Supplementary Materials for "Frequency-Aware GAN for Imperceptible Transfer Attack on 3D Point Clouds"

Anonymous Authors

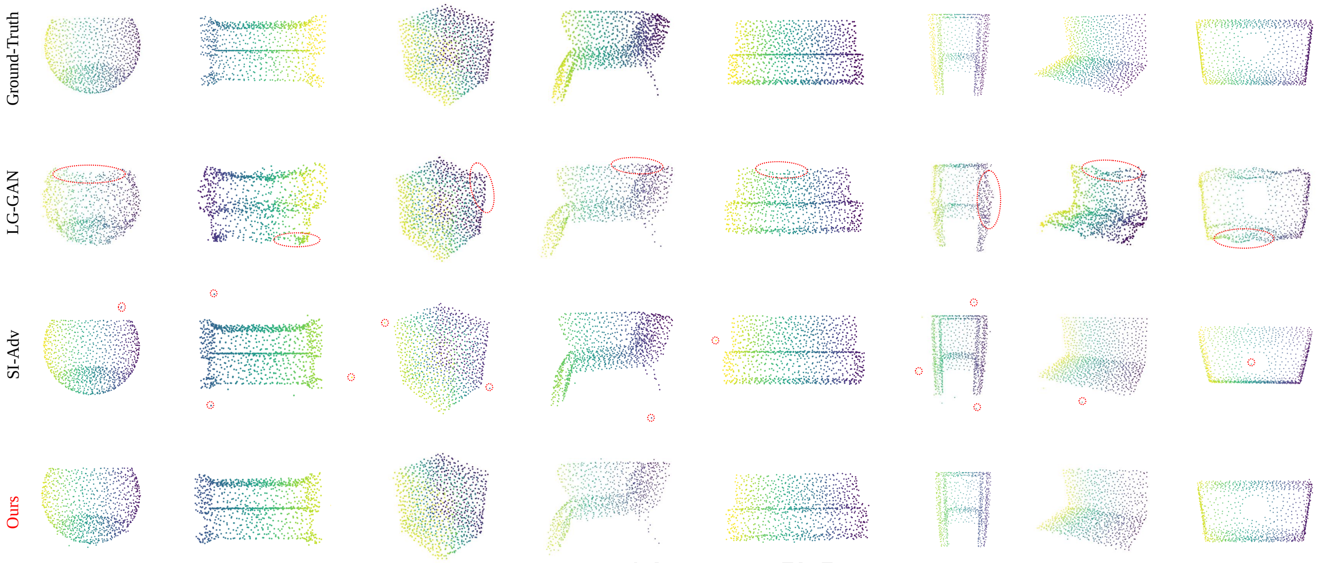


Figure 1: More visualization results of adversarial samples.

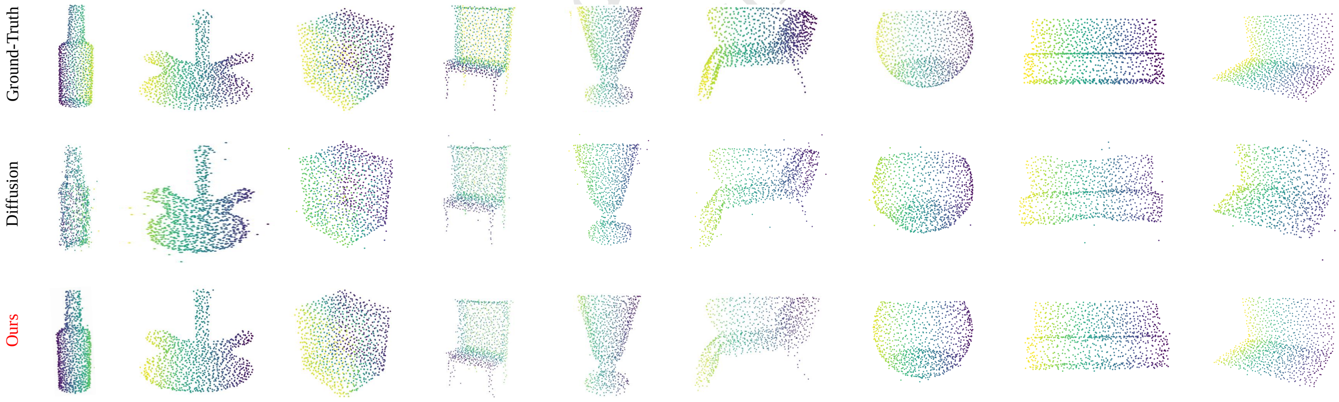


Figure 2: Visualization results of diffusion baseline model and our method.

1 MORE VISUALIZATION RESULTS

More visualizations of adversarial samples from existing attack methods are shown in Figure 1. Compared to LG-GAN, our adversarial samples have less shape distortion. Compared to SI-Adv, our method mitigates the outlier points problem. Moreover, we provide visualizations of diffusion baseline model in Figure 2. Compared to diffusion, our method produces adversarial samples with less deformation and noise. This is because we extract the spectral frequencies of the point cloud to explicitly explore and capture its geometric structure. Meanwhile, the high-frequency components of spectral frequencies can encode fine-grained details. By combining both spatial and frequency features in generator with skip connections of the high-frequency components, our adversarial samples are more imperceptible than others.

2 MORE ABLATION RESULTS

2.1 The influence of frequency features and skip connections in frequency-aware generator

The results presented in the main paper are obtained using PointNet as the experimental object. To further verify the imperceptibility

Table 1: Effects of GFT and IGFT ablation in the frequency-aware generator on imperceptibility on PointNet++.

GFT	IGFT		D_h	D_c	D_{norm}
	high-frequency	low-frequency			
✓	✓	×	**0.0190**	**0.0006**	**0.9757**
✓	×	✓	0.0210	0.0009	1.2582
✓	✓	✓	0.0204	0.0010	1.2090
✓	×	×	0.0216	0.0008	1.1351
×	×	×	0.0276	0.0013	1.4702

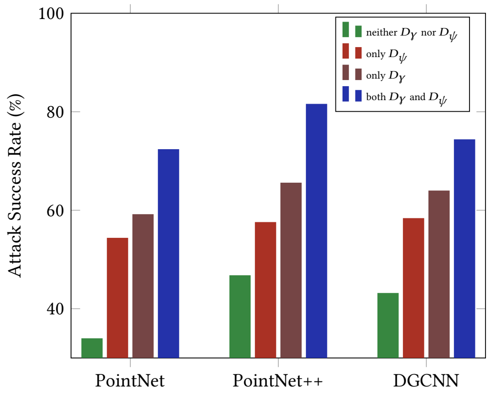


Figure 3: Effects of each component in the dual discriminator on transferability. The white-box target model is PCT and the x-axis is the black-box victim models.

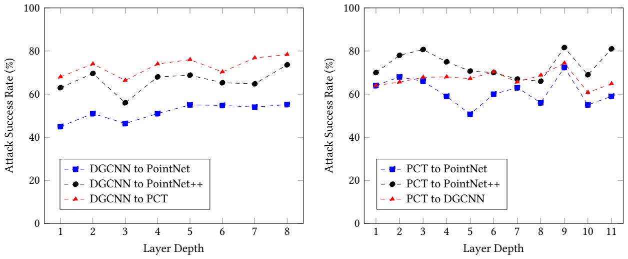
of our method, we have conducted ablation experiments using PointNet++ as shown in Table 1. By comparing the first and fifth rows, we observe that the use of frequency features significantly reduces three metrics. By comparing the first, second, third, and fourth rows, we also see that retaining high-frequency components has the greatest effect on improving point cloud quality. These quantitative results indicate that the frequency features and high-frequency skip connections play a predominant role in our model.

2.2 The influence of dual discriminator

Besides the experiments on PointNet presented in the main paper, we also conduct ablations on PCT to test the transferability. As shown in Figure 3, combining frequency-aware discriminator with feature discriminator greatly improves the success rate of attacking other models by enriching the feature types in spectral frequency and destroying the similarity of intermediate layer features. This is because the adversarial samples produced by the generator after adversarial learning can fool the powerful dual discriminator, and thus are also capable of fooling other unknown models.

2.3 The influence of intermediate layer selection in feature discriminator

In addition to the experiments on PointNet and PointNet++ presented in the main paper, Figure 4 shows the effects of selecting intermediate layer features on transferability when the feature discriminator is configured with the DGCNN and PCT, respectively. By using the 8th layer of DGCNN and the 9th layer of PCT, our method achieves the best attack success rates when the adversarial samples are transferred to attack three other models. Therefore, we select the optimal layer for feature extraction to optimize the generator by maximizing the feature distance.

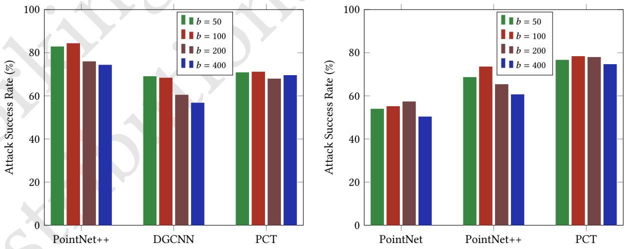


Feature Discriminator: DGCNN Feature Discriminator: PCT

Figure 4: Effects of feature layer selection on transferability.

Table 2: Sensitivity on hyper-parameter b on DGCNN.

Variant Metric	$b = 50$	$b = 100$	$b = 200$	$b = 400$
D_h	0.0185	**0.0177**	0.0181	0.0187
D_c	0.0006	**0.0005**	0.0006	**0.0005**
D_{norm}	0.9957	**0.9561**	0.9730	0.9631



White-box target model: PointNet White-box target model: DGCNN

Figure 5: Effects of b in the dual discriminator on transferability. The x-axis is the black-box victim models.

2.4 Sensitivity on hyper-parameter b

The b serves as the dividing band of spectral frequency. It is used in the frequency-generator to improve imperceptibility and in the dual-discriminator to improve transferability. Besides the experiments on PointNet presented in the main paper, we conduct ablation experiments on DGCNN. In summary, attacking appropriate positions among the entire spectra, i.e. $b = 100$, achieves the optimal results.

b in frequency-generator. The results on DGCNN are shown in Table 2. When b is 100 and 400, the D_c remains consistent. However, D_h and D_{norm} achieve good performances at $b = 100$.

b in dual-discriminator. From Figure 5, although there are very few instances where the attack success rate is higher than at $b = 100$, overall, our method achieves smaller values for the three metrics and higher attack success rates at $b = 100$.