The Crowd Wisdom for Location Privacy of Crowdsensing Photos: Spear or Shield?

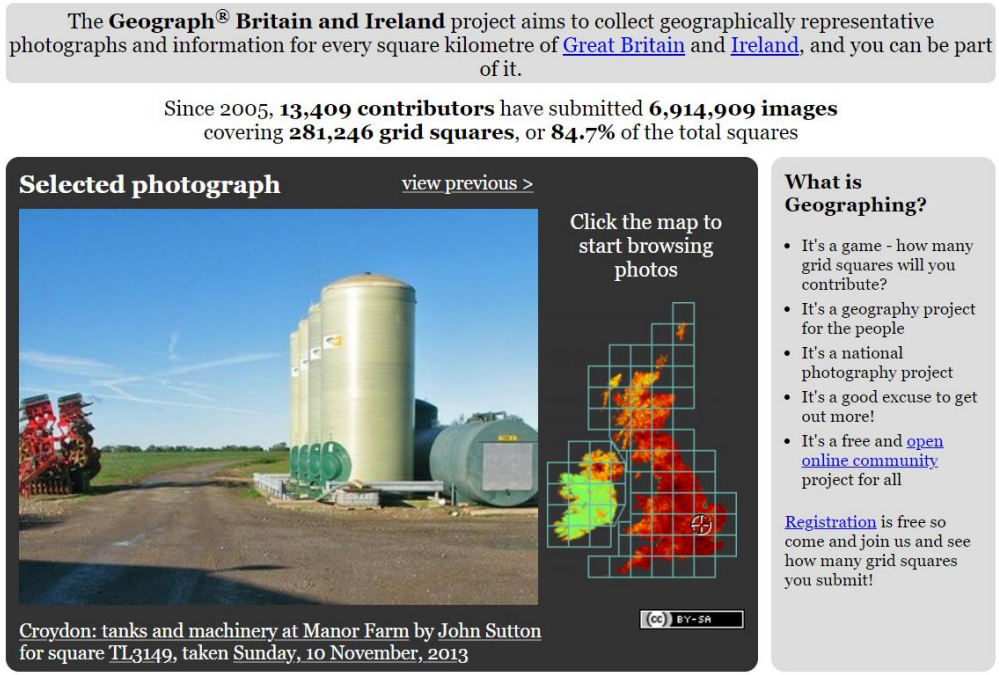
Tongqing Zhou[*], Zhiping Cai[*], Fang Liu[#]

[*] National University of Defense Technology, [#] Hunan University

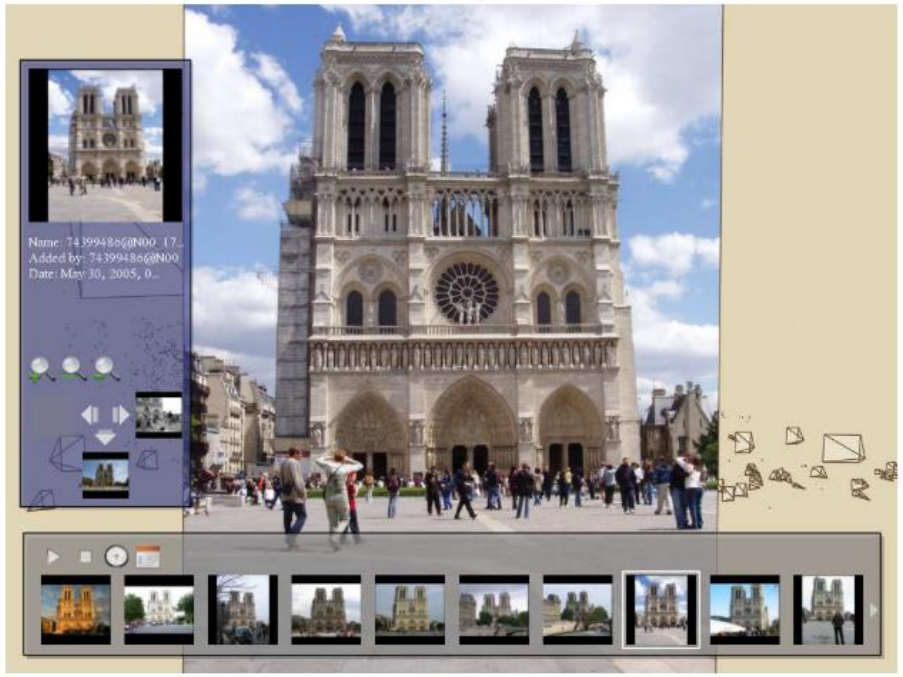
UBiCOMP, Sept. 2021

Background of Photo Crowdsensing

- Photo crowdsensing incorporates the mobile crowd into visual sensing for monitoring and understanding the physical world.
- Representative applications include: city viewing[Geograph®, Phototourism'06] and event sensing[CrowdStory'17].



Source: https://www.geography.org.uk



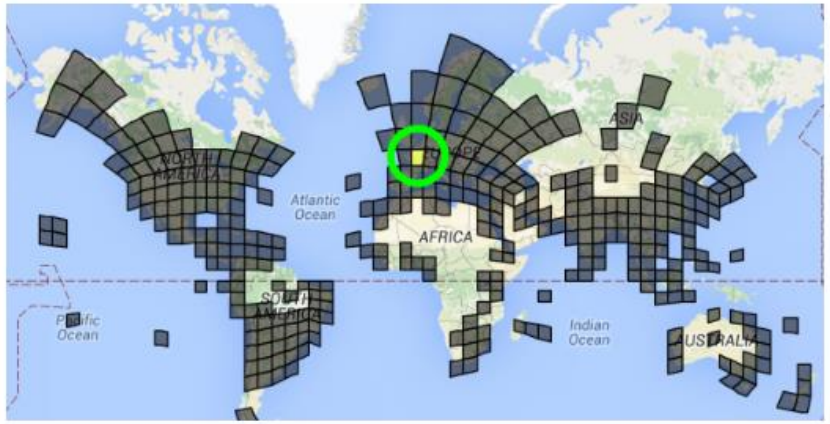
Source: http://phototour.cs.washington.edu/

Privacy of Photo Crowdsensing

- A serious concern of the crowd/participants: contributing real-world photos may expose their locations.
- Even perfectly hiding the raw location, a participant's location can still be inferred from its photos.

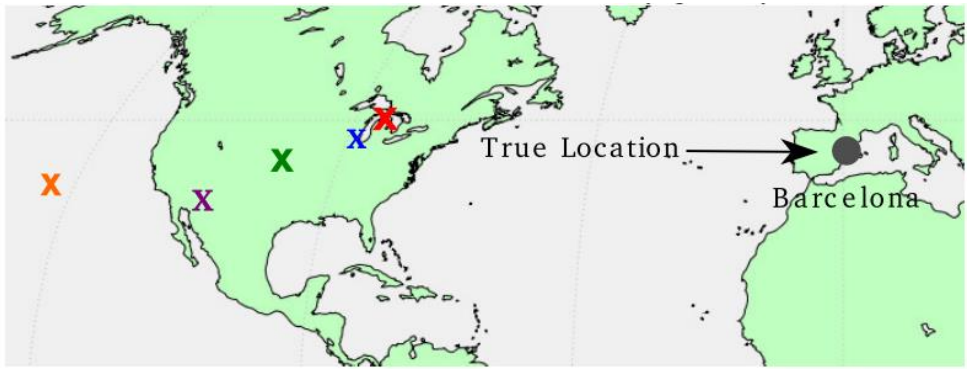
Threat: Google's PlaNet [ECCV'16]

Regarding each location with sufficient photos as a class and training a deep learning model for location inference.



Protection: Photo pruning [AAAI'20]

Degrading the classifier's inference accuracy by pruning the submission photo collection before posted publicly.



Our Motivations

- Usually no prior knowledge for the uncharted target of photo crowdsensing.
- Hence, for the practically no-references-situations, we investigate:
  - Would one's involvement in a crowd during sensing increase its risk of location disclosure?

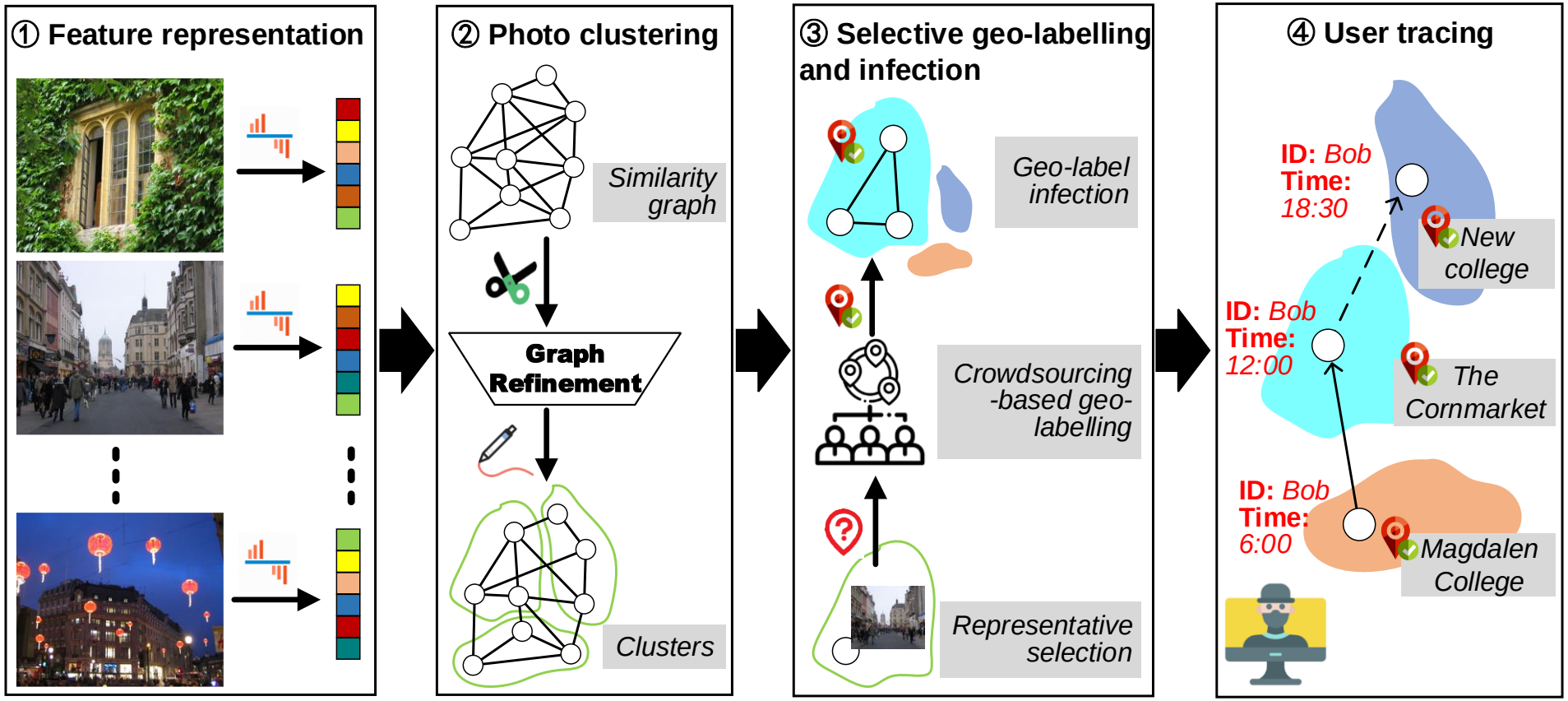
Is the crowd wisdom a spear?

  - Can the crowd of users take active measures collaboratively to avoid such information leakage?

Is the crowd wisdom a shield?

The Spear: No-reference Location Inference

- Building blocks: ① feature representation knowledge of an existed crowd of photos; ② visual correlations of crowdsensing photos; ③ mobile crowdsourcing for geo-annotation.



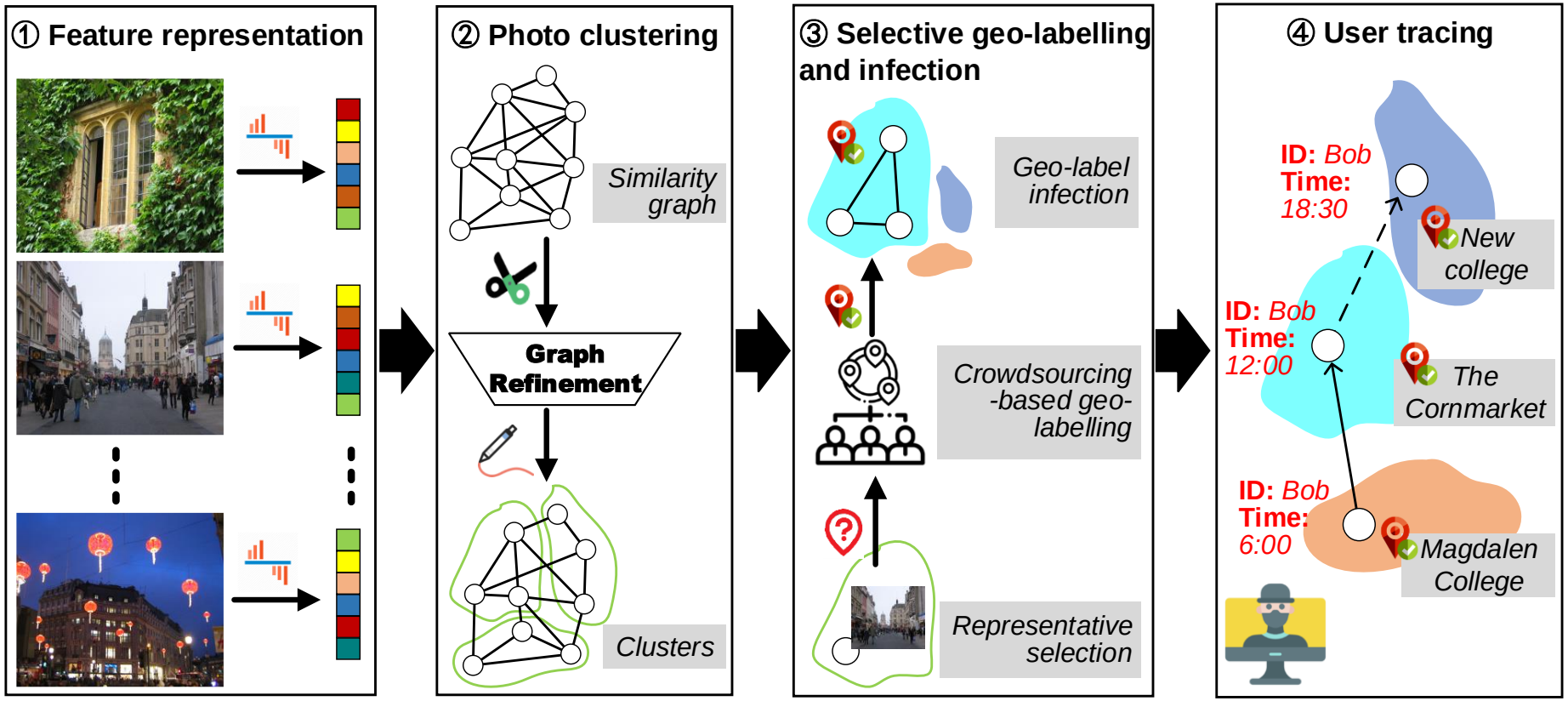
The Spear: No-reference Location Inference

Step 1. Extract features using a BoVW model and a deep model.

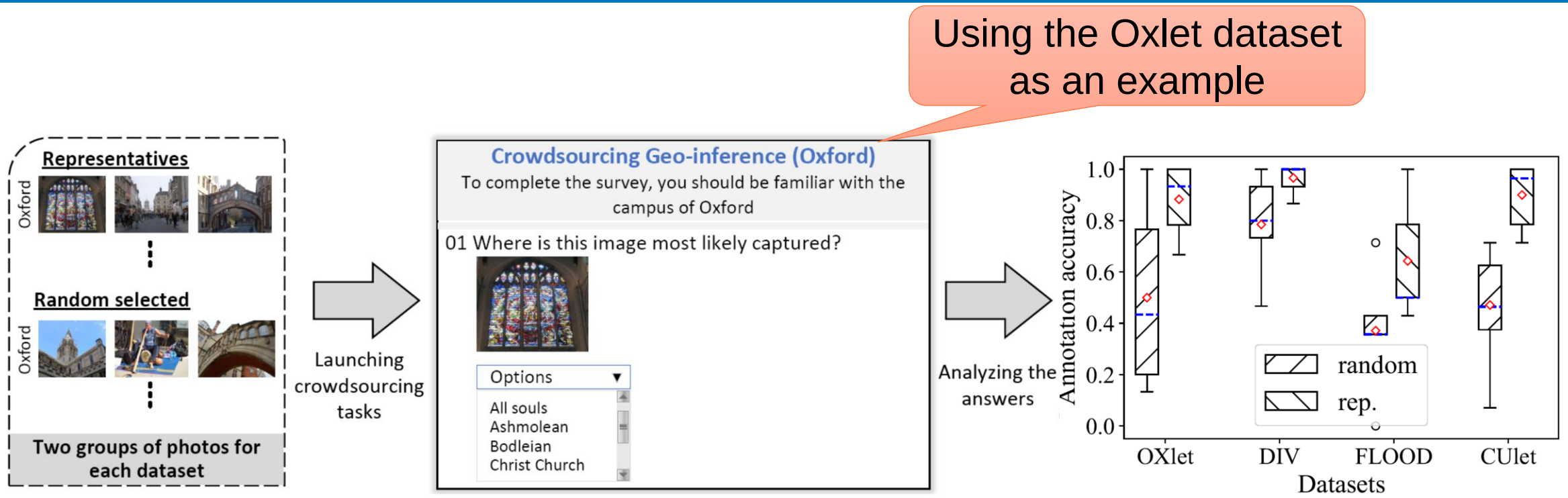
Step 2. Perform spectral clustering on the top-k refined similarity graph.

Step 3. Select a seed in each cluster for geo-labelling and infer the rests.

Step 4. Combine several inferred locations into a track.

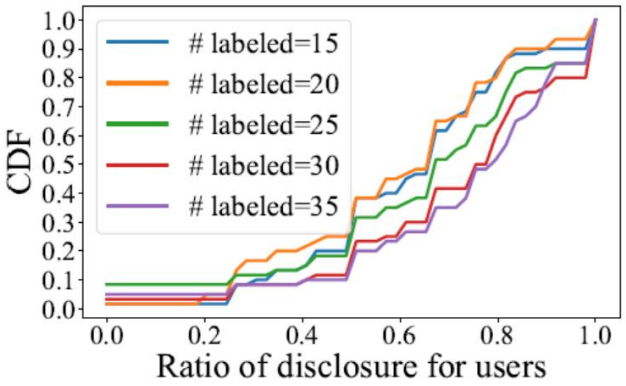


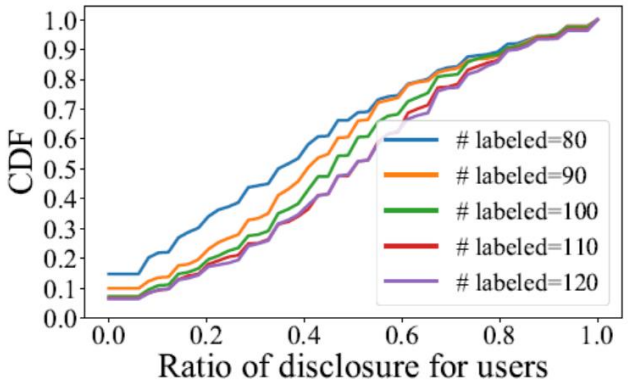
Experiments on the Spear

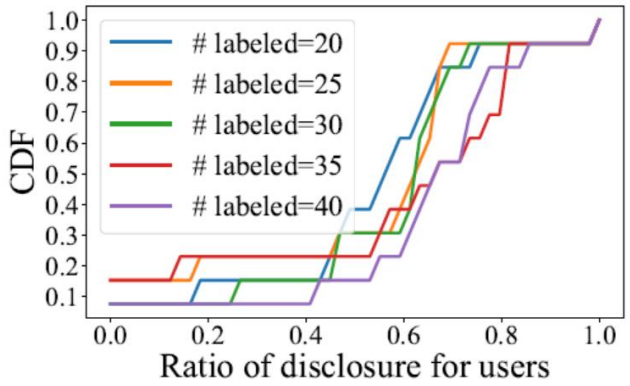


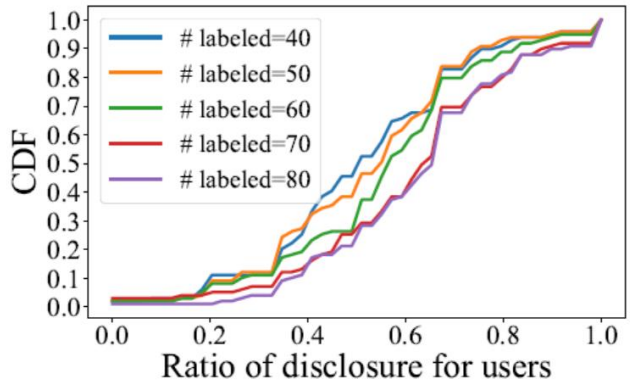
- We construct crowdsourcing tasks for the selected photos using the Tencent Questionnaire.
- The correlations among a crowd of photos can lead to more accurate geographic annotation.

Experiments on the Spear







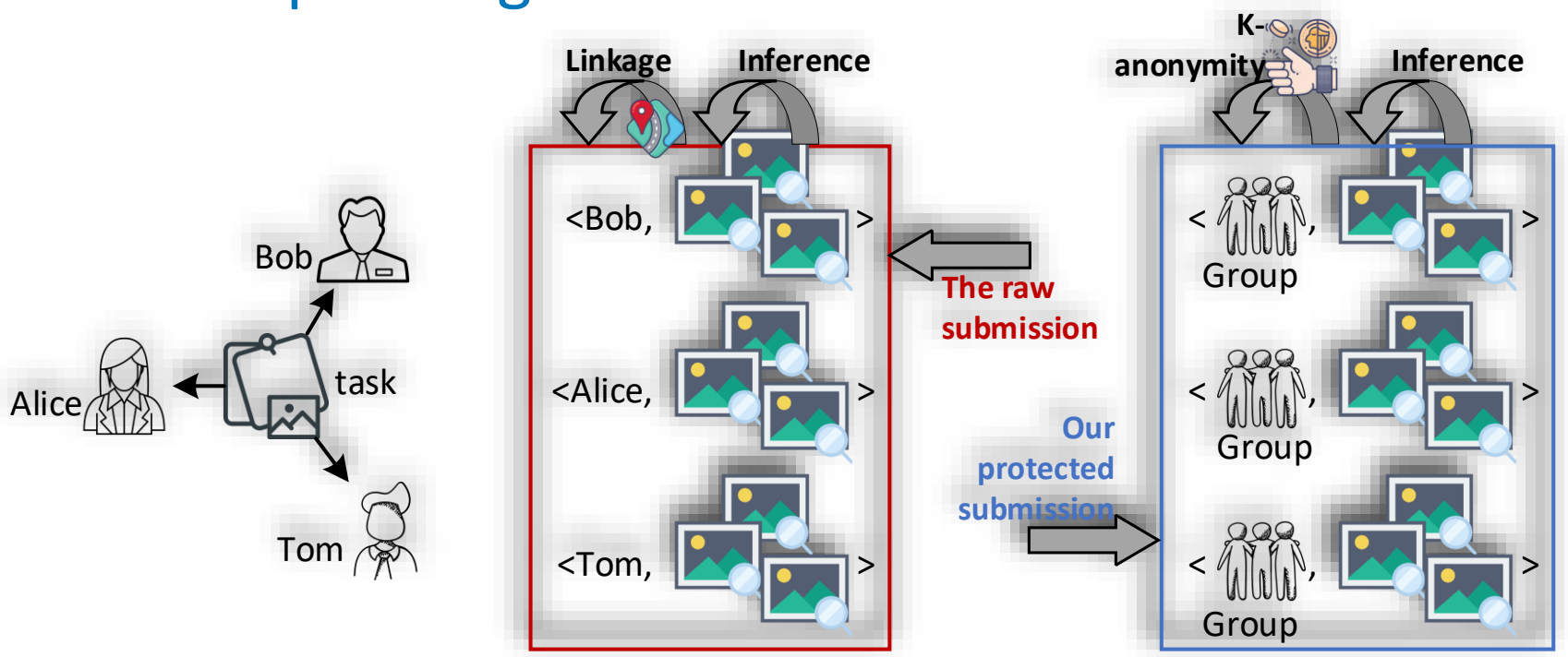


Ratios of correctly geo-identified photos for each user (From Left to Right: OXlet, DIV, FLOOD, CUlet)

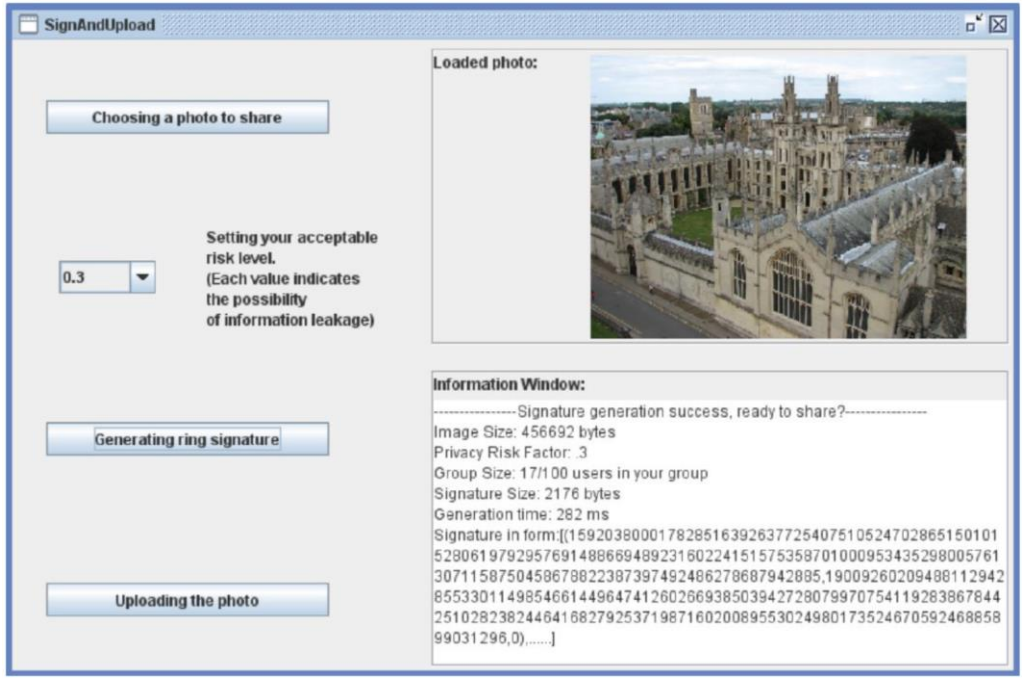
- Almost over 80% of users get at least one location correctly inferred (y-values of the curves for the ratio of disclosure 0), indicating serious privacy threats.
- Contributing submissions together with a crowd of photos will, unfortunately, increase one's risk of being geo-identified.

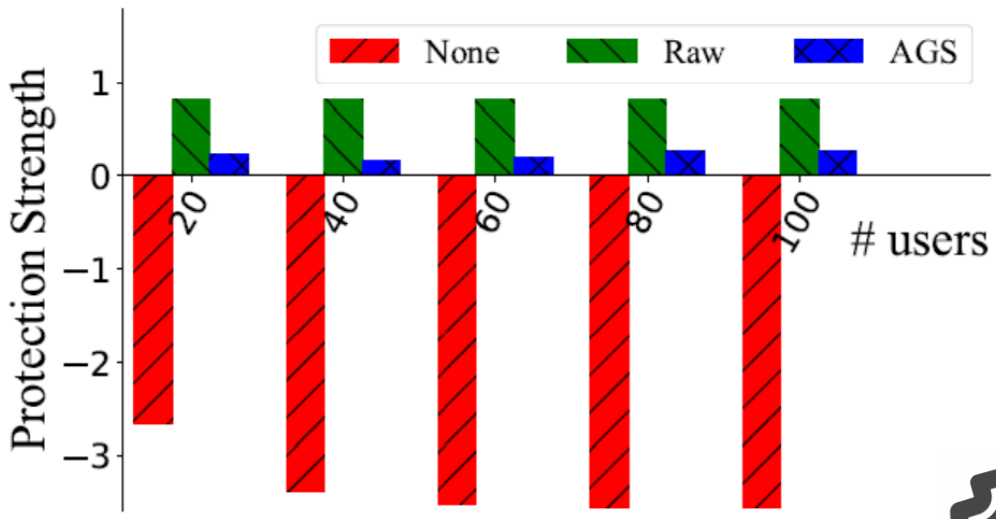
The Shield: Signing photos with ring signature

- Basic idea: Users of the same task share the same security concern, thus making their community itself a nature camouflage.
- Overview: Modify the ring signature technique to adaptatively grouping users and cut off the linkage between inferred locations and their corresponding users.



The Shield: Implementation & Experiments





- We develop a light-weight prototype for the defense model.
- Supporting user to specify its privacy preferences.
- We theoretically prove the security of our defense model (i.e., AGS).
- Our AGS can provide efficient privacy protection given all the preferences.

Thanks for your attention!

Q&A

Contact Information: zhoutongqing@nudt.edu.cn