applied sciences

MDPI

Article

SEPIM: Secure and Efficient Private Image Matching †

Zaid Ameen Abduljabbar [1,2], Hai Jin [1,*], Ayad Ibrahim [2], Zaid Alaa Hussien [1,3], Mohammed Abdulridha Hussain [1,2], Salah H. Abbdal [1] and Deqing Zou [1]

1 Cluster and Grid Computing Lab, Services Computing Technology and System Lab, School of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan 430074, China; alsulamizaid@gmail.com (Z.A.A.); zaidpc2005@gmail.com (Z.A.H.); mohsubber@gmail.com (M.A.H.); salahrfesh@gmail.com (S.H.A.); deqingzou@hust.edu.cn (D.Z.)

2 Department of Computer Science, University of Basrah, Basrah 61001, Iraq; mraiadibraheem@gmail.com

3 Department of Management, Southern Technical University, Basrah 61001, Iraq

* Correspondence: hjin@hust.edu.cn; Tel.: +86-27-8754-3529 (ext. 8033); Fax: +86-27-8755-7354

† This paper is an extended version of paper published in the 11th International Conference on Green, Pervasive and Cloud Computing (GPC'16), Xi'an, China, 6–8 May 2016.

Academic Editor: Antonio Fernández-Caballero
Received: 24 May 2016; Accepted: 22 July 2016; Published: 29 July 2016

Abstract: Matching a particular image within extensive datasets has become increasingly pressing in many practical fields. Hence, a number of matching methods have been developed when confidential images are used in image matching between a pair of security agencies, but they are limited by either search cost or search precision. In this paper, we propose a privacy-preserving private image matching scheme between two parties where images are confidential, namely secure and efficient private image matching (SEPIM). The descriptor set of the queried party needs to be generated and encrypted properly with the use of a secret key at the queried party side before being transferred to the other party. We present the development and validation of a secure scheme to measure the cosine similarity between two descriptor sets. To hasten the search process, we construct a tree-based index structure by utilizing the *k*-means clustering algorithm. The method can work without using any image encryption, sharing, and trusted third party. SEPIM is relatively efficient when set against other methods of searching images over plaintexts, and shows a higher search cost of just 14% and reduction in search precision of just 2%. We conducted several empirical analyses on real image collections to demonstrate the performance of our work.

Keywords: secure private image matching; feature protection; *k*-means clustering; secure multiparty computing (SMC); speeded up robust features (SURF) descriptors; homomorphic encryption

1. Introduction

The recent explosion of the World Wide Web and increasing interest from various multimedia fields has seen a concurrent significant elevation of the importance of digital images. The increased requirements placed on efficient private image matching (PIM) techniques in various applications interacting with reality have coincided with this. These applications may include social media [1,2] business community [3], e-health [4], and criminal suspect identification, etc. In the context of private image retrieval, similar images are usually brought together such that similar images can be retrieved efficiently once a query image is sent. In general, the PIM method refers to a process whereby a pair of parties determines their common matching values or similarities, whilst maintaining privacy for their own data. Hence, PIM only requires the magnitude of similarity, rather, content similarity.

According to [5], private matching (PM) can be classified into three scenarios. In the first scenario, the parties involved, namely *Alice* and *Bob*, must both learn the final results of PM as a result of the so-called symmetric PM. The second scenario involves a non-symmetric PM where only one party