Privacy Preserving Localization via Coordinate Permutations

Linfei Pan[1] Johannes L Schönberger[2] Viktor Larsson[3] Marc Pollefeys[1,2]
[1]ETH Zurich [2]Microsoft [3]Lund University

ICCV23 PARIS

Preliminaries

Localization

Privacy Concern

- Feature inversion can synthesize images with high fidelity from raw features
- Point cloud and line cloud can be inverted to reveal scene information
- Protect the image features (point cloud) from revealing

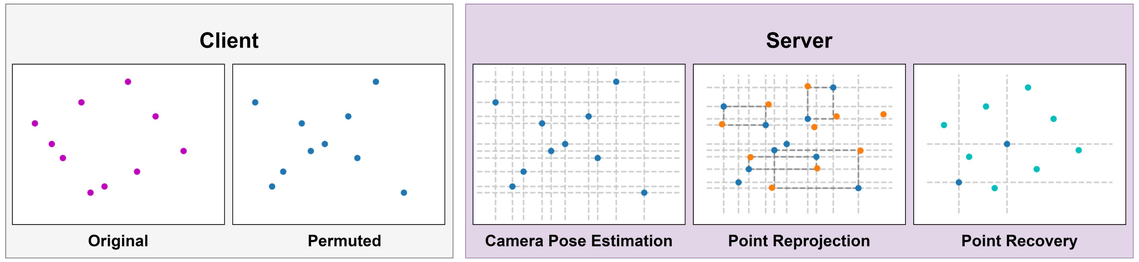
Task

- Perform localization in a privacy preserving way
- Preserve privacy for both queries (image) and maps (point cloud)
- Improve both privacy and accuracy

Overview

- Introduce uncertainty by permuting points
- Improve localization performance by point recovery
- Decrease performance gap between privacy-preserving and traditional localization and increase complexity

Pipeline

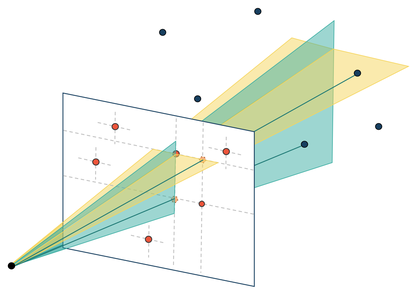


Point Recovery

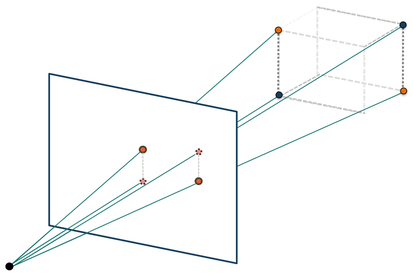
- Corresponding 3D point lies on one of two planes passing through the image point
- The minimal solver needs 6 2D-line-to-3D-point correspondences ➔ iterate all $2^6 = 64$ configurations to get a pose
- With a camera pose, the reprojected point of an inlier should be close to the original points
- A pair would form a rectangle if both points are inliers (permuted + reprojected)
- Rectangles ➔ original pairs

$$\boldsymbol{\ell}_1^\top (R\boldsymbol{X} + \boldsymbol{t}) = 0 \quad \vee \quad \boldsymbol{\ell}_2^\top (R\boldsymbol{X} + \boldsymbol{t}) = 0$$

$2^6 = 64$ possible configurations

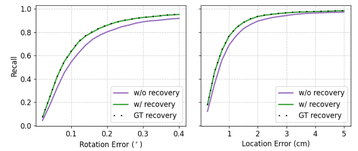


- Swapping and recovery in 3D

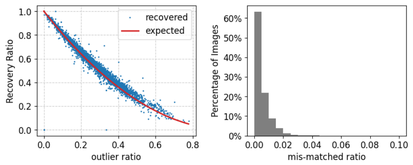


Experiments

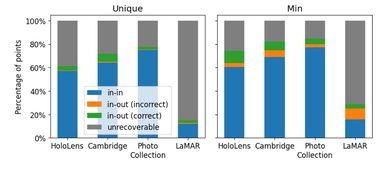
Effectiveness of Point Recovery



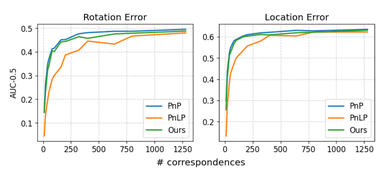
Recovery Ratio



One-side Recovery Attack



Impact of the Number of Correspondences



Results (Privacy-Preserving Query)

Cambridge

	MED (°)	AUC@1°	MED (cm)	AUC@10cm	(1°, 10 cm)	Time (s)
PnLP [47]	0.18	71.59	12.13	18.38	41.29	0.36
Proposed	0.18	72.61	11.73	20.03	44.26	2.31
PnP	0.17	73.09	11.66	20.22	43.95	0.20

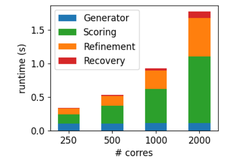
Photo Collection

	MED (°)	AUC@1°	MED (cm)	AUC@10cm	(1°, 10 cm)	Time (s)
PnLP [47]	0.02	88.32	2.24	59.57	78.23	0.09
Proposed	0.02	89.67	1.92	63.62	81.33	0.68
PnP	0.02	90.74	1.85	64.58	82.62	0.08

HoloLens

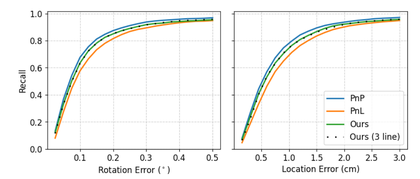
	MED (°)	AUC@1°	MED (cm)	AUC@10cm	(1°, 10 cm)	Time (s)
PnLP [47]	0.08	84.79	0.63	88.88	97.80	0.07
Proposed	0.07	86.69	0.56	90.12	98.41	0.36
PnP	0.07	87.92	0.51	90.85	98.80	0.05

Runtime Analysis



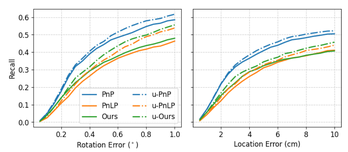
Amortized linear runtime $O(n)$ complexity on average

Results (Privacy-Preserving Map)



	MED (°)	AUC@1°	MED (cm)	AUC@10cm	(1°, 10 cm)	Time (s)
PnL [6]	0.08	84.71	0.64	88.66	97.71	1.16
Proposed (w/)	0.07	86.31	0.56	89.71	97.92	6.61
Proposed (w/o)	0.08	86.32	0.55	89.78	98.02	59.55
PnP	0.07	87.85	0.51	90.84	98.83	0.07

Results (Gravity Prior)

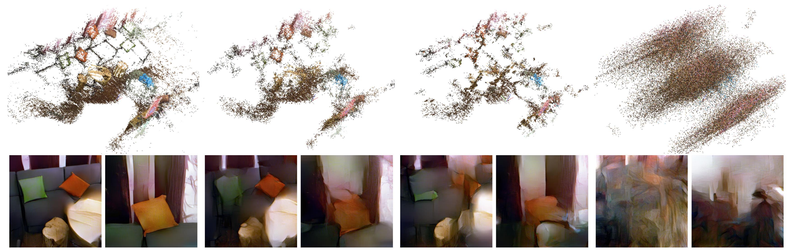


LaMAR	(1°, 10 cm)	(5°, 1 m)	Time (s)
PnLP [7]	45.81	64.25	0.21
Proposed	46.63	63.49	2.50
PnP	52.68	67.93	0.09
u-PnLP [7]	53.24	73.63	0.11
u-Proposed	55.12	72.44	0.28
u-PnP	60.67	75.60	0.06

One-side Recovery Attack

(a) Raw Features (b) Symmetric Error Recovery (c) Unique Attack (d) Min Attack

Line Cloud Inversion Attack



(a) Original (b) Random line (c) Oracle (d) Proposed

References

[1] P. Speciale, et. al. Privacy Preserving Image Queries for Camera Localization. ICCV 2019
[2] P. Speciale, et. al. Privacy Preserving Image-Based Localization. ECCV, 2020
[3] Pittaluga, et al. Revealing Scenes by Inverting Structure from Motion Reconstructions, CVPR 2019

Project Page

https://lpanaf.github.io/iccv23_privacy_permute/