2016 IEEE TrustCom-BigDataSE-ISPA

Privacy-preserving Image Retrieval in IoT-Cloud

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], 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
[2]University of Basrah, Basrah, Iraq. [3]Southern Technical University, Basrah, Iraq
Email: zaidalsulami@yahoo.com, hjin@hust.edu.cn

***Abstract*—Within the IoT-cloud, security has a very significant role to play. One of the best means by which the security and privacy of an image may be safeguarded confidentially is through encryption. However, this methodological process engenders a disadvantage in that it is difficult to search through encrypted images. A number of different means by which encrypted image can be searched have been devised; however, certain security solutions may not be used for smart devices within an IoT-cloud due to the fact that such solutions are not lightweight. We present a lightweight scheme that is able to provide a content-based search through images that have been encrypted. More specifically, images are represented using local features. A similar methodology further described in [1] is also used for image similarity discrimination. In addition, we use a hashing method concerning a *locality sensitive hash* (LSH) so that the searchable index can be devised. The use of the LSH index means that the proficiency and effectiveness of the system is increased, which allows the retrieval of only relevant images with a minimum number of distance evaluations. Refining vector techniques are used to refine relevant results efficiently and securely. Our index construction process ensures that stored data and trapdoors are kept private.**

***Keywords*—Searchable encryption; secure image retrieval; IoT-cloud; LSH; local feature; smart devices**

I. Introduction

Searching a particular image within extensive datasets using smart mobility devices has become increasingly pressing in many practical fields, such as criminal suspect identification, advertising, disease detection and diagnosis, and online shopping. Particularly with regard to third and fourth generation cell phones, smart devices users are able to connect to the internet speedily and relay, send and acquire images with ease while simultaneously collecting a number of images from various sources. However, the management and retention of these images makes significant demands in terms of storage and its associated costs and computing power. These facilities may be unavailable for all smart devices users, particularly those users of lightweight smart devices such as iPhones [2].

Due to significant advances in cloud computing technologies, several companies such as Apple, Google, Microsoft and Amazon have adopted cloud computing technology to support users of smart devices with facilities that include mass storage and large-scale data management services at an efficient cost [3]. However, despite the technical and economic benefits of cloud computing technology, moving particularly vulnerable or important images to insecure cloud servers presents difficulties in safeguarding users' private images. In order to combat unsolicited access attempts, users generally choose to encrypt such images prior to outsourcing them to the cloud. However, this presents a notable barrier when traditional encryption services are used and when searching for and through encrypted images. Additionally, despite the computing power of smart devices increasing, it is currently unable to achieve the capacity of personal computers.

Simply stated, modern *informational retrieval* (IR) systems such as Google have introduced an original technology that permits clients to send an image as a query and then search through images retained on the database in question, wherein those images that are comparable in visual content are identified. Original technological processes are referred as *content-based image retrieval* (CBIR). In consequence of this, the development of a *searchable encryption* (SE) scheme that is able to manage image-based searches in a proficient and precise manner is needed.

More precisely, focus has lately shifted to questions concerning privacy in the context of searching groups of encrypted images [4]–[7]. These concerns primarily concentrate on global features, and are, critically, not lightweight and consequently are not suitable for smart portable applications and other instances where available computing power is comparatively low. The only local-feature based CBIR available to date is the approach further described by Xia et al. in 2015 [8]. In contrast with global feature approaches, local-feature based CBIR achieves enhanced accuracy in terms of retrieval, but requires comparatively complex metrics relating to distance; for example, the *earth mover's distance* (EMD). Nevertheless, interest and provision of privacy-preserving CBIR services are not forthcoming with respect to smart mobility devices communicating in the IoT-cloud environment.

This paper's contributions are set forth below. Initially, we address the question of how to search and retrieve similar images between smart device users and the cloud server in a privacy-preserving manner without losing image confidentiality. Secondly, our scheme shall make use of *local-feature speeded up robust features* (SURF)-based CBIR with the appealing lightweight aspects of the [1]'solution as similarity metric to speed up the search process. LSH is employed to achieve high search index efficiency. Finally, our proposed scheme is able to index considerable numbers of databases containing images in an efficient manner, thereby lowering storage requirements as well as run time. Therefore, our scheme marks a considerable step towards practical deployment of privacy-preserving data hosted within an IoT-cloud environment.

2324-9013/16 $31.00 © 2016 IEEE
DOI 10.1109/TrustCom.2016.140