1. Teacher-based Virtual Adversarial Training (T-VAT)

Virtual adversarial training (VAT) [1] aims to produce a gradient-oriented perturbation that maximises the divergence between the prediction distributions of the original and perturbed inputs. After maximising the divergence between the predictions of the original and its perturbed version, the classification boundary will move towards the classification boundary, producing a more challenging classification sample that can improve training generalization. During training, the teachers ensemble predictions yield more accurate performance than the student predictions, as shown in Fig. 3-(b). This demonstrates that the teachers ensemble results follow more closely the true classification boundary than the student predictions. Therefore, the adversarial samples provided by the teachers (i.e., T-VAT) can be more “accurate” to alter the student model’s gradient than the adversarial samples provided by the student.

1.1. Implementation Details

Our T-VAT results are produced based on the embedding produced by the student encoder, which is $z^s = h_{\theta_s}^s(x)$. We first sample the noise $r$ from a Gaussian distribution, which has the same dimensionality of $z^s$. Then, we compute the gradient of the KL divergence, as in

$$g = \nabla d\left(0.5 \times g_{\theta_1}^s(z^s) + 0.5 \times g_{\theta_2}^s(z^s), 0.5 \times g_{\theta_1}^s(z^s + r) + 0.5 \times g_{\theta_2}^s(z^s + r)\right).$$

(1)

Lastly, we obtain the teacher-gradient adversarial perturbation $r_{adv}$, which is normalised as follows

$$r_{adv} = \epsilon \frac{g}{\|g\|},$$

(2)

where we use $\epsilon = 2$ for all experiments. We inject the perturbation $r_{adv}$ into the original embedding with $z^* = z^s + r_{adv}$.

1.2. T-SNE Visualisation

In Fig. 2, we visualise the perturbation impact using T-SNE. We randomly sample 25,000 correctly predicted pixels based on 5 different classes (each class represented by a different colour) in (a). Then we apply the VAT noise using the student model in (b) and our T-VAT noise in (c) to observe the perturbations of the original results (from correct to incorrect). T-VAT demonstrates more challenging predictions compared with the VAT (with more incorrect predictions), which shows better perturbation efficiency.

2. Ramp-up Function

Due to the prediction instability of the unlabelled data in the early training stages, we introduce a ramp-up weight to be applied to the unsupervised loss [2]. In Fig. 3-(a), we illustrate our Gaussian ramp-up function applied for the weight $\beta$ in Eq. (1) of the main paper. The final weight is
Figure 2. T-SNE visualization. We visualise the incorrect predictions after the feature perturbation, shown with red stars. More incorrect predictions demonstrates more effective perturbations.

1.5 and the ramp-up length of 12 is used for all the experiments.

Figure 3. (a) Ramp-up function for $\beta$ in Eq. (1). This diagram shows the ramp-up curve that we use to weight the unsupervised loss as a function of the iterations. (b) mIoU of the Teachers Ensemble and Student on the validation set during the training process.

3. Single teacher Inference

After the training, two teachers will converge into same local minimal and the single teacher’s performance will be similar with the ensemble result.

References

