


Efficient encrypted image retrieval in IoT-cloud with multi-user authentication

International Journal of Distributed
Sensor Networks
2018, Vol. 14(2)
© The Author(s) 2018
DOI: 10.1177/1550147718761814
journals.sagepub.com/home/dsn


Mustafa A Al Sibahee¹, Songfeng Lu¹, Zaid Ameen Abduljabbar²,
Ayad Ibrahim², Zaid Alaa Hussien³, Keyan Abdul-Aziz Mutlaq² and
Mohammed Abdulridha Hussain²

Abstract

Encryption is one of the best methods to safeguard the security and privacy of an image. However, looking through encrypted data is difficult. A number of techniques for searching encrypted data have been devised. However, certain security solutions may not be used in smart devices in IoT-cloud because such solutions are not lightweight. In this article, we present a lightweight scheme that can enable a content-based search through encrypted images. In particular, images are represented using local features. We develop and validate a secure scheme for measuring the Euclidean distance between two feature vectors. In addition, we use a hashing method, namely, locality-sensitive hashing, to devise the searchable index. The use of an locality-sensitive hashing index increases the proficiency and effectiveness of a system, thereby allowing 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. Our system also efficiently supports multi-user authentication by avoiding the expensive traditional method, which enables data owners to define who can search for a specific image. Compared with other similarity-based encryption methods predicated upon searchability, the option presented in this study offers superior search speed and storage efficiency.

Keywords

Searchable encryption, secure image retrieval, IoT-cloud, locality-sensitive hashing, local feature, smart devices, multi-user authentication

Date received: 23 September 2017; accepted: 15 January 2018

Handling Editor: Geng Yang

Introduction

The need to conduct searches within extensive datasets using smart mobile devices has become increasingly vital in a number of different disciplines.¹ Practical applications that require this process include medical diagnosis, criminal identification, and Internet retail and advertising. In the case of third- and fourth-generation smart devices, users can connect rapidly to the Internet and easily relay, send, and acquire images while simultaneously collecting a number of images

from various sources. However, the management and retention of these images make significant demands in

¹School of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan, China

²University of Basrah, Basra, Iraq

³Southern Technical University, Basra, Iraq

Corresponding author:

Mustafa A Al Sibahee, School of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan 430074, China.
Email: mustafa.a@hust.edu.cn

