J. Vis. Commun. Image R. 40 (2016) 111–117

Contents lists available at ScienceDirect

J. Vis. Commun. Image R.

journal homepage: www.elsevier.com/locate/jvci

Short Communication

Encrypted JPEG image retrieval using block-wise feature comparison ☆

Hang Cheng [a,b,*], Xinpeng Zhang [a,c], Jiang Yu [a], Yuan Zhang [a,d]

[a] School of Communication and Information Engineering, Shanghai University, Shanghai 200444, China
[b] College of Mathematics and Computer Science, Fuzhou University, Fuzhou 350108, China
[c] The Key Laboratory of Specialty Fiber Optics and Optical Access, Shanghai University, Shanghai 200444, China
[d] College of Information Engineering, Huzhou University, Huzhou 313000, China

ARTICLE INFO

Article history:
Received 14 January 2016
Revised 1 May 2016
Accepted 20 June 2016
Available online 21 June 2016

Keywords:
Image retrieval
Image encryption
JPEG image
Feature descriptor

ABSTRACT

This paper proposes a novel scheme for encrypted JPEG image retrieval, which includes image encryption and retrieval phases. Using the scheme, the content owner encrypts JPEG images by jointly applying permutation cipher and stream cipher to their corresponding bit-streams, and then transmits encrypted versions to a database server. With an encrypted query image, although the server learns nothing about the plaintext content, it may extract local statistical feature of intra-block AC coefficients using a new feature descriptor. Subsequently, exploiting block-wise feature comparison, the server can measure the similarity between encrypted query image and database image. After that, the encrypted images with plaintext content similar to the query image are returned to the authorized user. Experimental results show that the proposed scheme can ensure both format compliance and file size preservation while providing effective retrieval service in encrypted domain.

1. Introduction

With the rapid technological development of cloud computing, the users would like to store their multimedia data into the cloud for lower cost and more convenience. For privacy protection, the users tend to encrypt the multimedia data before transmission to the server, which may impede further processing operations, such as information retrieval. Therefore, it becomes highly desirable to develop retrieval techniques for the purpose of providing privacy-preserving and effective retrieval service in encrypted multimedia databases.

So far, a few effective techniques have been proposed for performing information retrieval in encrypted databases. Using the methods in [1–4], the presence or absence of a keyword in encrypted documents can be identified, and the plaintext keyword is not leaked to the server. In recent years, various secure keyword searchable schemes supporting more advanced searching functionalities have been proposed, such as secure ranked keyword search [5], privacy-assured similarity search [6] and [7–9]. In addition to the above text-based secure search schemes, there are also many works for performing image retrieval in encrypted domain. Shashank et al. [10] exploits hierarchical structures and hashing techniques to address the problem of one-way privacy search, i.e., query image by a user is encrypted, but the server database is public. Another similar work is also found in [11], where high-level discussion on one-way privacy search is given. However, in many cases both the server and the user need to protect their data confidential from each other. For the benefit of two parties, some related approaches have been developed in [12–15], which design similarity measurements for biometric recognition by adopting the additive homomorphic encryption technique. Although the homomorphic encryption based retrieval systems can obtain higher security, huge computation and communication cost make them difficult to practical applications. Compared to these methods, Lu et al. [16–18] investigate the retrieval of encrypted images from a practical perspective, where the server without anything about the plaintext content only provides storage and retrieval service for users. In [16], the authors introduce the three distance preserving mechanisms to encrypt visual features, aiming to remain approximately the similarity between images before and after encryption. In another work [17], two efficient secure search indexes instead of visual features are built using order-preserving encryption, and min-hash function, respectively. As an extension of [16,17], the literature [18] gives a comprehensive discussion on privacy-preserving image retrieval. In addition, common to [16–18] is that feature extraction/encryption is independent of the image encryption. The common characteristic,

☆ This paper has been recommended for acceptance by M.T. Sun.

* Corresponding author at: School of Communication and Information Engineering, Shanghai University, Shanghai 200444, China.
E-mail addresses: hcheng@fzu.edu.cn (H. Cheng), xzhang@shu.edu.cn (X. Zhang), sxyj1981@shu.edu.cn (J. Yu), zhangyuan@hutc.zj.cn (Y. Zhang).

http://dx.doi.org/10.1016/j.jvcir.2016.06.016
1047-3203/

however, readily incurs extra computation cost and inconvenience for the users. To overcome this limitation, in our previous work [19], we propose a retrieval scheme for JPEG encrypted images based on histogram invariance of DCT coefficients before and after encryption, in which the feature extraction/encryption is needless. Nevertheless, the file size increase after encryption becomes the key issue of this method, raising the storage and communication cost. What is more, another disadvantage is that the information of the plaintext image is partly visible. In another work [20], we introduce a Markov process based retrieval scheme for encrypted JPEG images, in which the shortcomings of [19] can be overcome. But, it is a supervised retrieval scheme and the image dataset used to train the desired retrieval model need be provided in advance. In the retrieval scheme of [21], users encrypt the color information by the deterministic encryption while considering the probabilistic encryption of the texture information to further enhance the security. And the cloud server can return encrypted images similar to the encrypted query image through the global color feature comparison. But the encryption algorithm in [21] is based on the space domain, namely, image pixels, and cannot ensure JPEG file size preservation and format compliance. The same issue exists in the work [22]. Furthermore, some perceptual encryption methods in [23–27] are suited to privacy-preserving image retrieval. In these methods, however, the contour information is partly leaked.

In this paper, we propose a novel unsupervised scheme to perform image retrieval in encrypted domain, where no training sets are provided. Using this scheme, the images are entirely encrypted along with format compliance and file size preservation. With an encrypted query image, the server may extract local statistic of intra-block AC coefficients from the encrypted query image, without first decrypting query image. Based on the local statistic characterized by a new block-based descriptor, the similarity between the encrypted query image and database image is measured by using block-wise feature comparison. As a result, the encrypted images with plaintext content similar to the query image are returned to the user for decrypting and viewing.

2. Proposed scheme

As given in Fig. 1, the proposed scheme mainly contains the three entities: content owner, authorized user, and server. The content owner encrypts JPEG images, and uploads encrypted versions to the server. An authorized user requesting image retrieval service just provides an encrypted query JPEG image to the server. Once an encrypted query image is obtained, the server can measure the similarities between the query image and images in the database, and sort them to return the encrypted images closest to query image. In the following, the mechanisms of image encryption and retrieval will be described detailedly.

2.1. Overview of JPEG encoding

To better explain the proposed encryption mechanism, we will briefly introduce color JPEG encoding. As we all know, a color JPEG image is composed of Y, U and V components, and each component is partitioned into 8×8 non-overlapped blocks, each of which contains one quantized DC coefficient and 63 quantized AC coefficients. According to JPEG standard [28], the DC and AC quantized coefficients are dealt with separately. For a block of a certain component, the DC coefficient is entropy encoded as a binary sequence by exploiting the difference between the current block and the previous block. The remaining 63 AC coefficients in the same block are first ordered into a zig-zag sequence. Then, with Run Length Encoding, the zig-zag sequence is converted into pairs of (r, v). The symbol r represents the number of consecutive zero-valued AC coefficients, and the symbol v defines a nonzero AC coefficient. As an example, suppose the zig-zag sequence of a block is $\{-6, 4, 0, -1, 0, 0, 3, 0, 0, 0, -8, \text{EOB}\}$ that can be converted into several (r, v) pairs: $\{(0, -6), (0, 4), (1, -1), (2, 3), (3, -8), (0, 0)\}$, where the symbol EOB (end-of-block) implies that all remaining AC coefficients in the block are zero, and denotes as one specific pair (0,0). Each (r, v) pair is then further encoded as a binary sequence using entropy encoding separately. Whether DC coefficients or AC

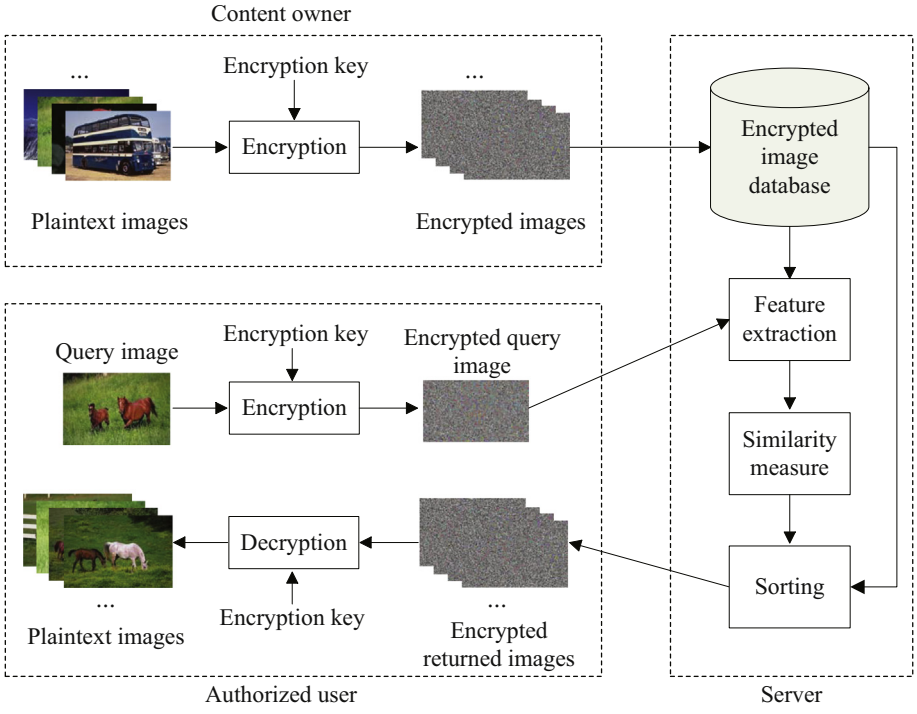

Fig. 1. Diagram of proposed scheme.