Information Sciences 179 (2009) 2283–2293

Contents lists available at ScienceDirect

Information Sciences

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

Preserving robustness and removability for digital watermarks using subsampling and difference correlation

Chin-Chen Chang [a,b], Pei-Yu Lin [b,*], Jieh-Shan Yeh [c]

[a] Department of Information Engineering and Computer Science, Feng Chia University, 100 Wenhwa Rd., Seatwen, Taichung 40724, Taiwan
[b] Department of Computer Science and Information Engineering, National Chung Cheng University, 168 University Rd., Min-Hsiung, Chai-Yi 621, Taiwan
[c] Department of Computer Science and Information Management, Providence University, 200 Chung-chi Rd., Shalu, Taichung 433, Taiwan

ARTICLE INFO

Article history:
Received 24 January 2008
Received in revised form 14 January 2009
Accepted 8 March 2009

Keywords:
Robust watermark
Removable
Copyright protection
Subsampling
Difference correlation

ABSTRACT

Watermarking techniques are applied to digital media to protect their integrity and copyright. The embedding of a watermark, however, often distorts the quality of the protected image. This may be intolerable since the protected media is for preserving artistic and valuable images. Hence, engineers have proposed removable solutions permitting authorized users to restore watermarked images to unmarked images with satisfactory quality. Unfortunately, these mechanisms cannot resist signal processing attacks to protect the ownership. In this article, we propose a novel watermarking mechanism by utilizing pair-difference correlations upon subsampling and the technique of JND. This new approach can guarantee the robust essentials of watermarking schemes. Experimental results reveal that the new method outperforms others in terms of restored image quality. More specifically, this novel approach can resist various attacks to which related works are vulnerable.

1. Introduction

Digital watermarking techniques have recently been utilized to protect the integrity, validity, and ownership of digital multimedia [2,3,7,8,11–13,15,16,18,20]. They allow users to embed verifiable watermarks, such as logos, trademarks, or copyright information, into the host images. The verifiers can later extract the watermarks and confirm their ownership through watermarked images. Such techniques often alter the significant areas of the host image and distort the quality of the watermarked images. This distortion, however, is intolerable when the protected image is an artistic or valued one. To mitigate this problem, engineers have defined the removability requirement which guarantees that an authorized user can remove the embedded watermark to obtain an unmarked image.

Currently, there are two conventional approaches for restoring unmarked images: the reversible method and the removable one. The first mechanism permits authorized users to embed information into the host image. A verifier can then restore the lossless host image by removing the embedded information [1,4–6,9,17]. These reversible methods have been applied to fragile watermarking to provide information authentication. However, these methods are incapable of resisting malicious attacks. That is, the reversible methods cannot achieve the robust requirement of watermark mechanisms, since the embedded information in the watermarked image is sensitive and vulnerable. Once the watermarked image has been tampered, verifiers cannot retrieve the valid watermark to confirm the copyright.

The second conventional approach involves removing embedded information from the watermarked image to reconstruct an original-like image of satisfactory quality [10]. The removable schemes can be applied to preserve artistic or

* Corresponding author. Tel.: +886 4 24517250x3790; fax: +886 27066495.
E-mail address: linpy@cs.ccu.edu.tw (P.-Y. Lin).

0020-0255/$ - see front matter Crown Copyright © 2009 Published by Elsevier Inc. All rights reserved.
doi:10.1016/j.ins.2009.03.003

valuable images. Hence, the quality of the restored image is an important concern in evaluating a removable watermark mechanism.

In 2006, Hu et al. [10] proposed a removable watermark scheme that embedded a visible watermark into the host image. The authorized user was permitted to remove the embedded watermark and reconstruct an unmarked image of high quality. However, this watermark was incapable of resisting malicious attacks; thus, it was unable to protect the copyright of legal owners [10].

The invisible watermarking mechanism is currently utilized worldwide for protecting digital media. Here, the watermark embedding procedure is more difficult to achieve the robustness and removing ability. Thus, the invisible watermarking mechanism that possesses the removable ability is pressing and significant for protecting valuable images.

In this article, we aim to propose a removable watermark approach that will contribute to the literature in the following ways: (1) provide a removable mechanism in the invisible watermarking application, (2) reconstruct an unmarked image with high fidelity to approximate the original image, (3) achieve the robustness requirement to protect the ownership of an image, and (4) be suitable for preserving the valuable images.

The new method allows the authorized user to validate the embedded watermark and reconstruct an unmarked image with satisfactory quality. The proposed scheme is robust to resist malicious attacks, unlike related lossless or removable watermark schemes. Furthermore, the new approach utilizes the Just Noticeable Distortion (JND) [21] to guarantee the quality of watermarked image for HVS. The JND coefficients are adjustable and visually optimized, according to individual DCT coefficients. This is why the difference between the watermarked image and the host image in image quality is visually imperceptible in the novel mechanism. The rest of this paper is organized as follows. The novel removable watermark embedding procedure is elaborated in Section 2, followed by the watermark verifying procedure illustrates in Section 3. The experimental results and performance are demonstrated in Section 4. The analysis and discussions of the new method are given in Section 5. Finally, we make conclusions in Section 6.

2. Removable watermark embedding procedure

In this section, we describe how to embed the removable watermark in the DCT domain of the subsampling host image.

2.1. Preliminary phase

Assume that the protected host gray-level image O possesses $N \times N$ pixels and the watermark image $W = \{w_i | i = 1, 2, \ldots, ((N/2)/8) \times ((N/2)/8)\}$. The preliminaries are described as follows.

Step 1: Adopt the subsampling technique [13] to obtain four subimages O_1, O_2, O_3, and O_4 from the host image O:

$$\begin{aligned} O_1(m,n) &= O(2m, 2n), \quad O_2(m,n) = O(2m, 2n+1), \\ O_3(m,n) &= O(2m+1, 2n), \quad O_4(m,n) = O(2m+1, 2n+1), \end{aligned} \tag{1}$$

where $m = 0, 1, \ldots, (N/2) - 1$ and $n = 0, 1, \ldots, (N/2) - 1$.

Step 2: Divide subimages O_1, O_2, O_3, and O_4 into 8×8 non-overlapping blocks. That is, there are $((N/2)/8) \times ((N/2)/8)$ blocks for each subimage.

Step 3: DCT transform the blocks of subimages O_k to obtain four corresponding DCT coefficients sets $D_k = \{B_k(i)\}$, where $k = 1, 2, 3, 4$ and $i = 1, 2, \ldots, ((N/2)/8) \times ((N/2)/8)$. Here, $B_k(i)$ is the ith DCT coefficient block in D_k.

Step 4: Generate a sequence of random number pairs $P = \{(\alpha, \beta)\}$ by the secret key SK, where $\alpha, \beta \in \{1, 2, 3, 4\}$ and $\alpha \neq \beta$. The number of pairs is equal to $((N/2)/8) \times ((N/2)/8)$.

Here, α and β indicate the two subimages selected to embed the watermark. Since there are four available subimages randomly determined by SK, the combination of the possible random pairs is various. Without SK, an intruder cannot retrieve the watermark to completely restore an unmarked image with satisfactory quality within a reasonable computation time.

Let (α, β) be the selected random number pair of P. As illustrated in Fig. 1, we aim to embed the watermark bit w_i into the DCT coefficient block pair $B_\alpha(i)$ and $B_\beta(i)$, where $B_\alpha(i) \in D_\alpha$, $B_\beta(i) \in D_\beta$, and $i = 1, 2, \ldots, ((N/2)/8) \times ((N/2)/8)$. The energy of the image processed by DCT transformation mainly aggregates in the low-frequency and middle-frequency subbands, we divide the embedding procedure into two phases: low-frequency subband watermarking phase and middle-frequency subband watermarking phase as expressed in Sections 2.2 and 2.3.

2.2. Low-frequency subband watermarking phase

Let x and y be the coefficients at the uth zigzag scan order of blocks $B_\alpha(i)$ and $B_\beta(i)$, respectively. Here, parameter u is a zigzag position used to embed the watermark bit in the low-frequency subband. It is obviously that the four subimages are highly correlated, thus we can expect that the correlation of the DCT coefficients x and y are similar, i.e. $x \approx y$. The scheme utilizes the correlation difference between x and y to embed the watermark bit, the verifier hence can retrieve the watermark bit without comparison with the original image. The zigzag scan order is listed in Fig. 2. Note that we do not embed the