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

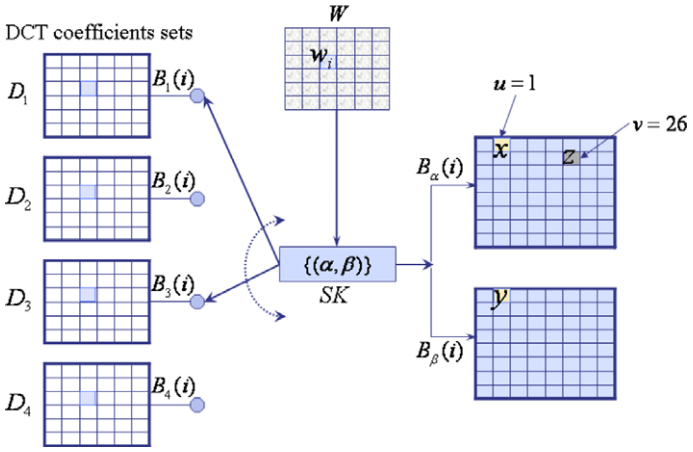


Fig. 1. The embedding process.

0	1	5	6	14	15	27	28
2	4	7	13	16	26	29	42
3	8	12	17	25	30	41	43
9	11	18	24	31	40	44	53
10	19	23	32	39	45	52	54
20	22	33	38	46	51	55	60
21	34	37	47	50	56	59	61
35	36	48	49	57	58	62	63

Fig. 2. The zigzag scan order.

watermark into the DC coefficients for avoiding the serious distortion of the embedded image, i.e. $u \geqslant 1$. The detailed embed algorithm is described as follows:

Step 1: Generate a JND map for DCT block $B_\alpha(i)$. The coefficient value at the position u is considered as zero while constructing the JND map by [21]. This guarantees that both the signer and verifier can calculate the same JND map.

Step 2: If $w_i = 0$ and $x \geqslant y$, set $s = 1$, and then exchange the values of x and y; if $w_i = 1$ and $x < y$, set $s = 1$, and then exchange the values of x and y; otherwise, $s = 0$. Here, s is a swap element.

Step 3: Enhance the coefficients of x and y according to

$$\begin{cases} x' = x + (2w_i - 1)JND(u), \\ y' = y - (2w_i - 1)JND(u). \end{cases} \tag{2}$$

Here, the $JND(u)$ is the JND value at uth zigzag scan order in the JND map.

2.3. Middle-frequency subband watermarking phase

In this phase, we embed the swap element s in the middle-frequency subband in order to reconstruct the modified coefficients in the low-frequency subband. Let z be the coefficient at the vth zigzag scan order of the DCT block $B_\alpha(i)$. Here, parameter v is a zigzag position used to embed swap element in the middle-frequency subband. The detailed embedding processes are stated as follows.

Step 1: For the coefficient value z, we first compute $\tilde{z}$ as

$$\tilde{z} = \lfloor |z| \rfloor. \tag{3}$$

Step 2: Transform $\tilde{z}$ to the binary representation as

$$\tilde{z} = (b_{11}b_{10}b_9b_8b_7b_6b_5b_4b_3b_2b_1b_0)_2.$$

Here, b_{11} is the most significant bit (MSB), and b_0 is the least significant bit (LSB). Note that, for a 8×8 DCT block, we need 12 bits (at most) to represent a coefficient value.

Step 3: Modify the binary representation $\tilde{z}$ by inserting the swap element s in the lth LSB. For instance, if $l = 3$, we insert the element s in the third-least significant bit to obtain

$$\tilde{z} = (b_{11}b_{10}b_9b_8b_7b_6b_5b_4b_3b_2\underline{s}b_1b_0)_2.$$

Step 4: Eventually, we can obtain the embedded coefficient z' as follows:

$$z' = \begin{cases} +(\tilde{z} + \text{decimal}(z)), & \text{if } z \text{ is positive,} \\ -(\tilde{z} + \text{decimal}(z)), & \text{if } z \text{ is negative,} \end{cases} \tag{4}$$

where decimal(z) represents the decimal part of $|z|$.

Observing the phenomenon of DCT domain, the coefficients located at the middle-frequency subband are near to zeros. We employ the property to expand the coefficients for lossless embed the secret s and avoid causing the coefficients underflow predicament.

Finally, we apply the IDCT to all coefficient blocks of the four subimages and combine the four watermarked subimages to form a complete watermarked image O'. Besides, the novel scheme adopts the voting mechanism to enhance the robustness. According to the zigzag scan order, we embed the watermark bit into the same block with r times.

2.4. An instance for embedding the watermark

Assume that the selected random number pair $(\alpha, \beta) = (3, 1)$, the watermark $w_i = 1$, $l = 3$, and $r = 3$. We embed $w_i = 1$ in the correlation difference between blocks $B_3(i) \in D_3$ and $B_1(i) \in D_1$. Fig. 3a and b illustrates the DCT coefficients blocks $B_3(i)$ and $B_1(i)$, respectively. Furthermore, Fig. 3d displays the JND map generated from the modified block $B_3(i)$ shown in Fig. 3c. Here, set system parameters $u = 1$ and $v = 26$.

For $r = 1$, We have the coefficient values $x = 5.9$ and $y = 7.1$ at zigzag position u. Since $w_i = 1$ and $x < y$, we must exchange the values of x and y such that $x = 7.1$ and $y = 5.9$. The swap element s thereby is set to 1. We obtain the following by Eq. (2):

129	5.9	-1	-5	3	-1	2.5	7.3
-4.8	18	3	4	-4	-5.2	0	1
6.7	9	3	-2	3	1	0	1
-2	3	-2	-1	-1	-1	2	0
4	0	1	1	-1	0	-1	0
1	0	0	0	0	0	2	0
1	-1	-1	0	0	0	0	1
0	0	0	0	0	0	0	0

(a) The protected host block $B_3(i)$

133	7.1	2	-2	-1	3	-5	1
3.3	9	5	5	-3	2	1	0
4.5	8	3	-2	3	1	0	1
1	4	-2	-2	-1	0	2	1
5	0	1	1	-2	0	0	0
2	0	0	0	0	0	0	1
3	-2	-1	0	-1	0	0	0
1	0	0	0	0	0	0	0

(b) The protected host block $B_1(i)$

129	0	-1	-5	3	-1	2.5	7.3
0	18	3	4	-4	-5.2	0	1
0	9	3	-2	3	1	0	1
-2	3	-2	-1	-1	-1	2	0
4	0	1	1	-1	0	-1	0
1	0	0	0	0	0	2	0
1	-1	-1	0	0	0	0	1
0	0	0	0	0	0	0	0

(c) The modified block

0	2	3	4	4	3	6	8
1	2	4	5	5	7	9	4
3	4	5	2	4	5	7	9
3	4	5	2	2	9	8	10
5	5	6	6	3	7	8	9
4	4	5	4	6	7	8	10
6	6	6	6	5	5	10	12
7	8	7	9	8	10	12	20

(d) The JND map

129	9.1	-1	-5	3	-1	6.5	11.3
4.3	18	3	4	-4	-13.2	0	1
9.7	9	3	-2	3	1	0	1
-2	3	-2	-1	-1	-1	2	0
4	0	1	1	-1	0	-1	0
1	0	0	0	0	0	2	0
1	-1	-1	0	0	0	0	1
0	0	0	0	0	0	0	0

(e) The watermarked block $B_3'(i)$

133	3.9	2	-2	-1	3	-5	1
-5.8	9	5	5	-3	2	1	0
1.5	8	3	-2	3	1	0	1
1	4	-2	-2	-1	0	2	1
5	0	1	1	-2	0	0	0
2	0	0	0	0	0	0	1
3	-2	-1	0	-1	0	0	0
1	0	0	0	0	0	0	0

(f) The watermarked block $B_1'(i)$

Fig. 3. The example of the watermark embedding procedure.

$$x' = 7.1 + JND(1) = 7.1 + 2 = 9.1 \quad \text{and}$$
$$y' = 5.9 - JND(1) = 5.9 - 2 = 3.9.$$

In the middle-frequency subband, for $v = 26$, we learn the original coefficient $z = -5.2$ and $\tilde{z} = \lfloor |z| \rfloor = \lfloor |-5.2| \rfloor = 5 = (101)_2$. Since $l = 3$, embedding the swap element $s = 1$ into the third least significant bit of $\tilde{z}$, we have $\tilde{z} = (1\underline{s}01)_2 = (1\underline{1}01)_2 = 13$. Finally, by Eq. (4), the embedded coefficient value

$$z' = -13 + (-0.2) = -13.2.$$

Employing the same procedure, for $r = 2$, we embed $w_i = 1$ in the next zigzag position for robustness, i.e. $u = 2$ and $v = 27$. Thus we have the watermarked coefficient values

$$x' = 3.3 + JND(2) = 3.3 + 1 = 4.3,$$
$$y' = -4.8 - JND(2) = -4.8 - 1 = -5.8 \quad \text{and}$$
$$z' = 6 + (0.5) = 6.5.$$

In case $r = 3$, the watermarked coefficient values

$$x' = 6.7 + JND(3) = 6.7 + 3 = 9.7,$$
$$y' = 4.5 - JND(3) = 4.5 - 3 = 1.5 \quad \text{and}$$
$$z' = 11 + (0.3) = 11.3.$$

Fig. 3e and f shows the final watermarked blocks $B'_3(i)$ and $B'_1(i)$, respectively.

3. Watermark verifying procedure

An authorized user is permitted to validate the embedded watermarking and remove the embedded information along with the secret information $\{SK, u, v, r, l\}$. As the same manner, the verifier can apply the DCT technique to each subimage constructed by Eq. (1) to obtain $((N/2)/8) \times ((N/2)/8)$ DCT blocks. The secret key SK is used to generate the same pairs $P = \{(\alpha, \beta)\}$, where $\alpha, \beta \in \{1, 2, 3, 4\}$ and $\alpha \neq \beta$.

3.1. Watermark verification

In this subsection, we demonstrate how an authorized user can verify the watermarked image O'. Specifically, the voting mechanism is adopted to determine whether the involved watermark bit equals to "1" or "0". Let (α, β) be the selected random number pair of P. Also, assume that x' and y' are the uth coefficient values of blocks $B'_\alpha(i)$ and $B'_\beta(i)$ at the zigzag scan order, respectively, for $i = 1, 2, \ldots, ((N/2)/8) \times ((N/2)/8)$.

Step 1: If $x' \geqslant y'$, then the vote of watermark bit w'_i is cast to be "1"; otherwise, it is cast to be "0".
Step 2: Repeat Step 1 with the next coefficient values of blocks $B'_\alpha(i)$ and $B'_\beta(i)$ at the zigzag scan order.

By repeating the process r times, we obtain the votes for each watermark bit w'_i. If the number of votes with a value of "1" is larger than that of vote value "0", then the watermark bit w'_i is set to be 1; otherwise, $w'_i = 0$.

After extracting the watermark bits from blocks $B'_\alpha(i)$ and $B'_\beta(i)$ for $i = 1, 2, \ldots, ((N/2)/8) \times ((N/2)/8)$, we rearrange all of the watermark bits to form $W' = \{w'_i | i = 1, 2, \ldots, ((N/2)/8) \times ((N/2)/8)\}$. The obtained recognizable logo image W' can be used to verify the validity of the watermarked image O'.

3.2. Watermark removing

In this phase, we describe how to remove the embedded information to restore an original-like image from the watermarked image. At the middle-frequency subband, we must retrieve a swap element s for block, for $i = 1, 2, \ldots, ((N/2)/8) \times ((N/2)/8)$. Hereafter, we can use this element to restore the coefficient values of blocks $B'_\alpha(i)$ and $B'_\beta(i)$ in the low-frequency subband.

3.2.1. Middle-frequency subband removing phase

Step 1: Let z' be the vth coefficient value of block $B'_\alpha(i)$ at zigzag scan order. We first compute the following:

$$\tilde{z}' = \lfloor |z'| \rfloor. \tag{5}$$

Step 2: Transform $\tilde{z}'$ into its binary representation as

$$\tilde{z}' = (b_{12} b_{11} b_{10} b_9 b_8 b_7 b_6 b_5 b_4 b_3 b_2 b_1 b_0)_2,$$

where b_{12} is the most significant bit (MSB) and b_0 is the least significant bit (LSB). Thereby, we can obtain the swap element s by extracting the lth least significant bit from the binary representation of $\tilde{z}'$.

Step 3: Eliminate the lth LSB from the binary representation of $\tilde{z}'$ to form $\tilde{z}$. We subsequently can reconstruct the coefficient value z as

$$z = \begin{cases} +(\tilde{z} + \text{decimal}(z')), & \text{if } z' \text{ is positive}, \\ -(\tilde{z} + \text{decimal}(z')), & \text{if } z' \text{ is negative}, \end{cases} \tag{6}$$

where decimal(z') represents the decimal part of $|z'|$.

3.2.2. Low-frequency subband removing phase

Let x' and y' be the uth coefficient values of blocks $B'_\alpha(i)$ and $B'_\beta(i)$ at the zigzag scan order, respectively. The repairing processes are stated as follows.

Step 1: By the extracted information w'_i in the watermark verifying phase, we repair the watermarked coefficient values x' and y' as follows:

$$\begin{cases} x = x' - (2w'_i - 1)JND(u), \\ y = y' + (2w'_i - 1)JND(u). \end{cases} \tag{7}$$

Here, JND are generated as the precedent manner.

Step 2: If the corresponding element $s = 1$, exchange the coefficient values of x and y; otherwise, the values of x and y remain the same.

By repeating above middle-frequency and low-frequency subband removing phases r times with next coefficient values at the zigzag scan order, we can restore the unmarked coefficient values of x, y and z. Note that an intruder cannot extract the watermark to completely remove the embedded information without the secret parameters.

4. Experimental results

In this section, we conducted several simulations to demonstrate the practicability of the new scheme. Moreover, we compared the novel scheme with related schemes in terms of image quality and robustness (see Sections 4.1 and 4.2).

For a specific attack, we utilized the accuracy rate *AR* to evaluate the robustness of a copyright protection scheme. The accuracy rate *AR* is defined as

$$AR = \frac{\sum_{i=0}^{H_w-1}\sum_{j=0}^{W_w-1}\overline{w_{ij} \oplus \tilde{w}_{ij}}}{H_w \times W_w}, \tag{8}$$

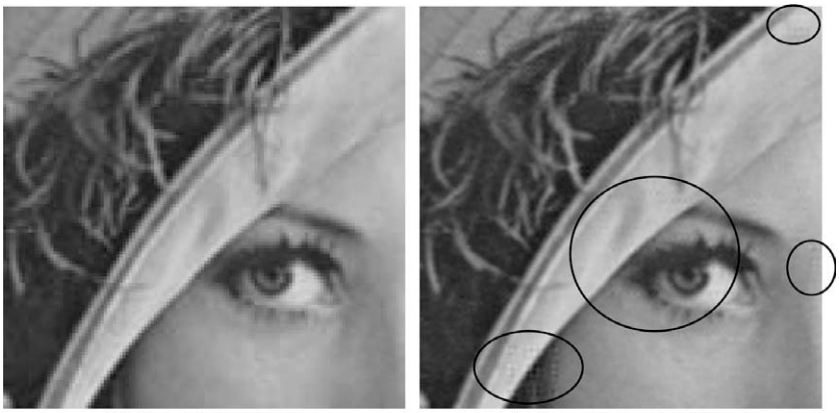
Table 1
The image quality of watermarked and restored images, and *AR*'s of extracted watermarks under different *r*'s.

Original image	*r*	Image quality						*AR*
		Watermarked			Restored			
		PSNR (dB)	wPSNR (dB)	SSIM	PSNR (dB)	wPSNR (dB)	SSIM	
Airplane	3	40.24	60.74	0.9899	56.60	76.65	0.9997	1.00
	5	37.40	58.99	0.9795	52.37	73.93	0.9994	1.00
Baboon	3	35.06	46.97	0.9843	49.68	61.87	0.9992	1.00
	5	33.45	46.07	0.9781	49.12	63.39	0.9991	1.00
Girl	3	40.87	52.81	0.9766	56.36	71.66	0.9995	1.00
	5	38.35	51.54	0.9658	52.75	64.65	0.9979	1.00
Goldhill	3	41.23	56.50	0.9849	56.10	71.96	0.9995	1.00
	5	39.14	55.89	0.9806	53.97	71.38	0.9995	1.00
Lena	3	42.66	59.53	0.9964	59.88	75.33	0.9999	1.00
	5	39.40	57.76	0.9936	56.07	72.59	0.9998	1.00
Peppers	3	41.99	57.65	0.9968	55.37	74.54	0.9999	1.00
	5	39.75	55.94	0.9944	52.31	71.06	0.9997	1.00
Sailboat	3	39.07	52.03	0.9931	54.59	69.71	0.9999	1.00
	5	36.66	50.75	0.9897	51.57	67.86	0.9998	1.00
Tiffany	3	41.81	59.88	0.9915	50.38	73.73	0.9996	1.00
	5	39.81	58.12	0.9859	50.69	73.92	0.9997	1.00
Average	3	40.37	55.76	0.9892	54.87	71.93	0.9997	1.00
	5	38.00	54.38	0.9835	52.36	69.85	0.9994	1.00

where H_w and W_w are the height and width of the watermark image, w_{ij} is the original watermark value, and $\tilde{w}_{ij}$ is the altered watermark value at the coordinate (i,j). The sizes of test images and the watermark image CCU are set to 512×512 pixels and 32×32 pixels, respectively. Furthermore, we set system parameters of $u = 10$, $v = 21$, and $l = 4$.

Table 2
The differences between original pixel values and restored pixel values.

Original image	r	DV (%)		
		0	$\{-1,1\}$	>1 or <−1
Airplane	3	95.71	3.51	0.78
	5	93.05	5.30	1.65
Baboon	3	94.38	3.68	1.94
	5	91.69	4.88	3.43
Girl	3	96.36	3.00	0.64
	5	93.08	5.15	1.77
Goldhill	3	95.09	3.67	1.24
	5	92.51	5.36	2.13
Lena	3	96.07	3.38	0.55
	5	94.03	4.99	0.98
Peppers	3	95.05	3.95	1.00
	5	92.71	5.55	1.74
Sailboat	3	94.97	3.63	1.40
	5	92.57	5.04	2.39
Tiffany	3	95.75	3.53	0.72
	5	93.41	5.39	1.20
Average	3	95.42	3.55	1.03
	5	92.88	5.21	1.91



(a) The original image (b) The watermarked image

(c) The novel restored image

Fig. 4. The enlarged partial image of 'Lena', $r = 5$.

4.1. Analysis of restored image quality

For a removable watermark mechanism, the quality of the watermarked images and the restored images are the major concerns. As shown in Table 1, the PSNR (peak signal-to-noise ratio) values of the watermarked images are approximately 40.37 dB and 38 dB with $r = 3$ and $r = 5$, respectively. The difference between the watermarked image and the host image is indistinguishable for human visual perception. Further examining the quality of the restored images, the PSNR values of reconstructed images are progressively around 54.87 dB and 52.36 dB with $r = 3$ and $r = 5$, respectively. Aside from, we adopt the wPSNR (weight peak signal-to-noise ratio) [14] and the SSIM (structural similarity) [19] values to evaluate the performance of the new scheme in the human visual system and similarity. The high values of the wPSNR and SSIM specifically indicate that the recovered images are nearly lossless after the watermark embedding and removing processes. In Table 1, it shows that all of the extracted logo images are unabridged, i.e. $AR = 1$. This implies that the novel scheme not only offers excellent quality of the restored image but also achieves complete accuracy rates of the extracted watermark images.

More precisely, Table 2 illustrates three cases to demonstrate the advantage of the novel method. The DV denotes the difference between two corresponding pixel values in the original image and the recovered image.

Case 1: $DV = 0$
Averagely, there are 95.42% pixels with the same value in the comparison between the original image and the restored image for $r = 3$. This implies that the novel method approximates to a lossless one.

Case 2: $DV = \{-1, 1\}$
For $r = 3$, the difference between the pixel value of the original image and the corresponding one of the restored image equal to -1 or 1 only takes 3.55%, while it takes 5.21% for $r = 5$.

Table 3
The comparison of the restored PSNR values between [10] and ours.

Original image	Restored PSNR (dB)		
	Hu et al. [10]	r	Ours
Airplane	44.16	3	56.60
		5	52.37
Girl	43.54	3	56.36
		5	52.75
Lena	44.15	3	59.88
		5	56.07
Peppers	44.11	3	55.37
		5	52.31
Sailboat	44.15	3	54.59
		5	51.57

Table 4
The comparison between [13] and ours under various signal processing attacks $r = 5$.

Attack	Lu et al. [13]		Ours	
	PSNR	*AR*	PSNR	*AR*
Blurring (Gaussian 0.5)	38.98	59.47	38.83	90.34
Brightness (50)	14.17	90.53	14.17	99.71
Brightness (50) + Contrast (50)	9.83	80.95	9.83	87.70
Contrast (50)	16.72	83.69	16.69	95.61
Cropping (rate 10%)	15.29	82.42	15.29	95.02
Cropping (rate 20%)	12.39	78.22	12.38	87.50
Cropping (rate 30%)	10.58	75.10	10.58	81.84
Cropping (rate 40%)	9.41	70.02	9.41	76.86
Cropping (rate 50%)	8.34	64.65	8.33	72.56
Cropping (rate 60%)	7.36	59.77	7.35	66.31
Cropping (around)	9.04	57.81	9.03	72.56
Equalization	19.15	90.13	19.11	100
Gaussian Noising (3%)	30.13	80.96	29.84	97.95
Gaussian Noising (6%)	24.48	73.73	24.54	87.21
Gaussian Noising (9%)	20.81	68.46	20.84	80.77
JPEG (Q = 6)	39.62	67.38	38.59	92.29
JPEG (Q = 8)	40.04	72.26	38.62	97.27
JPEG (Q = 10)	41.66	86.62	38.94	100
PSNR100	20.15	90.63	20.12	100
Rotation (degree 2)	13.99	49.21	13.98	51.47
Scaling (75%)	25.28	66.21	25.21	95.90
Scaling (200%)	25.64	89.36	25.56	100
Sharpening	33.55	91.40	26.19	100

Case 3: DV > 1 or DV < -1
In particular, the difference in the corresponding pixel values is greater than 1 or less than -1 approximates to 1.03% for $r = 3$, while it is nearly 1.91% for $r = 5$. That is, the novel scheme can effectively prevent the restored images from suffering serious distortions.

In general, the distortion of the restored image is mainly resulted from the DCT integer truncation operation. Hence, it is difficult to obtain a lossless restored image after the DCT transformation. Specifically, the influence of these DCT operations is more noticeable while the test image is a rough one such as Baboon. To mitigate this problem, we can increase the parameter u such that the embedding process begins at the coefficient value possessing lower energy.

Fig. 5. The attacked images and the extracted watermarks under various signal processing attacks.

From the view of human visual perception, we enlarge Lena to examine the performance of the novel scheme. For $r = 5$, the enlarged partial images of the original image and the watermarked image are shown in Fig. 4a and b, respectively. The marked areas in Fig. 4b indicate the distinct alteration in contrast with the original. The distortion of the watermarked image mainly occurs in the edge margins; this is caused by the swap operation near the edge margins. Nevertheless, Fig. 4c displays an excellent restored result from Fig. 4b. In human visual perception, the new scheme is capable of removing embedded information such that the reconstructed image is nearly identical to the original one.

For demonstrating the removability, we compare our method with [10] which possesses the best quality of the removed image so far. The average restored image quality of [10] is around 44 dB. The PSNR values of the reconstructed images listed in Table 3 show that our method outperforms that of Hu et al.

4.2. Analysis of robustness

The robustness is a significant concern for rightful protection mechanisms. However, it is also a drawback of the reversible and removable watermarking technique. For highlighting the robustness, we compare a traditional robust watermark scheme [13] with the new one through several simulation results. Lu et al. [13] propose a robust watermarking technique based on subsampling, which can resist common malicious attacks.

We apply attacks (including blurring, brightness, contrast, color reduction, cropping, equalization, Gaussian noising, JPEG compression, rotation, scaling, and sharpening) to the watermarked image with $r = 5$ to show the robustness of the novel method. According to the *AR*s displayed in Table 4, the proposed scheme is robust against most malicious attacks. However, the correlations between subimages must be seriously distorted, due to the rotation. Thus, the *AR* value was found to be unsatisfactory after we mounted the rotation attack on the test images. Few watermarking mechanisms can resist all malicious attacks. Hence, improving the *AR* value after rotation and other serious attacks is an important future challenge. So far, the proposed scheme can against the most common attacks to protect ownership and reconstruct the unmarked image for preserving the valuable images. The visual perception and the watermark logos retrieved by our method are presented in Fig. 5. Under these attacks, the retrieved logo images were recognizable, even though the images had been seriously distorted.

5. More discussions

The setting of system parameters will influence the receivable results. Here, the parameter u is used to indicate the zigzag position embedded with watermark bit in the low-frequency subband. According to the characteristic of DCT, that the embedded positions are close to the DC value will enhance the robustness of the watermarked image while it will seriously distort the watermarked image. Thus the parameter u influences the trade off between the restored image quality and the robustness. Through various experimental results, we suggest that $u = [6,20]$ is suitable for most images.

The parameters r is adopted to enhance the robustness of watermarked image. In case that the owners want to increase the robustness of the protected image, they can raise the value of r. This increase, however, may slightly fall the quality of restored image down. According to experiments, the setting of $r = 3$ or $r = 5$ is practicable for owners to balance the robustness of the protected image and the quality of unmarked image.

As to the parameter l, it indicates the position that we insert the element s into binary representation $\tilde{z}$. If the position is close to the MSB of $\tilde{z}$, our method may occur overflow of DCT coefficients. In case that it is near the LSB of $\tilde{z}$, the swap element s may be truncated after DCT operation. The extracted element s significantly influences the fidelity of the restored image. Thus, the element s shall be embedded in the middle bits of $\tilde{z}$. Here, we suggest the setting of l in range of [3,5] is appropriate.

Table 5
The functionality comparison between traditional watermarking schemes and the novel scheme.

	[1,4–6,9,17]	Hu et al. [10]	The novel scheme
Restorability	Reversible	Removable	Removable
Transparency	Lossless	Some distortion	Approximately-lossless
Security	Yes	Yes	Yes
Unambiguity	Yes	Yes	Yes
Blindness	Yes	Yes	Yes
Suitability for Medical Image	Yes	Yes	Yes
Visual recognizable logo	Yes	Yes	Yes
Robustness	None	None	Blurring Brightness Contrast Cropping Equalization JPEG Noising Scaling Sharpening

The functionality comparisons between the well-known watermarking mechanisms and ours are illustrated in Table 5. It is claimed in [1,4–6,9,17] that the proposed methods allow authorized users to losslessly recover the host image from the watermarked image. However, they cannot be used to protect the copyright of the watermarked image. According to the simulation results, the novel scheme not only achieves the essentials of general lossless and removable watermarking schemes but also possesses stronger robustness against common signal processing and geometric transformation attacks. This implies that the new method is indeed able to protect the ownership of the watermarked image under various kinds of attacks. Besides, the removability of the new scheme is practical for the application of preserving valuable images.

6. Conclusions

Traditional well-known lossless or removable watermarking schemes have been incapable of achieving the robustness requirement. That is, they cannot be used to protect the copyright of the watermarked image. In this article, we proposed a novel removable watermarking algorithm utilizing the Just Noticeable Distortion (JND) technique and the correlation difference between two selected subsampling images. Simulation results revealed that the new scheme approximated a lossless watermarking scheme. Moreover, the novel scheme resisted various signal processing attacks and geometric transformation attacks; therefore, it can be used to protect the ownership of important watermarked images. Furthermore, the novel method permitted authorized users to extract and restore the watermarked image without the host image. The new scheme confirms the essentials of robustness and restored image fidelity, which are practical for preserving valuable images.

References

[1] A.M. Alattar, Reversible watermark using the difference expansion of a generalized integer transform, IEEE Transactions on Image Processing 13 (8) (2004) 1147–1156.
[2] M. Barni, F. Bartolini, A. Piva, Improved wavelet-based watermarking through pixel-wise masking, IEEE Transactions on Image Processing 10 (5) (2001) 783–791.
[3] C.C. Chang, K.F. Hwang, M.S. Hwang, Robust authentication scheme for protecting copyrights of images and graphics, IEE Proceedings – Vision, Image and Signal Processing 149 (1) (2002) 43–50.
[4] C.C. Chang, C.C. Lin, C.S. Tseng, W.L. Tai, Reversible hiding in DCT-based compressed images, Information Sciences 177 (13) (2007) 2768–2786.
[5] C.C. Chang, W.L. Tai, C.C. Lin, A reversible data hiding scheme based on side match vector quantization, IEEE Transactions on Circuits and Systems for Video Technology 16 (10) (2006) 1301–1308.
[6] M.U. Celik, G. Sharma, A.M. Tekalp, Lossless watermarking for image authentication: a new framework and an implementation, IEEE Transactions on Image Processing 15 (4) (2006) 1042–1049.
[7] I.J. Cox, J. Kilian, F.T. Leighton, T. Shamoon, Secure spread spectrum watermarking for multimedia, IEEE Transactions on Image Processing 6 (12) (1997) 1673–1687.
[8] H. Guo, Y. Li, S. Jajodia, Chaining watermarks for detecting malicious modifications to streaming data, Information Sciences 177 (1) (2007) 281–298.
[9] Y. Hu, B. Jeon, Reversible visible watermarking and lossless recovery of original images, IEEE Transactions on Circuits and Systems for Video Technology 16 (11) (2006) 1423–1429.
[10] Y. Hu, S. Kwong, J. Huang, An algorithm for removable visible watermarking, IEEE Transactions on Circuits and Systems for Video Technology 16 (1) (2006) 129–133.
[11] C.H. Huang, J.L. Wu, Fidelity-guaranteed robustness enhancement of blind-detection watermarking schemes, Information Sciences 179 (6) (2009) 791–808.
[12] W.S. Kim, O.H. Hyung, R.H. Park, Wavelet based watermarking method for digital images using the human visual system, Electronics Letters 35 (6) (1999) 466–468.
[13] W. Lu, H. Lu, F.L. Chung, Robust digital image watermarking based on subsampling, Applied Mathematics and Computation 181 (2) (2006) 886–893.
[14] M. Makoto, Objective picture quality scale (PQS) for image coding, IEEE Transactions on Communications 46 (9) (1998) 1215–1226.
[15] A.A. Reddy, B.N. Chatterji, A new wavelet based logo-watermarking scheme, Pattern Recognition Letters 26 (2005) 1019–1027.
[16] F.Y. Shih, Y.T. Wu, Robust watermarking and compression for medical images based on genetic algorithms, Information Sciences 175 (3) (2005) 200–216.
[17] J. Tian, Reversible data embedding using difference expansion, IEEE Transactions on Circuits and Systems for Video Technology 13 (8) (2003) 890–896.
[18] H.H. Tsai, D.W. Sun, Color image watermark extraction based on support vector machines, Information Sciences 177 (2) (2007) 550–569.
[19] Z. Wang, A.C. Bovik, H.R. Sheikh, E.P. Simoncelli, Image quality assessment: from error visibility to structural similarity, IEEE Transactions on Image Processing 13 (4) (2004) 600–612.
[20] F.H. Wang, K.K. Yen, L.C. Jain, J.S. Pan, Multiuser-based shadow watermark extraction system, Information Sciences 177 (12) (2007) 2522–2532.
[21] A.B. Watson, DCT quantization matrices visually optimized for individual images, Human Vision, Visual Processing, and Digital Display IV, Bellingham, WA, SPIE 1913 (1993) 202–216.