ImageProof: Enabling Authentication for Large-Scale Image Retrieval

PI : **Prof. XU Jianliang**

OBJECTIVES

1. To design novel frameworks and query authentication algorithms for the verification of large-scale image retrieval.
2. To propose novel ADSs and several optimization techniques for robust and efficient authenticated top-k image queries.
3. To evaluate the proposed techniques by combining theoretical analysis and empirical experiments.

HIGHLIGHTS

Problem Statement

- **Outsourced Content-Based Image Retrieval**
  - o The image owner outsources its image retrieval system to a third party service provider (SP).
  - o SIFT-based image retrieval: bag-of-visual-words (BoVW) encoding and inverted index search
  - o Top-k similarity query based on randomized k-d tree and impact-ordered inverted index.
- **Threat Model**
  - o The SP could return incorrect or tampered search results.
  - o Soundness: The results must be the outsourced images which have not been tampered with.
  - o Completeness: The results include the k most similar images, i.e., the similarity values of the other images are smaller than those of the returned images.

ImageProof System

- **Authenticated Data Structures**
  - o Merkle Randomized k-d Tree
  - o Merkle Inverted Index With Cuckoo Filters
- **Authenticated Query Processing**
  - o Search the approximate nearest neighbors and generate verification object (VO) for the BoVW encoding.
  - o Search the top-k images and generate the VO for the inverted index search.
  - o Send the VOs, corresponding image signatures, and the top-k results to the client.
- **Result Verification**
  - o Check the correctness of the termination conditions.
  - o Verify the integrity of the BoVW encoding and invert index search.
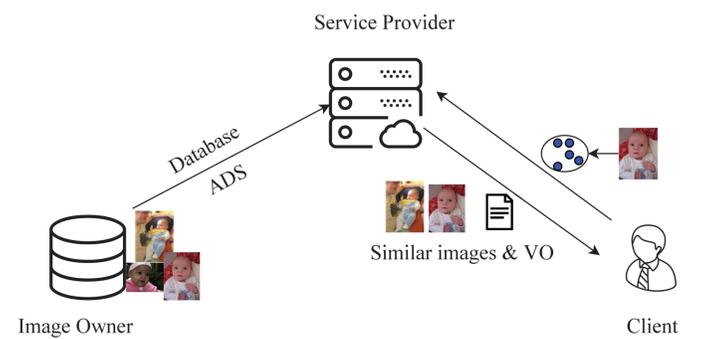 - o Verify the integrity of raw image data.

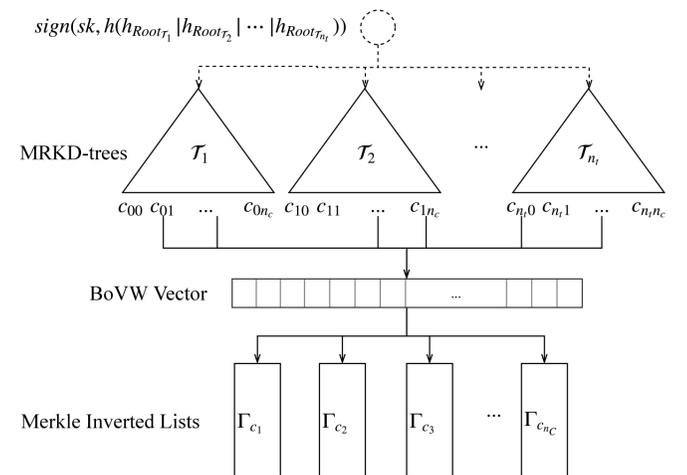**Fig. 1**: System Model of Authenticated Image Retrieval System
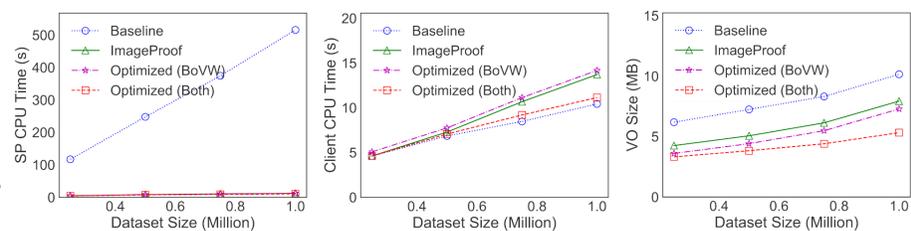

Fig. 2: Overview of ADSs in ImageProof

Fig. 3: Performance Evaluation

SELECTED PUBLICATIONS

1. S. Guo, J. Xu, C. Zhang, C. Xu, and T. Xiang, "ImageProof: Enabling Authentication for Large-Scale Image Retrieval," in *Proceedings of the 35th IEEE International Conference on Data Engineering* (ICDE '19), Macau SAR, China, 2019, pp. 1070–1081.
2. C. Zhang, C. Xu, J. Xu, and B. Choi, "Distributed kNN Query Authentication," in *Proceedings of the 19th IEEE International Conference on Mobile Data Management* (MDM '18), Aalborg, Denmark, 2018, pp. 167–176.
3. C. Xu, Q. Chen, H. Hu, J. Xu, and X. Hei, "Authenticating Aggregate Queries over Set-Valued Data with Confidentiality," *IEEE Transactions on Knowledge and Data Engineering* (TKDE), vol. 30, no. 4, pp. 630–644, Apr. 2018.