified as one of the classes in the list because of the background, and lastly, *iv*) an unknown image gets successfully flagged as unknown. Over-rejection error (*i*), which unnecessarily triggers fallback will hurt system efficiency, while overconfidence error (*iii*), bypasses the fallback mechanism, risking unsafe downstream decisions.

(2025); Xu et al. (2024). In fact, works such as Chen et al. (2023) found that large foundation models can produce correct answers, but lack internal self-awareness of their own output. Moreover, Zhang et al. (2024); Mitra et al. (2025); Jiang et al. (2025) concluded that VLMs are *bad* at both open-world and closed-world image classification, with training data being the primary cause. Therefore, in order to deploy VLMs to meet the demands of a solution without relying on additional training, alternative procedures need to be taken to make their answers more reliable.

We first explore VLMs on a strict instruction-following setting as illustrated in Figure 1. Given an image and a closed-set label list, the model must assign a label from such a list, and either *i*) declare the image as "known", or *ii*) trigger a fallback decision of "unknown" when the image is judged to fall outside the intended label space. We define this problem as *fallback-enabled closed-set classification* with VLMs. Despite clear instructions and examples, our experiments on the DomainNet dataset expose a paradox: strong categorical labeling ability but weak logical boundary keeping, *i.e.*, very high true-negative rates for unknowns, yet poor true-positive rates for the known set, which results in many in-set images being mislabeled as "unknown". Importantly, clear instructions alone do not make the concept of "unknown" operational or sufficiently clear for these models.

Therefore, in order to use VLMs to address this problem, we propose a framework that tasks the VLM with reasoning along two arms and accepts a prediction only when they agree. Specifically, we make the following contributions.

- We propose a simple, model-agnostic framework that uses cross-modal consistency to perform closed-set classification with a fallback action. The method requires no fine-tuning or access to model internals. Moreover, it is easy to implement with existing VLM APIs.
- We define fallback-enabled closed-set classification with VLMs as a problem that is conceptually aligned with SF-UniDA. We explicitly bridge VLM reasoning with SF-UniDA, analyze their similarities and differences.
- We evaluate the performance of the proposed framework in comparison to the state-of-the-art SF-UniDA methods, not only using harmonic-mean accuracy and overall accuracy, but also the ratio of known *vs.* unknown accuracies as *balance* metric. This ratio reveals when a model is biased toward either over-accepting unknowns or over-rejecting knowns, which is critical for deploying fallback behavior in practice.
- Across six scenarios with three well-known datasets, we show that VLMs equipped with the proposed method can consistently outperform specialized SF-UniDA methods.

2 A Paradoxical Finding in VLM Probing

We begin by investigating whether VLMs can accurately distinguish between known and unknown categories given a predefined list of labels. Specifically, we ask:

- (Closet-set Classification) Can a VLM accurately determine whether an image belongs to a given list of labels?
- (Fallback Behavior) Can a VLM recognize when an image lies outside this list and thus should be classified as "unknown"?
- (Fallback-Enabled Classification) How good are VLMs at closed-set image classification and "unknown" label detection?

We first evaluate the above using a direct prompting approach using GPT 4o-mini on three domains, specifically, Painting, Real, and Sketch, of DomainNet. The prompt we use is as follows, with {this image} and {known class list} being placeholders for the image query and the predefined list of class labels (the details are shown in Appendix A.1).

```
<System Prompt> You are an AI that classifies images based on a predefined list of categories.  If the image belongs to
a category in the GIVEN list (ONLY from the GIVEN list), then provide classname with the correct category name from
the given list and respond with unknown:  False; if the image does not belong to any category in the GIVEN list, then
select the closest possible match from the GIVEN list (DO NOT reply with labels outside of the list) as classname and
respond with unknown:  True.

<User Prompt> Does {this image} belong to one of the categories in the following list {known class list}?  Please format
the answer csv format with keys unknown and classname separated by ','
Example 1:
Image:  (picture of a aeroplane)
Response:  unknown:  False, classname:  'aeroplane'
Example 2:
Image:  (picture of a donkey)
Response:  unknown:  True, classname:  'horse'
```

This prompt explicitly articulates what constitutes an unknown image, encodes the task logic in a system prompt, clearly marks the predefined label set as a given list of classes to make these constraints less likely to be overlooked, and provides concrete formatting examples. These choices, *i.e.*, providing examples and setting the expected output format, follow structured prompting practices for multimodal LLMs to improve adherence to instructions Sahoo et al. (2024); Zhang et al. (2023); Bsharat et al. (2023).

Figure 2 summarizes the empirical results of two prediction outputs from the VLM (GPT 4o-mini), the categorical label and the binary label "unknown", together in a confusion matrix, for all three domains (Painting, Real, and Sketch) of DomainNet. For each confusion matrix, the rows indicate the ground truth binary label: in-set (known) and out-of-set (unknown), while the columns indicate model predictions. We treat "known" (in-set) as the positive class, so the cells are true positives (TPs) (top-left), false negatives (FNs) (top-right), false positives (FPs) (bottom-left) and false negatives (FNs) (bottom-right). The percentage values in each cell denote the prediction accuracies of categorical labels within that subset. With the above definition, $\text{TPR} = \frac{\text{TP}}{\text{TP+FN}}$ measures how many known samples are correctly identified by a model, while $\text{TNR} = \frac{\text{TN}}{\text{TN+FP}}$ shows how often unknown images are correctly recognized. Our observations of the results in this setting revealed significant insights described below.

Weak known/unknown discrimination. When we analyze the predicted value of "unknown", the VLM is highly effective at identifying unknown images, correctly classifying these cases as "unknown" with up to 90% accuracy. However, the VLM shows limitations in identifying known images correctly, achieving accuracy as low as 20% in classifying known images as "known". In order to argue that a model is good at detecting what is "unknown", it should be able to have not only a good classification accuracy for "unknown", but also for "known" images. However, the high TNR but low TPR scores in Figure 2 indicate an imbalanced performance to correctly recognize "known" *vs.* "unknown", which does not match the desired behavior.

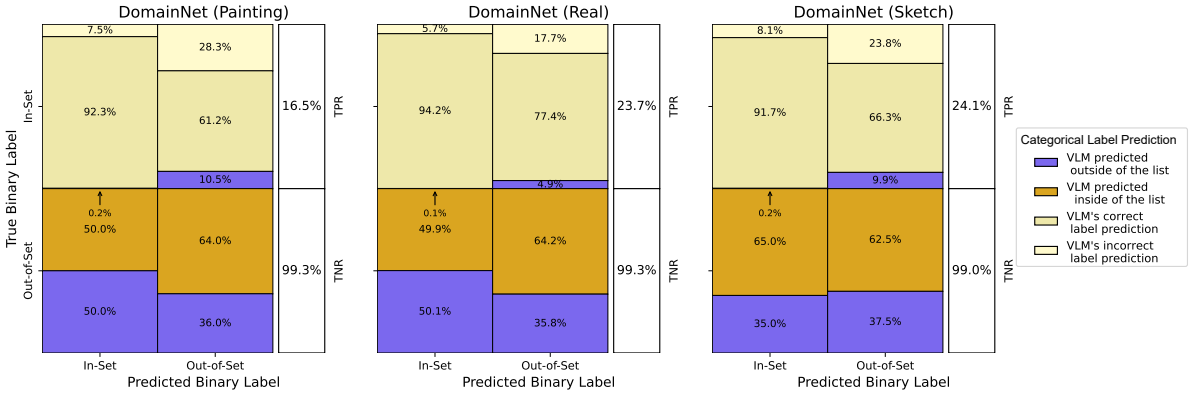

Figure 2: Preliminary analysis demonstrating the paradoxical behavior of VLMs on the DomainNet dataset. Even though the prompt explicitly defines the notions of in-set (known) and out-of-set (unknown) categories, the model fails to internalize this distinction, *i.e.*, it recognizes categorical labels accurately but struggles with binary discrimination between known and unknown samples. High TNR but low TPR indicates that while the model reliably rejects truly out-of-set images, it frequently misclassifies in-set ones as unknown, which reveals that clear instruction alone is insufficient for logical understanding of the concept "unknown".

Strong label recognition. Despite poor known-sample detection, the high percentages in the top two cells of each of the confusion matrices in Figure 2 indicate that the VLM achieves high accuracy when assigning labels to known images, thus excelling at closed-set classification.

Paradoxical results. These findings suggest that the VLM has a solid label recognition ability (closed-set classification), but struggles with the discrimination of "known" *vs.* "unknown", *i.e.*, the desired fallback behavior, even with explicit instructions for them in the prompt.

3 A Solution using Cross-Modal Consistency

Section 2 illustrated that explicit instructions alone cannot reliably realize the fallback mechanism in closed-set classification that we seek to address. Specifically, VLMs may correctly find the category of the known labels, *i.e., the closed set*, but still misjudge in- *vs.* out-of-set membership, *i.e.*, the fallback behavior, even with strict task logic enforced in the prompt wording. A common practice for solving such a problem is to train a classifier with an additional class, thus extending the closed-set with an "unknown" class Zhan et al. (2021); Shu et al. (2021). Other lines of work, such as UniDA Liang et al. (2021) and SF-UniDA handle unknowns by thresholding uncertainty scores or synthesizing unknown samples Bai et al. (2022) in open-world classification. Although effective when source data and retraining are available, these approaches are brittle under domain shift, sensitive to thresholding, and scale poorly as label lists change, especially in source-free settings. Here, we take a different route, by proposing a solution that leverages VLM's broad knowledge without additional training. Before providing the details, we first define the problem studied.

3.1 Problem Definition

To define what is "unknown", we first need to recognize what is "known". Given an image $I \in \mathcal{I}$, and a predefined and known list of labels (the closed set) $\mathcal{C} = \{c_1, c_2, \cdots, c_N\}$, with N being the total number of labels in the list, each image has two labels, one is its ground truth categorical label y which may or may not be in $\mathcal{C}$, and the other is a binary label δ denoting "known" *vs.* "unknown". Specifically, an image is defined as "known" if and only if its ground truth label is within the predefined known class list C. We define δ as

$$\delta = \begin{cases} 1 & \text{if } y \in \mathcal{C} \text{ (known)} \\ 0 & \text{if } y \notin \mathcal{C} \text{ (unknown)} \end{cases} .$$

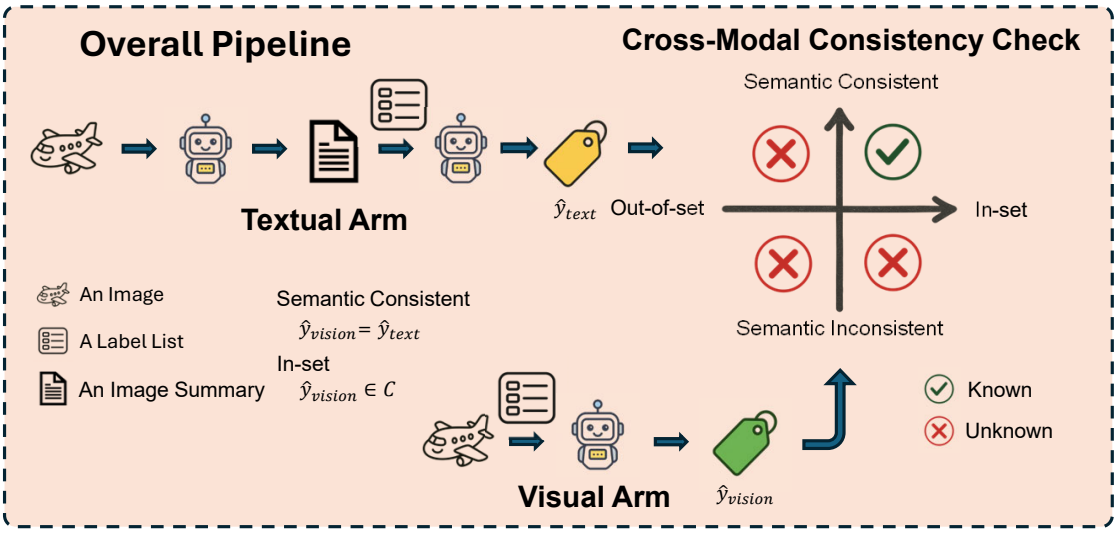

Figure 3: Illustration of the proposed method. The model makes predictions through a visual and a textual arm. A sample is marked known only when predictions from both arms agree on a label within the predefined set; otherwise, it is flagged as unknown.

We seek to understand whether a VLM model $f_{VLM}(\cdot)$ is able to determine whether the image I is "known" and can be appropriately labeled as any label in the set $\mathcal{C}$, or "unknown" and cannot be assigned any label in $\mathcal{C}$. To this end, we propose an approach that utilizes the cross-modal consistency of the VLM for unknown image identification. Specifically, query the VLM along two arms: *i*) prompt directly with the image; and *ii*) first summarize the image into text, then prompt the same question with such a summary. The details of the proposed framework are described below.

3.2 Direct Prompting (Visual Arm)

Given an image I, we first directly task the VLM model through prompting with giving a predicted label given the predefined list of known class labels $\mathcal{C}$. We show the partial prompt below for brevity and the full version is provided in the Appendix A.1.

```
"...  Does this image belong to one of the categories in the following list {known class list}?  Please format the answer
csv format with keys unknown and classname separated by ','..."
```

Let $f_{VLM} : \mathcal{I} \times \mathcal{P} \rightarrow \mathcal{R}$, where $\mathcal{P}$ represents the prompt space and $\mathcal{R}$ is the unprocessed response space. We write

$$r_{vision} = f_{VLM}(I, p_{vision}(\mathcal{C})), \tag{1}$$

with $p_{vision}(\cdot)$ being a template for the prompt, which can be found in Appendix A.1.

We then define a parsing function $\phi(\cdot)$ (the detailed definition of which can be found in Appendix A.2) that extracts the categorical class label from the unprocessed response. Specifically, the two possible outcomes are $\hat{y}_{vision} = \phi(r_{vision}) \in \mathcal{C}$ if the parsing is successful and returns a categorical label from $\mathcal{C}$, while $\hat{y}_{vision} = \phi(r_{vision}) = \emptyset$, *i.e.*, the empty set, if the parsing fails or no valid categorical label is found because of failures following the instructions.

This process of generating $\hat{y}_{vision}$ constitutes the model's direct visual reasoning arm, which solely relies on its visual understanding and the label list $\mathcal{C}$.

3.3 Summary-Based Prompting (Textual Arm)

Then we task the VLM model to give a summary of the visual features of the image I with the following prompt. We denote the prompt by $p_{text}(\cdot)$.

```
"Can you give a summary of the image?"
```

The generated text $r_{summary} = f_{VLM}(I, p_{text}(\cdot))$ is then used as the context for a second classification prompt shown below (the full version of the prompt can be found in the Appendix A.1).

```
"...  Does this image belong to one of the categories in the following list {known class list} based on the following
summary {image summary}?  Please format the answer csv format with keys unknown and classname separated by ','..."
```

The output of the VLM given this prompt produces a textual prediction

$$r_{text} = f_{VLM}(r_{summary}). \tag{2}$$

With the same parsing function $\phi(\cdot)$, we can obtain the predicted class label $\hat{y}_{text} = \phi(r_{text})$. Similarly to the direct prompting arm, we expect two outcomes, with $\hat{y}_{text}$ being a parsed string or an empty set.

3.4 Cross-modal Consistency of VLMs

Finally, we define the cross-modal consistency criterion to determine whether the model "knows what it knows", thus eliciting the desired fallback behavior. An image is predicted as known only when both reasoning arms agree on the class prediction and such class is within the label list $\mathcal{C}$:

$$\hat{\delta} = 1[\hat{y}_{vision} = \hat{y}_{text}] \cdot \mathbb{1}[\hat{y}_{vision} \in \mathcal{C}]\,, \tag{3}$$

where $\mathbb{1}[\cdot]$ is the indicator function. If the two predictions disagree or the predicted label is not a member of $\mathcal{C}$, the image is labeled "unknown". This dual-arm validation filters out internally inconsistent predictions, reducing overconfidence from a single modality. Although prior work Manakul et al. (2023); Wang et al. (2022) has considered multi-arm reasoning for reliability, we focus on the minimal and interpretable two-arm case due to the consideration of computational cost. Figure 3 illustrates the full workflow of the proposed cross-modal consistency approach. Given an image and a closed set of labels $\mathcal{C}$, it leverages the VLM by using two decision arms: a visual arm that takes $(I, \mathcal{C})$ and a textual arm that uses a generated description of that image, each of which produces a categorical label. An image is only accepted as "known" when the predicted labels from both arms agree and it is in the closed set $\mathcal{C}$; otherwise, it produces the fallback behavior, thus marking the prediction as "unknown". This procedure does not require training, source data (for the closed set $\mathcal{C}$) and is agnostic to the choice of VLM, thus specifically defining a decision rule for "unknown" labels rather than using separate classifiers Qu et al. (2023) or thresholds on uncertainty estimation like in SF-UniDA approaches Qu et al. (2023); Liang et al. (2021).

4 Comparison to Source-free Universal Domain Adaptation

The fallback-enabled closed-set classification problem we study shows a close resemblance to Source-Free Universal Domain Adaptation (SF-UniDA) You et al. (2019a); Liang et al. (2021); Qu et al. (2023; 2024). In SF-UniDA, one only has access to a pretrained source model for $\mathcal{C}$ (its training data are inaccessible), and the objective is to adapt this classification model to a new target domain so that samples from the known classes $\mathcal{C}$ are correctly classified, while unknown categories are reliably marked as "unknown". For example, in GLC Qu et al. (2023), they leverage adaptive global one-vs-all clustering and local consensus clustering to effectively separate known and unknown samples. LEAD Qu et al. (2024) proposes a decomposition-based learning framework that disentangles the source space into known and unknown components, thus improving its robustness over general category-shift scenarios. These works underscore growing efforts to develop approaches that upcycle pre-trained models into new domains without accessing source data.

Large-scale VLMs share a similar trait: their training data is hidden from the user, yet they are expected to perform classification when prompted with a given set of labels. Furthermore, in the problem we study,

since both VLMs and SF-UniDA models operate as predictors without access to source data, the nature of the problem is fundamentally similar in the sense that the objective is to elicit a fallback mechanism by distinguishing known versus unknown categories from model outputs.

Nevertheless, there are critical distinctions between these two settings. Specifically, SF-UniDA assumes a specific source-target domain relationship with partially overlapping label spaces You et al. (2019a), whereas VLMs are foundation models trained on broad and multimodal corpora whose "source domain" is implicit and unobservable. Consequently, while SF-UniDA focuses on adapting decision boundaries between known and unknown target samples, our work analyzes how a large-scale VLM internally reasons about task-defined label boundaries when its pretraining data is inaccessible. These comparisons indicate that our cross-modal consistency framework can serve as an effective alternative to adaptation-based SF-UniDA pipelines for implementing fallback with strong VLMs. Later, we will show empirically that our rule matches or surpasses representative SF-UniDA baselines on the evaluated benchmarks in our setting.

5 Additional Related Work

Self-Consistency has recently emerged as an effective way to boost the reasoning abilities of large foundation models Wang et al. (2022). Khan & Fu (2024) explores a way to judge the reliability of the answer of a VLM by accessing the inconsistency of the model's answers over paraphrased versions of the original question, which are generated dynamically using a VQG model. Then, low consistency is used as a strong indicator of abstaining the model from answering. Han et al. (2025) harnesses the VLM's consistency between long and short answers to reduce hallucinations and improve the reliability of answers. In contrast, our method uses the cross-modal self-consistency of the outputs of a VLM as a primary signal to decide whether the system should output a categorical label prediction or trigger the "unknown" fallback behavior. Our method is different in the objective of the task and in that it is designed to operate under a constrained budget by limiting the number of VLM calls.

Open-World Classification is a classic natural language processing task Fei & Liu (2016) where, in an open environment, an ideal classifier must both assign inference examples to the correct classes seen during training and identify those examples that do not belong to any known classes (learned during training). For example, ODIST Shu et al. (2021) addresses the issue by creating distributionally shifted samples with the help of a pretrained BART model. ANS Bai et al. (2022) tackles this challenge by synthesizing negative examples in the feature space and pairing them with one-vs-all binary classifiers for each known class. While specific formulations vary, these methods generally assume access to labeled data for the in-scope classes during training, and learn the unknown detector jointly with or on top of such supervised representations. By contrast, the problem we consider forgoes using source samples when adapting or evaluating the method and instead focuses on the real-world deployment of a pretrained frozen model.

6 Experiments

6.1 Datasets

We test the proposed method on two well-known domain adaptation benchmarks, **DomainNet** Peng et al. (2019) and **VisDA** Peng et al. (2017), to compare against state-of-the-art UniDA approaches. **DomainNet** is a large-scale benchmark that contains 345 classes, with approximately 48K–172K images per domain. Following prior work Qu et al. (2023; 2024), we conduct experiments with the Painting (P), Real (R), and Sketch (S) domains. **VisDA** is another challenging benchmark consisting of 12 object classes, where the source domain includes synthetic object renderings and the target domain consists of photo-realistic images.

In addition, we construct two datasets derived from **INaturalist-2021** iNaturalist 2021 competition dataset based on different taxonomic hierarchies, *phylum* and *class*. We explain the details of how the datasets are constructed in the Appendix A.5. The full dataset contains nearly 2.7M images across 10,000 species, with the phylum taxonomy yielding 13 classes and the class taxonomy yielding 51 classes. We selected **INaturalist-2021** for two main reasons. One is that it allows us to evaluate how well the models perform when the class imbalance issue is more severe, and the other is that it enables us to study how our method

Table 1: Comparison to SoTA SF-UniDA methods on weighted accuracies for known (acc_{k-w}) and unknown (acc_{u-w}) classes. The results are formatted as acc_{k-w}/acc_{u-w}. (Best in bold and second best in underline)

Method	**DomainNet**			**VisDA**	**INaturalist**		**Avg**
	Painting	Real	Sketch		Phylum	Class	
GLC	45.9/77.3	49.1/80.5	37.3/77.7	69.1/67.5	61.7/29.9	87.8/76.0	56.8/68.1
LEAD	41.1/68.7	51.9/73.3	34.8/69.7	72.6/87.1	77.6/<u>65.6</u>	63.5/64.6	56.9/71.5
Visual-only (V):							
GPT 4o-mini	70.9/36.3	85.0/37.3	**87.0**/36.9	**96.8**/1.72	93.6/0.26	**93.6**/2.87	<u>87.8</u>/19.2
Gemini	72.2/21.9	78.3/35.4	74.0/26.6	91.7/6.70	**98.4**/0.07	74.9/17.5	81.6/18.0
Llama	60.0/69.2	63.5/78.7	46.9/79.4	60.8/53.8	93.6/10.8	56.5/51.5	63.5/57.2
Qwen	**87.6**/46.4	**89.2**/48.9	<u>79.8</u>/42.1	<u>92.7</u>/8.79	95.6/20.8	90.0/25.9	**89.1**/32.1
Texual-only (T):							
GPT 4o-mini	68.2/40.0	80.9/42.2	73.7/40.0	89.5/2.35	94.0/0.26	<u>93.3</u>/3.98	83.3/21.5
Gemini	65.6/35.2	71.3/47.9	62.4/37.0	85.2/6.70	96.9/0.07	90.2/18.5	78.6/24.2
Llama	47.9/70.1	55.3/79.8	40.1/79.9	64.6/53.8	83.6/64.6	57.0/51.5	58.1/66.6
Qwen	73.6/60.2	80.6/68.9	70.2/56.6	80.9/57.2	83.4/42.5	82.1/25.9	78.5/51.9
Cross-Modal Consistency (V+T)(Ours):							
GPT 4o-mini (w/ Ours)	<u>73.9</u>/62.1	<u>85.0</u>/62.8	81.2/62.1	94.3/37.7	93.8/42.4	86.9/49.0	85.9/52.7
Gemini (w/ Ours)	71.7/68.5	74.0/73.7	72.7/74.8	90.7/54.7	<u>97.1</u>/43.7	87.9/52.1	82.3/61.3
Llama (w/ Ours)	49.7/**88.9**	55.7/**91.8**	42.3/**91.3**	55.7/**77.0**	85.6/58.0	53.4/**94.4**	57.1/<u>83.6</u>
Qwen (w/ Ours)	72.4/<u>85.6</u>	83.3/<u>87.4</u>	76.0/<u>84.0</u>	84.2/<u>73.8</u>	83.8/**87.3**	80.3/<u>94.3</u>	80.0/**85.4**

behaves when the labels are scientific terms instead of common words. To further illustrate the challenge of class imbalance, we visualize the distribution of sample sizes per class in Figure 5 in Appendix A.5.

6.2 Baselines

- GLC Qu et al. (2023): separates known and unknown data through adaptive one-vs-all clustering with Silhouette-based pseudo-labeling, which adaptively handles category shifts without prior knowledge.
- LEAD Qu et al. (2024): applies orthogonal decomposition to separate features associated with known and unknown source samples, thus allowing instance-level identification in target data. This is the state-of-the-art SF-UniDA method.

6.3 VLM Models

We consider four VLMs, including two commercial APIs: GPT 4o-mini Achiam et al. (2023) and Gemini-2.0-flash Comanici et al. (2025), and two open-source models: LLaMA-3.2-Vision Grattafiori et al. (2024) and Qwen-2.5-7B-VL Bai et al. (2025). The implementation details can be found in Appendix A.3.1. Moreover, for reproducibility purposes, the source code is also included in the supplementary material and will be publicly available upon publication.

6.4 Metrics

***H* score**: Equation 4 below is the harmonic mean between the average of per-class accuracies ($\overline{acc_k}$) over the K classes in $\mathcal{C}$, and the binary accuracy of the unknown samples (acc_u).

$$H = \frac{2 \cdot \overline{acc_k} \cdot acc_u}{\overline{acc_k} + acc_u} \,. \tag{4}$$

Advantages The $\overline{acc_k}$ focuses on maintaining discrimination within known classes. The average per-class accuracy prevents the dominant classes from masking the poor performance of rare known classes, while the

Table 2: Comparison to SoTA SF-UniDA methods on the balance ratio R. $R \to 1$ indicates balanced behavior for known and unknown recognition. (Best in bold and second best in underline)

Method	**DomainNet**			**VisDA**	**INaturalist**		**Avg**
	Painting	Real	Sketch		Phylum	Class	
GLC	0.599	0.614	0.481	**1.025**	2.063	<u>1.023</u>	<u>0.833</u>
LEAD	0.600	0.710	0.502	0.834	<u>1.182</u>	**0.983**	0.736
GPT 4o-mini (w/ Ours)	<u>1.190</u>	1.354	1.306	2.501	2.212	1.775	1.732
Gemini (w/ Ours)	**1.046**	**1.004**	**0.971**	1.660	2.224	1.687	1.432
Llama (w/ Ours)	0.560	0.611	0.463	0.722	1.476	0.565	0.733
Qwen (w/ Ours)	0.845	<u>0.953</u>	<u>0.905</u>	<u>1.141</u>	**0.960**	0.852	**0.943**

Table 3: H score (%) comparison with SoTA SF-UniDA methods. The first two rows show the SF-UniDA baseline results, cited from Qu et al. (2024). The last four rows show results with VLM models using our cross-modal consistency method (best in bold and second best is underlined).

Method	**DomainNet**			**VisDA**	**INaturalist**		**Avg**
	Painting	Real	Sketch		Phylum	Class	
GLC	59.1	50.5	50.7	73.1	32.4	47.8	53.8
LEAD	52.5	62.5	51.2	<u>76.8</u>	50.7	46.9	56.3
GPT 4o-mini (w/ Ours)	67.2	72.4	70.2	54.0	56.0	50.5	61.7
Gemini (w/ Ours)	<u>69.9</u>	<u>74.0</u>	<u>73.3</u>	68.2	<u>57.5</u>	<u>53.3</u>	<u>66.0</u>
Llama (w/ Ours)	63.0	68.6	56.8	65.0	54.3	36.1	57.3
Qwen (w/ Ours)	**77.3**	**85.7**	**80.1**	**78.2**	**73.1**	**57.5**	**75.3**

binary unknown accuracy acc_u measures the task of unknown detection. When combined by harmonic mean, one intends to capture both aspects (closed-set classification and unknown detection) of the performance of UniDA methods.

Limitations Since $\overline{acc_k}$ is the unweighted mean average accuracy over K classes, class imbalance can distort its value, *i.e.*, the rare classes receive equal weights as the more frequent ones. If these infrequent classes have poor performance, then $\overline{acc_k}$ can be severely penalized by the poor performance of classes with few samples. Furthermore, since the harmonic mean is dominated by the component with the smaller value, the H score primarily reflects the worse metric, thus it cannot show whether the model is better with known or unknown classes. In practice, we often wish to evaluate not only the absolute performance on known and unknown samples separately (*e.g.*, their respective accuracies), but also the balance between them, that is, whether the model performs comparably well in recognizing known categories and rejecting unknown ones.

In order to address the limitations of the H score, we also separately show the **weighted accuracy** for known and unknown classes. The weighted accuracies acc_{k-w} and acc_{u-w} incorporate class sample sizes to better reflect the influence of class imbalance. To further show whether each model has a balanced performance for known *vs.* unknown, we also show the **balance ratio** between weighted known accuracy and weighted unknown accuracy.

$$acc_{k-w} = \frac{\sum_K n_k \cdot acc_k}{\sum_K n_k} \tag{5}$$

$$acc_{u-w} = \frac{\sum_M n_m \cdot acc_m}{\sum_M n_m} \tag{6}$$

$$R = \frac{acc_{k-w}}{acc_{u-w}}, \tag{7}$$

where k is the number of known classes in $\mathcal{C}$, M is the number of unknown classes (often called *private classes* in UniDA), which are assumed to be known only for evaluation purposes, acc_k, which is weighted by sample size n_k, is the accuracy of the known class k, while acc_m, the accuracy of the unknown class m, is weighted by sample size n_m. We expect a good model to have good and balanced performance for both known and unknown classes. Therefore, the closer the ratio R is to 1, the more balanced the model is. For comparison, we also show the mean accuracy for known classes *vs.* unknown classes in Appendix A.4. Furthermore, in the ablation study, we also evaluate the H score between the mean accuracy of the known classes and the accuracy of each private class, individually, specifically $H_{u-m} = \frac{2 \cdot \overline{acc_k} \cdot acc_{u-m}}{\overline{acc_k} + acc_{u-m}}$, where acc_{u-m} indicates the accuracy of the unknown samples from the unknown class m.

7 Results

We evaluate the proposed cross-modal consistency framework with the four VLMs across six scenarios in DomainNet, VisDA, and INaturalist-2021, as described above, to assess its ability to distinguish known and unknown categories compared to the state-of-the-art (SoTA) source-free UniDA (SF-UniDA) methods.

As shown in Table 3, across all benchmarks, our cross-modal consistency framework makes VLMs outperform the classical SoTA SF-UniDA baselines. Specifically, Qwen 2.5-7B-VL consistently achieves the highest H scores, surpassing classical UniDA approaches by up to 20% to 25%, while Gemini 2.0-flash consistently ranks second. The results demonstrate that VLMs equipped with cross-modal reasoning can rival or outperform UniDA algorithms that are *specialized* for such tasks. Table 1 further illustrates how well are the weighted accuracies are for known and unknown samples, while table 2 shows their ratio R. The ideal behavior of a model is $R \approx 1$ with high scores for both acc_w and acc_w. Qwen 2.5-7B-VL achieves both the highest accuracy and the mostbalanced value for R. Gemini 2.0-flash also achieves strong absolute accuracies, but its R values shift away from 1 for certain datasets. In comparison, SF-UniDA methods exhibit a decent average balance ratio at times, yet their weighted accuracies are much lower in general. As a result, even though GLC performance looks "balanced" by ranking second in R value, its overall weighted accuracy cannot compete with Qwen 2.5-7B-VL and the other VLMs that are both more accurate and comparably (or better) balanced.

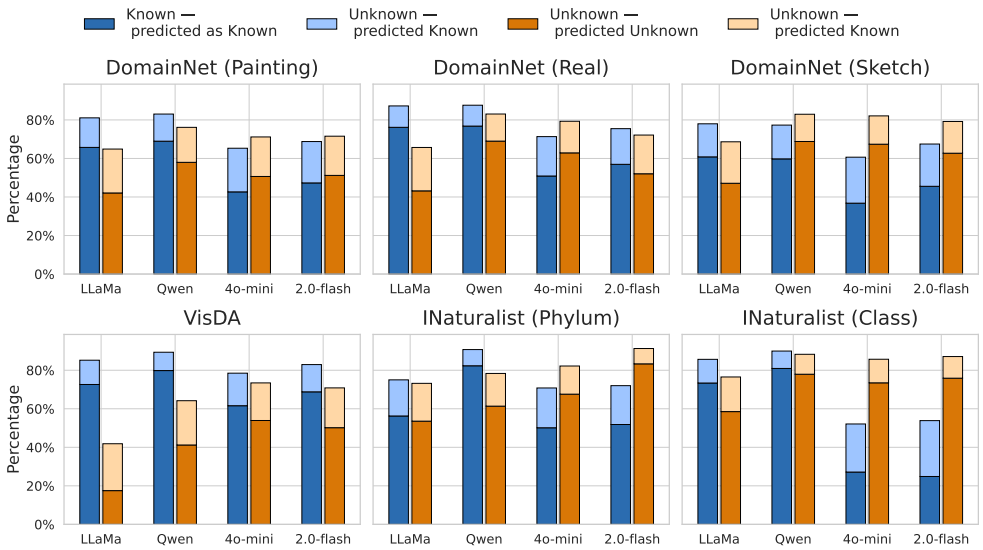

Figure 4: Positive Predictive Value (PPV, blue) and Negative Predictive Value (NPV, orange) of all four VLM models across six datasets. The lighter segments indicate the proportion of samples misclassified within that group for each dataset, while the darker bars correspond to correctly classified known / unknown samples.

Table 4: Ablation Study on prompt variations with Qwen 2.5-7B-VL. We show H_{u-m} scores (%) for the individual target private classes in the VisDA validation dataset. Numbers in each cell represent the results on the validation set.

	Target Private Class			**Overall H score**
	skateboard	train	truck	
original	57.36	87.29	63.14	72.56
var 1	58.29	87.80	61.34	72.29
var 2	72.75	**90.56**	64.00	76.91
var 3	**84.45**	87.38	**65.21**	**78.24**

Furthermore, we show positive predictive value (PPV) and negative predictive value (NPV) results in Figure 4 to show how reliable a VLM can be with our framework to behave like it "knows when it knows and when it does not", and observe that Qwen 2.5-7B-VL achieves the most reliable behavior. Overall, these results confirm that enforcing cross-modal consistency framework leads to more stable reasoning and balanced accuracy, reducing the bias between known and unknown recognition that characterizes classical UniDA baselines.

In the following section, we introduce our ablation studies to demonstrate the influence of prompt variations and removal of framework components.

7.1 Ablation Study

Influence of Prompt Variation To examine how image summary influences prediction with our framework, we tested three variations of $p_{text}(\cdot)$: *i*) Variation 1 (var 1) prompts with shorter length of image summaries to evaluate the effect of description verbosity. The motivation of this variation is to test whether reducing linguistic richness helps the models predict more accurately. *ii*) Variation 2 (var 2) "Describe the main object of the image". A prompt that explicitly directed the model to focus on the main object of the image. *iii*) Variation 3 (var 3) "Identify the primary object in the image, excluding any background elements". A prompt that went a step further by specifying that the background should be excluded, restricting attention solely to the primary object. This study allows us to disentangle whether richer contextual descriptions or stronger object-centric guidance lead to more reliable recognition. As shown in Table 4, both the overall H score and the H score wrt. each individual target private class (which is class that do not show in the known label set but only exists in the target dataset) increase for VisDA as the prompts become more object-centric (from original to var 3, the view gets more object-centric). However, when we experiment with a similar ablation study for INaturalist, this trend reverses on INaturalist, for both phylum and class taxonomy, where variation 3 performs worse than the original prompt, the results of which are shown in the Appendix A.4. The explanation for the difference in performance trends lies in the fine-grained taxonomy of the dataset, in which many species can only be distinguished by subtle contextual cues such as texture, color tone, or typical habitat. When the prompt suppresses background information, these discriminative cues are lost and the model's alignment between visual features and (scientific) labels weakens. In addition, scientific names have limited pretraining data of such VLM models, which makes contextual signals even more crucial. As a whole, these results show that the decision of whether to exclude the background is image- and task-dependent. For example, for an image of "an arm with a dreamcatcher tattoo" in DomainNet, the ground-truth label "arm" competes with a plausible interpretation "tattoo", and the "right" choice of label depends on what the user intends to infer. Such image examples are discussed in the Appendix A.6. In summary, these observations highlight that prompt design should respect the semantic granularity of the task: use object-focused prompting enhances logical consistency in structured object domains, whereas prompt with context-aware phrasing for fine-grained classes or ecologically / environmentally dependent recognition.

Discussion of VisDA results In Table 5, we observe that the VLMs achieve significantly lower H scores compared to the UniDA baselines. To better understand this gap, we examined the experimental setup

Table 5: H_{u-m} scores (%) for the individual target private classes in the VisDA validation set.

	Target Private Class			**Overall H score**
	skateboard	train	truck	
GLC	69.72	73.92	70.53	71.60
LEAD	75.56	57.92	**76.08**	77.10
Qwen	**84.45**	**87.38**	65.21	**78.24**

in detail. The predefined label list contains nine known classes (aeroplane, bicycle, bus, car, horse, knife, motorcycle, person, plant), while the target private set consists of only three classes: skateboard, train, and truck. We calculate H_{u-m} scores for each target private class in VisDA. The results, which are shown in Table 5, reveal that the H_{u-m} score drops substantially when the private class is a truck. A closer inspection of the source data indicates why: the "car" category is represented exclusively by sedans, SUVs, hatchbacks, and sports cars, with no overlap with truck. For methods such as GLC and LEAD, which rely on pretrained source models, this restricted source definition of "car" enables them to more easily separate truck as an unknown class. In contrast, VLMs, trained on broader corpora, likely encode a richer concept of "car" that encompasses truck as a subtype. Consequently, the greater semantic knowledge of VLMs paradoxically makes it harder to avoid misclassifying a truck as a car, leading to a lower H_{u-m} score.

Influence of Cross-modal Consistency. To isolate the contribution of our cross-modal consistency mechanism, we ablate three configurations: (i) *visual-only* ($\hat{y}_{vision} \in \mathcal{C}$), (ii) *textual-only* ($\hat{y}_{text} \in \mathcal{C}$), and (iii) our full method combining both arms with consistency. As shown in Table 1, visual-only is prone to a *closed-set bias*: very high known-class weighted accuracy while severely under-rejecting unknowns. For example, on VisDA, Qwen's visual-only variant reaches 92.7/8.79 (acc_{k-w},acc_{u-w}), indicating many private-class images are incorrectly accepted as known. Introducing the textual arm helps mitigate this by enabling semantic mismatch reasoning, typically increasing unknown-class accuracy but sometimes at the cost of known accuracy. Our cross-modal consistency framework provides an additional, non-redundant check: by requiring agreement between what the model "sees" and what it can justify from its own summary, it increases recognition of "unknowns" while preserving strong known recognition. The large performance gain shows that by leveraging the consistency between visual and textual reasoning paths, we enhance the model's ability to recognize what it truly knows.

8 Conclusion

We present a cross-modal consistency framework that enables VLMs to better distinguish known from unknown images by requiring agreement between visual and textual classification arms. Experiments on DomainNet, VisDA, and INaturalist-2021 demonstrate that our approach for fallback-enabled closed-set classification consistently improved balanced known *vs.* unknown weighted accuracy and H score relative to SoTA SF-UniDA baselines. The results suggest that enforcing agreement enhances a VLM's logical understanding of "unknown", marking a step toward more self-aware and reliable vision-language reasoning. Moreover, our results suggest that the traditional SF-UniDA paradigm may no longer be the most effective way to obtain fallback behavior when strong VLMs are available. In our experiments, a frozen VLM equipped with a cross-modal consistency framework consistently matches or outperforms SF-UniDA methods, pointing toward a future in which open-world recognition relies more on VLM-based decision rules than on dedicated adapters on pretrained source classifiers.

9 Limitations and Future Works

Our study has several limitations. First, we focus on single-label image classification with fallback action, leaving multi-label classification and more complex vision tasks to interesting future work. Second, the proposed framework still requires multiple prompts per sample, which would increase latency and cost in large-scale commercial use. In the future, we plan to explore ways to reduce query cost.

References

Josh Achiam, Steven Adler, Sandhini Agarwal, Lama Ahmad, Ilge Akkaya, Florencia Leoni Aleman, Diogo Almeida, Janko Altenschmidt, Sam Altman, Shyamal Anadkat, et al. Gpt-4 technical report. *arXiv preprint arXiv:2303.08774*, 2023.

Jinze Bai, Shuai Bai, Yunfei Chu, Zeyu Cui, Kai Dang, Xiaodong Deng, Yang Fan, Wenbin Ge, Yu Han, Fei Huang, et al. Qwen technical report. *arXiv preprint arXiv:2309.16609*, 2023.

Ke Bai, Guoyin Wang, Jiwei Li, Sunghyun Park, Sungjin Lee, Puyang Xu, Ricardo Henao, and Lawrence Carin. Open world classification with adaptive negative samples. In *Proceedings of the 2022 conference on empirical methods in natural language processing*, pp. 4378–4392, 2022.

Shuai Bai, Keqin Chen, Xuejing Liu, Jialin Wang, Wenbin Ge, Sibo Song, Kai Dang, Peng Wang, Shijie Wang, Jun Tang, et al. Qwen2. 5-vl technical report. *arXiv preprint arXiv:2502.13923*, 2025.

Sondos Mahmoud Bsharat, Aidar Myrzakhan, and Zhiqiang Shen. Principled instructions are all you need for questioning llama-1/2, gpt-3.5/4. *arXiv preprint arXiv:2312.16171*, 2023.

Wanxing Chang, Ye Shi, Hoang Tuan, and Jingya Wang. Unified optimal transport framework for universal domain adaptation. *Advances in Neural Information Processing Systems*, 35:29512–29524, 2022.

Angelica Chen, Jason Phang, Alicia Parrish, Vishakh Padmakumar, Chen Zhao, Samuel R Bowman, and Kyunghyun Cho. Two failures of self-consistency in the multi-step reasoning of llms. *arXiv preprint arXiv:2305.14279*, 2023.

Seun-An Choe, Keon-Hee Park, Jinwoo Choi, and Gyeong-Moon Park. Universal domain adaptation for semantic segmentation. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, pp. 4607–4617, June 2025.

Gheorghe Comanici, Eric Bieber, Mike Schaekermann, Ice Pasupat, Noveen Sachdeva, Inderjit Dhillon, Marcel Blistein, Ori Ram, Dan Zhang, Evan Rosen, et al. Gemini 2.5: Pushing the frontier with advanced reasoning, multimodality, long context, and next generation agentic capabilities. *arXiv preprint arXiv:2507.06261*, 2025.

Choubo Ding and Guansong Pang. Improving open-world classification with disentangled foreground and background features. In *ACM Multimedia 2024*, 2024. URL `https://openreview.net/forum?id=6GLwA6jR3N`.

Geli Fei and Bing Liu. Breaking the closed world assumption in text classification. In Kevin Knight, Ani Nenkova, and Owen Rambow (eds.), *Proceedings of the 2016 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies*, pp. 506–514, San Diego, California, June 2016. Association for Computational Linguistics. doi: 10.18653/v1/N16-1061. URL `https://aclanthology.org/N16-1061/`.

Aaron Grattafiori, Abhimanyu Dubey, Abhinav Jauhri, Abhinav Pandey, Abhishek Kadian, Ahmad Al-Dahle, Aiesha Letman, Akhil Mathur, Alan Schelten, Alex Vaughan, et al. The llama 3 herd of models. *arXiv preprint arXiv:2407.21783*, 2024.

Mingfei Han, Haihong Hao, Jinxing Zhou, Zhihui Li, Yuhui Zheng, Xueqing Deng, Linjie Yang, and Xiaojun Chang. Self-consistency as a free lunch: Reducing hallucinations in vision-language models via self-reflection. *arXiv preprint arXiv:2509.23236*, 2025.

Lei Huang, Weijiang Yu, Weitao Ma, Weihong Zhong, Zhangyin Feng, Haotian Wang, Qianglong Chen, Weihua Peng, Xiaocheng Feng, Bing Qin, et al. A survey on hallucination in large language models: Principles, taxonomy, challenges, and open questions. *ACM Transactions on Information Systems*, 43(2): 1–55, 2025.

iNaturalist 2021 competition dataset. iNaturalist 2021 competition dataset. `https://github.com/visipedia/inat_comp/tree/master/2021`, 2021.

Yiwen Jiang, Deval Mehta, Siyuan Yan, Yaling Shen, Zimu Wang, and Zongyuan Ge. WISE: Weak-supervision-guided step-by-step explanations for multimodal LLMs in image classification. In Christos Christodoulopoulos, Tanmoy Chakraborty, Carolyn Rose, and Violet Peng (eds.), *Proceedings of the 2025 Conference on Empirical Methods in Natural Language Processing*, pp. 14674–14685, Suzhou, China, November 2025. Association for Computational Linguistics. ISBN 979-8-89176-332-6. doi: 10.18653/v1/2025.emnlp-main.741. URL https://aclanthology.org/2025.emnlp-main.741/.

Adam Tauman Kalai, Ofir Nachum, Santosh S. Vempala, and Edwin Zhang. Why language models hallucinate, 2025. URL https://arxiv.org/abs/2509.04664.

Sanyam Kapoor, Nate Gruver, Manley Roberts, Katie Collins, Arka Pal, Umang Bhatt, Adrian Weller, Samuel Dooley, Micah Goldblum, and Andrew G Wilson. Large language models must be taught to know what they don't know. *Advances in Neural Information Processing Systems*, 37:85932–85972, 2024.

Zaid Khan and Yun Fu. Consistency and uncertainty: Identifying unreliable responses from black-box vision-language models for selective visual question answering. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, pp. 10854–10863, 2024.

Jian Liang, Dapeng Hu, Jiashi Feng, and Ran He. Umad: Universal model adaptation under domain and category shift. *arXiv preprint arXiv:2112.08553*, 2021.

Potsawee Manakul, Adian Liusie, and Mark Gales. Selfcheckgpt: Zero-resource black-box hallucination detection for generative large language models. In *Proceedings of the 2023 conference on empirical methods in natural language processing*, pp. 9004–9017, 2023.

Chancharik Mitra, Brandon Huang, Tianning Chai, Zhiqiu Lin, Assaf Arbelle, Rogerio Feris, Leonid Karlinsky, Trevor Darrell, Deva Ramanan, and Roei Herzig. Enhancing few-shot vision-language classification with large multimodal model features. In *Proceedings of the IEEE/CVF International Conference on Computer Vision (ICCV)*, pp. 2760–2772, October 2025.

Xingchao Peng, Ben Usman, Neela Kaushik, Judy Hoffman, Dequan Wang, and Kate Saenko. Visda: The visual domain adaptation challenge. *arXiv preprint arXiv:1710.06924*, 2017.

Xingchao Peng, Qinxun Bai, Xide Xia, Zijun Huang, Kate Saenko, and Bo Wang. Moment matching for multi-source domain adaptation. In *Proceedings of the IEEE International Conference on Computer Vision*, pp. 1406–1415, 2019.

Sanqing Qu, Tianpei Zou, Florian Röhrbein, Cewu Lu, Guang Chen, Dacheng Tao, and Changjun Jiang. Upcycling models under domain and category shift. In *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*, pp. 20019–20028, 2023.

Sanqing Qu, Tianpei Zou, Lianghua He, Florian Röhrbein, Alois Knoll, Guang Chen, and Changjun Jiang. Lead: Learning decomposition for source-free universal domain adaptation. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, pp. 23334–23343, 2024.

Pranab Sahoo, Ayush Kumar Singh, Sriparna Saha, Vinija Jain, Samrat Mondal, and Aman Chadha. A systematic survey of prompt engineering in large language models: Techniques and applications. *arXiv preprint arXiv:2402.07927*, 2024.

Kuniaki Saito and Kate Saenko. Ovanet: One-vs-all network for universal domain adaptation. In *Proceedings of the IEEE/CVF International Conference on Computer Vision (ICCV)*, pp. 9000–9009, October 2021.

Lei Shu, Hu Xu, and Bing Liu. Doc: Deep open classification of text documents. *arXiv preprint arXiv:1709.08716*, 2017.

Lei Shu, Yassine Benajiba, Saab Mansour, and Yi Zhang. Odist: Open world classification via distributionally shifted instances. 2021. URL https://www.amazon.science/publications/odist-open-world-classification-via-distributionally-shifted-instances.

Xuezhi Wang, Jason Wei, Dale Schuurmans, Quoc Le, Ed Chi, Sharan Narang, Aakanksha Chowdhery, and Denny Zhou. Self-consistency improves chain of thought reasoning in language models. *arXiv preprint arXiv:2203.11171*, 2022.

Jason Wei, Xuezhi Wang, Dale Schuurmans, Maarten Bosma, Fei Xia, Ed Chi, Quoc V Le, Denny Zhou, et al. Chain-of-thought prompting elicits reasoning in large language models. *Advances in neural information processing systems*, 35:24824–24837, 2022.

Ziwei Xu, Sanjay Jain, and Mohan Kankanhalli. Hallucination is inevitable: An innate limitation of large language models. *arXiv preprint arXiv:2401.11817*, 2024.

Zhangyue Yin, Qiushi Sun, Qipeng Guo, Jiawen Wu, Xipeng Qiu, and Xuanjing Huang. Do large language models know what they don't know? *arXiv preprint arXiv:2305.18153*, 2023.

Kaichao You, Mingsheng Long, Zhangjie Cao, Jianmin Wang, and Michael I. Jordan. Universal domain adaptation. In *The IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, June 2019a.

Kaichao You, Mingsheng Long, Zhangjie Cao, Jianmin Wang, and Michael I Jordan. Universal domain adaptation. In *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*, pp. 2720–2729, 2019b.

Li-Ming Zhan, Haowen Liang, Bo Liu, Lu Fan, Albert YS Lam, and Xiao-Ming Wu. Out-of-scope intent detection with self-supervision and discriminative training. In *Proceedings of the 59th Annual Meeting of the Association for Computational Linguistics and the 11th International Joint Conference on Natural Language Processing (Volume 1: Long Papers)*, pp. 3521–3532, 2021.

Yuhui Zhang, Alyssa Unell, Xiaohan Wang, Dhruba Ghosh, Yuchang Su, Ludwig Schmidt, and Serena Yeung-Levy. Why are visually-grounded language models bad at image classification? *Advances in Neural Information Processing Systems*, 37:51727–51753, 2024.

Zhuosheng Zhang, Aston Zhang, Mu Li, Hai Zhao, George Karypis, and Alex Smola. Multimodal chain-of-thought reasoning in language models. *arXiv preprint arXiv:2302.00923*, 2023.