Geometry Cloak: Preventing TGS-based 3D Reconstruction from Copyrighted Images

Qi Song[1, 2], Ziyuan Luo[1, 2], Ka Chun Cheung[2], Simon See[2], Renjie Wan[1, *]
[1]Hong Kong Baptist University [2]NVIDIA AI Technology Center

NEURAL INFORMATION PROCESSING SYSTEMS

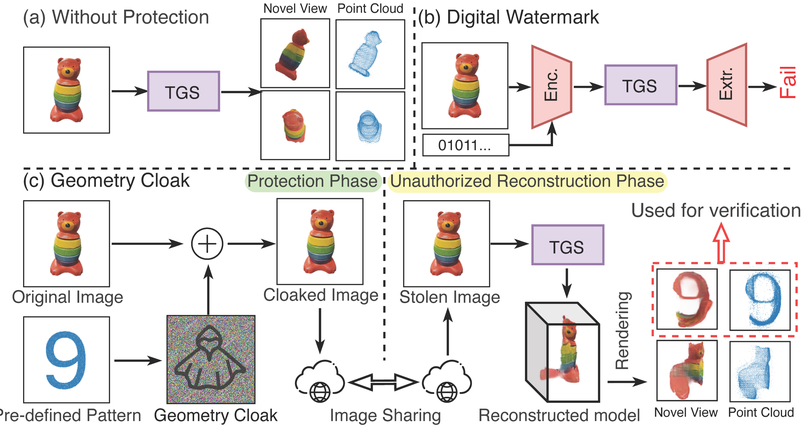
Project page

Two key objectives of Geometry Cloak:

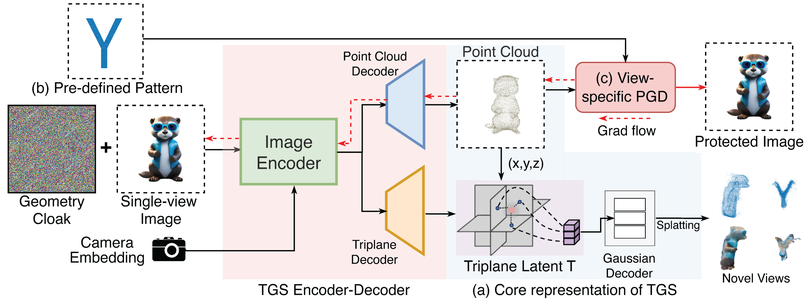
1) Comprise 3D reconstructed result

2) Reveal distinguishable patterns

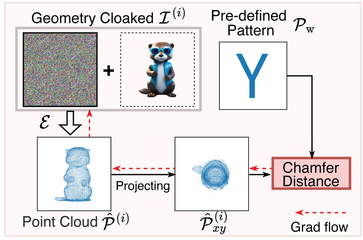
➢ Overview of our scenario



➢ Overview of our framework



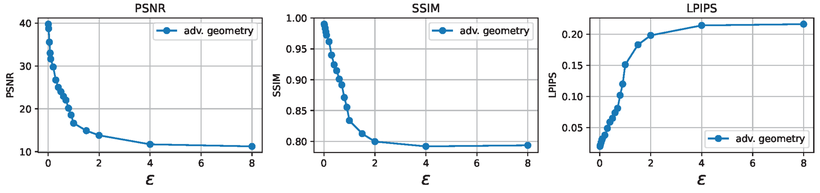
➢ View-specific PGD



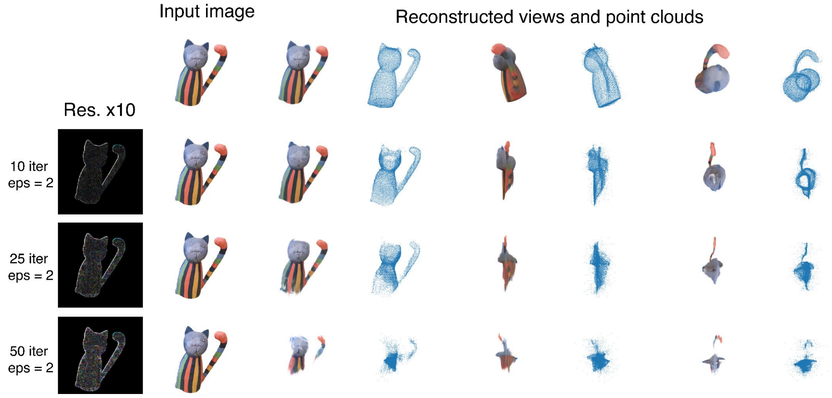
Input: Input image $\mathcal{I}$, Point cloud encoder $\mathcal{E}$ from TGS, pre-defined pattern $\mathcal{P}_w$ number of steps N, step size α, perturbation budget ϵ, viewing direction θ
Output: Geometry cloaked image $\hat{\mathcal{I}}$
Initialize geometry cloak $\delta \leftarrow 0$, and geometry cloaked image $\hat{\mathcal{I}} \leftarrow \mathcal{I}$
for $i \leftarrow 1$ **to** N **do**
  $\hat{\mathcal{P}} \leftarrow \mathcal{E}(\hat{\mathcal{I}})$ // Estimate point cloud representations;
  $\hat{\mathcal{P}}_\theta \leftarrow \text{Proj}_\theta(\hat{\mathcal{P}})$ // Project the point cloud at view direction θ;
  $Loss \leftarrow \mathcal{L}_{\text{CD}}(\hat{\mathcal{P}}_\theta, \mathcal{P}_w)$ // Calculate CD between two 2D point clouds;
  $\delta \leftarrow \alpha \cdot \text{sgn}(\nabla_{\mathcal{I}} Loss)$ // Update geometry cloak;
  $\hat{\mathcal{I}} \leftarrow \hat{\mathcal{I}} + \delta$ // Update cloaked image;
  $\hat{\mathcal{I}} \leftarrow \text{clip}(\hat{\mathcal{I}}, \mathcal{I} - \epsilon, \mathcal{I} + \epsilon)$ // Clip cloaked image $\hat{\mathcal{I}}$;
end
Return $\hat{\mathcal{I}}$

Results

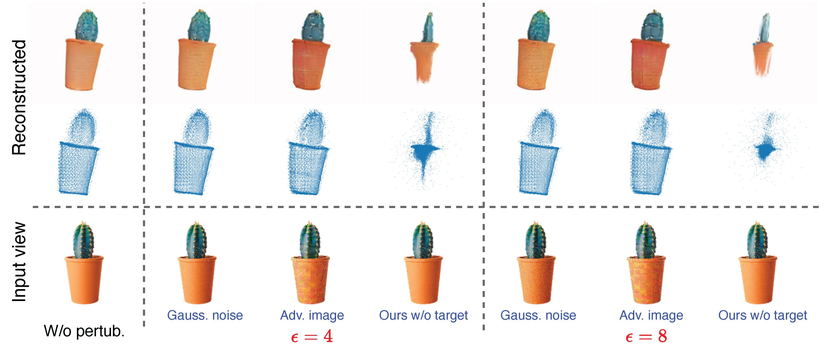
➢ Privacy/perturbation budget



➢ Geometry cloak w/o target



➢ Reconstructed results with different perturbation strategy



➢ Watermark patterns & Customized patterns