

GEO-Detective Unveiling Location Privacy Risks in Images with LLM Agents

👤 Xinyu Zhang, Yixin Wu , Boyang Zhang , Chenhao Lin ,
Chao Shen , Michael Backes , Yang Zhang

📍 CISPA Helmholtz Center for Information Security



paper

code



CISPA

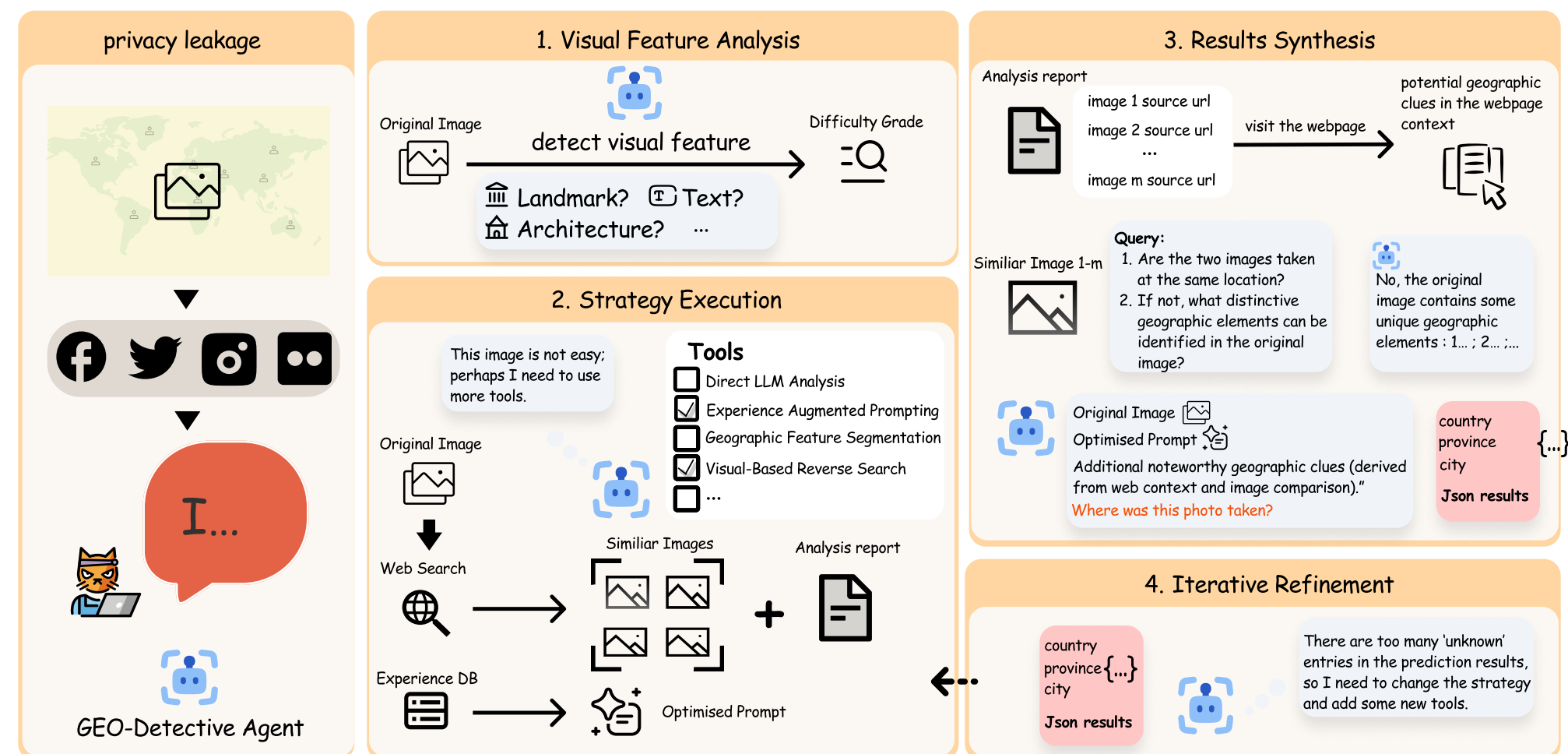


Introduciton

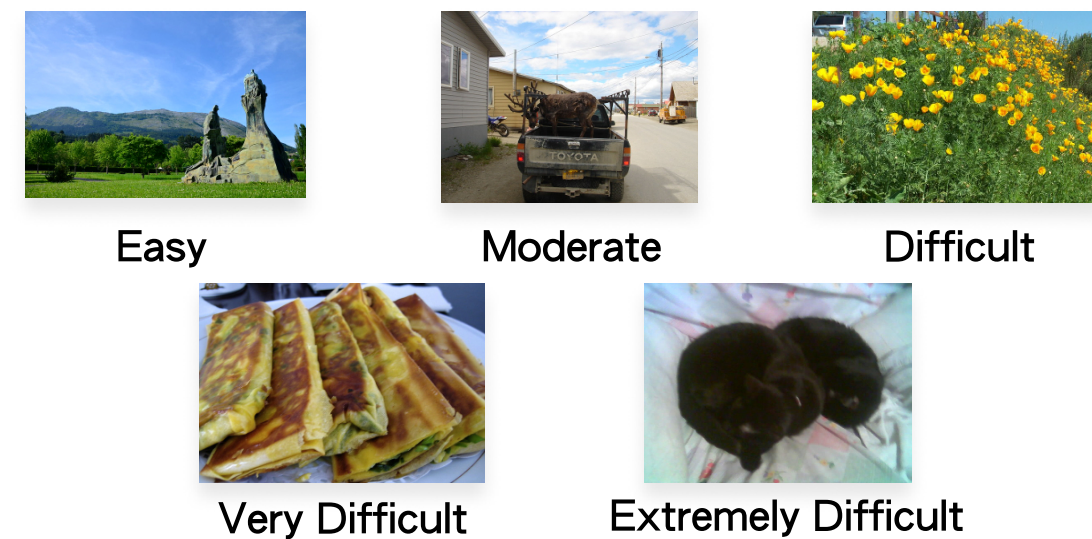
- Images can reveal location cues even after metadata such as EXIF is removed.
- LVLMS combined with web tools lower the expertise barrier, making image geolocation attacks more scalable.
- Existing approaches are either coarse-grained or not designed for adaptive, adversarial geolocation inference.

Can a difficulty-aware LLM agent combine visual reasoning, external tools, and iterative evidence gathering to infer locations from sparse-cue images—and can existing defenses still protect users?

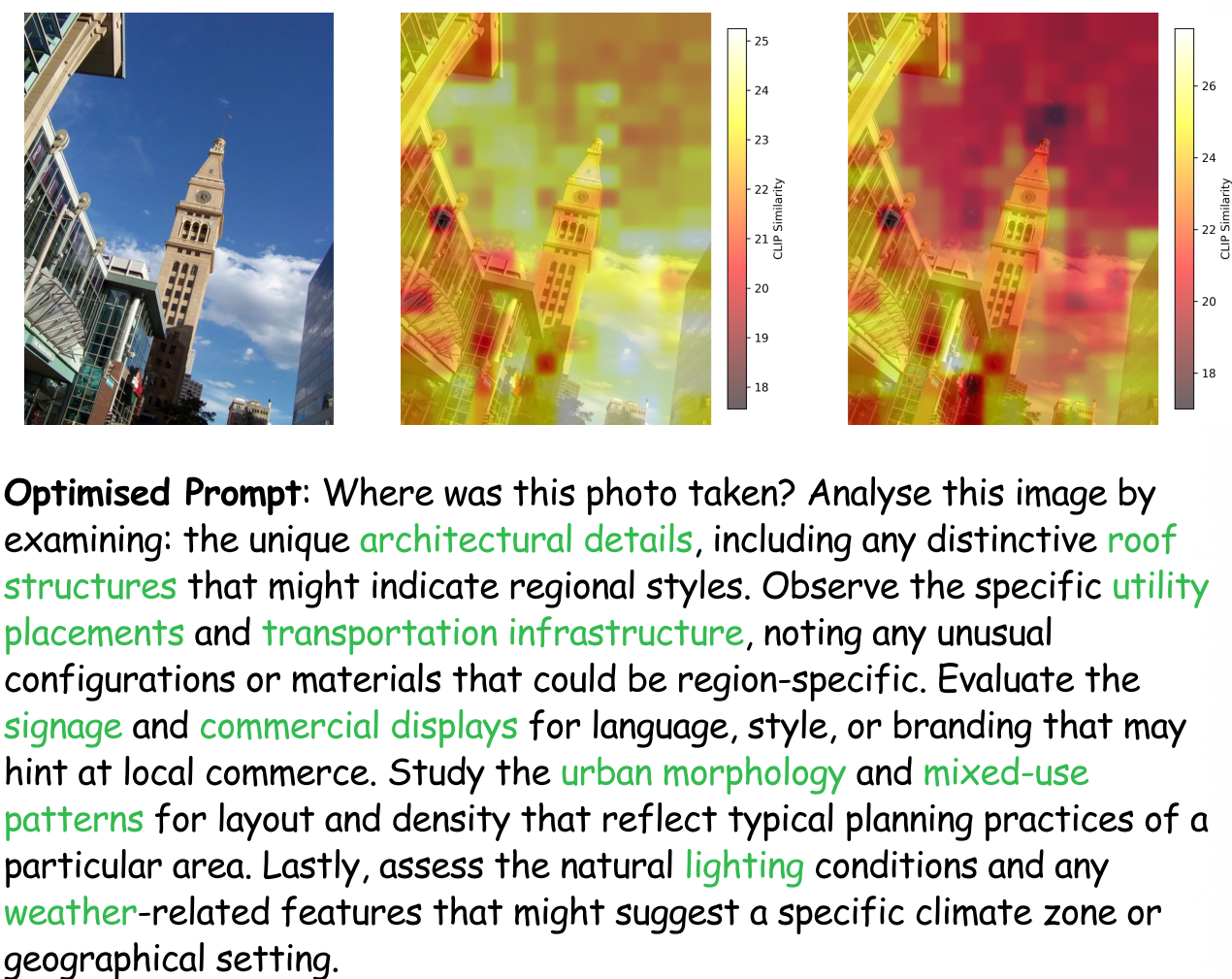
Method



Difficulty Assessment



Optimised Prompt



Experiments

Comparison with existing geolocation methods on IM2GPS3K.

Type	Method	@1km	@25km
Agent	GEO-Detective (Ours)	11.3	47.5
	GeoMiner (Luo et al., ICLR'26)	10.8	46.7
	smileGeo (Han et al., KDD'25)	10.9	38.2
LVLM	G3 (Jia et al., NeurIPS'24)	16.6	40.9
	Img2Loc (Zhou et al., SIGIR'24)	15.3	39.8
	GeoReasoner (Li et al., ICML'24)	9.9	33.8
Trained	PIGEON (Haas et al., CVPR'24)	11.3	36.7
	GeoCLIP (Vivanco et al., NeurIPS'23)	14.1	34.5

Accuracy comparison of the baseline LVLM and GEO-Detective across difficulty levels.

