Towards Secure 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
zaidalsulami@yahoo.com, hjin@hust.edu.cn

[2] University of Basrah, Basrah, Iraq

[3] Southern Technical University, Basrah, Iraq

Abstract. Currently, image matching is being used in many daily life applications such as *content-based image retrieval* (CBIR), computer vision, and near duplicate images. Hence, a number of matching methods have been developed. However, most proposed methods do not address the challenges involved when confidential images are used in image matching between two security agencies. Thus, interest to develop a secure method, particularly one that can be used in privacy-preserving image matching, is growing. This paper addresses the challenge of privacy-preserving image matching between two parties where images are confidential. 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. The method can work without using any image encryption, sharing, and trusted third party. We conduct several empirical analyses on real image collections to demonstrate the performance of our work.

Keywords: Secure private image matching · Feature protection · Secure multiparty computing · Surf descriptors · Homomorphic encryption

1 Introduction

Digital images have become a significant part of our lives because of the development of the Internet and the growing demand from various multimedia fields. This demand raises the need for efficient and robust *private image matching* (PIM) methods in many real-world applications, including social media [1,2] business community [3], and e-health [4]. 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, PIM method is a set of operations through which two parties determine their common matching values without disclosing extra information. Hence, PIM only requires the magnitude of similarity rather contents similarity.

X. Huang et al. (Eds.): GPC 2016, LNCS 9663, pp. 301–315, 2016.
DOI: 10.1007/978-3-319-39077-2_20