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**
  - The image owner outsources its image retrieval system to a third party service provider (SP).
  - SIFT-based image retrieval: bag-of-visual-words (BoVW) encoding and inverted index search
  - Top-k similarity query based on randomized k-d tree and impact-ordered inverted index.

- **Threat Model**
  - The SP could return incorrect or tampered search results.
  - Soundness: The results must be the outsourced images which have not been tampered with.
  - 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**
  - Merkle Randomized k-d Tree
  - Merkle Inverted Index With Cuckoo Filters

- **Authenticated Query Processing**
  - Search the approximate nearest neighbors and generate verification object (VO) for the BoVW encoding.
  - Search the top-k images and generate the VO for the inverted index search.
  - Send the VOs, corresponding image signatures, and the top-k results to the client.

- **Result Verification**
  - Check the correctness of the termination conditions.
  - Verify the integrity of the BoVW encoding and invert index search.
  - Verify the integrity of raw image data.

SELECTED PUBLICATIONS