Safe Self-Refinement for Transformer-based Domain Adaptation

Tao Sun\(^1\), Cheng Lu\(^2\), Tianshuo Zhang\(^2\), Haibin Ling\(^1\)
\(^1\)Stony Brook University, \(^2\)XPeng Motors
\{tao,hling\}@cs.stonybrook.edu, luc@xiaopeng.com, tonyzhang2035@gmail.com

Abstract

Unsupervised Domain Adaptation (UDA) aims to leverage a label-rich source domain to solve tasks on a related unlabeled target domain. It is a challenging problem especially when a large domain gap lies between the source and target domains. In this paper we propose a novel solution named SSRT (Safe Self-Refinement for Transformer-based domain adaptation), which brings improvement from two aspects. First, encouraged by the success of vision transformers in various vision tasks, we arm SSRT with a transformer backbone. We find that the combination of vision transformer with simple adversarial adaptation surpasses best reported Convolutional Neural Network (CNN)-based results on the challenging DomainNet benchmark, showing its strong transferable feature representation. Second, to reduce the risk of model collapse and improve the effectiveness of knowledge transfer between domains with large gaps, we propose a Safe Self-Refinement strategy. Specifically, SSRT utilizes predictions of perturbed target domain data to refine the model. Since the model capacity of vision transformer is large and predictions in such challenging tasks can be noisy, a safe training mechanism is designed to adaptively adjust learning configuration. Extensive evaluations are conducted on several widely tested UDA benchmarks and SSRT achieves consistently the best performances, including 85.43\% on Office-Home, 88.76\% on VisDA-2017 and 45.2\% on DomainNet.

1. Introduction

Deep neural networks have achieved impressive performance in a variety of machine learning tasks. However, the success often relies on a large amount of labeled training data, which can be costly or impractical to obtain. Unsupervised Domain Adaptation (UDA) [36] handles this issue by transferring knowledge from a label-rich source domain to a different unlabeled target domain. Over the past years, many UDA methods have been proposed [4, 12, 14, 24, 44]. Among them, adversarial adaptation [4, 14, 44] that learns domain-invariant feature representation using the idea of adversarial learning has been a prevailing paradigm. Deep UDA methods are usually applied in conjunction with a pretrained Convolutional Neural Network (CNN, e.g., ResNet [8]) backbone in vision tasks. On medium-sized classification benchmarks such as Office-Home [33] and VisDA [20], the reported state-of-the-arts are very impressive [12]. However, on large-scale datasets like DomainNet [19], the most recent results in the literature by our submission report a best average accuracy of 33.3\% [10], which is far from satisfactory.

With the above observations, we focus our investigation on challenging cases from two aspects:

- First, from the representation aspect, it is desirable to use a more powerful backbone network. This directs our attention to the recently popularized vision transformers, which have been successfully applied to various vision tasks [2, 3, 42]. Vision transformer processes an image as a sequence of tokens, and uses global self-attention to refine this representation. With its long-range dependencies and large-scale pre-training, vision transformer obtains strong feature representation that is ready for downstream tasks. Despite this, its application in UDA is still under-explored. Hence we propose to integrate vision transformer to UDA. We find that by simply combining ViT-B/16 [3] with adversarial adaptation, it can achieve 38.5\% average accuracy on DomainNet, better than the current arts using ResNet-101 [8, 10]. This shows that the feature representation of vision transformer is discriminative as well as transferable across domains.

- Second, from the domain adaptation aspect, a more reliable strategy is needed to protect the learning process from collapse due to large domain gaps. As strong backbones with large capacity like vision transformer increase the chance of overfitting to source domain data, a regularization from target domain data is desired. A common practice in UDA is to utilize model predictions for self-training or enforce clustering structure on target domain data [12, 24, 43]. While this helps generally, the supervisions can be noisy when the domain gap is large. Therefore, an adaptation method is expected to be Safe [11] enough to avoid model collapse.
Motivated by the above discussions, in this paper, we propose a novel UDA solution named SSRT (Safe Self-Refinement for Transformer-based domain adaptation). SSRT takes a vision transformer as the backbone network and utilizes predictions on perturbed target domain data to refine the adapted model. Specifically, we add random offsets to the latent token sequences of target domain data, and minimize the discrepancy of model’s predicted probabilities between the original and perturbed versions using the Kullback Leibler (KL) divergence. This imposes a regularization on the corresponding transformer layers in effect. Moreover, SSRT has several important components that contribute to its excellent performance, including multi-layer perturbation and bi-directional supervision.

To protect the learning process from collapse, we propose a novel Safe Training mechanism. As UDA tasks vary widely even when they are drawn from the same dataset, a specific learning configuration (e.g., hyper-parameters) that works on most tasks may fail on some particular ones. The learning configuration is thus desired to be automatically adjustable. For example, for perturbation-based methods [17, 25], a small perturbation may under-exploit their benefits while a large one may result in collapse. Recent works [1, 29] apply a manually defined ramp-up period at the beginning of training. However, this cannot solve the issue when its maximum value is improper for the current task. In contrast, we propose to monitor the whole training process and adjust learning configuration adaptively. We use a diversity measure of model predictions on the target domain data to detect model collapse. Once it occurs, the model is restored to a previously achieved state and the configuration is reset. With this safe training strategy, our SSRT avoids significant performance deterioration on adaptation tasks with large domain gaps. The code is available at https://github.com/tsun/SSRT.

In summary, we make the following contributions:

- We develop a novel UDA solution SSRT, which adopts a vision transformer backbone for its strong transferable feature representation, and utilizes the predictions on perturbed target domain data for model refinement.
- We propose a safe training strategy to protect the learning process from collapse due to large domain gaps. It adaptively adjusts learning configuration during the training process with a diversity measure of model predictions on target domain data.
- SSRT is among the first to explore vision transformer for domain adaptation. Vision transformer-based UDA has shown promising results, especially on large-scale datasets like DomainNet.
- Extensive experiments are conducted on widely tested benchmarks. Our SSRT achieves the best performances, including 85.43% on Office-Home, 88.76% on VisDA-2017 and 45.2% on DomainNet.

2. Related Work

Unsupervised Domain Adaptation. There are several prevailing categories of UDA methods. Discrepancy-based methods minimize the distribution divergence between source and target domains with discrepancy measures [15, 28, 32]. Adversarial adaptation methods learn domain-invariant representations by playing a two-player min-max game between the feature extractor and a domain discriminator [4, 28, 31, 32]. Recently, many works exploit self-training for domain adaptation [16, 45, 46]. They generate pseudo labels for target domain data and take them as labeled data to refine the model.

Transformer in Vision. Vision Transformer (ViT) [3] is a pioneering work that applies a convolution-free transformer structure for image classification. Following that, many ViT variants have been proposed [7, 13, 30, 41]. Transformer has been applied successfully to various vision tasks including image classification [3, 30], object detection [2], semantic segmentation [27], etc.

The application of vision transformer in domain adaptation, however, is still very scarce. Notably, two concurrent explorations [39, 40] have been recently reported on arXiv. Specifically, CDTrans [39] is a pure transformer solution for UDA, and it applies cross attention on source-target image pairs. TVT [40] proposes a transferable multi-head self-attention module and combines it with adversarial adaptation. Our method is different in that it uses pairs of target domain data and their perturbed version to refine the model. This guarantees the same semantic class. Besides, we deliberately design the components of our model and the training strategy to avoid collapse on challenging tasks.

Consistency Regularization. Consistency regularization is an important technique in semi-supervised learning that achieves state-of-the-art results [25]. It leverages the idea that model predictions should be similar for semantically identical data. Some methods create perturbed inputs with adversarial training [17], while others use standard data augmentations [1, 25, 37]. These works mostly manipulate raw input images. In contrast, our study focuses on the latent token sequence representation of vision transformer.

3. Proposed Method

3.1. Problem Formulation

In Unsupervised Domain Adaptation, there is a source domain with labeled data \( \mathcal{D}_s = \{(x_i^s, y_i^s)\}_{i=1}^n \) from \( \mathcal{X} \times \mathcal{Y} \) and a target domain with unlabeled data \( \mathcal{D}_t = \{(x_i^t)\}_{i=1}^n \) from \( \mathcal{X} \), where \( \mathcal{X} \) is the input space and \( \mathcal{Y} \) is the label space. UDA aims to learn a classifier \( h = g \circ f \), where \( f(\cdot; \theta_f) : \mathcal{X} \rightarrow \mathcal{Z} \) denotes the feature extractor, \( g(\cdot; \theta_g) : \mathcal{Z} \rightarrow \mathcal{Y} \) denotes the class predictor, and \( \mathcal{Z} \) is the latent space. Adversarial adaptation learns domain-invariant feature via a bi-
nary domain discrimination $d(\cdot; \theta_d) : \mathcal{Z} \rightarrow [0, 1]$ that maps features to domain labels.

The objective is formulated as

$$
\min_{f,g} \max_{d} \mathcal{L} = \mathcal{L}_{CE} - \mathcal{L}_d + \beta \mathcal{L}_{tgt},
$$

where $\mathcal{L}_{CE}$ is the standard cross-entropy loss on source domain data, $\mathcal{L}_d$ is domain adversarial loss, defined as

$$
\mathcal{L}_d = -\mathbb{E}_{x \sim D_s}[\log d(f(x))] - \mathbb{E}_{x \sim D_t}[\log(1 - d(f(x)))],
$$

$\beta$ is a trade-off parameter, and $\mathcal{L}_{tgt}$ is a loss on target domain data. A common choice of $\mathcal{L}_{tgt}$ is the Mutual Information Maximization loss [6, 23]. In our method, we instantiate it as the self-refinement loss $\mathcal{L}_{SR}$, introduced in Sec. 3.4.

### 3.2. Method Framework

We aim to regularize the latent feature spaces of transformer backbone by refining the model with perturbed target domain data. Figure 1 illustrates the framework of our proposed SSRT. Only target domain data are shown here. The network consists of a vision transformer backbone and a classifier head. Domain discriminator is not plotted. For each target domain image, the Patch Embedding layer transforms it into a token sequence including a special class token and image tokens. Then the sequence is refined with a series of Transformer Blocks. The classifier head takes the class token and outputs label prediction. We randomly choose one transformer block and add a random offset to its input token sequence. Then the corresponding predicted class probabilities of original and perturbed versions are used for bi-directional self-refinement. To avoid noisy supervision, only reliable predictions are used via a Confidence Filter. To reduce the risk of model collapse, we use a safe training mechanism to learn the model.

### 3.3. Multi-layer Perturbation for Transformer

While many works manipulate the raw input images [1, 17, 25], it may be better to do that at hidden layers [34]. Vision transformer has some particular properties due to its special architecture. Since the Patch Embedding layer is merely a convolutional layer plus the position embedding, a linear operation on raw input can be shifted equivalently to the first transformer block. Besides, due to residual connections within transformer blocks, the token sequences at adjacent blocks are highly correlated. The best layer to add perturbation, however, varies across tasks. Empirically, perturbing relatively deep layers performs better but at a higher risk of model collapse. Therefore, we randomly choose one from multiple layers, which proves to be more robust than perturbing any single layer from them. In fact, it imposes a regularization on multiple layers simultaneously, making the learning process safer.

Given a target domain image $x$, let $b^l_x$ be its input token sequence of the $l$-th transformer block. $b^l_x$ can be viewed as a latent representation of $x$ in a hidden space. Since its dimension is high while the support of target domain data is limited in the space, it is inefficient to perturb $b^l_x$ arbitrarily. Instead, we utilize the token sequence $b^l_{xr}$ of another randomly chosen target domain image $x_r$ to add an offset. The perturbed token sequence of $b^l_x$ is obtained as

$$
\tilde{b}^l_x = b^l_x + \alpha [b^l_{xr} - b^l_x],
$$

where $\alpha$ is a scalar and $[\cdot]_\times$ means no gradient backpropagation. Note that although gradients cannot backpropagate through the offset, they can pass through $b^l_x$. The importance of this is elaborated in the following section.

In addition to the manually injected perturbation, the Dropout layer in the classifier head also works randomly for the two branches. This creates another source of discrepancy for the self-refinement loss.
3.4. Bi-directional Self-Refinement

Now we are ready to define the loss function used for self-refinement. Let \( p_t \) and \( \tilde{p}_s \) be the predicted probability vectors corresponding to \( b_t \) and \( b_s \), respectively. To measure their distance, KL divergence is commonly used:

\[
D_{\text{KL}}(p_t\|p_s) = \sum_i p_t[i] \log \frac{p_t[i]}{p_s[i]},
\]

where \( p_t \) is the teacher probability (a.k.a. target probability) and \( p_s \) is the student probability. Note that KL divergence is asymmetric in \( p_t \) and \( p_s \). While it is natural to take \( p_s \) as the teacher probability since it corresponds to the original data, we find the reverse also works. Moreover, as shown in Sec. 4.3, it is more robust to combine them together. Our bi-directional self-refinement loss is defined as

\[
\mathcal{L}_{SR} = E_{B_i \sim D_i} \left\{ \omega E_{x \sim F(B_i; p)} D_{KL}(p_x\|\tilde{p}_x) \right\} + (1 - \omega) E_{x \sim F(B_i; \tilde{p})} D_{KL}(p_x\|p_t),
\]

where \( \omega \) is a random variable drawn from a Bernoulli distribution \( B(0.5) \), \( F \) is a Confidence Filter defined as

\[
F[D; p] = \{ x \in D | \text{max} (p_x) > \epsilon \},
\]

and \( \epsilon \) is a predefined threshold. \( \mathcal{L}_{SR} \) refines the model with confident predictions and regularizes it to predict smoothly in the latent feature spaces.

Typically, the loss gradient is only back-propagated through the student probability (i.e., \( p_s \) in Eq. 3) [1, 17, 18]. We find, however, it is better to back-propagate gradient through both teacher and student probabilities in our framework. Recall that \( \partial \mathcal{L}_{SR} / \partial \tilde{b}_s \) is propagated to \( \tilde{b}_s \) identically in Eq. 2. Each model parameter is therefore updated based on the joint effects from \( p_t \) and \( \tilde{p}_s \). This avoids excessively large gradients from any single probability. We observe degraded performance when either the gradients of teacher probabilities in KL divergence or that of \( \tilde{b}_s \) are blocked.

3.5. Safe Training via Adaptive Adjustment

In the proposed self-refinement strategy, setting a proper value of the perturbation scalar \( \alpha \) and the self-refinement loss weight \( \beta \) is critical. Excessively large perturbations lead to a collapse of the predicted class distribution, while a small one may under-exploit its benefit. Since the target domain is fully unlabeled and domain adaptation tasks vary widely even for the same dataset, it is desired to adjust these values adaptively. Some works [1, 29] apply a ramp-up period at the beginning of training. While this alleviates the tendency to collapse during this period, it cannot solve the issue when the maximum value is improper for current adaptation tasks.

**Algorithm 1 Safe Training Mechanism.**

**Initialization:** \( \text{last\_restore} = 0 \); save snapshot of \( M \)

1: \( \text{procedure SafeTraining}(M, div, T, iter) \)
2: \( \text{for } l = 1 \text{ to } L \) do \( \triangleright \) check at multi-scales
3: \( \text{divs} = \text{div}(\text{iter} - T, \ldots, \text{iter}) \) \( \triangleright \) get diversity
4: \( \text{divs} = \text{split}(	ext{divs}, 2^k) \) \( \triangleright \) to even sub-intervals
5: \( \text{for } i = 0 \text{ to } \text{len(divs)} - 1 \) do
6: \( \text{if } \text{avg(divs[i+1])} < \text{avg(divs[i])} - 1 \text{ then} \)
7: \( \text{return True} \) \( \triangleright \) significant dropping
8: \( \text{end if} \)
9: \( \text{end for} \)
10: \( \text{end for} \)
11: \( \text{return False} \)
12: \( \text{end procedure} \)
13:

14: \( \text{procedure SafeTraining}(M, div, T, iter) \)
15: \( \text{if } \text{iter} \% T == 0 \text{ and } \text{iter} >= T \text{ then} \)
16: \( \text{if } \text{CheckDivDrop(div, T, iter)} \text{ then} \)
17: \( \text{Restore \( M \) to last snapshot, } t_r = \text{iter} \)
18: \( \text{if } \text{iter} - \text{last\_restore} \leq T_r \text{ then} \)
19: \( T_r = t_r \times 2 \) \( \triangleright \) avoid oscillation
20: \( \text{end if} \)
21: \( \text{last\_restore} = \text{iter} \)
22: \( \text{end if} \)
23: \( \text{Save snapshot of } M \)
24: \( \text{end if} \)
25: \( \text{return } M, T_r, t_r \)
26: \( \text{end procedure} \)

**Algorithm 2 SSRT algorithm.**

**Input:** Model \( M \), source data \( D_s \), target data \( D_t \), confidence threshold \( \epsilon \), self-refinement loss weight \( \beta \), perturbation scalar \( \alpha \), Safe Training parameters \( T \) and \( L \), diversity measure \( \text{div}() \).

**Initialization:** \( T_r = T, t_r = 0 \)

1: \( \text{for } \text{iter} = 0 \text{ to } \text{max\_iter} \text{ do} \)
2: \( \text{Sample a batch from source data and target data} \)
3: \( \text{Obtain } r \text{ via Eq. 6, } \alpha_r = r\alpha, \beta_r = r\beta \)
4: \( \text{Randomly choose } l \in \{0, 4, 8\}, \text{ add perturbation} \)
5: \( \text{via Eq. 2 using } \alpha_r, \text{ obtain } L_{SR} \text{ via Eq. 4} \)
6: \( \text{Update model parameters via Eq. 1 using } \beta_r \)
7: \( \text{return } M, T_r, t_r \leftarrow \text{SafeTraining}(M, \text{div}, T, L, \text{iter}) \)

We propose a Safe Training mechanism. The observation is that whenever the model begins to collapse, the diversity of model predictions will decrease simultaneously. Our goal is to detect such events while monitoring the training process. Once it occurs, the learning configuration is reset and meanwhile the model is restored to a previously achieved state. Specifically, an adaptive scalar \( r \in [0, 1] \) is
Table 1. Accuracies (%) on Office-Home. *CDTrans uses DeiT-base backbone. *TVT uses ViT-base backbone. “-S/B” indicates ViT-small/base backbones, respectively.

<table>
<thead>
<tr>
<th>Method</th>
<th>Ar→Cl</th>
<th>Ar→Pr</th>
<th>Ar→Rw</th>
<th>Cl→Ar</th>
<th>Cl→Pr</th>
<th>Cl→Rw</th>
<th>Pr→Ar</th>
<th>Pr→Cl</th>
<th>Pr→Rw</th>
<th>Rw→Ar</th>
<th>Rw→Cl</th>
<th>Rw→Pr</th>
<th>Avg.</th>
</tr>
</thead>
<tbody>
<tr>
<td>ResNet-50 [8]</td>
<td>34.9</td>
<td>50.0</td>
<td>58.0</td>
<td>37.4</td>
<td>41.9</td>
<td>46.2</td>
<td>38.5</td>
<td>31.2</td>
<td>60.4</td>
<td>53.9</td>
<td>41.2</td>
<td>59.9</td>
<td>46.1</td>
</tr>
<tr>
<td>CDAN+E [14]</td>
<td>50.7</td>
<td>70.6</td>
<td>76.0</td>
<td>57.6</td>
<td>70.0</td>
<td>70.0</td>
<td>57.4</td>
<td>50.9</td>
<td>77.3</td>
<td>70.9</td>
<td>56.7</td>
<td>81.6</td>
<td>65.8</td>
</tr>
<tr>
<td>SAFN [36]</td>
<td>52.0</td>
<td>71.7</td>
<td>76.3</td>
<td>64.2</td>
<td>69.9</td>
<td>71.9</td>
<td>63.7</td>
<td>51.4</td>
<td>77.1</td>
<td>70.9</td>
<td>57.1</td>
<td>81.5</td>
<td>67.3</td>
</tr>
<tr>
<td>CDAN-TN [35]</td>
<td>50.2</td>
<td>71.4</td>
<td>77.4</td>
<td>59.3</td>
<td>72.7</td>
<td>73.1</td>
<td>61.0</td>
<td>53.1</td>
<td>79.5</td>
<td>71.9</td>
<td>59.0</td>
<td>82.9</td>
<td>67.6</td>
</tr>
<tr>
<td>SHOT [12]</td>
<td>57.1</td>
<td>78.1</td>
<td>81.5</td>
<td>68.0</td>
<td>78.2</td>
<td>78.1</td>
<td>67.4</td>
<td>54.9</td>
<td>82.2</td>
<td>73.3</td>
<td>58.8</td>
<td>84.3</td>
<td>71.8</td>
</tr>
<tr>
<td>DCAN+SCDA [10]</td>
<td>60.7</td>
<td>76.4</td>
<td>82.8</td>
<td>69.8</td>
<td>77.5</td>
<td>78.4</td>
<td>68.9</td>
<td>59.0</td>
<td>82.7</td>
<td>74.9</td>
<td>61.8</td>
<td>84.5</td>
<td>73.1</td>
</tr>
<tr>
<td>CDTrans* [30]</td>
<td>68.8</td>
<td>85.0</td>
<td>86.9</td>
<td>81.5</td>
<td>87.1</td>
<td>87.3</td>
<td>79.6</td>
<td>63.3</td>
<td>88.2</td>
<td>82.0</td>
<td>66.0</td>
<td>90.6</td>
<td>80.5</td>
</tr>
<tr>
<td>TVT* [40]</td>
<td>74.9</td>
<td>86.8</td>
<td>89.7</td>
<td>82.8</td>
<td>87.9</td>
<td>88.2</td>
<td>79.8</td>
<td>71.9</td>
<td>90.1</td>
<td>85.4</td>
<td>76.2</td>
<td>90.5</td>
<td>83.56</td>
</tr>
</tbody>
</table>

ViT-S [3] 74.01 76.98 83.54 69.84 77.11 80.42 68.15 44.08 82.86 74.78 47.97 84.66
Baseline-S 59.59 80.11 84.67 79.84 84.19 78.41 66.78 50.90 87.22 79.56 53.79 88.80
SSRT-S (ours) 67.03 84.21 88.32 80.59 84.28 87.58 66.03 53.17 82.27 71.96 59.0 82.9
SAFN [38] 52.0 71.7 76.3 64.2 69.9 71.9 63.7 51.4 77.1 70.9 57.1 81.5
CDAN+E [14] 50.7 70.6 76.0 59.3 72.7 73.1 61.0 53.1 79.5 71.9 59.0 82.9
ResNet-50 [8] 34.9 50.0 58.0 37.4 41.9 46.2 38.5 31.2 60.4 53.9 41.2 59.9 46.1

Table 2. Accuracy (%) on DomainNet clp→qdr and qdr→clp. (Left) Plots of the diversity of model predictions on target domain data and the adaptive scalar \( r \). For better visualization, both original values (light color) and smoothed values (dark color) of diversity are shown. (Right) Plots of comparison test accuracies on target domain data.


div \( r; B_t \) = unique_labels(h(\( B_t \))).

To detect diversity dropping, we split the interval into sub-intervals and check whether the average diversity value drops across each sub-interval. We implement this at multiscales to improve the sensitivity of detection. Every consecutive sub-intervals of \( T/2^1, \cdots, T/2^L \) steps are checked for a given integer \( L \). Details are listed in Alg. 1 and Alg. 2.
4. Experiments

We evaluate our method on four popular UDA benchmarks. Office-31 [22] contains 4,652 images of 31 classes from three domains: Amazon (A), DSLR (D) and Webcam (W). Office-Home [33] consists of 15,500 images of 65 classes from four domains: Artistic (A), Clip Art (C), Product (Pr), and Real-world (Rw) images. VisDA-2017 [20] is a Synthetic-to-Real dataset, with about 0.2 million images in 12 classes. DomainNet [19] is the largest DA dataset containing about 0.6 million images of 345 classes in 6 domains: Clipart (clp), Infograph (inf), Painting (pnt), Quickdraw (qdr), Real (rel), Sketch (skt).

We use the ViT-base and ViT-small with 16×16 patch size [3, 26], pre-trained on ImageNet [21], as the vision transformer backbones. For all tasks, we use an identical set of hyper-parameters ($\alpha = 0.3, \beta = 0.2, \epsilon = 0.4, T = 1000, L = 4$). Ablation studies on them are provided in Sec. 4.6. More details can be found in the supplementary material.

Table 3. Accuracies (%) on VisDA-2017.

<table>
<thead>
<tr>
<th>Method</th>
<th>plane</th>
<th>bicyc</th>
<th>bus</th>
<th>car</th>
<th>horse</th>
<th>knife</th>
<th>mcyc</th>
<th>person</th>
<th>plant</th>
<th>sbkbr</th>
<th>train</th>
<th>track</th>
</tr>
</thead>
<tbody>
<tr>
<td>ResNet-101 [8]</td>
<td>51.5</td>
<td>53.3</td>
<td>61.9</td>
<td>59.1</td>
<td>80.6</td>
<td>17.9</td>
<td>79.7</td>
<td>31.2</td>
<td>81.0</td>
<td>26.5</td>
<td>73.5</td>
<td>8.5</td>
</tr>
<tr>
<td>DANN [4]</td>
<td>81.9</td>
<td>77.7</td>
<td>82.8</td>
<td>44.3</td>
<td>81.2</td>
<td>29.5</td>
<td>65.1</td>
<td>28.6</td>
<td>51.9</td>
<td>54.6</td>
<td>82.8</td>
<td>7.8</td>
</tr>
<tr>
<td>CDAN [14]</td>
<td>85.2</td>
<td>66.9</td>
<td>83.0</td>
<td>50.8</td>
<td>84.2</td>
<td>74.9</td>
<td>88.1</td>
<td>74.5</td>
<td>83.4</td>
<td>76.0</td>
<td>81.9</td>
<td>38.0</td>
</tr>
<tr>
<td>SAFN [38]</td>
<td>93.6</td>
<td>61.3</td>
<td>84.1</td>
<td>70.6</td>
<td>94.1</td>
<td>79.0</td>
<td>91.8</td>
<td>79.6</td>
<td>89.9</td>
<td>55.6</td>
<td>89.0</td>
<td>24.4</td>
</tr>
<tr>
<td>SWD [9]</td>
<td>90.8</td>
<td>82.5</td>
<td>81.7</td>
<td>70.5</td>
<td>91.7</td>
<td>69.5</td>
<td>86.3</td>
<td>77.5</td>
<td>87.4</td>
<td>63.6</td>
<td>85.6</td>
<td>29.2</td>
</tr>
<tr>
<td>SHOT [12]</td>
<td>94.3</td>
<td>88.5</td>
<td>80.1</td>
<td>57.3</td>
<td>93.1</td>
<td>94.9</td>
<td>80.7</td>
<td>80.3</td>
<td>91.5</td>
<td>89.1</td>
<td>86.3</td>
<td>58.2</td>
</tr>
<tr>
<td>CDTrans* [39]</td>
<td>97.1</td>
<td>90.5</td>
<td>82.4</td>
<td>77.5</td>
<td>96.6</td>
<td>96.1</td>
<td>93.6</td>
<td>88.6</td>
<td>97.9</td>
<td>86.9</td>
<td>90.3</td>
<td>62.8</td>
</tr>
<tr>
<td>TTVT* [40]</td>
<td>92.9</td>
<td>85.58</td>
<td>77.1</td>
<td>60.48</td>
<td>93.60</td>
<td>98.17</td>
<td>89.35</td>
<td>76.40</td>
<td>93.56</td>
<td>92.02</td>
<td>91.69</td>
<td>55.73</td>
</tr>
</tbody>
</table>

Our comparison methods include DANN [4], CDAN [14], CDAN+E [14], SAFN [38], SAFN+ENT [38], CDAN+TN [35], SHOT [12], DCAN+SCDA [10], MDD+SCDA [10], SWD [9], MIMTFEL [5], TVT [40] and CDTrans [39]. “Baseline” is ViT with adversarial adaptation (see Sec. 3.1). We also include a combination with Mutual Information (MI) loss [6, 23] in comparison.

4.1. Results on Benchmarks

Tables 1–4 present evaluation results on four benchmarks. We use “-SB” to indicate results using ViT-small base backbones, respectively. For Office-Home and Office-31, CNN-based methods use ResNet-50 as their backbones; whereas for DomainNet and VisDA they use ResNet-101. Generally, the transformer-based results are much better. This is attributed to its strong transferable feature representations. ViT-base is better than ViT-small, due to higher model complexity. Apparently, Baselines improve over source-only training. Integrating Mutual Information
Table 4. Accuracies (%) on Office-31.

<table>
<thead>
<tr>
<th>Method</th>
<th>A→W</th>
<th>D→W</th>
<th>W→D</th>
<th>A→D</th>
<th>D→A</th>
<th>W→A</th>
<th>Avg.</th>
</tr>
</thead>
<tbody>
<tr>
<td>ResNet-50</td>
<td>68.4</td>
<td>96.7</td>
<td>99.3</td>
<td>68.9</td>
<td>62.5</td>
<td>60.7</td>
<td>76.1</td>
</tr>
<tr>
<td>DANN [4]</td>
<td>82.0</td>
<td>96.9</td>
<td>99.1</td>
<td>79.7</td>
<td>68.2</td>
<td>67.4</td>
<td>82.2</td>
</tr>
<tr>
<td>SAFN+ENT [38]</td>
<td>90.1</td>
<td>98.6</td>
<td>99.8</td>
<td>90.7</td>
<td>73.0</td>
<td>70.2</td>
<td>87.1</td>
</tr>
<tr>
<td>CDAN+TN [35]</td>
<td>95.7</td>
<td>98.7</td>
<td>100.</td>
<td>94.0</td>
<td>73.4</td>
<td>74.2</td>
<td>89.3</td>
</tr>
<tr>
<td>SHOT [12]</td>
<td>90.1</td>
<td>98.4</td>
<td>99.9</td>
<td>94.0</td>
<td>74.7</td>
<td>74.3</td>
<td>88.6</td>
</tr>
<tr>
<td>MDD+SCDA [10]</td>
<td>95.3</td>
<td>99.0</td>
<td>100.</td>
<td>95.4</td>
<td>72.7</td>
<td>75.9</td>
<td>90.5</td>
</tr>
<tr>
<td>CDTrans* [39]</td>
<td>96.7</td>
<td>99.0</td>
<td>100.</td>
<td>97.0</td>
<td>81.1</td>
<td>81.9</td>
<td>92.6</td>
</tr>
<tr>
<td>TVT* [40]</td>
<td>96.4</td>
<td>99.4</td>
<td>100.</td>
<td>96.4</td>
<td>84.9</td>
<td>86.1</td>
<td>93.8</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Method</th>
<th>OH</th>
<th>DN</th>
<th>clp†</th>
<th>inf†</th>
<th>pnt†</th>
<th>qdr†</th>
<th>rel†</th>
<th>skl†</th>
</tr>
</thead>
<tbody>
<tr>
<td>Baseline-B</td>
<td>81.1</td>
<td>38.5</td>
<td>50.6</td>
<td>25.6</td>
<td>44.9</td>
<td>11.6</td>
<td>57.0</td>
<td>41.5</td>
</tr>
<tr>
<td>SSRT-B (raw)</td>
<td>85.0</td>
<td>44.2</td>
<td>58.6</td>
<td>26.7</td>
<td>51.7</td>
<td>13.7</td>
<td>63.9</td>
<td>50.8</td>
</tr>
<tr>
<td>SSRT-B</td>
<td>85.4</td>
<td>45.2</td>
<td>60.0</td>
<td>28.2</td>
<td>53.3</td>
<td>13.7</td>
<td>65.3</td>
<td>50.4</td>
</tr>
</tbody>
</table>

(MI) loss further improves. Compared with other methods, SSRT-B performs the best on Office-Home, DomainNet and VisDA. It improves 4.38% on Office-Home, 3.53% on VisDA-2017 and 6.7% on DomainNet over Baseline-B despite that Baseline-B is already very strong. In particular, on the challenging DomainNet dataset, SSRT-B achieves an impressive 45.2% average accuracy. It is worth mentioning that in DomainNet some domains have large gaps from the others, such as inf and qdr. Transferring among these domains and others is very difficult. It is thus desired to transfer safely and not deteriorate the performance significantly. Looking at tasks with qdr being target domain, SSRT-B obtains 29.3% average accuracy, while many other methods perform poorly. We illustrate the effects of some important components that contribute to our excellent performance in the following sections.

4.2. Effects of Multi-layer Perturbation

Table 5 verifies that applying perturbation to the latent token sequences performs better than to the raw input images on Office-Home (OH) and DomainNet (DN). Fig. 5a compares performances when adding the same amount of perturbation to each layer while not using safe training. As can be seen, the best layer to apply perturbation varies across tasks. Besides, a layer that works for one task may fail on others. In our experiments, we uniformly choose one layer from \{0,4,8\}. As a comparison, perturbing any single layer from it decreases the average accuracy on DomainNet by -1.0%, -1.5% and -1.5%, respectively.

Table 5. Accuracies (%) compared with perturbing raw inputs. X† means averaged over all 5 tasks with X being the target domain.

<table>
<thead>
<tr>
<th>Method</th>
<th>OH</th>
<th>DN</th>
<th>clp†</th>
<th>inf†</th>
<th>pnt†</th>
<th>qdr†</th>
<th>rel†</th>
<th>skl†</th>
</tr>
</thead>
<tbody>
<tr>
<td>Baseline-B</td>
<td>81.1</td>
<td>38.9</td>
<td>50.7</td>
<td>25.5</td>
<td>46.1</td>
<td>11.9</td>
<td>57.4</td>
<td>42.0</td>
</tr>
<tr>
<td>ω = 0</td>
<td>85.5</td>
<td>41.1</td>
<td>57.3</td>
<td>22.0</td>
<td>52.2</td>
<td>1.8</td>
<td>63.4</td>
<td>49.9</td>
</tr>
<tr>
<td>ω = 1</td>
<td>85.7</td>
<td>40.1</td>
<td>56.6</td>
<td>23.4</td>
<td>48.1</td>
<td>0.3</td>
<td>63.3</td>
<td>49.0</td>
</tr>
<tr>
<td>ω ~ B(0.5)</td>
<td>85.4</td>
<td>41.8</td>
<td>57.0</td>
<td>26.6</td>
<td>53.0</td>
<td>1.8</td>
<td>63.2</td>
<td>49.5</td>
</tr>
<tr>
<td>ω ~ B(0.5)†</td>
<td>85.4</td>
<td>43.4</td>
<td>57.0</td>
<td>28.2</td>
<td>51.8</td>
<td>13.0</td>
<td>62.9</td>
<td>47.4</td>
</tr>
</tbody>
</table>

4.3. Effects of Bi-directional Self-Refinement

Our method adopts bi-directional supervision for self-refinement in Eq. 4. The main consideration is to improve method’s safeness. Figure 3 compares with uni-directional self-refinement by fixing ω to be 0 or 1. In the upper two figures, their performance drops for relatively large confidence threshold ε. In the lower two figures, model collapse occurs after training for some steps. In contrast, bi-directional self-refinement is more robust as it combines the two losses, thus reduces the negative effect of either one. Table 6 presents some quantitative results. On Office-Home, all losses perform similarly well. On DomainNet, bi-directional self-refinement works better. However, they all fail on challenging tasks when target domain is qdr. This is solved with Safe Training.

Another important issue is when to back-propagate gradients. Table 7 shows that the performance degrades when either the gradient for \( w_l \) in Eq. 2 or the teacher probability of KL divergence in Eq. 4 are blocked. An interesting finding is that the bi-directional self-refinement appears to be more robust even when the gradients are blocked. We believe this is because the two losses are complementary.
4.4. Effects of Safe Training

As observed previously, the vanilla training strategy may fail on some tasks. The reason is that the predicted class distribution on target domain data collapses due to excessive perturbation or too large loss weight, even if they work well on other tasks. Safe Training adjusts their values adaptively to avoid such situation. Figure 2 presents detailed training histories on two representative tasks to show how it works. For qdr→clp, the adaptive scalar $r$ quickly converges to 1.0 and the diversity stabilizes to a relatively high value. Training model with or without Safe Training performs similarly. For clp→qdr, diversity drops after some steps, and $r$ resets to smaller values. A clear correlation between diversity and accuracy can be observed. For example, at step of 10k, the accuracy drops abruptly and diversity drops concurrently. Without Safe Training, model collapses after about 10k iterations. With Safe Training, the model trains normally and surpasses the baseline finally. It should be noted that model collapse mainly affects target domain data. For clp→qdr without safe training, the final accuracy on source domain is 96.9% while that on target domain is only 0.3%.

4.5. Visualization of Perturbation

To visualize the perturbed version of a target domain image $x$, we initialize a trainable variable $x_{vis}$ as $x$, and optimize $x_{vis}$ to minimize $\|b_{x_{vis}}^{p} - b_{x_{vis}}^{\tilde{x}}\|_2^2$, where $b_{x_{vis}}^{p}$ is the perturbed token sequence of $x$ and $b_{x_{vis}}^{\tilde{x}}$ is the corresponding token sequence of $x_{vis}$. Then $x_{vis}$ gives us an idea on how the perturbation in the latent space reflects on the raw input images. Figure 4 visualizes perturbed version of two images when adding perturbation to different transformer blocks. For shallow layers, an effect of blending with the other image can be observed. However, for deep layers, this effect is less noticeable due to highly non-linear transformation of the network. This also indicates the complementary in using multi-layer perturbation.

4.6. Ablation Studies

Figure 5 presents ablation studies on hyper-parameters. Figure 5a plots results of perturbing different layers. Figure 5b plots Safe Training with different parameters. $T$ and $L$ affects its granularity. A smaller $T$ implies more quick response. A larger $L$ increases sensitivity but at the risk of more false-positive detections. Many combinations of $T$ and $L$ work well in our method. Figure 5c and 5d plots accuracy curves vs. the perturbation scalar $\alpha$ and the self-refinement loss weight $\beta$. Even for obviously unreasonable values like $\alpha = 0.5$, Safe Training can still adjust them adaptively to avoid model collapse. When $\alpha = 0$, our method still has some gain over baseline. This is due to random dropout operations in the classifier head.

5. Conclusion

In this paper, we propose a novel UDA method named SSRT. It leverages a vision transformer backbone, and uses perturbed target domain data to refine the model. A safe training strategy is developed to avoid model collapse. Experiments on benchmarks show its best performance.

**Limitation.** Although we advance the average accuracy on DomainNet to 45.2%, it is far from saturated. One way is to combine multiple source domains. Another way is to incorporate some meta knowledge about target domains. We plan to extend our study in these directions in the future.
References


[10] Xiaohua Zhai, Thomas Unterthiner, Mostafa Dehghani, Matthias Minderer, Georg Heigold, Sylvain Gelly, et al. An image is worth 16x16 words: Transformers for image recognition at scale. ICLR, 2021. 1, 2, 5, 6, 7


