Digital Signal Processing 41 (2015) 98–109

Contents lists available at ScienceDirect

Digital Signal Processing

www.elsevier.com/locate/dsp

Robust hashing for image authentication using quaternion discrete Fourier transform and log-polar transform

Junlin Ouyang [a,d], Gouenou Coatrieux [b], Huazhong Shu [a,c,*]

[a] Laboratory of Image Science and Technology, Southeast University, Key Laboratory of Computer Network and Information Integration (Southeast University), Ministry of Education, 210096, Nanjing, China
[b] Institut Mines-Telecom, Telecom Bretagne, INSERM U1101 Latim, Brest, F-29238, France
[c] Centre de Recherche en Information Médicale Sino-français (CRIBs), Rennes, F-35000, France
[d] Hunan University of Science and Technology, 411201, Xiangtan, China

ARTICLE INFO

Article history:
Available online 20 March 2015

Keywords:
Robust image hashing
Quaternion discrete Fourier transform
Log-polar transform
Image authentication

ABSTRACT

In this work, a novel robust image hashing scheme for image authentication is proposed based on the combination of the quaternion discrete Fourier transform (QDFT) with the log-polar transform. QDFT offers a sound way to jointly deal with the three channels of color images. The key features of the present method rely on (i) the computation of a secondary image using a log-polar transform; and (ii) the extraction from this image of low frequency QDFT coefficients' magnitude. The final image hash is generated according to the correlation of these magnitude coefficients and is scrambled by a secret key to enhance the system security. Experiments were conducted in order to analyze and identify the most appropriate parameter values of the proposed method and also to compare its performance to some reference methods in terms of receiver operating characteristics curves. The results show that the proposed scheme offers a good sensitivity to image content alterations and is robust to the common content-preserving operations, and especially to large angle rotation operations.

1. Introduction

With the widespread use of sophisticated image editing tools, image contents can be easily tampered or forged. Verifying image authenticity is therefore a major issue in many applications. Robust image hashing is widely applied in image authentication [1–3]. Schematically, image hashing methods extract essential image features from which a short binary or real number sequence, called hash, is generated to represent the image content. Such a hash should be robust to image content-preserving operations while being sensitive to malicious tampering ones. Because robust image hashing captures the main image characteristics, it has attracted interest for other applications like image forensic [4,5], image retrieval [6,7], digital watermarking [8,9], and so on. Regarding image authentication, a robust image hash should also have good anti-collision (discriminative) capability for visually distinct images as well as a satisfactory level of security in order to make very difficult for an adversary to forge the hash value. To meet these requirements simultaneously, the construction of a robust image hashing is still a challenging task.

In general, the construction of an image hash is based on three basic steps, i.e., pre-processing, image feature extraction and construction of hash. Among them, the most critical one is certainly the image feature extraction step [10]. Existing feature extraction methods for robust image hashing can be roughly classified into the following categories.

Discrete Cosine Transform (DCT)-based image hashing methods: Fridrich and Goljan [8] used the DCT to capture the essential features of image blocks. They observed that it is very difficult to change the correlation of the low-frequency DCT coefficients without tampering the content of an image. Therefore, low-frequency DCT coefficients can be utilized as features to build the hash. De Roover et al. [11] defined a radial variance vector (RAV) based on the radial projection of the image pixels, and then applied the DCT to compress the RAV feature vector and construct the image hash. This method is robust to content-preserving operations and small angle rotations.

Discrete wavelet transform (DWT)-based image hashing methods: Ahmed et al. [1] used a wavelet transform to extract the image features. Since the wavelet transform has a good time–frequency localization property, their method can locate tampered regions

* Corresponding author at: Laboratory of Image Science and Technology, School of Computer Science and Engineering, Southeast University, 210096, Nanjing, China. Fax: +86 25 83 79 26 98.
E-mail address: shu.list@seu.edu.cn (H. Shu).

http://dx.doi.org/10.1016/j.dsp.2015.03.006
1051-2004/

with a good accuracy but at the price of a longer image hash. Wu et al. [12] combined the Radon transform (RT) and the DWT to deal with print-scan attacks. Tang et al. [13] developed an image hashing scheme after observing that the entropy of pixel blocks, a measure used to characterize image texture, is approximately linearly changed after content-preserving operations. Then, they applied DWT to image block's entropies to realize feature compression and construct the image hash. Recently, color vector angle combined with DWT [14] were applied to robust image hashing. Their results show good robustness to common content-preserving operations and small angle rotation. Liu et al. [15] utilized the wave atom transform to extract image features arguing that this approach has a sparse expansion and is capable to better capture texture properties. Furthermore, they observed that the coefficients of the third scale band are more suitable to serve as image hash features than the other scale bands.

Discrete Fourier transforms (DFT)-based image hashing methods: Most DFT based approaches are combined with other transforms in order to resist to geometric distortions. For example, Swaminathan et al. [10] proposed a robust image hashing scheme based on the Fourier–Mellin transform. Qin et al. [16] introduced another scheme where a secondary image is first obtained after a rotation projection similar to the RAV of the image. A non-uniform sampling is then performed to extract the image features after applying the DFT. This method is robust to small angle rotations. Lei et al. [11] first carried out a RT and then computed moment features before applying DFT on these moments. The first fifteen significant DFT coefficients were then normalized and quantized to obtain the image hash value. This method shows satisfactory results when facing geometrical distortions.

Matrix decomposition-based image hashing methods: Kozat et al. [17] used singular value decomposition (SVD) to get robust image features and to generate an image hash. Their hashing algorithm consists of two major steps. In the first one, intermediate features are extracted from pseudo-random (PR) semi-global regions via SVD. In the second step, the SVD is again applied to the intermediate features so as to construct the final hash. Monga et al. [18] also introduced a new PR signal representation method using non-negative matrix factorization (NMF) to capture the features and to form the image hash. Their method shows better performance than the SVD based method. Recently, Tang et al. [19] proposed a robust image hashing method based on ring partition and NMF. Their results show good performance to common content-preserving operations and large angle rotation operation.

Others image hashing methods: In [20], Xiang et al. proposed a histogram-based image hashing scheme, which is robust to geometric distortions but not to additive noise, brightness adjustment and contrast enhancement. Battiato et al. [21] adopted an image representation based on a set of SIFT features (called "bag of features", BOF) to construct the hash and explored a non-uniform quantization of histograms of oriented gradients (HOG) to get tamper localization capabilities. Zhao et al. [3] combined global and local features to construct an image hash. The global features correspond to the Zernike moments of the luminance and chrominance components of the image, while the local ones include the positions and the texture information of salient regions. This algorithm can identify the type of image tamper as well as the modified areas' location. Other robust feature extraction methods for constructing image hashes were also reported including the random Gabor filtering [22], the ring partition [23] and shape contexts [24].

When applied to color images, most of the above schemes convert three color channels (i.e., Red, Green, Blue or RGB) into gray-scale images while discarding the chrominance information. However, exploiting the chrominance information may not only improve the detection performance [3,16], but may also make image forgery more difficult due to the fact that the hash contains both luminance and chrominance information. Quaternions can offer a sound way to simultaneously deal with the three color channels without discarding the chrominance information. They have already been successfully employed in color image registration [25], image analysis [26–30] and watermarking [31–33]. Recently, quaternion discrete Fourier transform (QDFT) was used to generate image hashing and applied to image retrieval [34]. By following the same path, we proposed a novel image hashing method based on QDFT and log-polar transform for image authentication. QDFT can handle simultaneously the three channels (RGB) of color image without discarding chrominance information. Similar to DFT, the low-frequency coefficients of QDFT contain the main energy of the image and represent essential image features. In addition, QDFT can be combined with the log-polar transform so as to achieve a set of features that are rotation invariant. We propose thus to take advantage of QDFT used here to build a novel and compact image hash that is robust to content-preserving operations, geometric attacks while being sensitive to malicious tampering operations.

The rest of this paper is organized as follows. Section 2 gives a brief overview of quaternion and QDFT. Section 3 introduces the proposed scheme including its pre-processing, image feature extraction, and hash construction steps as well as its image authentication procedure. Experiments and comparison results are provided in Section 4. Some concluding remarks are given in Section 5.

2. Preliminaries

2.1. Quaternion

Quaternion is a generalization of complex numbers and was introduced by Hamilton in 1843 [26]. A quaternion number has four parts: one real part and three imaginary parts, and can be written as follows:

$$q = a + b\boldsymbol{i} + c\boldsymbol{j} + d\boldsymbol{k}, \tag{1}$$

where a, b, c and d are real numbers, $\boldsymbol{i}$, $\boldsymbol{j}$ and $\boldsymbol{k}$ are imaginary units obeying the following rules:

$$\boldsymbol{i}^2 = \boldsymbol{j}^2 = \boldsymbol{k}^2 = -1, \quad \boldsymbol{i}\boldsymbol{j} = -\boldsymbol{j}\boldsymbol{i} = \boldsymbol{k},$$
$$\boldsymbol{j}\boldsymbol{k} = -\boldsymbol{k}\boldsymbol{j} = \boldsymbol{i}, \quad \boldsymbol{k}\boldsymbol{i} = -\boldsymbol{i}\boldsymbol{k} = \boldsymbol{j}. \tag{2}$$

From Eq. (2), it can be found that the multiplication rule of quaternion is not commutative. The conjugate and modulus of a quaternion q are respectively defined as follows:

$$\bar{q} = a - b\boldsymbol{i} - c\boldsymbol{j} - d\boldsymbol{k}, \qquad |q| = \sqrt{a^2 + b^2 + c^2 + d^2}. \tag{3}$$

A quaternion q with a zero real part is called a pure quaternion. One pixel of a color image f at the spatial position (x, y) has three components, and can be represented as a pure quaternion [27]:

$$f(x, y) = f_R(x, y)\boldsymbol{i} + f_G(x, y)\boldsymbol{j} + f_B(x, y)\boldsymbol{k}, \tag{4}$$

where $f_R(x, y)$, $f_G(x, y)$ and $f_B(x, y)$ are respectively the RGB component values of $f(x, y)$.

2.2. Quaternion discrete Fourier transform

Quaternion or hypercomplex Fourier transform was first introduced in the image processing community by Ell [28]. Due to the non-commutative property of the quaternion multiplication, there are three different types of QDFT, namely, right-side, left-side and two-side [29]. Since that the right side QDFT can be processed in a similar way as the left side QDFT, and the operations are much