Signal Processing 90 (2010) 331–343

Contents lists available at ScienceDirect

Signal Processing

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

Recover the tampered image based on VQ indexing

Chun-Wei Yang, Jau-Ji Shen *

Department of Management Information Systems, National Chung Hsing University, 250, Kuo Kuang Road, Taichung 402, Taiwan, ROC

ARTICLE INFO

Article history:
Received 6 January 2009
Received in revised form
23 April 2009
Accepted 5 July 2009
Available online 17 July 2009

Keywords:
Image recovery
Tamper detection
Vector quantization
Watermark

ABSTRACT

In this paper, a tampered image recovery scheme is proposed by creating an index table of the original image via vector quantization (VQ) and embedding it into the original image as a basis for recovery. In order to complete the goal of image authentication and recovery, Wong's watermarking scheme [P.W. Wong, N. Memon, Secret an public key image watermarking schemes for image authentication and ownership verification, IEEE Trans. Image Process 10 (10) (2001) 1593–1601] is employed to perform tamper detection. Wong's watermarking scheme can be used to accurately locate tampered regions. If an image has been tampered, the index table can be used to recover the tampered regions. The experimental results indicate that our scheme has the higher probability of image recovery. Besides, compared with Lee and Lin's [Dual watermark for image tamper detection and recovery, Pattern Recognition 41 (2008) 3497–3506] scheme, our scheme provides not only a better quality of recovered images but also better results at edge regions.

1. Introduction

In recent years, with the constant progress of image processing techniques and networking technology, publishing photos on the web has become a common thing that most people do in everyday life. The rapid development of the Internet has also facilitated the access and acquisition of digital images published on the Internet. As a result, images may be tampered for specific purposes without prior consent of their original authors. This kind of behavior seriously undermines the ownership of original authors and the accuracy of original works. Thus, for important images, such as military images, medical images, and patented images, image authorization is needed so as to deter malicious tampering and maintain the integrity of original images. In these images, image precision and integrity are highly important, and any slight tampering cannot be accepted. To avoid infringement of ownership, issues such as image authentication [1–16] and watermarking technique [17–20] have been gradually emphasized.

Based on tamper resistance and user needs, the current research of watermarking techniques can be divided into three areas. The first is focused on robust watermarking [17–20]. This kind of techniques can better resist malicious attacks such as rotation, cutting, compression, blurring, and sharpening. After extraction and verification of watermarks, ownership of copyright can be immediately identified. The second type is called fragile watermarking [5–9], which is mainly characterized by the high fragility of watermarks. Any slight tampering of image pixels can result in a serious damage of embedded watermarks. Therefore, whether the embedded watermarks can be successfully extracted indicates the integrity of a watermarked image. The third is semi-fragile watermarking [10–16]. It can detect malicious tampering, locate tampered regions, and further extract watermarks from intact regions. Based on the extracted watermarks, which regions of the image have been tampered can be

* Corresponding author. Tel.: +886 4 2284 0864x613; fax: +886 4 2285 7173.
E-mail address: jjshen@dragon.nchu.edu.tw (J.-J. Shen).

0165-1684/$ - see front matter © 2009 Elsevier B.V. All rights reserved.
doi:10.1016/j.sigpro.2009.07.007

effectively identified. Since watermarks play an important role in copyright protection and user authentication, an appropriate technique should be selected and applied, depending on the needs of each situation, so as to achieve effective protection. For instance, for copyright protection, robust watermarking techniques should be used to resist malicious attacks. To detect image tampering, fragile watermarking techniques can be adopted. For further positioning of tampered regions, semi-fragile watermarking techniques are more suitable.

In previous studies of image authentication [1–16], the focuses were mainly placed on verifying whether an image has been tampered rather than on recovering tempered regions. If tampered regions can be located and recovered based on the recovery information extracted from the image, not only image authentication can be performed, a considerable amount time for retransmission can also be saved. This is why the research of image tamper detection and recovery [21–26] has been gradually emphasized and become a prominent domain in recent years. In 2005, Lin et al. proposed hierarchical digital watermarking scheme [23] which carried out image tamper scanning and detection in four stages. These four stages ensured 100% precision of tamper detection. However, two drawbacks have been discovered. One is its high sensitivity to invalid pixels. A block containing any invalid sub-block is also considered as invalid, so a large number of valid blocks may be misjudged as invalid. The other drawback is that recovery information is embedded once. In other words, if both block A and its corresponding block A' are tampered, the recovery quality will be significantly reduced. In 2008, Lee and Lin proposed dual watermarking scheme [25]. This scheme provided a solution to the drawbacks of Lin et al.'s method and ensured a higher recovery quality for images with large tampered regions. Meanwhile, aiming at Lin et al.'s watermarking method, Chang et al. presented a four-scanning attack scheme [27] which could effectively tamper watermarked images without being detected. Lee and Lin's method and Lin et al.'s method are all based on similar concepts, so it is also likely that watermarks embedded using Lee and Lin's method can be identified. In 2008, Wang and Tsai proposed an image authentication and recovery scheme. For regions of interest (ROI), fractal codes were used, and for non-ROI, image inpainting technique was adopted [26]. The quality of recovered ROI was high, but that of non-ROI was not ideal. Besides, a considerable amount of time was needed to compute fractal codes.

The above-mentioned methods used means of pixel values as features for recovery. Besides, malicious attackers can also use mean calculation algorithms to build a dictionary and use it to find and tamper embedded watermarks without being detected. Thus, in this paper, a new scheme is presented. First of all, we use a secret key to obtain a random sequence and determine where to embed watermarks on the basis of this random sequence. As a result, it is hard to find out the corresponding location of watermarks from embedded images. Later, through vector quantization (VQ), we create an index table as a basis for recovery and embed it in the original image. Wong's watermarking scheme [12] is then integrated to perform tamper detection and achieve image authentication and recovery. Our scheme ensures a higher image recovery quality than Lee and Lin's scheme and does not require as much computation efforts as fractal codes.

The remainder of paper is organized as follows: In Section 2, Wong's watermarking scheme and VQ are respectively introduced. Our scheme is presented in Section 3. Section 4 details the experimental results and discussions. Finally, conclusions are proposed in Section 5.

2. Backgrounds

The proposed scheme is integrated with Wong's watermarking scheme to achieve tamper detection. It computes index values of an image using VQ and embeds the obtained index table into the original image. In this section, these two schemes are respectively introduced.

2.1. Wong's watermarking scheme

We shall review Wong's watermarking scheme [12] in two stages: watermark embedding and watermark extraction, as shown in Figs. 1 and 2.

2.1.1. Watermark embedding

In this scheme, every gray-level image O is composed of $M_O \times N_O$ pixels, and watermark B is a binary image and with same size as image O. Because Wong's watermark embedding scheme embeds watermarks block by block, O and B should be segmented into non-overlapping blocks of $I \times J$ pixels. The detailed process of embedding each block is shown in Fig. 1. First of all, the r-th block of the gray-level image O is defined as O_r, and (p, q) denotes the coordinates of this block, as shown:

$$O_r = \{O_{pI+a,qJ+b} : \quad 0 \le a \le I-1; \quad 0 \le b \le J-1\}. \tag{1}$$

The block corresponding to O_r is called B_r, which can be defined as

$$B_r = \{B_{pI+a,qJ+b} : \quad 0 \le a \le I-1; \quad 0 \le b \le J-1\}. \tag{2}$$

A cryptographic hash function as shown is used:

$$H(S) = (d_1, d_2, \ldots, d_n), \tag{3}$$

where S is an input data string of any length, d_i is the binary output bits produced by the hash function, and n is the length of the output. There are three advantages of using the hash function: (1) Given a data string S of any length, the MD of a fixed length can be quickly computed, i.e. $d_1,d_2,\ldots,d_n$. (2) With a given MD, it is hard to find S using Eq. (3). (3) It is hard to find any S_1 and S_2 such that $H(S_1) = H(S_2)$. This is called strong collision resistance. In this scheme, Wong uses the well-known MD5 algorithm [28]. MD5 can compress input data string of any length into 128 bit strings, i.e. $n = 128$. Later, LSB1 (the first least significant bit) of each pixel in block O_r is set to zero to obtain $\tilde{O}_r$. The five parameters are then input into the hash function, as shown:

$$H(M_O, N_O, I_O, r, \tilde{O}_r) = (d_1^r, d_2^r, \ldots, d_n^r). \tag{4}$$