Optik 125 (2014) 5582–5587

Contents lists available at ScienceDirect

Optik

journal homepage: www.elsevier.de/ijleo

Robust image hashing using invariants of Tchebichef moments

Yongchang Chen, Weiyu Yu*, Jiuchao Feng

School of Electronic and Information Engineering, South China University of Technology, Guangzhou 510641, China

ARTICLE INFO

Article history:
Received 9 October 2013
Accepted 15 May 2014

Keywords:
Image hashing
Perceptual hashing
Image authentication
Tchebichef moments

ABSTRACT

The content authenticity is critical for secure transmission of multimedia information. As a promising solution, perceptual image hashing has gain great attention. In this paper, we develop a novel algorithm for generating an image hash based on invariants of radial Tchebichef moments. The idea is justified by the fact that the radial Tchebichef moments represent the image under the orthogonal kernel, which has the desirable qualities of orthogonality and robustness. The hash values are achieved by adaptive quantization of the invariants of radial Tchebichef moments, then the random Gay code is applied in the discrete–binary conversion stage to enhance the expected discriminability. Experiments are conducted to show that the proposed hashing algorithm has superior robustness and discrimination performance compared with other state-of-the-art algorithms, in terms of receiving operating characteristic (ROC) curves.

1. Introduction

With the rapid development of multimedia and network technology, the vast amount of information are transmitted and shared, which inevitably bring forward a higher requirements for digital image authentication techniques. Along with the various techniques in the literatures used for authentication, perceptual image hashing has been proven as an attractive way to verify the authenticity of digital images, by comparing the similarity of two image hashes that are extracted from the original image and suspect image [1].

Perceptual image hashing is the compact descriptor of the original contents, reducing the redundant information for the image, and lessening the overhead of transmission. It maps binary strings of arbitrary length to binary strings of small fixed length [2]. Similar to conventional cryptographic hashing, perceptual image hashing is required to generate different hash values for different inputs. Meanwhile, perceptual image hashing can allow image data for lossy representations with graceful degradation, and expects to change the hash value only if the input data is perceptually changed, while the former is sensitive to every bit of the input [3–5].

For a good perceptual hashing, three main design criteria should be satisfied: (1) Robustness: under the same key, the image hash value should be insensitive to incidental modifications that do not change image semantic content, such as JPEG compression, moderate levels of additive noise and geometric transforms. (2) Fragility or discriminative capability: the similarity value between hashes of the image and its malicious altered version should be very small, so as to effective distinguish the visual different. (3) Secure: to forge perceptually different inputs with similar hash values should be almost impossible. Moreover, robustness, fragility and security contradict each other.

Most of the existing schemes involve two main stages to generate a hash, feature extraction and hash generation, as shown in Fig. 1. In the feature extraction stage, key-dependent salient features from the image are extracted. Then these features are quantized, converted to binary representation, and maybe compressed using error-correcting codes.

Due to the wide applications, there are many different approaches to develop image hashing algorithms in recently years, which can be roughly classified into three categories: statistics based approaches [6,7], transform based approaches [8–11], and low-level feature based approaches [12–15]. In statistics based approaches, the hashes are constructed by using a certain class of statistics of the image that are largely invariant under visually insignificant perturbations to the image. The common adopted statistics are mean, variance, histogram, and higher moments of image blocks. In [6], Schneider and Chang make use of the intensity histograms of image blocks for authentication. The drawback of this method is that it easy to fake a histogram of the image. In [7], Venkatesan et al. developed a technique based on statistics vectors extracted from the various sub-bands in discrete wavelet domain, since they observed that statistics such as averages of coarse subbands and variances of other sub-bands stay invariant under a large

* Corresponding author. Tel.: +86 20 22236090.
E-mail address: yuweiyu@scut.edu.cn (W. Yu).

http://dx.doi.org/10.1016/j.ijleo.2014.07.006
0030-4026/

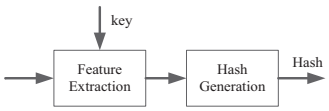

Fig. 1. The framework for generating a hash.

class of content-preserving modifications to the image. Although it shows great robustness than intensity statistics, it does not necessarily capture content changes well. In transform based approaches, various image transforms are utilized to extract the invariant features of the image directly or indirectly. For example, the invariant relationship in paper published by Lin and Chang [8] is identified between DCT coefficients pairs, i.e., it does not preserve certain transform coefficients, but look to identify invariant relationships between those coefficients. This is dissimilar to the approach in [11], where the selected DCT coefficients should be preserved and compared with a preset threshold to obtain binary string. In [10], Lu and Liao present a so-called structural digital signature by utilizing the relation of the multiscale structure on the wavelet transform. In low-level feature based approaches, the hashes are constructed from the image edges or salient feature points. These approaches possess good robustness, but still have limitations, due to that they are sensitive to some perceptually insignificant modifications, such as scaling, high quantization, and resolution reduction. Monga and Evans [12] exploits the end-stopped wavelet transform to detect significant image feature points. In [13], a perceptual image hashing scheme is proposed by Khelifi and Jiang based on virtual watermark detection employing an optimum multiplicative watermark detector and achieves great robustness at a low computational cost. Lv and Wang [14] introduce a SIFT-Harris detector to identify the most stable SIFT key points under various content preserving operations. The extracted local features are embedded into shape context based descriptors to generate an image hash.

In this paper, we present a new perceptual robust image hashing scheme based on invariants of radial Tchebichef moments. Unlike continuous orthogonal moments, such as Zernike, pseudo-Zernike and orthogonal Fourier–Mellin moments, Radial Tchebichef moments is a discrete orthogonal moment. They do not have discretization error, which accumulates as the order of the moment increases. They also possess good robustness in noise-free, noise and smooth distortion conditions, and have better recognition capabilities [16–18]. In the stage of hash generation, we apply random Gray code to convert the adaptive quantized hash vectors into binary hash string, which is likely to increase the detection sensitivity and the security of image hashing to some extent.

The rest of this paper is organized as follows. Sections 2 and 3 briefly describe the theory of radial Tchebichef moments and random Gray code, respectively. Section 4 presents the proposed image perceptual hashing method. Experimental results for evaluating the performance of the proposed method are given in Section 5. Finally, the conclusions are given in Section 6.

2. Radial Tchebichef moments

Radial Tchebichef moments are effective discrete orthogonal moments that have been successfully used in the field of image recognition. They retain the basic form of Zernike moments, but only use one-dimensional Tchebichef polynomials, and have the powerful characteristics of discrete orthogonal and rotational invariance.

For a given image $f(x, y)$ of size $L \times L$, there are two typical mapping methods to transform the image coordinates to a suitable domain inside a circle [19]. In the first method, the square image plane is mapped to the interior of the disk, while the other method is mapped to the exterior of the disk. The first mapping method

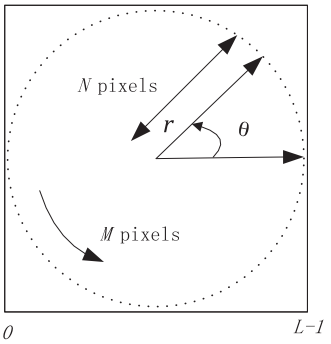

Fig. 2. The uniform sampling of radial Tchebichef moment.

is often used to calculate the invariants of image moments. The transformed coordinates for the first method is given by

$$r_{ij} = \frac{L\sqrt{(c_1 i + c_2)^2 + (c_1 j + c_2)^2}}{2} \tag{1}$$

$$\theta_{ij} = \tan^{-1}\left(\frac{c_1 j + c_2}{c_1 i + c_2}\right) \tag{2}$$

where c_1=2/(L − 1), c_2 = −1, with i, j = 0, 1, ..., $L-1$, and $0 \le r_{ij} \le 1$.

The uniform sampling based on $f(r, \theta)$ is illustrated in Fig. 2 $N = L/2$, and M denotes the maximum number of pixels along the circumference of the circle in Fig. 2 The parameter r varies from 0 to N, and the θ varies from 0 to 2π in M discrete steps, $\theta_k = 2\pi k/M$, k = 0, 1, ..., $M-1$.

Then the radial Tchebichef moments of order n and repetition m can be defined using the equation [17]

$$S_{nm} = \frac{1}{M}\sum_{r=0}^{N-1}\sum_{k=1}^{M-1}\tilde{t}_n(r)exp\left(-jm\frac{2\pi\theta_k}{M}\right)f(r, \theta_k) \tag{3}$$

The inverse moment transform is given by the following equation [17]:

$$f(r, \theta) \approx \sum_{n=0}^{n\max}\sum_{m=1}^{m\max} S_{nm}\tilde{t}_n(r)exp\left(jm\frac{2\pi\theta}{M}\right) \tag{4}$$

where $n$max, $m$max denote the maximum order and repetition of moments.

The radial Tchebichef polynomials $\tilde{t}_n(r)$ are given by

$$\begin{aligned}\tilde{t}_n(r) &= \frac{t_n(r)}{\beta(n, N)} \\ &= \frac{1}{\beta(n, N)}\sum_{k=0}^{n} n!(-1)^{n-k}\binom{N-1-k}{n-k}\binom{n+k}{n}\binom{r}{k}\end{aligned} \tag{5}$$

where $t_n(r)$ is the discrete Tchebichef polynomial of order n, which satisfies the following orthogonal property in discrete domain

$$\sum_{r=0}^{N-1} t_n(r)t_m(r) = \rho(n, N)\delta_{nm} \tag{6}$$

δ_{nm} denotes the Kronecker symbol and the squared-norm $\rho(n, N)$ is given by

$$\rho(n, N) = \frac{N\left(1-\frac{1}{N^2}\right)\left(1-\frac{2}{N^2}\right)\cdots\left(1-\frac{n^2}{N^2}\right)}{2n+1}, \quad n = 0, 1, \ldots, N-1$$

and $\beta(n, N)$ is a suitable constant which is independent of r. A particular and interesting choice of $\beta(n, N)$ is [20]

$$\beta(n, N) = \sqrt{\rho(n, N)} \tag{7}$$