Data-Free Generalized Zero-Shot Learning

Bowen Tang\textsuperscript{1*}, Jing Zhang\textsuperscript{1††}, Long Yan\textsuperscript{1*}, Qian Yu\textsuperscript{1}, Lu Sheng\textsuperscript{1}, Dong Xu\textsuperscript{2}

\textsuperscript{1} School of Software, Beihang University
\textsuperscript{2} Department of Computer Science, The University of Hong Kong
tbw.broHan@qq.com, \{zhangjing, yanlong, qianyu, lsheng\}@buaa.edu.cn, dongxu@hku.hk

Abstract

Deep learning models have the ability to extract rich knowledge from large-scale datasets. However, the sharing of data has become increasingly challenging due to concerns regarding data copyright and privacy. Consequently, this hampers the effective transfer of knowledge from existing data to novel downstream tasks and concepts. Zero-shot learning (ZSL) approaches aim to recognize new classes by transferring semantic knowledge learned from base classes. However, traditional generative ZSL methods often require access to real images from base classes and rely on manually annotated attributes, which presents challenges in terms of data restrictions and model scalability. To this end, this paper tackles a challenging and practical problem dubbed as data-free zero-shot learning (DFZSL), where only the CLIP-based base classes data and a pre-trained classifier is available for zero-shot classification. Specifically, we propose a generic framework for DFZSL, which consists of three main components. Firstly, to recover the virtual features of the base data, we model the CLIP features of base class images as samples from a von Mises-Fisher (vMF) distribution based on the pre-trained classifier. Secondly, we leverage the text features of CLIP as low-cost semantic information and propose a feature-language prompt tuning (FLPT) method to further align the virtual image features and textual features. Thirdly, we train a conditional generative model using the well-aligned virtual image features and corresponding semantic text features, enabling the generation of new classes features and achieve better zero-shot generalization. Our framework has been evaluated on five commonly used benchmarks for generalized ZSL, as well as 11 benchmarks for the base-to-new ZSL. The results demonstrate the superiority and effectiveness of our approach. Our code is available in https://github.com/ylong4/DFZSL.

Introduction

The power of deep learning models lies in their ability to extract rich knowledge, including visual features and semantic information, from large-scale datasets. However, the sharing of data across different companies, institutions, and countries has become increasingly challenging and sensitive. Concerns related to data copyright and privacy, particularly in sensitive domains such as health and security, pose significant obstacles to the seamless transfer of knowledge from large-scale datasets to novel downstream tasks and concepts. These challenges impede the widespread utilization of deep learning models and limit their potential impact in various fields.

Inspired by the mounting concerns regarding data and model privacy issues, particularly in the context of knowledge transfer to new concepts, this paper addresses the problem of data-free zero-shot learning without access to any real data. Zero-shot learning (ZSL) addresses the challenge of recognizing new classes by leveraging semantic knowledge transferred from base classes. Despite the notable advancements in ZSL, most ZSL methods often require access to labeled images from base classes, either for aligning visual-semantic embeddings or training conditional generative models (Xian et al. 2018a,b; Narayan et al. 2020). Unfortunately, obtaining real data from base classes is often impractical in real-world applications due to privacy or copyright restrictions. Moreover, existing approaches heavily rely on manually annotated attributes, which present challenges in terms of scalability and the difficulty of annotation (Farhadi et al. 2009; Gan et al. 2015; Shigeto et al. 2015; Romera-Paredes and Torr 2015).

The recent progress in large-scale pre-trained vision-language models, such as CLIP (Radford et al. 2021), have demonstrated impressive zero-shot generalization abilities. These models achieve this capability through extensive training on vast collections of image-caption pairs without the requirement of manually annotated attributes. However, effectively transferring the knowledge from these models, which are trained on weakly aligned image-caption pairs, to downstream fine-grained zero-shot classification tasks remains challenging and sub-optimal. This is primarily due to the discrepancy in class granularity between the pre-trained models and the specific classification tasks at hand. Prompt tuning deals with this issue by adding learnable prompts to the inputs. However, the recent prompt tuning methods (Zhou et al. 2022b; Bahng et al. 2022; Zhou et al. 2022a) still suffer from single-side alignment and rely on the access to the real images.

To this end, this paper addresses a challenging and practical problem dubbed as data-free zero-shot learning (DFZSL). In this setting, the only available resource for zero-shot classification is a pre-trained base classes classi-
fier based on CLIP features. Notably, we do not have access to any real data from either the base or new classes, and manual attribute annotations are not required. Our setting is closely related to Absolute Zero-Shot Learning (Gao et al. 2022). However, their method still relies on manual attribute annotations and performs poorly in both conventional and generalized ZSL.

The proposed framework consists of three main components. Firstly, to recover the base class data, we model the CLIP features of base class images as samples from a von Mises-Fisher (vMF) distribution, with learnable mean ($\mu$) and proper concentration ($\kappa$) parameters based on the pre-trained classifier. This allows us to recover the virtual features of the base data by sampling from the distribution. It is important to note that our method does not recover the original images. Instead, our focus is on recovering the high-level image feature vectors, which is more efficient and avoids the privacy and copyright concerns. Secondly, to bridge the base and new classes, we leverage the text encoder of CLIP to obtain low-cost semantic information in the form of generalizable text features, which eliminates the need for manual attribute annotations. Our framework is generic, and any vision-language foundation models can be potentially used. In order to enhance the adaptation to downstream fine-grained zero-shot classification tasks, we introduce a feature-language prompt tuning method. This method aims to further align the virtual image features of base classes with their corresponding text features by tuning both visual features and textual inputs. Thirdly, we train a conditional generative model using the well-aligned virtual image features and corresponding semantic text features, which enables us to generate labeled data for new classes. And then zero-shot classification is achieved through supervised learning. Our framework has been evaluated on five commonly used benchmarks for generalized ZSL, as well as 11 benchmarks for the base-to-new generalization. The results demonstrate the superiority of our approach.

Related Work

Traditional Zero-Shot Learning. Zero-shot learning (ZSL) is a research area that explores the generalizability of deep learning models. Specifically, it focuses on training a classifier that can recognize samples from the new classes that are unseen during training. It is broadened to generalized zero-shot learning (GZSL) where both base and new classes should be recognized during the testing phase. Embedding based methods and generative-model based methods are the two mainstream methodologies for GZSL. An embedding based approach aims to learn a mapping function that maps visual features and semantic information into a unified space (Romera-Paredes and Torr 2015; Jiang et al. 2019a; Reed et al. 2016; LeCun et al. 1998; Elman 1990). The absence of new class data makes it prone to overfitting so that the test samples of the new classes are easy to be incorrectly classified into a base class. To mitigate the data imbalance problem, recent studies prefer generative-model based methods because they can convert the challenging ZSL problem into a fully-supervised recognition task by synthesizing the absent samples of the new classes. Most generative-model based methods use GAN or VAE for generation (Ye et al. 2019; Han et al. 2021; Chen et al. 2021b; Ye et al. 2022), and some studies have explored the combination of them which we termed as VAEGAN (Larsen et al. 2016; Xian et al. 2019a). A significant drawback in both embedding based methods and generative-model based methods is that they rely on a large amount of real image data to learn the shared embedding space or train the generator. This requirement raises concerns related to copyright infringement and privacy issues. Moreover, these methods often necessitate experts attribute annotations, which are labor-intensive and expensive.

Fine-Tuning for Vision-Language Models. Recently, the contrastive trained vision-language model CLIP (Radford et al. 2021) shows impressive zero-shot performance on recognition tasks. When we directly infer with the pre-trained CLIP, which is denoted as Zero-Shot CLIP, the performance is still limited on some downstream datasets. It is because of the domain shift between the pre-training dataset and the downstream datasets for specific tasks, especially when the task is fine-grained. Adapter methods focus on further learning a mapping network for the output features. One of them is CLIP-Adapter (Romera-Paredes and Torr 2015), which uses a residual connected MLP after the last vision layer and the last text layer. Prompt tuning methods introduce parameters to the input. CoOp (Zhou et al. 2022b) establishes a set of learnable vectors on the textual side to learn a generic prompt template. CoCoOp (Zhou et al. 2022a) leverages information from the visual side and builds instance-level prompt templates to achieve base-to-new generalization. VP (Bahng et al. 2022) and VPT (Derkhshani et al. 2022) design the tunable visual prompts either on the images or on the patch tokens. MaPLe (Khattak et al. 2023) inserts learnable tokens inside the visual encoder and text encoder for deep fine-tuning, but it still relies on images and requires more training. Unlike existing prompt tuning methods that focus on learning single-modality prompts or rely on the original images, our approach involves tuning prompts for both visual features (without need of the original images) and textual inputs.

Data-Free Transfer Learning. Data plays a significant role in the development of artificial intelligence. The value of data is more and more appreciative so real data is always not accessible due to copyright or privacy issues nowadays. Thus, data-free transfer learning, which just needs the source model for training but leaves the source data protected, receives increased attention. Existing research under the Data-Free setting can be divided into three categories based on the level of the guards of the source model parameters: available source model parameters (Gao et al. 2022; Tian et al. 2021), inaccessible parameters but enable gradient propagation (Chen et al. 2019), and a black-box service, where the source model just exposes an API for the client to request predictions (Gao et al. 2022). Despite their exhaustive experiments with various guard levels, the results are not satisfactory in the most realistic black-box scenario.
Methodology

Problem Formulation and Overview

In this paper, we propose and address a novel problem called data-free zero-shot learning (DFZSL). In the data-free setting, data from base classes are protected considering privacy or copyrights and cannot be directly used for training zero-shot learning methods.

Formally, consider a data owner as the server and there are images of base classes on the server. The image encoder of pre-trained CLIP can be used to extract image features $x_\text{base} \in X_\text{base}$. The corresponding labels for base classes are $y_{\text{base}} \in Y_{\text{base}}$. A classifier for base classes can be trained with image features extracted from real images by the pre-trained CLIP model. We denote the trained base classifier as $f_{\text{base}} : X_{\text{base}} \rightarrow Y_{\text{base}}$. In a white-box scenario, the classifier weights are available. While in a black-box scenario, the server does not leak the classifier weights and just exposes an API for the client to request the prediction.

The client side does not have access to any images that can be used for training in the data-free setting. The image features and labels of new class data are denoted as $x_{\text{new}} \in X_{\text{new}}$ and $y_{\text{new}} \in Y_{\text{new}}$, respectively. The classes of base data and new data are disjoint so that $Y_{\text{base}} \cap Y_{\text{new}} = \emptyset$. Now we have $X = X_{\text{base}} \cup X_{\text{new}}$ and $Y = Y_{\text{base}} \cup Y_{\text{new}}$.

In data-free zero-shot learning, the objective is to classify test images from both base and new classes on the client side, utilizing the assistance of a base classifier located on the server, without directly accessing the training data.

Overview. To solve the proposed data-free zero-shot learning problem, we propose a generic framework consisting of three main stages. The overall pipeline is shown in Fig. 1. Firstly, we propose to recover the image features of base classes from the base classifier. Secondly, we leverage the CLIP text features as the semantic side information, and propose a feature-language prompt tuning method to extract well-aligned high-quality image features and text features. Thirdly, with both, we follow traditional generative model-based methods to train the generator and classifier for the downstream fine-grained zero-shot classification tasks.

Base-Class Data Recovery

While we want to transfer from base classes to disjoint new classes on downstream datasets via traditional generative methods, we have to prepare the training data. Therefore, we propose a novel method to recover the image features of base classes from the base classifier located on the server in both white-box and black-box setting. The general idea is to model the distribution of the original data properly and then sample virtual data from it.

The most commonly used softmax classifier in deep learning is in the form of a matrix that consists of weights for each class and is trained with cross-entropy loss. During the training process, these weights are forced to be closer to the image features of the corresponding class and keep away from other classes. Especially for CLIP, cosine similarity is used as the metric for prediction. As a result, the L2-normed weights are good representations of class prototypes.

To recover the base-class data, we hypothesise that the L2-normed image features follow a distribution on a hypersphere, where features belonging to the same class tend to cluster together. Therefore, we approximate the real image features of base classes using the von Mises-Fisher (vMF) distribution that is defined on the surface of a unit hypersphere. A vMF distribution is determined by two parameters, the mean direction $\mu$ and the concentration $\kappa$. We establish a set of class prototypes: $M = \{\mu_1, \mu_2, \cdots, \mu_{|Y_{\text{base}}|}\}$ as the mean direction of each class. In the white-box scenario, the base classifier weights $W = \{w_1, w_2, \cdots, w_{|Y_{\text{base}}|}\}$ are available, and we directly set $M = W$. In the black-box scenario, we turn the class prototypes $M$ into learnable parameters and initialize them by the text features $T = \{t_1, t_2, \cdots, t_{|Y_{\text{base}}|}\}$ of corresponding classes. The text features are extracted by CLIP’s text encoder $T_{\text{encoder}}$ from the prompt “a photo of a [CLS]”, where [CLS] is a class name.
With the mean direction, virtual image features can be sampled surrounding the center and the concentration controls the spread of sampled features. While we choose a proper concentration, the underlying principle is that if sampled features from the distribution belong to different classes, they should be sufficiently separable. We assume an isotropic covariance for simplicity. In statistics, vMF distribution is a close approximation to the wrapped Gaussian distribution. According to the empirical rules of the Gaussian distribution, approximately 99.73% of the sampled data deviates from the mean within a range of 3 standard deviations \(3\sigma\). Therefore, if we aim for the sampled virtual data from the two classes to be discriminative, the arc length between their respective prototypes should be at least greater than \(6\sigma\). Then the concentration parameter can be derived from the definition of the von Mises-Fisher (vMF) distribution, expressed as \(\kappa = \frac{1}{6\sigma^2}\). Thus, we set the concentration that caters to all class pairs in the downstream datasets with the class prototypes:

\[
\kappa_{\text{text}} = \max_{y \in Y} \frac{1}{|y\setminus y|} \left\{ \frac{1}{6} \arccos \left( \frac{\mu_y}{|\mu_y|} \cdot \frac{\mu_y'}{|\mu_y'|} \right) \right\}^{-2}
\] (1)

The virtual image features can be considered to follow the vMF distribution determined by prototypes \(M, \lambda, \kappa_{\text{text}}\):

\[
\tilde{x} \sim \text{vMF} (M, \lambda \cdot \kappa_{\text{text}}),
\] (2)

where \(\lambda\) is a hyper-parameter to refine the concentration (which is normally set to \(\lambda = 1\) and a greater \(\lambda\) produces a more concentrated distribution within each class).

We can now sample virtual image features of base classes \(\hat{x}^\text{base} \in \hat{X}^\text{base}\) from the vMF distribution. However, for the black-box scenario, we further tune the initial class prototypes to mitigate the modality gap between image and text. We first upload the sampled virtual image features as test samples to the base classifier on the server and obtain the prediction scores \(s^\text{base}\). Subsequently, we treat the learnable class prototypes as a base classifier on the client and predict scores for these virtual image features. The objective is to align the two sets of scores and make the prototypes closely resemble the classifier weights protected on the server:

\[
L_{\text{proto}}(M) = \frac{1}{|Y^\text{base}|} \sum_{y \in Y^\text{base}} \left( s^\text{base} - \cos \left( \hat{x}^\text{base}, M \right) \right)^2
\] (3)

**Feature-Language Prompt Tuning**

In addition to the recovered virtual image features, another crucial component for achieving the transfer from base to new classes is the semantic information. We use the text features extracted by the pre-trained CLIP model. However, due to the discrepancy in class granularity between the pre-trained models and the downstream fine-grained zero-shot classification tasks at hand, the semantic information produced by the CLIP models trained on weakly aligned image-caption pairs is sub-optimal.

To further enhance the quality of the semantic information, we propose a feature-language prompt tuning method. On the visual side, our method requires only the features of the image, not the original picture. Considering that the recovered virtual image features only cover base classes and we have to transfer to new classes, we tune the prompts in a class-agnostic way. Particularly, we replace the embeddings of class-agnostic prefix “a photo of a” used in CLIP with learnable parameters \(P = \{p_1, p_2, p_3, p_4\}\). In addition to the text prompts, we also introduce a shift term \(x_{\text{shift}}\) as class-agnostic learnable parameters added to the image features. To accumulate class-agnostic generalizable knowledge, we establish a connection between the text prompts and the image shift using a light mapping network \(F_\Theta\) parameterized by \(\Theta\). It serves as a bridge between the textual information and the image transformation, allowing for the integration of both modalities. The \(x_{\text{shift}}\) is then defined as:

\[
x_{\text{shift}} = \frac{1}{4} \sum_{i=1}^{4} F_\Theta (P).
\] (4)

We try to tune these parameters to better align the features of two modalities and mitigate the domain shift between CLIP’s pre-training dataset and the downstream datasets. Then we have the enhanced image features which can help us easily generalize to different classes:

\[
\hat{x}^\text{base} = \hat{x}^\text{base} + \alpha x_{\text{shift}},
\] (5)

where \(\alpha\) is the trade-off parameter that controls how much we add the shift term. The enhanced text features are:

\[
\tilde{t} = T_{\text{encoder}} (\{p_1, p_2, p_3, p_4, [CLS]\}),
\] (6)

where \([CLS]\) represents the embedding of class name. The parameters are optimized by lower the cross-entropy when classifying the image features by the text features:

\[
L_{\text{pt}}(\Theta, P) = -\log \frac{\exp (\cos (\hat{x}^\text{base}, \tilde{t}_y)/\tau)}{\sum_{y' \in Y^\text{base}} \exp (\cos (\hat{x}^\text{base}, \tilde{t}_{y'}/\tau))}
\] (7)

and \(\tau\) is the temperature used in CLIP which equals to 0.01.

**New Class Features Generation for Zero-shot Classification**

After we recovered the base class image features and conducted the feature-language prompt tuning, we have already prepared high-quality training data for traditional generative zero-shot learning methods.

**Generate Data of New Classes.** We choose to train a suitable generative model based on the enhanced base data. The loss function is termed as follows:

\[
L_{\text{generator}}(\Phi) = \ell (\hat{x}^\text{base}, G_{\Phi} (z, \tilde{x}^\text{base})),
\] (8)

where \(\ell\) can be GAN loss or other loss defined by the chosen generative model. \(G\) is the generator parameterized by \(\Phi\) and \(z\) represents the random noise. Then we condition the generator with text features of new classes and generate the new class image features:

\[
\hat{x}^\text{new} = G_{\Phi} (z, \tilde{x}^\text{new}.
\] (9)

**Supervised Image Classification.** With the enhanced virtual image features of base classes \(\hat{x}^\text{base}\) and the generated virtual image features of new classes \(\hat{x}^\text{new}\), the generalized zero-shot learning problem is converted into a fully-supervised image classification problem. Moreover, we initialize the weights of the final classifier by the enhanced text features to speed up the training process.
Experiments

Datasets and Implementation Details

Datasets. We evaluate our method in two different tasks: generalized zero-shot learning and base-to-new generalization. For generalized zero-shot learning, we follow the same setting as (Xian et al. 2018a). Our framework is evaluated on five datasets: Attribute Pascal and Yahoo (APY) (Farhadi et al. 2009), CaltechUCSD-Birds (CUB) (Welinder et al. 2010), Oxford Flowers (FLO) (Nilsback and Zisserman 2008), SUN Attribute (SUN) (Patterson and Hays 2012), and Animals with Attributes2 (AWA2) (Xian et al. 2018a), which contains 32, 200, 102, 717 and 50 classes, respectively. As for the base-to-new generalization, we follow the setting proposed in CoCoOp (Zhou et al. 2022a). We evaluate the performance of our framework on 11 different image classification datasets which covers a wide range of recognition tasks. This includes a large-scale visual dataset, ImageNet (Deng et al. 2009); a generic-objects datasets, Caltech101 (Fei-Fei 2004); five fine-grained image recognition datasets, OxfordPets (Parkhi et al. 2012), Stanford-Cars (Krause et al. 2013), Flowers102 (Nilsback and Zisserman 2008), Food101 (Bossard, Guillaumin, and Van Gool 2014) and FGVC Aircraft (Maji et al. 2013); a satellite-view topographic image dataset EuroSAT (Helber et al. 2019); an action recognition dataset UCF101 (Soomro, Zamir, and Shah 2012); a texture dataset DTD (Cimpoi et al. 2014); and a scene recognition dataset SUN397 (Xiao et al. 2010). These datasets will be detailed in the appendix.

Implementation Details. Our proposed framework consists of three stages: recover virtual image features of base classes, utilize FLPT to enhance both the virtual image features and semantic text features, and finally adopt traditional generative ZSL methods. We recover the base class data in the data-free setting at the first stage. In the white-box scenario, where the base classifier weights are accessible, we directly apply them as the class prototypes. In the black-box scenario, the class prototypes are initialized by text features, and \( \lambda \) is set to 1. We apply the Adam optimizer and the learning rate is set to 0.0003. In the second prompt tuning stage, we implement the light mapping network with a single-hidden-layer MLP activated by GELU. For the third stage, we use off-the-shelf generative-model based methods. The setup stays the same as what they proposed in their papers. All experiments are performed on an NVIDIA GeForce RTX3090, except for the ImageNet, which is performed on an NVIDIA A100.

Results of Generalized Zero-Shot Learning

Setup. We follow the splits and evaluation protocols proposed in (Xian et al. 2018a), train on base classes and then evaluated on test set that mixes the base classes and the new classes. Differently, the only input information of our base classes is the base classifier on the server. We do not use the attribute vectors provided in these benchmarks, but extract text features by CLIP with “a photo of a [CLS].” instead. The mean per-class top-1 accuracy is reported on base and new classes and the harmonic mean is computed to demonstrate the balanced performance of our framework.

Baselines. We choose f-CLSWGAN (Xian et al. 2018b), Cycle-WGAN (Felix et al. 2018), LisGAN (Li et al. 2019), TCN (Jiang et al. 2019b), f-VAEGAN (Xian et al. 2019b), TF-VAEGAN (Narayan et al. 2020), GCMCF (Yue et al. 2021), HSV-A (Chen et al. 2021a) MSDN (Chen et al. 2022b) AZSL (Gao et al. 2022) and SHIP+CoOp (Wang et al. 2023) as our baseline methods.

Main results. The results of generalized zero-shot learning on the five commonly used benchmarks are shown in Table 1. Firstly, in comparison to traditional generalized zero-shot learning approaches that utilize the ImageNet-1k pre-trained ResNet-101 as the backbone, the baseline data-free ZSL method (AZSL (Gao et al. 2022)) exhibits significantly inferior performance. This highlights the inherent challenge of the data-free ZSL task, as it performs notably worse than ZSL methods that have access to real base data. Secondly, our method improves both traditional generative ZSL methods using CLIP features and the state-of-the-art prompt-tuning methods even without access to the real data in both black-box (Data-Free) and white-box (Data-Free*) settings. For example, when compared with the state-of-the-art SHIP+CoOp method, our framework improves the harmonic mean accuracy by 4.5%, 6.3%, and 10.8% on the three standard benchmarks of AWA2, CUB and FLO, respectively. This verifies the effectiveness of the proposed framework. Thirdly, it is worth noting that the performance gain by our method does not solely originate from the base classes but primarily from the new classes. This observation validates the generalization ability of the proposed method.

Results of Base-to-New Generalization

Setup. We follow CoCoOp (Zhou et al. 2022a) to makes a half-and-half split on 11 datasets, which turns out to divide them into two non-overlapping subsets: the base classes and the new classes. The base-to-new generalization task requires the model to train on base classes and then separately test on base classes and new classes. It is just the same as the conventional ZSL when the model is tested on new classes.

Baselines. We take several recent prompt-tuning methods as baselines, including CoOp, CoCoOp, MaPLe (Khattak et al. 2023), CLIP-Adapter (Gao et al. 2021), VPT (Derkakhshani et al. 2022) and SHIP (Wang et al. 2023).

Main Results. As shown in Table 2, most of the prompt-tuning methods improve the performance of CLIP in the base classes, while they demonstrate limited performance gain or even degradation for new classes. This may be due to the fact that training only on the base classes leads the model to overfit the base classes. To mitigate overfitting to the base classes, SHIP generates the new-class data via the pre-trained CLIP encoders. However, the CLIP features may not be optimal due to the domain gap between the pre-training data and the downstream task data, leading to sub-optimal results. By contrast, our method generates new-class data based on the proposed FLPT method that further align the visual and textual features through multi-modal prompt-tuning strategy. The promising results achieved by FLPT+TFVAEGAN show that the further aligned features are better for training an effective conditional generator.
Table 1: Generalized zero-shot learning. The model is trained on the base classes and is evaluated on the mixture of base classes and new classes. ‘Base’ indicates the base-class results, ‘New’ indicates the new-class results, and ‘H’ is the harmonic mean. ‘Data-Free’ represents the black-box scenario. ‘Data-Free*’ means the white-box scenario. ‘CLIP*’ means that the hand-crafted prompt templates are used.

<table>
<thead>
<tr>
<th>Dataset</th>
<th>Average</th>
<th>ImageNet</th>
<th>Caltech101</th>
<th>OxfordPets</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Base</td>
<td>New</td>
<td>H</td>
<td>Base</td>
</tr>
<tr>
<td>Real-Data</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CoOp</td>
<td>82.69</td>
<td>63.22</td>
<td>71.66</td>
<td>76.47</td>
</tr>
<tr>
<td></td>
<td>79.68</td>
<td>65.97</td>
<td>73.39</td>
<td>75.98</td>
</tr>
<tr>
<td></td>
<td>82.28</td>
<td>75.14</td>
<td>78.55</td>
<td>75.74</td>
</tr>
<tr>
<td></td>
<td>83.05</td>
<td>65.20</td>
<td>73.05</td>
<td>74.73</td>
</tr>
<tr>
<td></td>
<td>71.98</td>
<td>74.76</td>
<td>73.34</td>
<td>75.87</td>
</tr>
<tr>
<td></td>
<td>80.03</td>
<td>73.69</td>
<td>76.73</td>
<td>76.00</td>
</tr>
<tr>
<td>Data-Free</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CLIP</td>
<td>69.34</td>
<td>74.12</td>
<td>71.70</td>
<td>72.43</td>
</tr>
<tr>
<td></td>
<td>78.08</td>
<td>75.46</td>
<td>76.85</td>
<td>76.99</td>
</tr>
<tr>
<td>Data-Free*</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CLIP*</td>
<td>63.37</td>
<td>74.89</td>
<td>68.65</td>
<td>72.08</td>
</tr>
<tr>
<td></td>
<td>65.24</td>
<td>75.74</td>
<td>70.10</td>
<td>88.79</td>
</tr>
<tr>
<td></td>
<td>77.06</td>
<td>75.41</td>
<td>76.23</td>
<td>94.11</td>
</tr>
<tr>
<td>Data-Free</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CLIP</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>80.60</td>
<td>65.89</td>
<td>72.51</td>
<td>79.44</td>
</tr>
<tr>
<td></td>
<td>79.74</td>
<td>76.86</td>
<td>78.27</td>
<td>77.01</td>
</tr>
<tr>
<td></td>
<td>80.82</td>
<td>78.70</td>
<td>79.75</td>
<td>80.36</td>
</tr>
<tr>
<td>Data-Free*</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CLIP*</td>
<td>69.36</td>
<td>75.33</td>
<td>72.23</td>
<td>53.24</td>
</tr>
<tr>
<td></td>
<td>77.84</td>
<td>76.25</td>
<td>77.04</td>
<td>70.37</td>
</tr>
<tr>
<td></td>
<td>82.23</td>
<td>76.23</td>
<td>79.12</td>
<td>80.32</td>
</tr>
</tbody>
</table>

Table 2: Base-to-new generalization. The model is trained on the base classes and is evaluated on the base classes and new classes independently. ‘Base’ indicates the base-class results, ‘New’ indicates the new-class results, and ‘H’ is the harmonic mean. ‘Data-Free’ represents the black-box scenario. ‘Data-Free*’ means the white-box scenario. ‘CLIP*’ means that the hand-crafted prompt templates are used.
### Table 3: Ablation Study

Comparison results of different prompt-tuning methods, different generative models, and ‘Data-Free’ vs. ‘Real-Data’ settings. ‘CLIP*’ means the hand-crafted prompt templates are used.

<table>
<thead>
<tr>
<th>Class</th>
<th>AWA2</th>
<th>APY</th>
<th>CUB</th>
<th>SUN</th>
<th>FLO</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Base</td>
<td>New</td>
<td>H</td>
<td>Base</td>
<td>New</td>
</tr>
<tr>
<td>ox</td>
<td>93.04</td>
<td>88.21</td>
<td>90.57</td>
<td>81.63</td>
<td>75.76</td>
</tr>
<tr>
<td>pig</td>
<td>94.35</td>
<td>85.27</td>
<td>89.58</td>
<td>82.21</td>
<td>78.47</td>
</tr>
<tr>
<td>tiger</td>
<td>93.57</td>
<td>92.92</td>
<td>93.24</td>
<td>83.00</td>
<td>80.11</td>
</tr>
<tr>
<td>zebra</td>
<td>93.84</td>
<td>93.60</td>
<td>93.72</td>
<td>84.50</td>
<td>79.95</td>
</tr>
<tr>
<td>panda</td>
<td>94.05</td>
<td>92.79</td>
<td>93.42</td>
<td>81.97</td>
<td>76.90</td>
</tr>
<tr>
<td>buffalo</td>
<td>94.50</td>
<td>88.76</td>
<td>91.54</td>
<td>83.11</td>
<td>79.69</td>
</tr>
<tr>
<td>real</td>
<td>94.37</td>
<td>93.69</td>
<td>94.03</td>
<td>83.99</td>
<td>80.59</td>
</tr>
<tr>
<td>virtual</td>
<td>92.66</td>
<td>96.05</td>
<td>94.32</td>
<td>83.54</td>
<td>81.91</td>
</tr>
<tr>
<td>CLIP*</td>
<td>93.14</td>
<td>93.69</td>
<td>93.41</td>
<td>82.02</td>
<td>76.37</td>
</tr>
<tr>
<td>CoOp+TF-VAEGAN</td>
<td>93.43</td>
<td>92.15</td>
<td>92.79</td>
<td>82.14</td>
<td>79.31</td>
</tr>
<tr>
<td>FLPT+ZLAP</td>
<td>92.47</td>
<td>95.30</td>
<td>93.87</td>
<td>84.10</td>
<td>80.20</td>
</tr>
<tr>
<td>FLPT+SDGZSL</td>
<td>93.94</td>
<td>93.03</td>
<td>93.48</td>
<td>83.72</td>
<td>81.20</td>
</tr>
<tr>
<td>CoOp+SVGZSL</td>
<td>94.51</td>
<td>88.50</td>
<td>91.41</td>
<td>83.01</td>
<td>79.39</td>
</tr>
<tr>
<td>FLPT+TF-VAEGAN</td>
<td>93.86</td>
<td>93.16</td>
<td>93.51</td>
<td>84.18</td>
<td>81.12</td>
</tr>
<tr>
<td>FLPT+TF-VAEGAN</td>
<td>93.84</td>
<td>93.39</td>
<td>93.71</td>
<td>84.56</td>
<td>80.75</td>
</tr>
</tbody>
</table>

**Ablation Study**

We conducted ablation studies under the setting of generalized zero-shot learning to demonstrate the validity and generalizability of our proposed framework.

**Quality of the Recovered Virtual Data.** We visualized the recovered virtual base data and the real base data of 6 classes in AWA2 in Figure 2. It can be seen that the recovered data exhibits a distribution similar to that of the real data and possesses sufficient class discriminative qualities. To further validate the quality of the recovered image features and make a fairer comparison with baselines, we performed the experiments on real and virtual data, respectively. As shown in Table 3, It can be seen that the performance gap between the real data and virtual data is small, especially for AWA2, APY and FLO, which validate the effectiveness of the proposed base class data recovery method. The gap is slightly larger for CUB and SUN datasets, which is due to their fine-grained and challenging nature.

**Comparisons of Different Prompt-tuning Methods.** To evaluate the proposed FLPT that enhances the image features and text features, we compare FLPT to hand-crafted prompts in CLIP and the learning-based CoOp in Figure 3 and Table 3. It can be seen that FLPT outperforms the other two on all the five GZSL benchmarks. Furthermore, the performance is further improved after applying the enhanced features to the generative-model based methods. Compared to hand-crafted prompts, FLPT is a data-driven method, which costs less and is more effective. While compared to CoOp, FLPT makes a link between two modalities and aligns both image features and text features simultaneously.

**Different Generative-Model-Based Methods.** The proposed FLPT method can be combined with any generative models to further improve the ZSL performance. We evaluate our method with three generative methods: GAN-based ZLAP (Chen et al. 2022a), VAEGAN-based SDGZSL (Chen et al. 2021c), and VAEGAN-based TF-VAEGAN (Narayan et al. 2020). As shown in Table 3, when integrating FLPT with...
the three types of generative models, all of them exhibit improved performance compared to FLPT alone.

Conclusion

This paper addresses a challenging and practical problem dubbed as data-free zero-shot learning (DFZSL). In DFZSL, the use of real images from both the base classes and the new classes is not necessary, thereby effectively preserving data copyright and privacy. To tackle DFZSL, we propose a CLIP-based framework, which consists of three main stages. Firstly, the virtual base-class data are recovered via a modeled von Mises-Fisher distribution based on the pre-trained CLIP classifier. Secondly, we propose a feature-language prompt tuning method to further align the virtual image features and textual features. Thirdly, to achieve better zero-shot classification, we generate the new-class data by training a conditional generative model based on the well-aligned base-class multi-modal features. Extensive experiments on both base-to-new ZSL and generalized ZSL demonstrate the effectiveness of the proposed framework.

Acknowledgments

This work was supported by the National Key Research and Development Program of China (No. 2021YFB1714300), National Natural Science Foundation of China (No.62006012, No.62132001, No.62002012), in part by the Hong Kong Research Grants Council General Research Fund (17203023), in part by The Hong Kong Jockey Club Charities Trust under Grant 2022-0174, in part by the Startup Funding and the Seed Funding for Basic Research for New Staff from The University of Hong Kong, and in part by the funding from UBTECH Robotics.

References


