Information Sciences 361–362 (2016) 84–99

Contents lists available at ScienceDirect

Information Sciences

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

A novel image hashing scheme with perceptual robustness using block truncation coding

Chuan Qin[a,*], Xueqin Chen[a], Dengpan Ye[b], Jinwei Wang[c], Xingming Sun[c]

[a] Shanghai Key Lab of Modern Optical System, and Engineering Research Center of Optical Instrument and System, Ministry of Education, University of Shanghai for Science and Technology, Shanghai 200093, China
[b] School of Computer, Wuhan University, Wuhan 430072, Hubei, China
[c] School of Computer and Software, Nanjing University of Information Science & Technology, Nanjing 210044, Jiangsu, China

ARTICLE INFO

Article history:
Received 9 December 2015
Revised 30 March 2016
Accepted 26 April 2016
Available online 11 May 2016

Keywords:
Image hashing
Block truncation coding
Local binary pattern
Principal component analysis

ABSTRACT

In this paper, we propose a novel perceptual image hashing scheme based on block truncation coding (BTC). In the proposed scheme, the pre-processing is first applied on original image through bilinear interpolation, Gaussian low-pass filtering, and singular value decomposition (SVD) to construct a secondary image for regularization. Then, BTC is conducted on the secondary image to extract perceptual image features, and the low and high reconstruction levels and the feature matrix of corresponding binary map after the computation of center-symmetrical local binary pattern (CSLBP) are compressed with quantization and data dimensionality reduction of PCA to produce the final compact binary hash. Experimental results demonstrate that the proposed scheme has the satisfactory performances of robustness, anti-collision, and security.

1. Introduction

With widespread applications of image processing tools, the contents of digital images can easily be modified. Therefore, the verification on image authenticity becomes an important and crucial issue in many actual scenarios [14,30]. In recent years, perceptual image hashing as a new technique in multimedia security has emerged and attracted many researchers' attentions [10,15,21]. The output of perceptual image hashing scheme can be considered as a compact summary of principle contents for image, which can be applied in many fields, such as image authentication, copy detection, and image retrieval [11,13,17,28,29]. Traditional cryptographic hash functions, such as MD5 and SHA-1, also can compress input message into a short string, but they are highly sensitive to even one-bit slight change, therefore, traditional cryptographic hash functions are not suitable for the application of digital images that can allow the changes caused by the content-preserving operations, such as JPEG compression, filtering, and scaling.

In general, a typical image hashing scheme contains three main stages, i.e., pre-processing, feature extraction, and hash generation, as illustrated in Fig. 1. Denote a given original image as $\mathbf{I}_o$, an image that is visually similar to $\mathbf{I}_o$ as $\mathbf{I}_s$, and an image that is visually distinct with $\mathbf{I}_o$ as $\mathbf{I}_t$. The calculation procedure of a perceptual image hashing scheme is represented as $\mathrm{H}_K(\cdot)$, where K is the secret key used in the scheme. In general, a perceptual image hashing scheme should satisfy the following three requirements.

* Corresponding author. Tel.: +86 21 55272562, +86 13918588359; fax: 86 21 55272982.
E-mail addresses: qin@usst.edu.cn (C. Qin), cxqmm0818@163.com (X. Chen), yedp@whu.edu.cn (D. Ye), wjwei_2004@163.com (J. Wang), sunnudt@163.com (X. Sun).

http://dx.doi.org/10.1016/j.ins.2016.04.036
0020-0255/

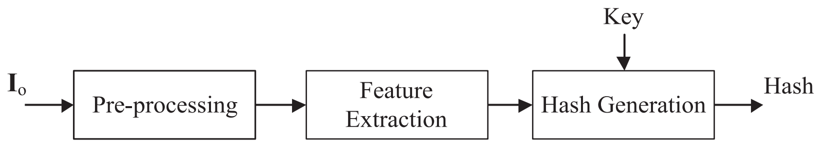

Fig. 1. Flowchart of image hashing scheme.

(1) Perceptual robustness: $\Pr\{\mathrm{H}_K(\mathbf{I}_o)=\mathrm{H}_K(\mathbf{I}_s)\} \geq 1-\varepsilon_1$. Visually similar images should have very similar hashes. It means that the calculation of image hashing should be robust to content-preserving operations on images.
(2) Anti-collision capability: $\Pr\{\mathrm{H}_K(\mathbf{I}_o)=\mathrm{H}_K(\mathbf{I}_t)\} \leq \varepsilon_2$. Visually distinct images should have significantly different hashes. In other words, the similarity probability of two hashes generated from two visually distinct images should be very small.
(3) Key-dependent security: $\Pr\{\mathrm{H}_{K1}(\mathbf{I}_o)=\mathrm{H}_{K2}(\mathbf{I}_o)\} \leq \varepsilon_3$. The output result of image hashing scheme cannot be predicted without the knowledge of secret key, which means different secret keys generate significantly different hashes.

Here, $\Pr\{\cdot\}$ denotes the calculation for probability, ε_1, ε_2 and ε_3 are very small positive numbers closing to zero.

Recently, a lot of image hashing schemes have been proposed in the field of multimedia security [2,5,8,12,16,19,20,24–27]. Observing that dominant DCT coefficients can represent principal image features, Tang et al. exploited the dominant DCT coefficients to construct robust hash against content-preserving digital manipulations [25]. The scheme was robust to popular content-preserving operations, but its discrimination capability was limited. Venkatesen et al. proposed to extract statistics features of wavelet coefficients to generate hash [27]. This method was resilient to JPEG compression, however, it was sensitive to contrast adjustment. In the scheme [26], an image hashing algorithm was presented by using entropies of image block and applying 2D-DWT to perform feature compression. But, the robustness toward rotation of this scheme was not very satisfactory. Qin et al. introduced another image hashing scheme [20], which first generated a secondary image by DFT and then utilized a non-uniform sampling strategy to extract robust salient image features from the magnitude matrix of Fourier coefficients. This scheme had good performances of robustness and anti-collision, but was only resistant to rotation with small angles. Kozat et al. viewed images as a sequence of linear operators and presented an image hashing scheme, which applied singular value decomposition (SVD) twice [12]. This hashing method was robust to rotation at the cost of increasing misclassification. Choi and Park presented a global to local (GLOCAL) image hashing method utilizing a hierarchical histogram, which depended on the populations of histogram bins [2]. Its robustness resisting the rotation operation was somewhat good, but this method was dependent on the size of images and was sensitive to the scaling operation. In [5], Davarzani et al. extracted the features of center-symmetrical local binary pattern from non-overlapping image blocks and then obtained the final image hash. This scheme produced satisfactory performance of perceptual robustness, but its discrimination was not good enough. As an optimal algorithm that can retain the essence of original image matrix, non-negative matrix factorization (NMF) was widely used in the areas of image processing. Monga and Mihcak utilized NMF twice through extracting the relevant coefficients to generate hashes [16]. The scheme was robust against several common digital operations but was sensitive to watermark embedding. Fridrich and Goljan proposed a typical image hashing method for the authentication of both video data and visual images [8]. Although the image features of this method were selected from the low-frequency DCT coefficients, the robustness and anti-collision capability can be further improved. Local linear embedding (LLE) has been widely adopted in digital signal processing, such as face recognition, data clustering and image identification. Tang et al. proposed a LLE-based image hashing scheme by investigating on the embedding vector variance of LLE [24], which was approximately, linearly changed with the content-preserving modifications. This scheme can achieve good performances of the perceptual robustness and the discrimination, however, the length of final hash was relatively longer.

Even though the above reported methods realized the fundamental functionalities of image hashing, there are still some problems and shortcomings required for solving. For example, the performances of anti-collision in the schemes [8,12,16,27] were not satisfactory. In this work, we propose an image hashing scheme using block truncation coding (BTC), which can effectively resist the content-preserving operations, such as JPEG compression, filtering, scaling and rotation of small angles. Furthermore, it can achieve a better trade-off between anti-collision capability and perceptual robustness. During the stage of hash generation, the secret key is utilized, which guarantees the security of the proposed scheme.

The rest of this paper is organized as follows. Section 2 describes the proposed perceptual image hashing scheme detailedly, including the pre-processing, perceptual feature extraction and hash generation. Experimental results and analysis are given in Section 3. Section 4 concludes the paper.

2. Proposed image hashing scheme

The proposed image hashing scheme consists of the three main stages, i.e., pre-processing, feature extraction, and hash generation. The schematic diagram of the proposed scheme is given in Fig. 2.