VPR-Cloak: A First Look at Privacy Cloak Against Visual Place Recognition
Supplementary Material

Shuting Dong[1,2*], Mingzhi Chen[3*], Feng Lu[1,2], Hao Yu[1],
Guanghao Li[1,3], Zhe Wu[2], Ming Tang[3†], Chun Yuan[1†]
[1]Tsinghua University, [2]Pengcheng Laboratory, [3]Southern University of Science and Technology
dst21@mails.tsinghua.edu.cn, 12211414@mail.sustech.edu.cn,
lf22@mails.tsinghua.edu.cn, longinyh@gmail.com, ligh24@mails.tsinghua.edu.cn,
wuzh02@pcl.ac.cn, tangm3@sustech.edu.cn, yuanc@sz.tsinghua.edu.cn

1. Additional Comparisons

Enhanced Visual Fidelity and Imperceptibility Table 1 highlights the superior image quality of our method compared to existing approaches. On PITTS30K-Sela, our method achieves the lowest LPIPS (0.041) and highest PSNR (33.67 dB). The integration of frequency-domain optimization ensures that perturbations primarily refine high-frequency components, preserving low-frequency structural information vital for human perception.

Superior Protection Effectiveness Against Black-Box and White-Box VPR Models. As shown in Table 2, our method consistently achieves the highest reduction in retrieval accuracy ($\Delta R@1$, $\Delta R@5$, $\Delta R@10$) across multiple datasets and VPR models. For instance, on the PITTS30K-Crica setup, our method outperforms ANDA and MULTI-ANDA by 15.6% and 11.7% in $\Delta R@1$, respectively, while achieving a significant 22.9% improvement in $\Delta R@5$. Similarly, on the NORDLAND-Sela setup, our method attains an unprecedented $\Delta R@1$ of 86.5%, surpassing MULTI-ANDA by 34.3%. These results validate the robustness of our method, which strategically concentrates perturbations on decisive regions critical for place recognition, thereby maximizing disruption to unauthorized VPR models.

Notably, in challenging scenarios such as MSLS CHALLENGE-Crica, our method achieves $\Delta R@1 = 73.2\%$, outperforming MULTI-ANDA by 6.0%, while maintaining high performance even under severe environmental variations (e.g., seasonal changes in NORDLAND). This demonstrates the transferability of our perturbations across diverse black-box models, attributed to the dynamic selection of surrogate VPR models during optimization.

Table 1. Image quality comparison (Epsilon=8/255).

Dataset	Method	LPIPS	PSNR	SSIM	Avg Epsilon
PITTS30K	ANDA	0.107	30.99	0.893	3.56
	MULTI-ANDA	0.098	31.18	0.901	3.10
	Our (Crica)	0.057	32.41	0.928	**2.84**
	Our (Sela)	**0.041**	**33.67**	**0.941**	2.88
TOKYO247	ANDA	0.057	**32.27**	0.912	3.92
	MULTI-ANDA	**0.054**	32.18	**0.920**	**3.42**
	Our (Crica)	0.059	30.27	0.914	3.64
	Our (Sela)	0.071	29.89	0.909	3.60
MSLS	ANDA	0.094	32.13	0.901	3.24
	MULTI-ANDA	0.088	31.58	0.909	2.88
	Our (Crica)	**0.066**	**32.21**	**0.916**	2.82
	Our (Sela)	0.070	32.19	0.911	**2.78**
MSLS CHALLENGE	ANDA	0.092	33.99	0.931	3.54
	MULTI-ANDA	0.073	34.20	0.936	2.76
	Our (Crica)	0.062	**35.99**	**0.942**	2.88
	Our (Sela)	**0.051**	34.25	0.931	**2.48**
NORDLAND	ANDA	0.087	31.58	0.902	2.42
	MULTI-ANDA	0.072	32.03	**0.917**	1.92
	Our (Crica)	**0.071**	**32.13**	0.915	**1.84**
	Our (Sela)	0.084	31.90	0.909	2.20

2. Additional Protection Performance on Commercial APIs

Figs. 1–3 visually demonstrate the effectiveness of our proposed method when tested on commercial APIs, including Google and Microsoft Bing. These commercial systems are designed to accurately identify and match locations based on visual cues extracted from images. However, after applying our method, the ability of these APIs to retrieve and recognize locations is significantly disrupted. The modified images effectively prevent the systems from extracting meaningful location-related features, rendering them unidentifiable.

*These authors contributed equally to this work.
†Corresponding authors.

Table 2. Protection success rate (%) comparisons (Epsilon=8/255). ΔR@1, ΔR@5 and ΔR@10 measure the reduction in the model's retrieval accuracy after applying protection, with larger values indicating stronger protection.

Dataset	Model	ANDA			MULTI-ANDA			Our (Crica)			Our (Sela)		
		ΔR@1	ΔR@5	ΔR@10	ΔR@1	ΔR@5	ΔR@10	ΔR@1	ΔR@5	ΔR@10	ΔR@1	ΔR@5	ΔR@10
PITTS30K	Crica	41.5	25.5	14.6	45.4	27.1	16.9	**57.1**	**47.7**	**37.5**	40.2	30.7	26.1
	DHE	15.2	6.5	1.9	29.2	18.2	10.6	35.5	20.3	14.4	**39.2**	**23.3**	**16.1**
	Salad	16.5	9.2	4.0	23.6	12.3	8.7	33.4	19.3	12.2	**37.5**	**23.1**	**17.9**
	Sela	14.7	10.6	3.3	15.9	12.2	4.5	30.3	19.6	16.2	**62.3**	**46.0**	**33.5**
	VLAD-BuFF	14.0	8.5	-	16.4	10.6	-	**31.0**	**19.8**	-	28.4	18.6	-
TOKYO247	Crica	42.1	28.6	18.0	43.2	30.2	23.2	**57.6**	**55.7**	**48.0**	44.2	27.9	22.8
	DHE	15.4	17.9	11.4	32.0	34.7	25.5	**41.3**	**45.4**	**44.1**	35.9	40.2	39.9
	Sela	30.3	22.7	12.3	33.0	24.4	9.5	41.3	30.5	20.4	**54.9**	**51.3**	**46.2**
	VLAD-BuFF	14.8	5.8	-	17.9	9.9	-	24.8	18.8	-	**27.3**	**21.7**	-
MSLS	Crica	51.8	44.1	25.4	53.2	45.3	25.5	**78.1**	**65.8**	**43.7**	38.0	27.5	24.1
	DHE	30.9	22.4	15.7	42.8	29.0	24.1	**46.4**	**32.9**	**27.2**	44.9	32.3	26.4
	Salad	31.0	23.1	14.4	36.1	30.1	17.8	**49.4**	**37.0**	**25.3**	45.3	34.1	22.8
	Sela	15.9	9.2	4.1	21.7	12.7	5.3	38.8	28.7	24.6	**70.4**	**64.2**	**45.4**
	VLAD-BuFF	22.6	12.9	-	23.3	14.5	-	**39.0**	**26.6**	-	35.5	24.4	-
MSLS CHALLENGE	Crica	66.9	74.5	64.0	67.2	74.9	66.4	68.6	76.3	75.4	**73.2**	**87.0**	**89.4**
	DHE	58.9	74.3	75.8	61.3	77.4	**81.5**	**61.5**	**77.6**	**81.5**	61.1	76.4	78.7
	Salad	71.4	82.9	81.2	73.9	87.2	86.5	74.2	87.6	89.4	**74.6**	**87.9**	**90.2**
	Sela	71.9	82.7	77.3	72.9	83.6	80.5	**73.3**	**86.9**	**89.5**	68.1	75.9	74.3
NORDLAND	Crica	57.8	52.1	40.4	59.3	55.6	46.9	**84.6**	**75.6**	59.0	60.9	67.2	**66.2**
	DHE	35.5	30.2	29.1	50.7	63.6	62.0	63.5	**76.4**	**76.1**	**63.6**	74.2	68.6
	Salad	48.2	49.8	40.3	61.9	64.9	52.4	**69.3**	**78.0**	**74.4**	66.2	75.8	70.4
	Sela	48.0	49.9	40.7	52.2	55.8	47.9	61.8	68.3	68.4	**86.5**	**80.5**	**60.2**
	VLAD-BuFF	55.8	55.8	-	58.4	63.3	-	**66.2**	**70.6**	-	64.6	67.8	-

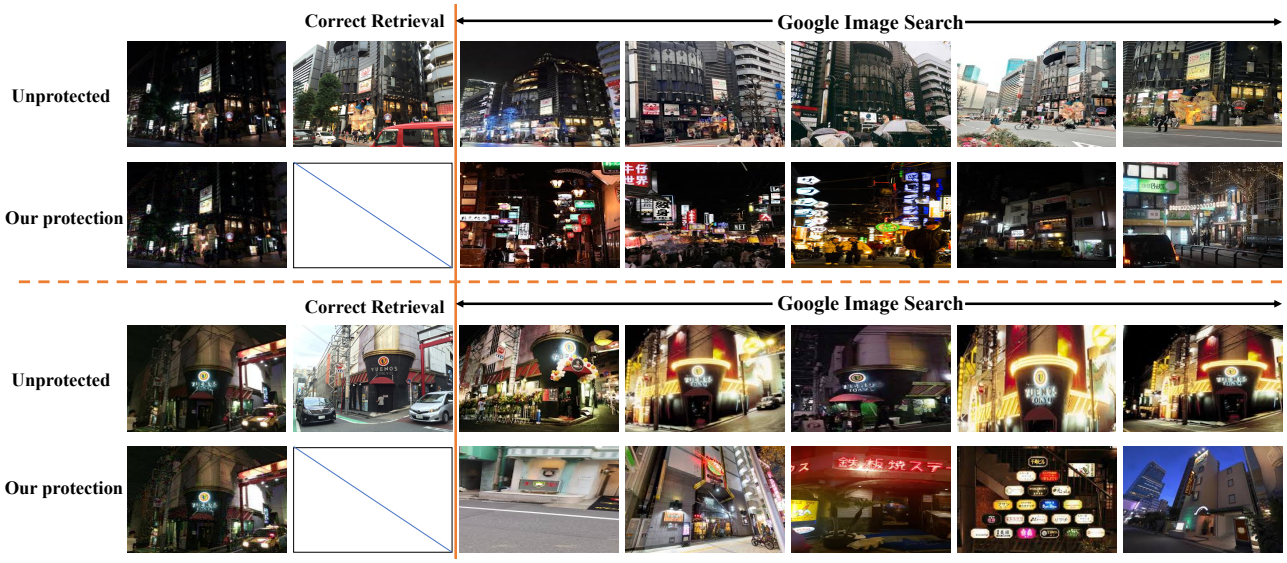

Figure 1. Protection on Commercial APIs. Our method successfully prevents **Google and Microsoft Bing** from retrieving location information while ensuring imperceptible modifications, highlighting our method's practical superiority.

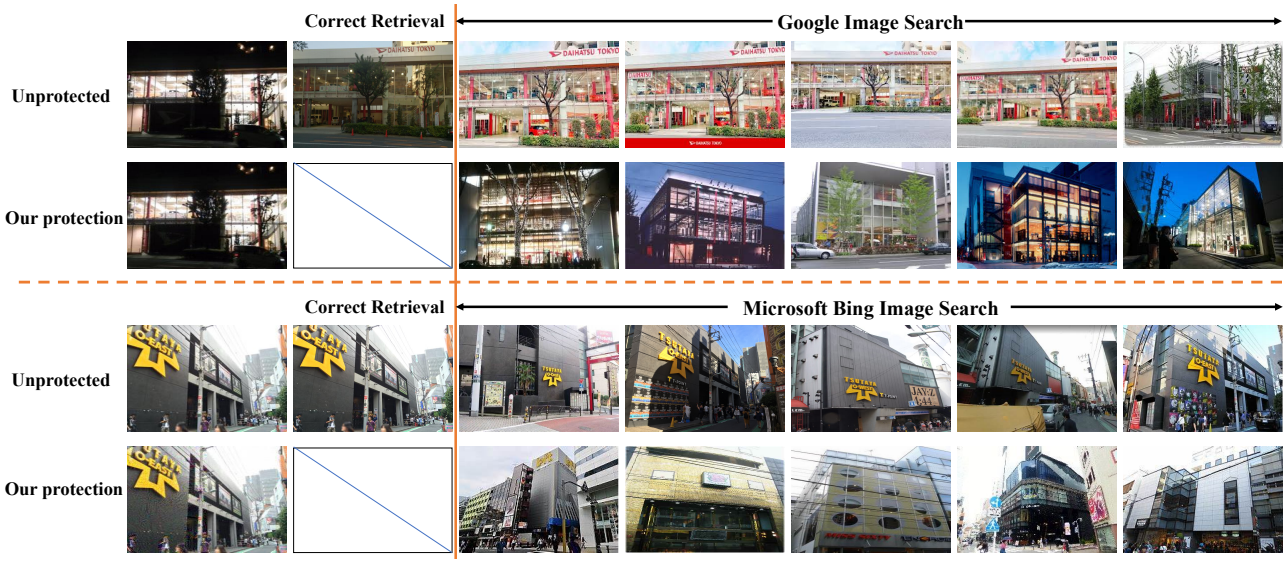

Figure 2. Protection on Commercial APIs. Our method successfully prevents **Google and Microsoft Bing** from retrieving location information while ensuring imperceptible modifications, highlighting our method's practical superiority.

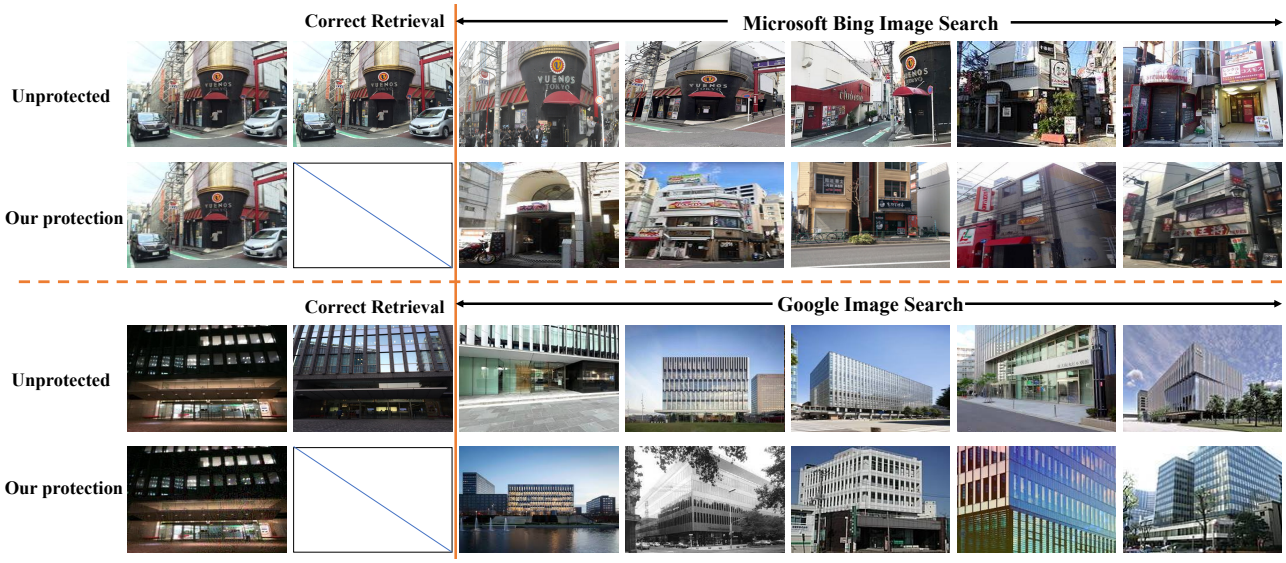

Figure 3. Protection on Commercial APIs. Our method successfully prevents **Google and Microsoft Bing** from retrieving location information while ensuring imperceptible modifications, highlighting our method's practical superiority.