



Seeing Through the Weights: Privacy Leakage in Scene Coordinate Regression

Oleksii Nasypanyi^{1,*}, Jaemin Cho^{1,*}, Utku Ozbulak^{2,3}, Byungkon Kang⁴, François Rameau^{4,†}

¹Stony Brook University, ²Ghent University Global Campus, ³George Mason University Korea, ⁴SUNY Korea

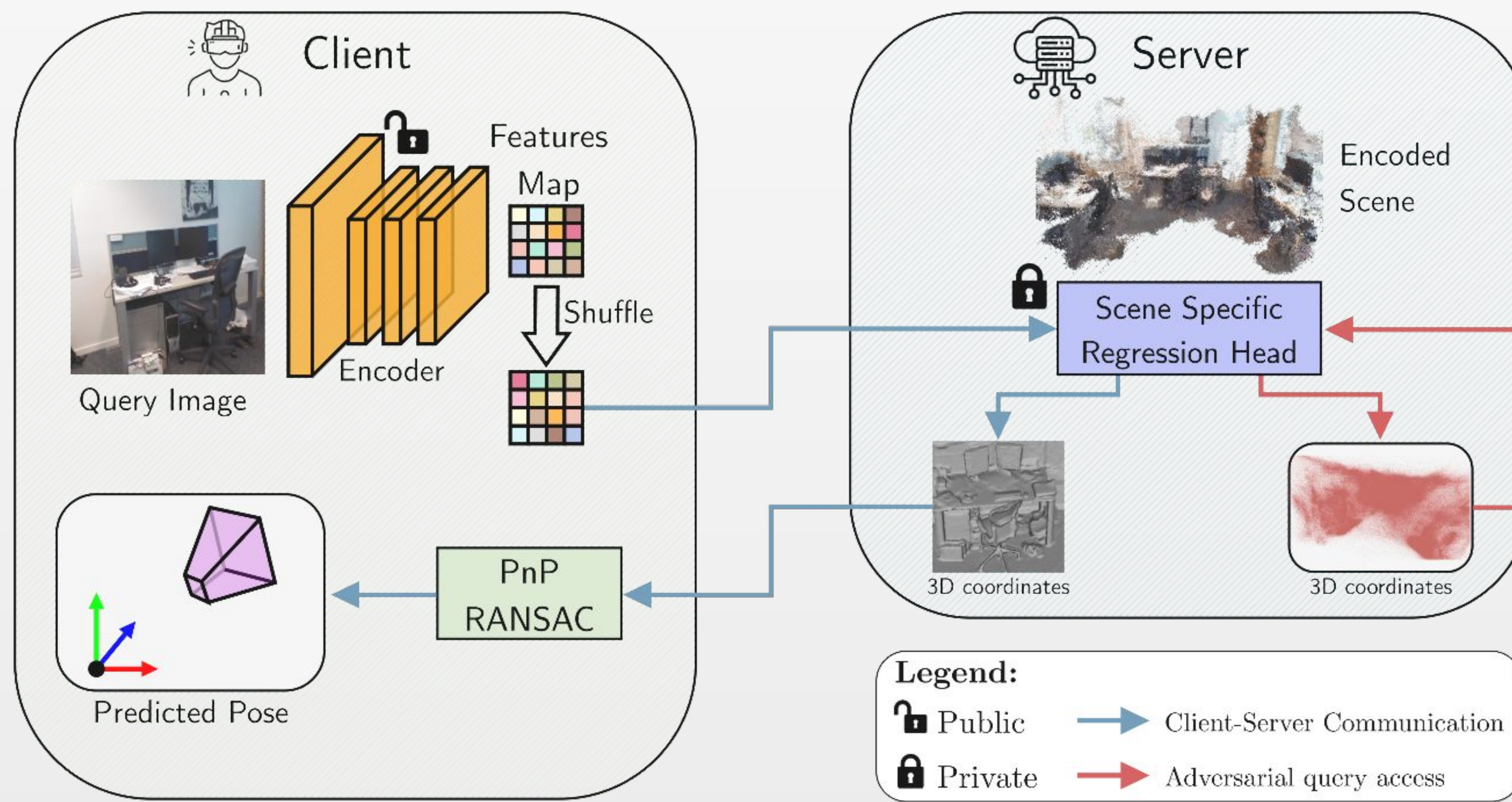


ECCV 2026 | MALMÖ | SEPT 8-12

ORAL

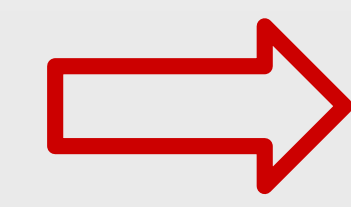
Sat. 2:45 PM – 3:00 PM

Overview



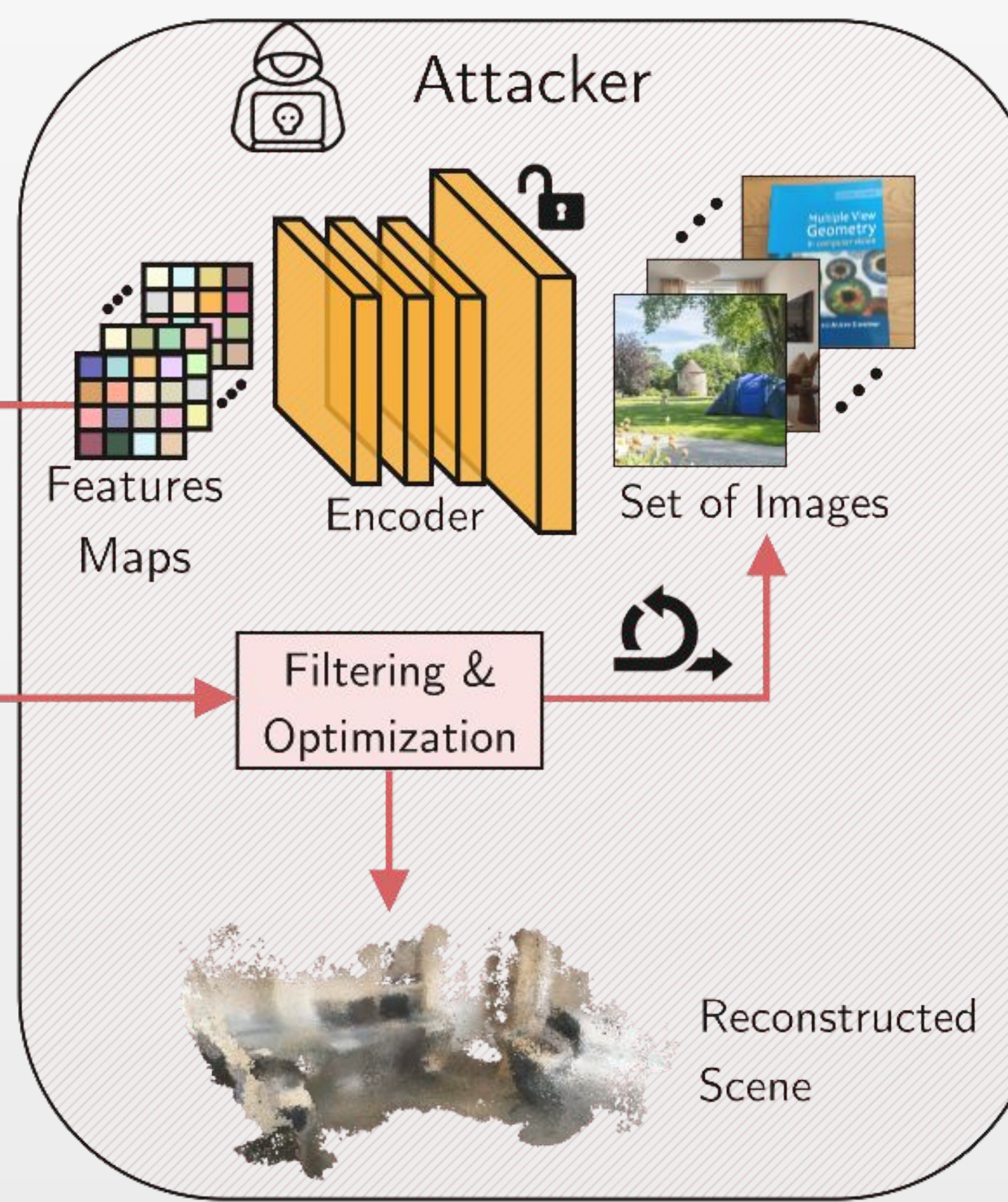
Scene Coordinate Regression does not store any explicit map representation.

"The resulting maps can be as small as 4MB, and privacy preserving"
"SCR is said to be inherently privacy-preserving because there is no set of 2D or 3D points to run the inversion attack on."
[1]
[2]



But Is It Enough?

Gray-box Scenario

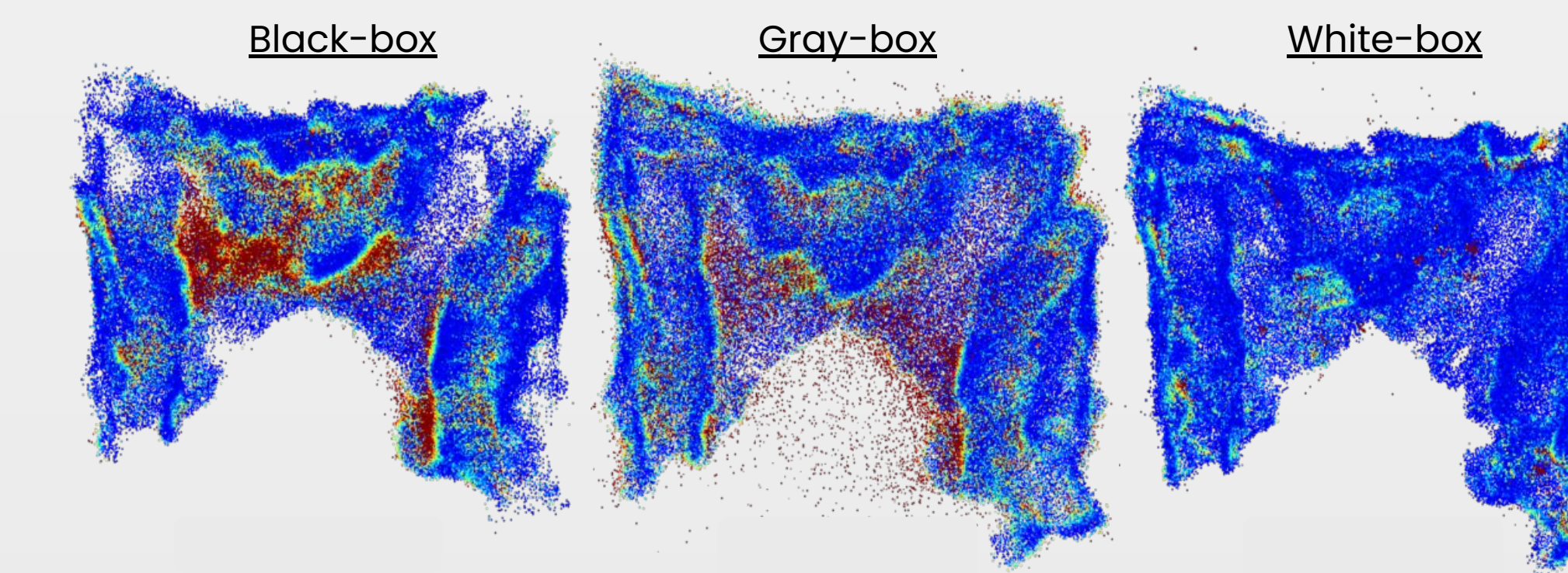


Results

Various Scenario on ACE (7scenes)

	Black-Box			Gray-Box			White-Box		
	F1 ² ↑	F1 ⁵ ↑	CD↓	F1 ² ↑	F1 ⁵ ↑	CD↓	F1 ² ↑	F1 ⁵ ↑	CD↓
Chess	71.2	88.0	2.55	77.7	93.3	1.90	83.0	97.2	1.59
Fire	60.3	80.7	3.13	76.2	94.0	1.83	79.9	95.8	1.72
Heads	52.0	77.8	3.03	70.3	92.6	1.91	78.1	95.3	1.78
Office	71.2	89.7	2.29	76.2	92.0	2.19	82.7	96.2	1.65
Pumpkin	61.1	79.7	3.67	68.5	87.1	2.56	76.1	93.4	2.04
Redkitch.	74.2	91.5	2.41	76.5	92.2	2.08	82.3	96.5	1.62
Stairs	46.2	72.1	4.79	48.9	76.1	3.57	58.8	84.8	2.96
Avg.	62.3	82.8	3.12	70.6	89.6	2.30	77.3	94.2	1.91

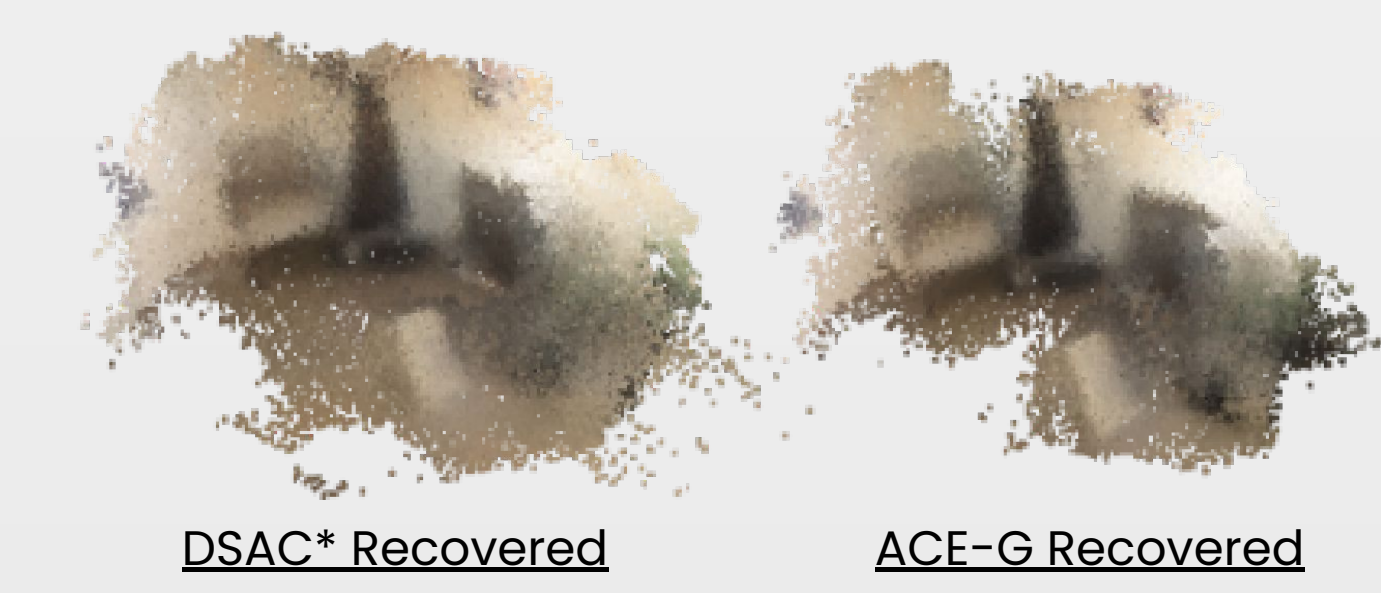
Qualitative result: 7scenes - Office



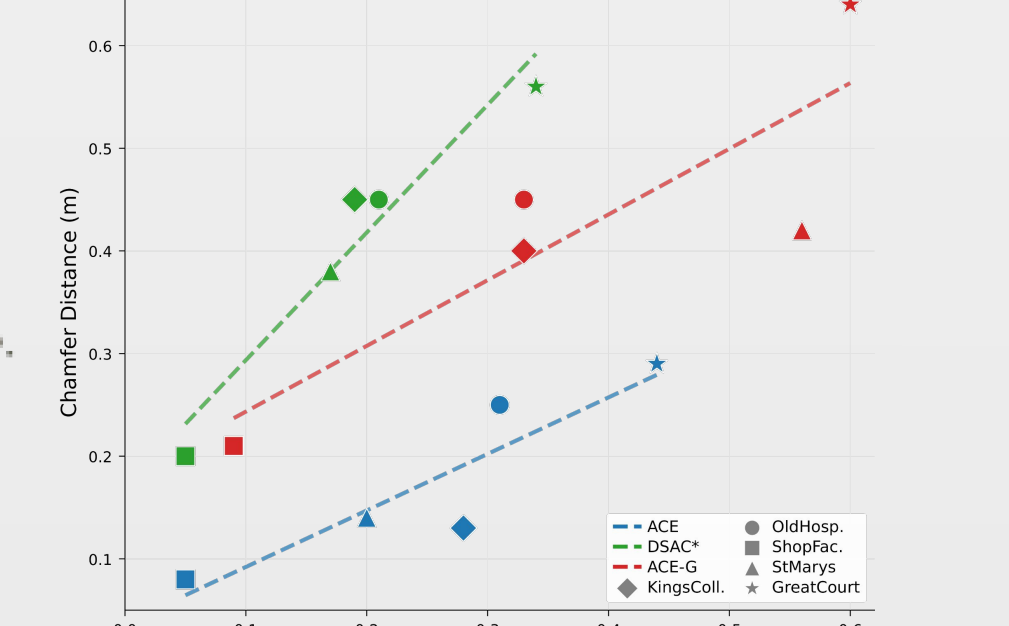
Generalization across SCR Architectures

	ACE [1]			GLACE [3]			DSAC* [4]			ACE-G [5]		
	F1 ² ↑	F1 ⁵ ↑	CD↓	F1 ² ↑	F1 ⁵ ↑	CD↓	F1 ² ↑	F1 ⁵ ↑	CD↓	F1 ² ↑	F1 ⁵ ↑	CD↓
7-Scenes	83.0	97.2	1.59	78.2	95.7	1.70	71.8	90.8	2.25	57.1	85.3	3.00
Chess	79.9	95.8	1.72	80.4	96.4	1.67	71.8	91.4	2.15	58.9	85.6	3.19
Fire	78.1	95.3	1.78	75.6	93.4	1.86	68.0	91.1	2.40	59.0	88.0	2.68
Heads	82.7	96.2	1.65	84.0	97.6	1.47	69.5	89.3	2.47	58.0	84.9	3.72
Pumpkin	76.1	93.4	2.04	72.7	92.3	2.13	58.6	82.7	3.40	46.1	78.6	4.55
Redkitch.	82.3	96.5	1.62	82.9	97.0	1.54	65.6	86.5	2.74	55.2	84.2	3.36
Stairs	58.8	84.8	2.96	61.7	86.8	2.64	40.1	66.8	6.05	33.4	68.0	5.29
Avg.	77.3	94.2	1.91	76.5	94.2	1.86	63.6	85.5	3.07	52.5	82.1	3.68
Cambridge	F1 ¹⁰ ↑	F1 ³⁰ ↑	CD↓	F1 ¹⁰ ↑	F1 ³⁰ ↑	CD↓	F1 ¹⁰ ↑	F1 ³⁰ ↑	CD↓	F1 ¹⁰ ↑	F1 ³⁰ ↑	CD↓
KingsColl.	64.0	92.5	0.13	39.0	73.9	0.25	22.5	57.1	0.45	25.1	62.3	0.40
OldHosp.	45.1	74.8	0.25	49.6	77.4	0.24	29.5	61.7	0.45	27.2	69.0	0.45
ShopFac.	83.5	98.8	0.08	58.2	86.3	0.16	50.6	84.9	0.20	39.5	80.6	0.21
StMarys	65.1	91.5	0.14	16.6	61.6	0.52	31.2	67.6	0.38	14.3	46.9	0.42
GreatCourt	43.3	74.8	0.29	9.0	26.9	1.36	33.9	63.7	0.56	22.2	57.7	0.64
Avg.	59.0	85.9	0.18	34.5	65.2	0.31	33.5	67.0	0.41	25.7	63.3	0.42

Qualitative result: 7scenes - Fire

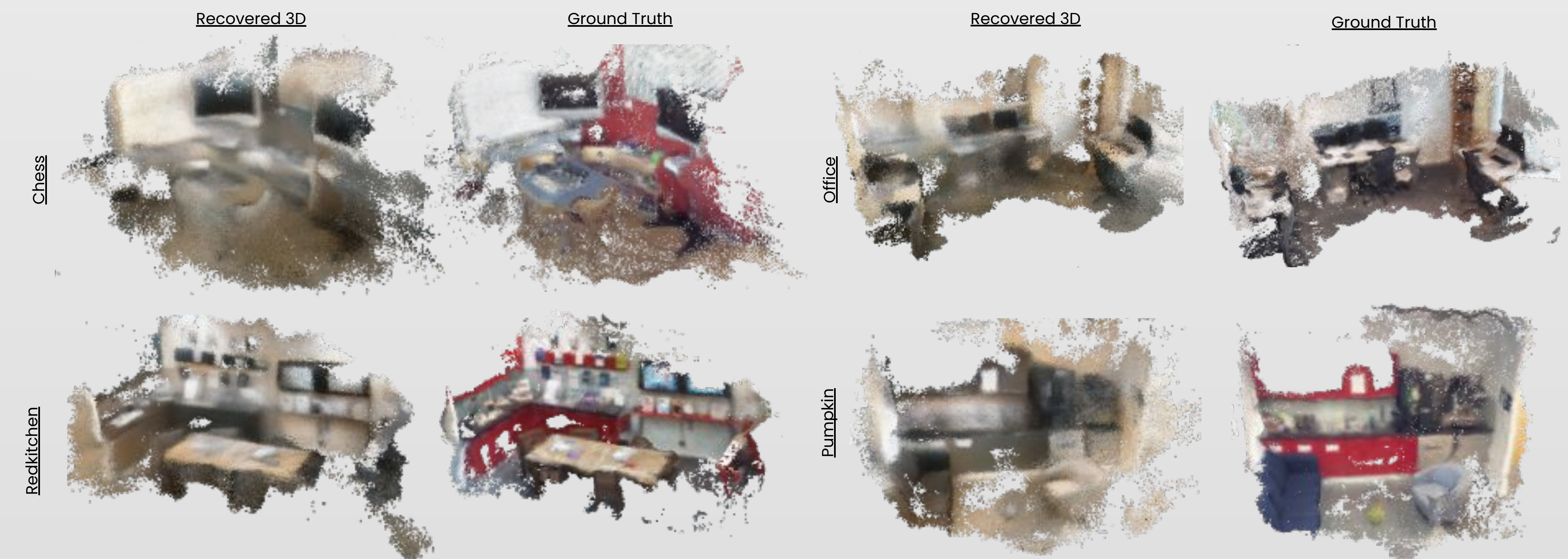


Analysis: Cambridge

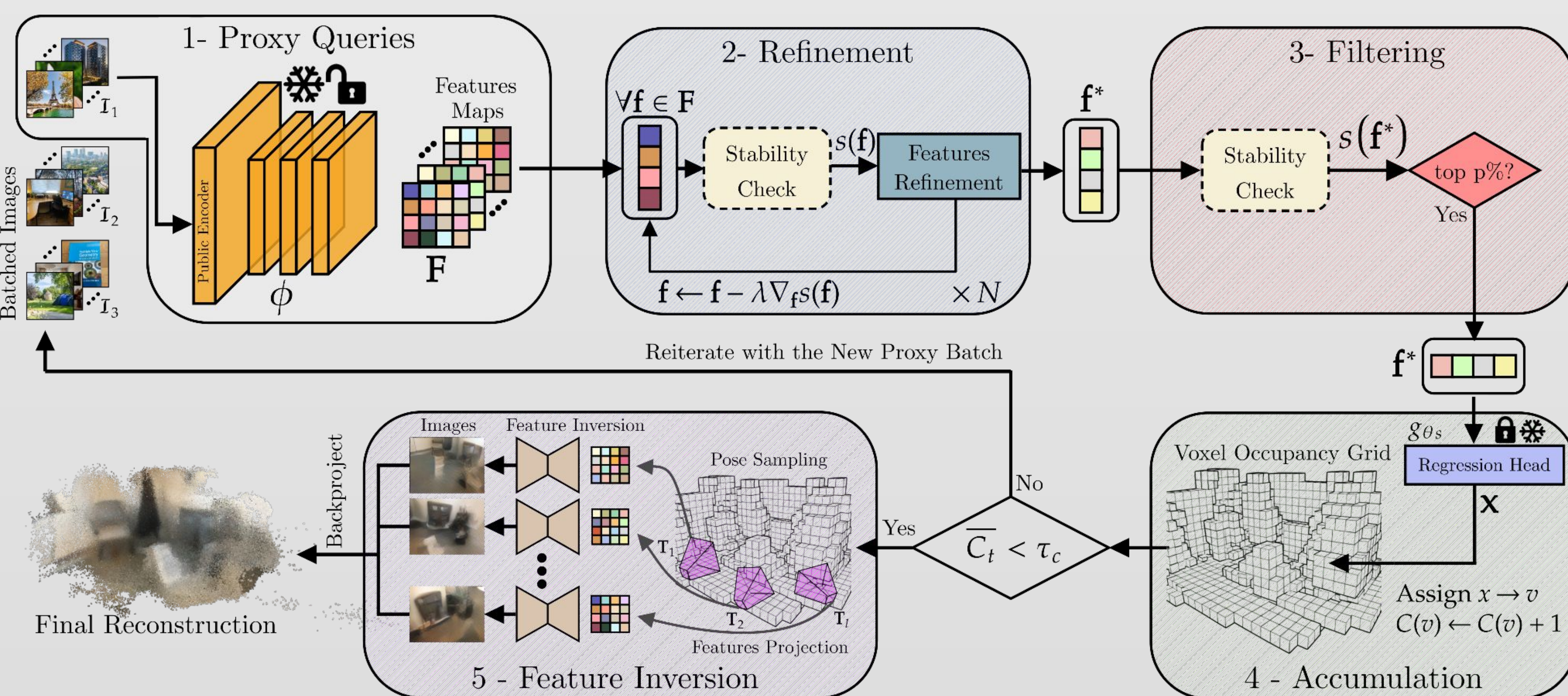


Model Accuracy vs. Reconstruction

Qualitative Reconstruction on ACE (7scenes)



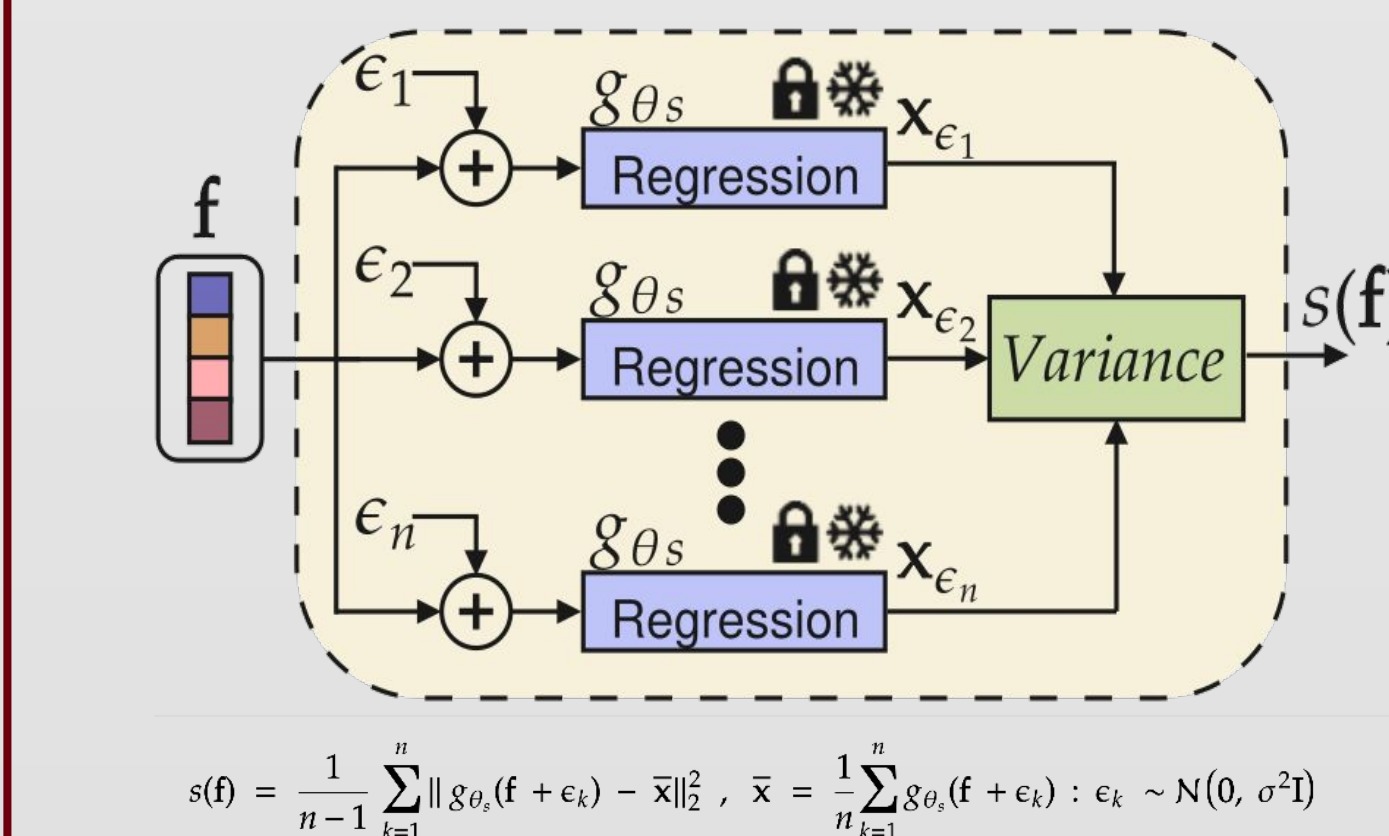
Method



- Proxy Queries.** Feature Extractor encodes proxy images to dense feature maps.
- Refinement.** Gradient descent refines features toward stable scene regions.
- Filtering.** Retain only the top p% stable features.
- Accumulation.** Aggregate 3D predictions into a voxel grid until threshold τ .
- Feature Inversion.** Synthesize novel views from recovered features.

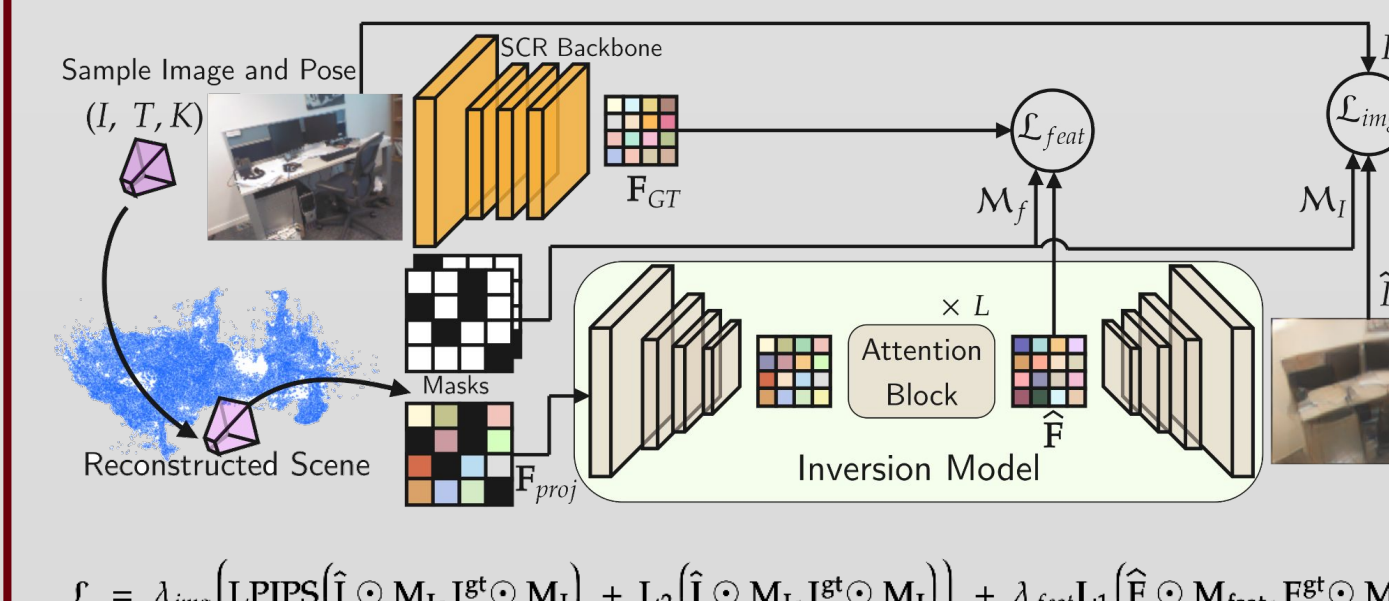
Submodules

1. Stability Estimation.



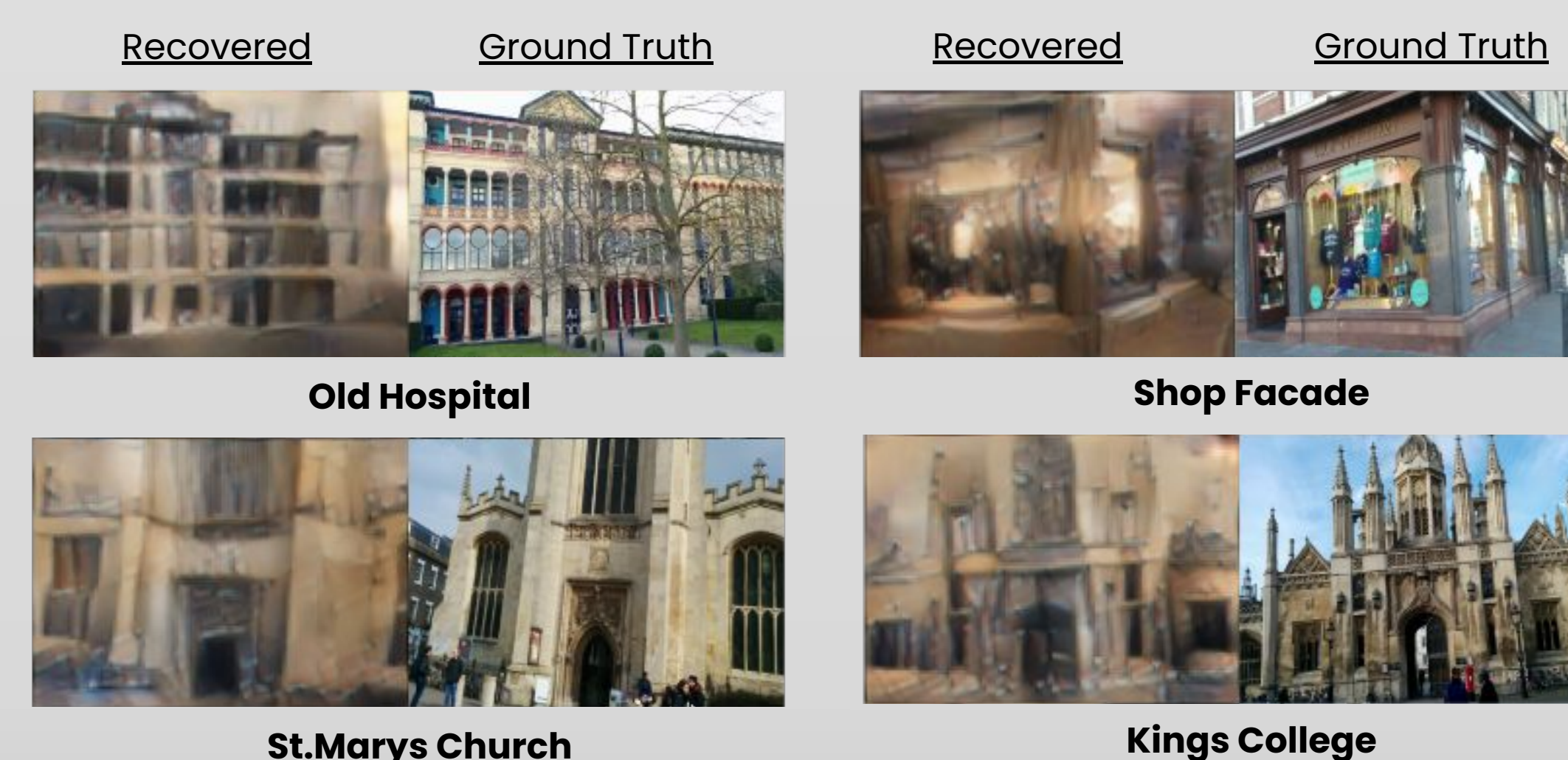
- Gray-box:** Filtering
- White-box:** Refinement + Filtering

2. Image Reconstruction.

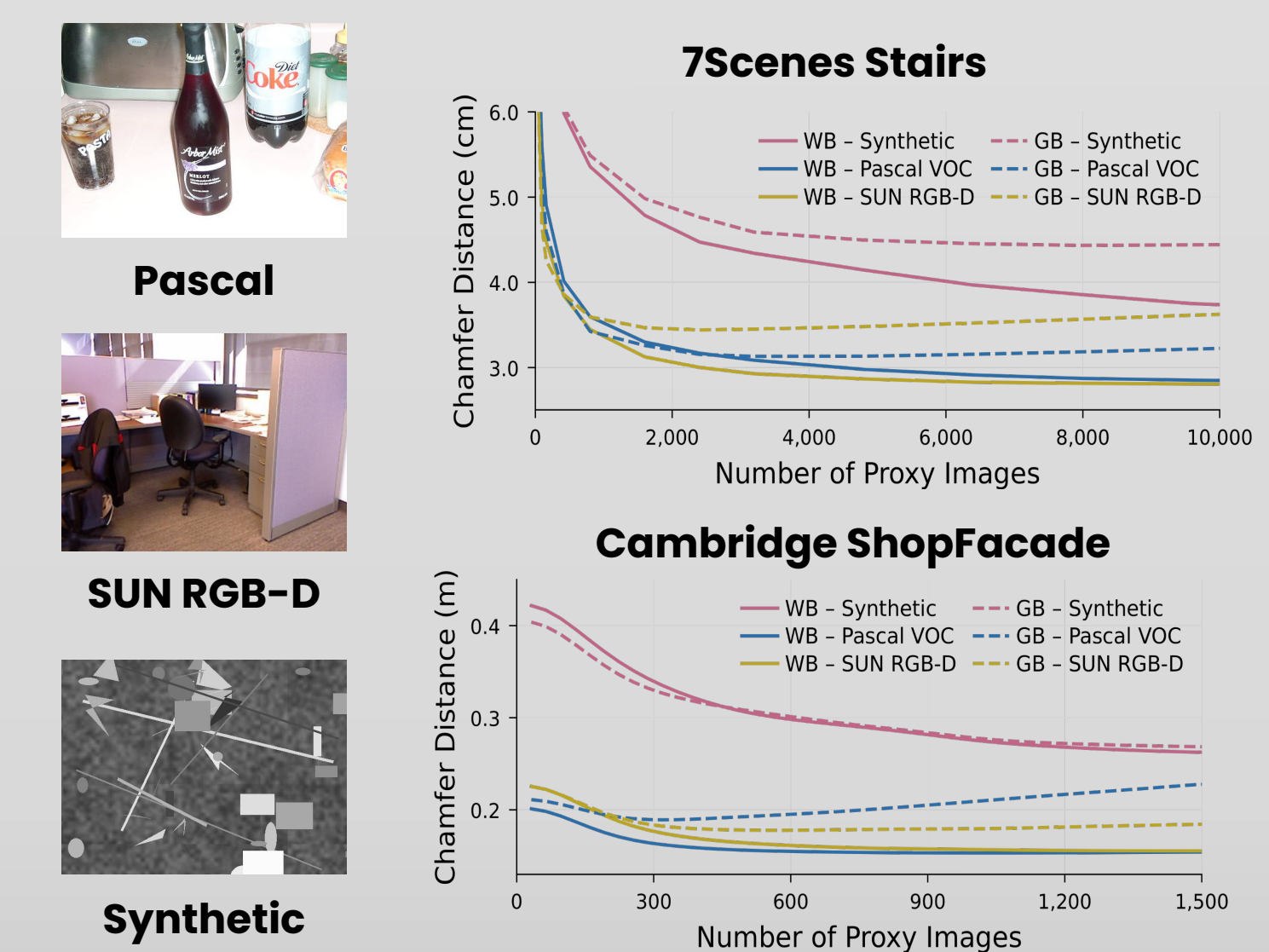


- Project 3D points on the image plane
- Aggregate corresponding features
- Reconstruct Image

Qualitative result on Cambridge



Effect on Proxy Domain



Leakage Quality

