2021 IEEE International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS) | 978-1-6654-0610-9/21/$31.00 ©2021 IEEE | DOI: 10.1109/CSITSS54238.2021.9683330

Privacy Preserving Image Matching Scheme with Aggregated Local Descriptors

Dhafer G. Honi
Computer Science Dept.
University of Basrah
Basrah, Iraq
dhafer.honi@uobasrah.edu.iq

Husam A. Abdulmalik
Computer Science Dept.
University of Basrah
Basrah, Iraq
husam.akif@uobasrah.edu.iq

Ayad I. Abdulsada
Computer Science Dept.
University of Basrah
Basrah, Iraq
ayad.abdulsada@uobasrah.edu.iq

Salah Al-Darraji
Computer Science Dept.
University of Basrah
Basrah, Iraq
aldarraji@uobasrah.edu.iq

***Abstract*—Detecting similar images, without violating their privacy, is a desirable method for many real-world applications. Existing schemes are based either on global features that are too rigid to describe images or local features which achieve more accurate results with higher complexity. The current local feature aggregation methods rely on constructing and sharing a visual word vocabulary, which leads to serious privacy concerns. In this paper, we proposed efficient schemes, of different security guarantees, for matching private images while maintaining their privacy. To do so, we developed a new method for aggregating the local features, by utilizing the locality-sensitive hashing functions without the need for predefined vocabulary. Extensive experiments on real-world datasets demonstrate the practical usage and security of our schemes.**

***Index Terms*—Image similairty, Local senesitive hashing, Multi party computing, Privacy preserving**

I. Introduction

Image similarity detection plays an essential role in variant real-world domains such as web image search [1] and content based image retrieval (CBIR) [2]. When digital images are centralized, the issue of evaluating their similarity scores is straightforward because the computation is carried out in place. However, digital data needs to be distributed, without complete mutual trust, among several parties due to glob- alization and functioning communities. In this case, image similarity detection is difficult, mainly due to data distribu- tion. Furthermore, this process becomes harder when two or more parties want to evaluate the similarity of their private collections without compromising the privacy of their data. Therefore, it is a challenging problem to design an efficient scheme that evaluates image similarity among several parties such that no sensitive information is leaked during the process. In this paper, we address such a challenge by presenting a secure scheme for evaluating the similarity of distributed im- age collections. To demonstrate the importance of this problem considers the following real-world applications. Suppose the existence of two security agencies who hold image collections of individual persons. Suppose one agency wants to identify how similar one of its images is in comparison to the collection of the other party by computing specific similarity metrics between their respective inputs. To protect data privacy, no party is allowed to reveal its private images to others. In the literature, this problem is known as secure image similarity detection (SISD). When the similarity score is above a certain threshold, the involved parties take further action to disclose such matched images.

Describing images as a set of local vectors is commonly used for vital applications such as content-based image re- trieval and image classification. However, under such rep- resentation, a large number of features are extracted from each image. Thus, distance computation between pairs of images requires heavy computational overhead. Furthermore, sophisticated algorithms are needed to deal with images with a variable number of features.

To make local features more practical for large datasets, several methods have been proposed to quantize (aggregate) image feature descriptors into a single compact vector at the cost of accuracy. Bag-of-features (BoF) [3] and vector of locally aggregated descriptors (VLAD) [4] are two well-known aggregation methods. Aggregation methods work by generating a vocabulary $\mathcal{V}$ of $\mathcal{K}$ centers from the entire feature space. Commonly, $\mathcal{K}$ -mean clustering algorithm is used for vocabulary generating. Image feature descriptors $f_i \in \mathbb{R}^d$ are transformed to integer tags between 1 and $\mathcal{K}$ according to their similarity for all vocabulary centers. Then, a histogram of size $\mathcal{K}$ is generated for each image, where each of its entries is associated with a certain tag and includes the number of local features that are mapped to that tag. Herein, matching a pair of images is reduced to measure the distance between their corresponding histograms.

When features aggregation methods are shifted towards the SISD problem, significant privacy concerns arise. This is because one party has to reveal its entire vocabulary to create the ability for the other party to construct a valid histogram for its query image. However, the adversary party can utilize such sensitive values to infer the underlying image collection. For this reason, we proposed a new aggregation method for local descriptors, which generates a compact vector (index) for each image without the need for a predefined vocabulary. Our aggregation method utilized local sensitive hashing [5] functions and Bloom filter [6] data structure.

Contribution. Our contributions can be summarized as follows:

1) A local features-based SISD is proposed to detect similar images in an efficient way while protecting their privacy.

978-1-6654-0610-9/21/$31.00 ©2021 IEEE