Hiding Imperceptible Noise in Curvature-Aware Patches for 3D Point Cloud Attack

Mingyu Yang[1*], Daizong Liu[2*], Keke Tang[3], Pan Zhou[1†], Lixing Chen[4†], and Junyang Chen[5]

[1] Huazhong University of Science and Technology, Wuhan, China
[2] Peking University, Beijing, China
[3] Guangzhou University, Guangzhou, China
[4] Shanghai Jiao Tong University, Shanghai, China
[5] Shenzhen University, Shenzhen, China
{mingyu_yang,panzhou}@hust.edu.cn,dzliu@stu.pku.edu.cn,
tangbohutbh@gmail.com,lxchen@sjtu.edu.cn,junyangchen@szu.edu.cn

In this supplementary, we provide additional analysis and experimental results, including:

- Description of ISS subsampling algorithm and its visualization of various categories of 3D shapes (Section A);
- More ablation experiments and analysis (Section B);
- More visualization results (Section C);

A ISS Critical Points

In our paper, we utilize Intrinsic Shape Signature (ISS) to obtain the critical points of each point cloud for decomposing the 3D object into patches. The ISS methodology [1] employs a dual approach for 3D shape analysis. It utilizes a view-independent representation to directly match shape patches across different perspectives, complemented by a view-dependent transformation that captures the geometry of observation, thus streamlining the process of rapid pose estimation. We can obtain the ISS critical points by computing weighted covariance matrix of point $\boldsymbol{p}_i$ over a radius $r_{density}$:

$$Cov(\boldsymbol{p}_i) = \frac{\sum\limits_{\|\boldsymbol{p}_j - \boldsymbol{p}_i\|_2 < r_{density}} w_j (\boldsymbol{p}_j - \boldsymbol{p}_i)(\boldsymbol{p}_j - \boldsymbol{p}_i)^T}{\sum\limits_{\|\boldsymbol{p}_j - \boldsymbol{p}_i\|_2 < r_{density}} w_j}, \tag{1}$$

where

$$w_j = \frac{1}{|\{\boldsymbol{p}_k : \|\boldsymbol{p}_k - \boldsymbol{p}_j\|_2 < r_{density}\}|} \tag{2}$$

donates the weight of point $\boldsymbol{p}_j$. Then we compute eigenvalues of $Cov(\boldsymbol{p}_i)$ as $\lambda_i^1, \lambda_i^2, \lambda_i^3$, in the order decreasing magnitude. To this end, we can acquire the

* Mingyu Yang and Daizong Liu contributed equally to this paper. † Corresponding authors: Pan Zhou and Lixing Chen

ISS critical point $\boldsymbol{p}_i$ if

$$\frac{\lambda_i^2}{\lambda_i^1} < \gamma_{21} \quad \text{and} \quad \frac{\lambda_i^3}{\lambda_i^2} < \gamma_{32}, \tag{3}$$

where γ_{21} and γ_{32} are two set parameters. Fig. 1 shows critical points in 3D point cloud of different categories. We can find that these points cover the main geometric shape of the 3D objects.

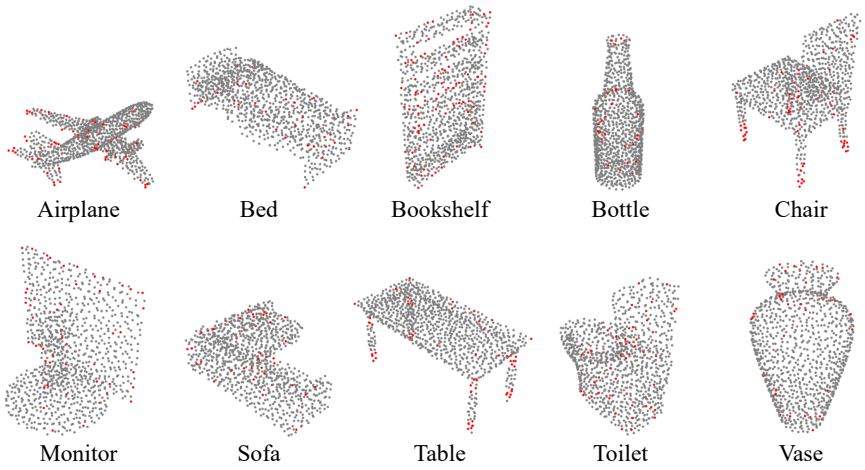

Fig. 1: Visualization of ISS critical points(red) in 3D points cloud of different categories.

B More Ablation Study

B.1 Sensitivity on hyperparameters K, s

We explore the impact of the choice of K in constructing the K-NN Graph and the scale s of the wavelet operator on attack performance, as illustrated in Tab. 1. The experiments on ModelNet40 and ShapeNetPart suggest that the values of K and s have minimal impact on the effectiveness of the attack. This is because variations in K for the K-NN Graph do not affect the selection of the ISS points targeted for the attack, and ours WPA induces perturbations with comparable CD and HD for patches centered on the same point. Additionally, increasing the scale s of the wavelet operator signifies a higher frequency band in the spectral domain addressed by the wavelet filter. Consequently, all our experiments are conducted with $K = 10$ and $s = 2$.

Table 1: Sensitive analysis on K, s. Victim model: PointNet.

Module	Variant	Method	ModelNet40			ShapeNetPart		
			ASR↑	CD↓	HD↓	ASR↑	CD↓	HD↓
K-NN Graph	$K=5$	WPA^{hc}	100%	0.0005	0.0025	100%	0.0006	0.0391
		WPA^{lc}	100%	**0.0004**	0.0024	100%	**0.0005**	0.0309
	$K=10$	WPA^{hc}	100%	**0.0004**	**0.0020**	100%	0.0006	0.0301
		WPA^{lc}	100%	**0.0004**	**0.0020**	100%	0.0006	**0.0299**
	$K=20$	WPA^{hc}	100%	**0.0004**	0.0022	100%	0.0007	0.0443
		WPA^{lc}	100%	**0.0004**	0.0022	100%	0.0006	0.0320
	$K=40$	WPA^{hc}	100%	**0.0004**	0.0021	100%	0.0007	0.0420
		WPA^{lc}	100%	**0.0004**	0.0021	100%	0.0006	0.0313
Wavelet Operator	$s=1$	WPA^{hc}	100%	**0.0004**	**0.0020**	100%	0.0006	0.0308
		WPA^{lc}	100%	**0.0004**	**0.0020**	100%	0.0006	0.0279
	$s=2$	WPA^{hc}	100%	**0.0004**	**0.0020**	100%	0.0006	0.0301
		WPA^{lc}	100%	**0.0004**	**0.0020**	100%	0.0006	0.0299
	$s=3$	WPA^{hc}	100%	0.0005	0.0029	100%	0.0005	0.0351
		WPA^{lc}	100%	0.0005	0.0029	100%	0.0005	0.0290
	$s=4$	WPA^{hc}	100%	0.0005	0.0031	100%	**0.0004**	**0.0205**
		WPA^{lc}	100%	0.0005	0.0031	100%	**0.0004**	0.0227

Table 2: Quantitative comparison of WPA^{hc}, WPA^{lc}, and WPA^{hc+lc}. The bold numbers donate the best attacks. *For fair comparison, we maintain a same number of perturbed points across the three methods.*

Dataset	Method	PointNet			DGCNN			PointConv			CurveNet		
		ASR↑	CD↓	HD↓	ASR↑	CD↓	HD↓	ASR↑	CD↓	HD↓	ASR↑	CD↓	HD↓
ModelNet40	WPA^{hc}	100%	**0.0004**	**0.0020**	100%	0.0008	0.0069	100%	0.0012	0.0075	100%	0.0007	0.0057
	WPA^{lc}	100%	**0.0004**	**0.0020**	100%	**0.0006**	**0.0043**	100%	**0.0010**	**0.0062**	100%	**0.0006**	**0.0047**
	WPA^{hc+lc}	100%	**0.0004**	0.0022	100%	0.0008	0.0069	100%	0.0012	0.0076	100%	0.0007	0.0057
ShapeNetPart	WPA^{hc}	100%	**0.0006**	0.0301	100%	0.0019	0.0306	100%	0.0025	0.0337	100%	0.0020	0.0445
	WPA^{lc}	100%	**0.0006**	**0.0299**	100%	**0.0018**	**0.0250**	100%	**0.0019**	**0.0234**	100%	**0.0019**	**0.0353**
	WPA^{hc+lc}	100%	0.0007	0.0432	100%	0.0019	0.0309	100%	0.0025	0.0336	100%	0.0021	0.0445

B.2 Introducing Noise into Both the Smoothness and Sharpness

We conduct experiments on the attack method named WPA^{hc+lc} that combines both WPA^{hc} and WPA^{lc}, and present the comparative results in Tab. 2. Specifically, WPA^{hc+lc} introduces noise to patches with the highest curvature while applying noise to other patches with the lowest curvature, treating the noise according to the methods of WPA^{hc} and WPA^{lc}, respectively. Notably, WPA^{hc+lc} maintains the same proportion(50%) of perturbed points, with other experiment settings remaining constant. The results indicate that WPA^{hc+lc} does not significantly enhance the attack performance, achieving a comparable attack success rate to the others. The perturbation size is slightly inferior to WPA^{lc} but within the same order of magnitude. This demonstrates the efficacy of the WPA method, indicating its insensitivity regardless of whether patches of the highest or lowest curvature are selected.

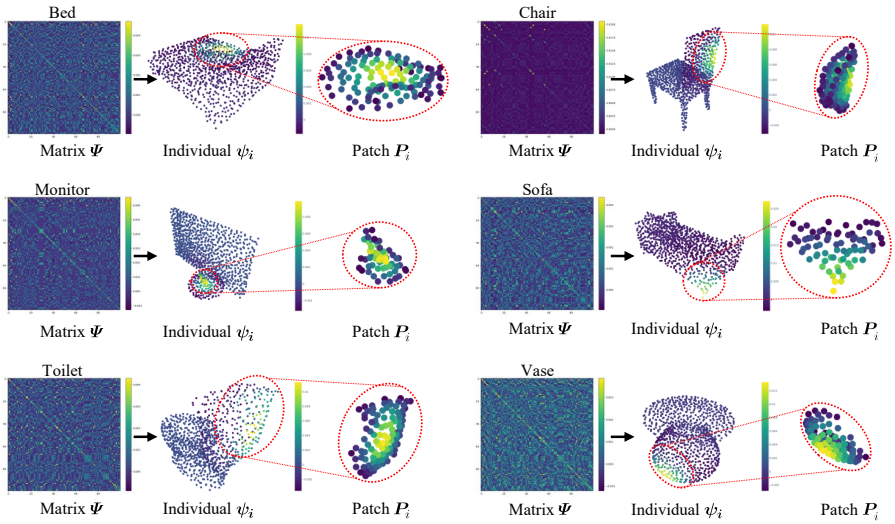

Fig. 2: Visualization on matrix $\boldsymbol{\Psi}$, individual wavelet $\boldsymbol{\psi}_i$ at point $\boldsymbol{p}_i$, and patch $\boldsymbol{P}_i$. For clearly reading, we only demonstrate a part of $\boldsymbol{\Psi}$.

C More Visualization Results

C.1 Decomposed Patches $\boldsymbol{P_i}$

We provide more visual results in Fig. 2 for illustrating how we decompose patches from the whole point cloud via wavelet analysis. The point cloud is transformed into a spectral domain representation, the wavelet coefficient matrix $\boldsymbol{\Psi}$, through the wavelet operator. A minor portion of the $\boldsymbol{\Psi}$ is highlighted, illustrating the excellent locality of the spectral graph wavelet transform. Moreover, each individual wavelet $\boldsymbol{\psi}_i$ in the $\boldsymbol{\Psi}$ corresponds one-to-one with points in the data domain, enabling the visualization of effectiveness across all points. Based on this, we decompose each point into its corresponding geometry-sensitive patch $\boldsymbol{P}_i$.

C.2 Patches $\{\boldsymbol{P_i}\}^{\boldsymbol{ISS}}$ Centering at ISS Critical Points

Fig. 3 shows patches $\{\boldsymbol{P}_i\}^{ISS}$ centering at critical points, which are subsampled from ISS methodology. After a critical point $\boldsymbol{p}_i$ obtained from ISS subsampling algorithm ϕ_{ISS}, we can decompose the origin point cloud into a instinct patch $\boldsymbol{P}_i$ according to corresponding the wavelet $\boldsymbol{\psi}_i$ in matrix $\boldsymbol{\Psi}$.

C.3 Adversarial Examples and Wavelet Coefficients

We also provide more visualization results in Fig. 4 of adversarial examples generating by WPA^{hc}/WPA^{lc}. Specifically, it includes an additional 6 categories

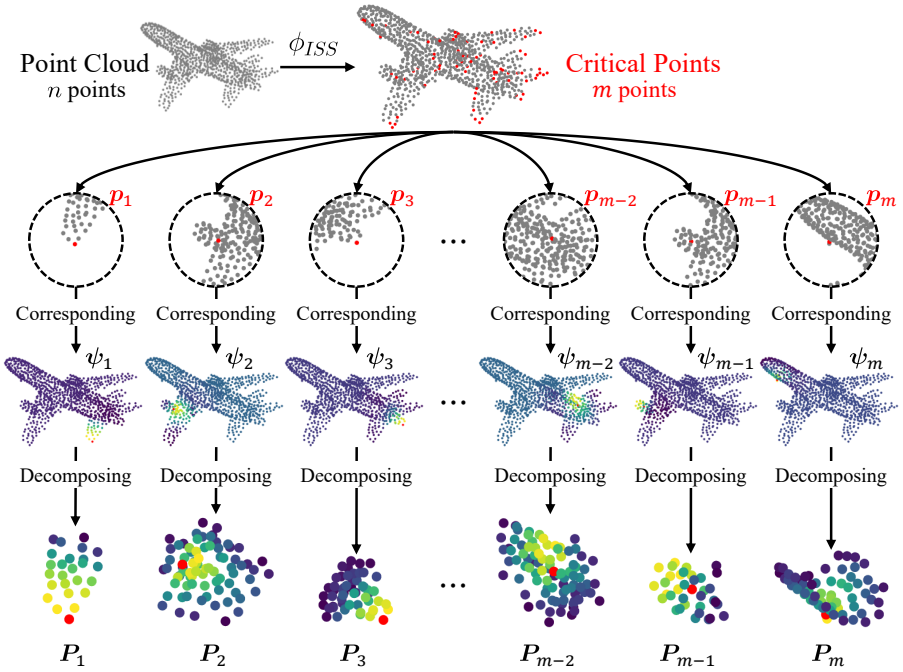

Fig. 3: Visualization of patches $\{\boldsymbol{P}_i\}^{ISS}$ centering at ISS critical points(red).

of 3D point clouds: bed, chair, monitor, sofa, toilet, and vase. The second and third rows of Fig. 4 respectively display the adversarial examples generated by WPA^{hc} and WPA^{lc}, which add geometrical consistency perturbations to patches with high and low curvature magnitudes. This strategy enables WPA to execute remarkably effective attacks by perturbing only a subset of points. The final row illustrates the visualization of the wavelet coefficient matrix $\boldsymbol{\Psi}$.

References

1. Zhong, Y.: Intrinsic shape signatures: A shape descriptor for 3d object recognition. In: 2009 IEEE 12th international conference on computer vision workshops, ICCV Workshops. pp. 689–696. IEEE (2009)

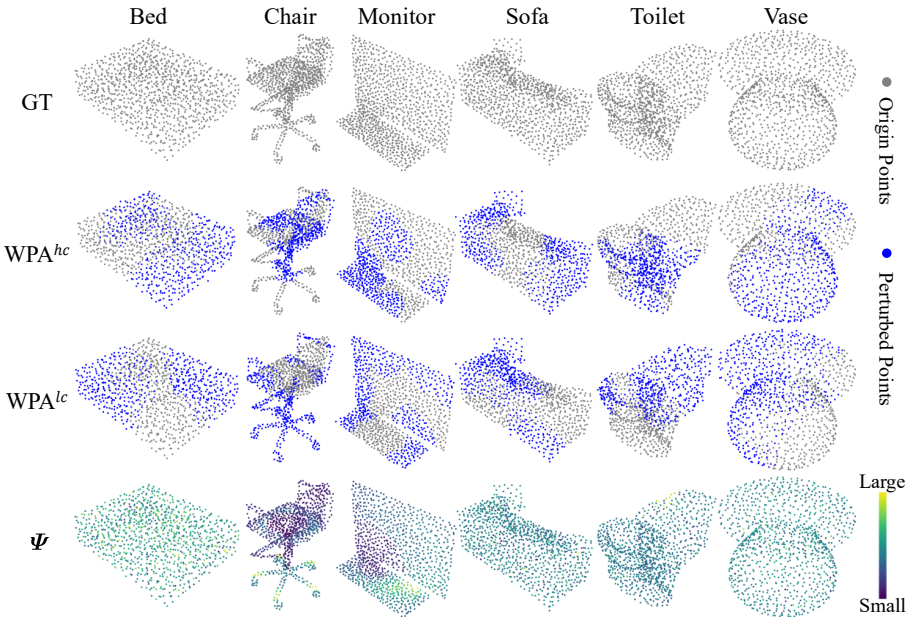

Fig. 4: Visualization on the adversarial examples and wavelet coefficients of GT.