Appendix

In the appendix, we first visualize more adversarial examples generated by various attacks. Then we provide more results for our methods integrated with DIM, TIM or SIM on the other three normally trained models, \( i.e. \) Inc-v4, IncRes-v2 and Res-101.

A. Visualizations on Adversarial Examples

We visualize eight randomly selected benign images and their corresponding adversarial examples crafted by various attacks in Figure 6. The adversarial examples are crafted on Inc-v3 model, using MI-FGSM, NI-FGSM, VMI-FGSM and VNI-FGSM, respectively. It can be observed that these crafted adversarial examples are human-imperceptible.

B. More Attacks with Input Transformations

Here we further provide the attack results of our methods with input transformations on the other three models, \( i.e. \) Inc-v4, IncRes-v2 and Res-101. The results are depicted in Figure 7 for DIM, Figure 8 for TIM and Figure 9 for SIM. Our methods can improve the transferability of these input transformations remarkably, especially against the adversarially trained models. The results are consistent with the results of adversarial examples crafted on Inc-v3 model.
Figure 6: Adversarial examples generated by MI-FGSM [6], NI-FGSM [18], the proposed VMI-FGSM and VNI-FGSM on Inc-v3 model [30] with the maximum perturbation of $\epsilon = 16$. 
Figure 7: The success rates (%) on seven models in the single model setting by various gradient-based iterative attacks enhanced by DIM.

Figure 8: The success rates (%) on seven models in the single model setting by various gradient-based iterative attacks enhanced by TIM.

Figure 9: The success rates (%) on seven models in the single model setting by various gradient-based iterative attacks enhanced by SIM.