Pattern Recognition 41 (2008) 3497 – 3506

Contents lists available at ScienceDirect

Pattern Recognition

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

Dual watermark for image tamper detection and recovery

Tien-You Lee*, Shinfeng D. Lin

Department of Computer Science and Information Engineering, National Dong Hwa University, No. 1, Sec. 2. Da Hsueh Rd., Shoufeng, Hualien 97401, Taiwan, ROC

ARTICLE INFO

Article history:
Received 11 April 2007
Received in revised form 25 March 2008
Accepted 6 May 2008

Keywords:
Dual watermark
Tamper recovery
Second chance
Partner-block

ABSTRACT

An effective dual watermark scheme for image tamper detection and recovery is proposed in this paper. In our algorithm, each block in the image contains watermark of other two blocks. That is to say, there are two copies of watermark for each non-overlapping block in the image. Therefore, we maintain two copies of watermark of the whole image and provide second chance for block recovery in case one copy is destroyed. A secret key, which is transmitted along with the watermarked image, and a public chaotic mixing algorithm are used to extract the watermark for tamper recovery. By using our algorithm, a 90% tampered image can be recovered to a dim yet still recognizable condition (PSNR $\approx$ 20 dB). Experimental results demonstrate that our algorithm is superior to the compared techniques, especially when the tampered area is large.

1. Introduction

In recent years, the image authentication comes to the front of the image processing. This is mainly a result of the rapid growth in computer power, Internet technology, electronic commerce, multimedia market, medical imaging applications, and the great mass fervor in World Wide Web. A huge amount of multimedia data is easily accessible for everyone through the Internet daily. Nevertheless, multimedia data in digital format can be modified or tampered with ease using a lot of image processing tools, whether it is malicious or not. In other words, we are not sure if the image we have received from the Internet is authentic. The protection of intellectual property rights is another increasingly important issue while a large number of digital images are interchanged on the Internet everyday. So, it is really a big problem to ensure the integrity of received images as well as the original ownership for potential security loopholes of the public Internet.

The integrity and authenticity of digital images can be guaranteed by using digital watermarking which is a technique to embed a digital signature into an image. The digital signature is a data string associated with something that can be used for a variety of purposes. It can be either perceptible or imperceptible. Perceptible watermark is usually an institution's logo or message which can be recognized together with the host image. On the other hand, imperceptible watermark is information hidden in the image. Imperceptible watermark could be a company logo, a literary message indicating the ownership of the image, parts of the host image, and even a full copy of the host image itself. It can later be extracted by using a pre-designed extracting scheme for various purposes, including content integrity verification, ownership authentication, secret message conveyance and so forth.

Various watermark schemes have been proposed for different missions and considerations, such as convenience, security, speed, multipurpose and so on. Traditional imperceptible watermark technique, based on the functionality, can be classified as fragile watermark, semi-fragile watermark and robust watermark. Fragile watermark [1–6] can be easily altered or destroyed by any sort of image operation such as compression, rotation, stretching, blurring, sharpening, scaling, cropping and various malicious manipulations. Since it is sensitive to all sorts of modifications, fragile watermark is usually used to verify the integrity of the received images. Semi-fragile watermark [7,8] can locate modified regions in an image and extract the remaining watermark from the undamaged regions. So, a semi-fragile watermark is capable of authenticating an image even after some manipulations on the image. Robust watermark [9–12] is designed to resist various attacks that attempt to destroy the watermark in the image. The main purpose of robust watermark is ownership authentication or copyright protection. However, watermark for tamper detection and recovery [13–16] has received much attention recently. Different from other types of digital watermarks, it not only detects and locates modifications in an image, but also recovers the modified regions with information hidden in the image. The watermark is no longer a logo or a piece of message; it is the image itself. The image is usually reduced to proper size called

* Corresponding author. Tel.: +886 3 8634040; fax:+886 3 8634010.
E-mail address: d9121003@em91.ndhu.edu.tw (T.-Y. Lee).

0031-3203/$30.00 © 2008 Elsevier Ltd. All rights reserved.
doi:10.1016/j.patcog.2008.05.003

feature image, which still contains enough information to represent the original image data. This feature image is then embedded into the original image through various techniques to form the watermarked image. The quality of the watermarked image is usually high enough and then publicized on the Internet as a replacement for the original image. In case, the watermarked image is damaged, the feature image can be extracted to reconstruct the image.

A representative of the watermarking technique for tamper detection and recovery is the hierarchical digital watermarking scheme proposed by Lin et al. [15]. In Lin's method, the detection of tampered regions is based on a 3-level hierarchical structure. If a tampered block is not detected in level-1 inspection, it will be detected in level-2 or level-3 inspection with a probability of nearly 1. Lin's method is also storage effective, as it only requires a secret key and a public chaotic mixing algorithm to recover a tampered image.

There are two main drawbacks in Lin's algorithm. First, it is too sensitive to error pixels. For example, if only a single pixel in a block of size 4×4 pixels is tampered, the whole block will be marked as invalid and replaced with some other value. Second, if block A and its mapping block A′ are both invalid, block A must be recovered by the average intensity of its 3×3 neighboring block values. There is no second chance for block A to be recovered from another block and usually results in blocky effect and degrades the image quality seriously.

In this paper, we restrict our attention to the processes of watermark embedding, tamper detection and tamper recovery without discussing the cryptographic issues. We propose an improved watermark embedding and tamper recovery scheme which is superior to Lin's method in four ways: (1) less sensitive to error pixels; (2) second chance for block recovery; (3) unobvious blocky effect; (4) better image resolution after tamper recovery. In our algorithm, there are two copies of watermark for each non-overlapping block in the image. So, we provide second chance for block recovery and the experimental results demonstrate that our algorithm is truly efficient and effective, especially when the tampered area is large.

The remainder of this paper is organized as follows. Section 2 describes the proposed dual watermark scheme including watermark embedding, detection of tampered blocks and recovery of tampered blocks. Experimental results are given in Section 3. Section 4 concludes this paper.

2. The proposed algorithm

Our method can be portrayed as the following 3-stage algorithm: (1) watermark embedding, which hides watermark of each pair of partner-block to another two mapping blocks; (2) tampered block detection, which can be achieved through a 3-level hierarchical error block checking; (3) tampered block recovery, which can be achieved through a 2-stage error block recovery scheme. The flowcharts of watermark generation, watermark embedding, tamper detection and tamper recovery are shown in Figs. 1 and 2, and the detail will be discussed thereafter.

2.1. Watermark embedding

All the images used in this paper are assumed to be of size $M \times M$ pixels, where M is a multiple of two and each block is of size 2×2 pixels.

2.1.1. Preparation

We need a block mapping sequence to encrypt watermark information. A 1-D transformation algorithm described in Ref. [15], which is shown in Eq. (1), is used to obtain a one-to-one mapping sequence.

$$X' = [f(X) = (k \times X) \bmod N] + 1, \quad (1)$$

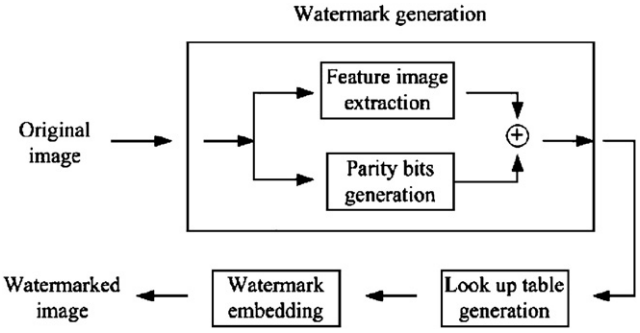

Fig. 1. Flowchart of watermark generation and embedding.

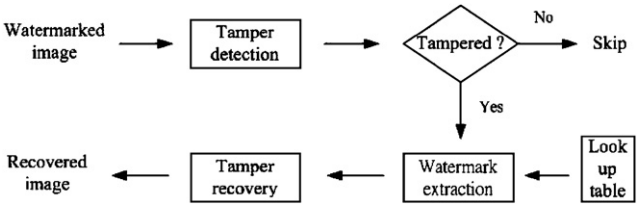

Fig. 2. Flowchart of tamper detection and recovery.

where X, X' ($\in [0, N-1]$) are the block number, k (a prime and$\in Z - \{N\text{'s factors}\}$) is a secret key and N ($\in Z - \{0\}$) is the total number of blocks in the image.

A look-up table is then constructed to record the mapping address of each block in the image. There are two important properties in the mapping sequence which are inherent by using the 1-D transformation algorithm. First, the mapping addresses of the blocks in the upper half of the image are complementary to those blocks at the same positions in the lower half of the image. For example, Fig. 3(a) is the original block sequence of an 8×8 table. Fig. 3(b) is the look-up table of Fig. 3(a) generated by Eq. (1) with $N = 64$ and $k = 13$. In Fig. 3(c), the original table is horizontally divided into two equal parts. Blocks 0 and 32 are partner-block, which are located at the same position in these two parts. Checking the look-up table in Fig. 3(b), the mapping address of block 0 is 1, denote by M_1; the mapping address of block 32 is 33, denote by M_2. Notice that $|M_1 - M_2| = N/2$ for all pairs of partner-block in the original table. It means that if block A's mapping block is located in one of these two parts, then the mapping block of A's partner-block will be located in the other part. This is also the way we choose partner-blocks in the watermark generation stage. Because even if the upper half or the lower half of the image is totally tampered, the information of the tampered region can be entirely restored by the information hidden in the other half of the image.

Second, the 1-D transformation scheme moves a whole column to another position within the table. The column mapping sequence $C_a \to C_b \to C_c \to \cdots \to C_a$ is decided by the secret key we have chosen. The elements in a column are exactly the same before and after the movement, yet the permutation is changed. For example, column 0 of Fig. 3(a) [0 8 16 24 32 40 48 56] is moved to column 3 after the 1-D transformation block mapping operation as shown in Fig. 3(b) [40 16 56 32 8 48 24 0], and column 1 of Fig. 3(a) [1 9 17 25 33 41 49 57] is moved to column 0 in Fig. 3(b) [1 41 17 57 33 9 49 25], etc. As is known to all, if a block is tampered, its neighboring blocks will most likely be tampered too. So, the watermark of a block should be hidden far from the block. The whole-column moving phenomenon exists for all prime keys and significantly debases the recovering rate. For example, suppose columns 0 and 1 of Fig. 3(a) are tampered concurrently. According to the look-up table

a

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

b

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

c

0							
32							

d

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

Fig. 3. (a) The original table; (b) the look-up table of (a); (c) two equal parts of the original table; (d) the modified look-up table after push-aside operation.

Table 1
Recovered blocks relative to tampered blocks (%)

Tampered (%)	Without push-aside operation	With push-aside operation
10	92.31	100
20	76.92	100
30	69.23	100
40	60.78	100
50	51.56	100
60	38.96	66.23
70	31.11	42.22
80	18.48	24.31

in Fig. 3(b), the watermarks of blocks in column 0 are hidden in column 1; the watermarks of blocks in column 1 are hidden in column 6. The information of all blocks in column 1 can be recovered from the watermarks hidden in column 6. However, the information of all blocks in column 0 together with their watermarks in column 1 had been tampered concurrently; we lose the information of all blocks in column 0 forever.

A push-aside operation is used to modify the look-up table and resolve this problem. Briefly speaking, the watermarks of the left half of the image are concentrated in the right half region of the image, and the watermarks of the right half of the image are concentrated in the left half region of the image. We simply push right the columns in Fig. 3(b) which originally belong to the left half of Fig. 3(a) and push left the columns in Fig. 3(b) which originally belong to the right half of Fig. 3(a), and result in a modified look-up table as shown in Fig. 3(d).

We simulate the attacks by cropping a portion of a 128×128 table, begin with the first column, from left to right, and the type of tampering is single-chunk distribution. Table 1 shows the recovering rate for the look-up table with and without the push-aside operation. It is clear that after the push-aside operation, the recovering rate of the tampered blocks is significantly exalted. With the push-aside operation, the information of the tampered blocks can be entirely recovered if the rate of tampering is less than or equal to 50%. Notice that the push-aside operation does not affect the recovering rate if the tampered region is located in the upper/lower half of the image.

2.1.2. Block watermark generation

The original image is first divided horizontally into two equal parts as shown in Fig. 4(a). Blocks A and B are partner-block which are located at the same position in these two parts. They are both of size 2×2 pixels as shown in Fig. 4(b). Fig. 4(c) calculates the average intensity of each block. Each pair of partner-block in the image is processed together in the embedding stage.

The representative information of block A is constructed by extracting the five most significant bits of block A's average intensity, and is then combined with (1) the representative information of block B and (2) the in-block parity-check bits p and v to construct

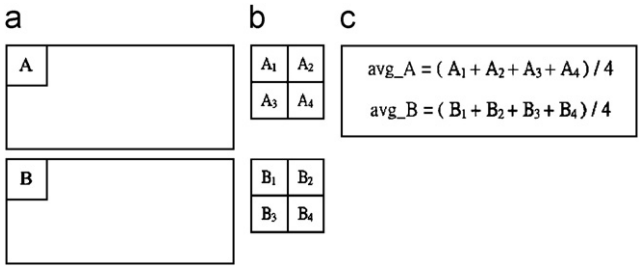

Fig. 4. (a) Two equal parts of the original image; (b) each block in (a) is of size 2×2 pixels; (c) average intensity of each block in (a).

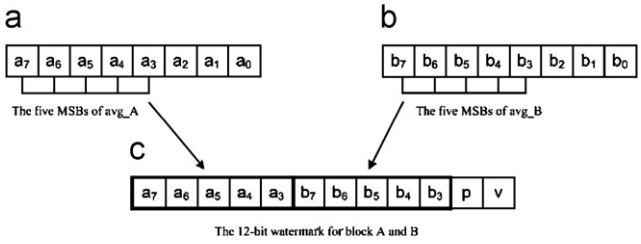

Fig. 5. (a) Average intensity of block A (avg_A); (b) average intensity of block B (avg_B); (c) the joint 12-bit watermark for blocks A and B.

the joint 12-bit watermark for blocks A and B as shown in Fig. 5.

The parity-check bits p and v are generated as below:

$$p = a_7 \oplus a_6 \oplus a_5 \oplus a_4 \oplus a_3 \oplus b_7 \oplus b_6 \oplus b_5 \oplus b_4 \oplus b_3, \tag{2}$$

$$v = \begin{cases} 1 & \text{if } p = 0, \\ 0 & \text{otherwise.} \end{cases} \tag{3}$$

2.1.3. Block watermark embedding

Two mapping blocks are needed to embed the joint 12-bit watermark of block A and its partner-block B. We check the look-up table, which is generated by the modified 1-D transformation function, to find these two mapping blocks. Fig. 6 shows how the 12-bit watermark of each pair of partner-block is embedded to their mapping blocks. The three LSBs of each pixel are used for watermark embedding. Suppose blocks C and D are the two mapping blocks which are going to be used to embed the 12-bit watermark resulted from blocks A and B. In Fig. 6(c), both blocks C and D contain the same 12-bit watermark and the same embedding sequence in the corresponding locations. That is to say, for each block of size 2×2 pixels in the image, we have two copies of its representative information hidden somewhere in the image. Therefore, if one copy is tampered

a

C_1	C_2
C_3	C_4

b

D_1	D_2
D_3	D_4

c

bit	7	6	5	4	3	2	1	0
C_1						a_7	a_6	a_5
C_2						a_4	a_3	b_7
C_3						b_6	b_5	b_4
C_4						b_3	p	v
D_1						a_7	a_6	a_5
D_2						a_4	a_3	b_7
D_3						b_6	b_5	b_4
D_4						b_3	p	v

Fig. 6. (a) Block C; (b) block D; (c) embedding sequence of the joint 12-bit watermark in blocks C and D.

Table 2
The PSNR of the watermarked images

Image	Sailboat	Lena	Zelda	Pepper	Baboon	Barbara
With smoothing function (dB)	40.70	40.68	40.71	40.73	40.73	40.72
Without smoothing function (dB)	38.57	38.21	38.21	38.42	38.31	38.19

by any chance, we have a second chance to recover this block from the other copy.

Before physically changing the value of a pixel in the mapping block, a smoothing function is applied to minimize the difference between the original pixel and the watermarked pixel, and hence improve the quality of the watermarked image. For example, the value of pixel X is 232 (11101000_2), and (111_2) is the 3-bit watermark which is going to be embedded in X. After watermark embedding, X', the watermarked X is 239 (11101111_2). The difference between X' and X is $239-232=7$. Instead of adding 7 to X, we subtract 1 from X and make $X'=232-1=231(11100111_2)$. The difference between X and X' becomes $232-231=1$, and the 3-bit watermark in X' is not affected at all. The smoothing function is given by

$$x' = \begin{cases} x_1 + v & \text{if } |v| < 5, \\ x_1 + v + 8 & \text{if } v \leqslant -5, \\ x_1 + v - 8 & \text{if } v \geqslant 5, \end{cases} \quad (4)$$

where $X_1 = X$ AND $(11111000)_2$, that is, replace the three LSBs of X with "0", and denote it by X_1; v is the difference between the value of the 3-bit watermark which is going to be embedded in X and the value of the three LSBs in X.

Table 2 shows the qualities of the watermarked images with and without the smoothing function. After applying the smoothing function, the quality of each watermarked image is promoted more than 2 db.

2.2. Detection of tampered blocks

A 3-level hierarchical tamper detection algorithm which is similar to Lin's method [15] is applied in our scheme. In the following, the procedure of our detection scheme is briefly described.

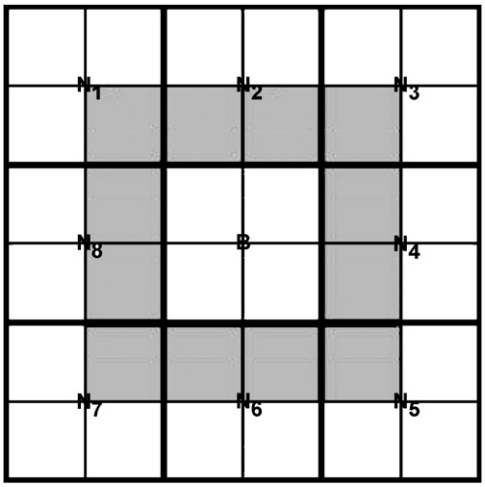

Fig. 7. Pixels used for recovery within the 3×3 block neighborhood.

Level-1 detection: For each non-overlapping block B of size 2×2 pixels in the image:

1. Retrieve the 12-bit watermark information of block B.
2. Get the parity-check bits p and v from the watermark.
3. Calculate the exclusive-or value of the first 10 bits of the watermark, denoted as p'.
4. If $p = p'$ and $p \neq v$, mark block B valid; otherwise, mark it invalid.

Level-2 detection: For each block B which is marked valid after level-1 detection, check the following four triples of neighboring block situation: (N, NE, E), (E, SE, S), (S, SW, W), (W, NW, N). The 3×3 block-neighborhood of the central block B can be denoted by the compass directions:

NW N NE

W B E

SW S SE

If all blocks in any of the four triples are marked invalid, mark block B invalid.

Level-3 detection: For each valid block after level-2 detection, mark this block invalid if there are five or more neighboring blocks in its 3×3 block-neighborhood that are invalid.

Our technique introduces much less false alarms because we use small block size (2×2 pixels). Yet, in Lin's method [15], if only a single pixel in a block of size 4×4 pixels is tampered, the whole block will be marked as invalid, and hence results in more false alarms than our method.

2.3. Recovery of tampered blocks

After the tamper detection process, all blocks in the image are marked either valid or invalid. Only those invalid blocks need to be recovered. A two-stage recovery scheme is applied for tamper recovery as follows.

Stage-1 recovery: For each non-overlapping block B of size 2×2 pixels which is marked invalid,

1. Find the mapping block of B from the look-up table, denote by B′.
2. If B′ is valid then B′ is the candidate block, go to 5.
3. Find the mapping block of B's partner-block, denote by B″.

Fig. 8. (a) The original Elvis; (a_1) the tampered Elvis (22% cropped); (a_2) result of Lin's algorithm (PSNR = 33.11 dB); (a_3) result of the proposed algorithm (PSNR = 36.39 dB); (b) the original sailboat; (b_1) the tampered sailboat (2% tampered); (b_2) result of Wang's algorithm (PSNR = 31.65 dB); (b_3) result of the proposed algorithm (PSNR = 42.22 dB); (c) the original Lena; (c_{11}) the tampered Lena (61% cropped); (c_{12}) result of Lin's algorithm (PSNR = 19.47 dB); (c_{13}) result of the proposed algorithm (PSNR = 25.20 dB); (c_{21}) the tampered Lena (1% tampered); (c_{22}) result of Wang's algorithm (PSNR = 33.36 dB); (c_{23}) result of the proposed algorithm (PSNR = 47.17 dB).

4. If B″ is valid then B″ is the candidate block; otherwise stop, leave block B alone.
5. Retrieve the 12-bit watermark information from the candidate block.
6. If block B locates in the upper half of the image, the 5-bit representative information of block B starts from the first bit (the left most bit) of the 12-bit watermark; otherwise, it starts from the sixth bit.
7. Pad three 0's to the end of the 5-bit representative information to form a new 8-bit intensity.
8. Replace each pixel in block B with this new 8-bit intensity and mark block B as valid.

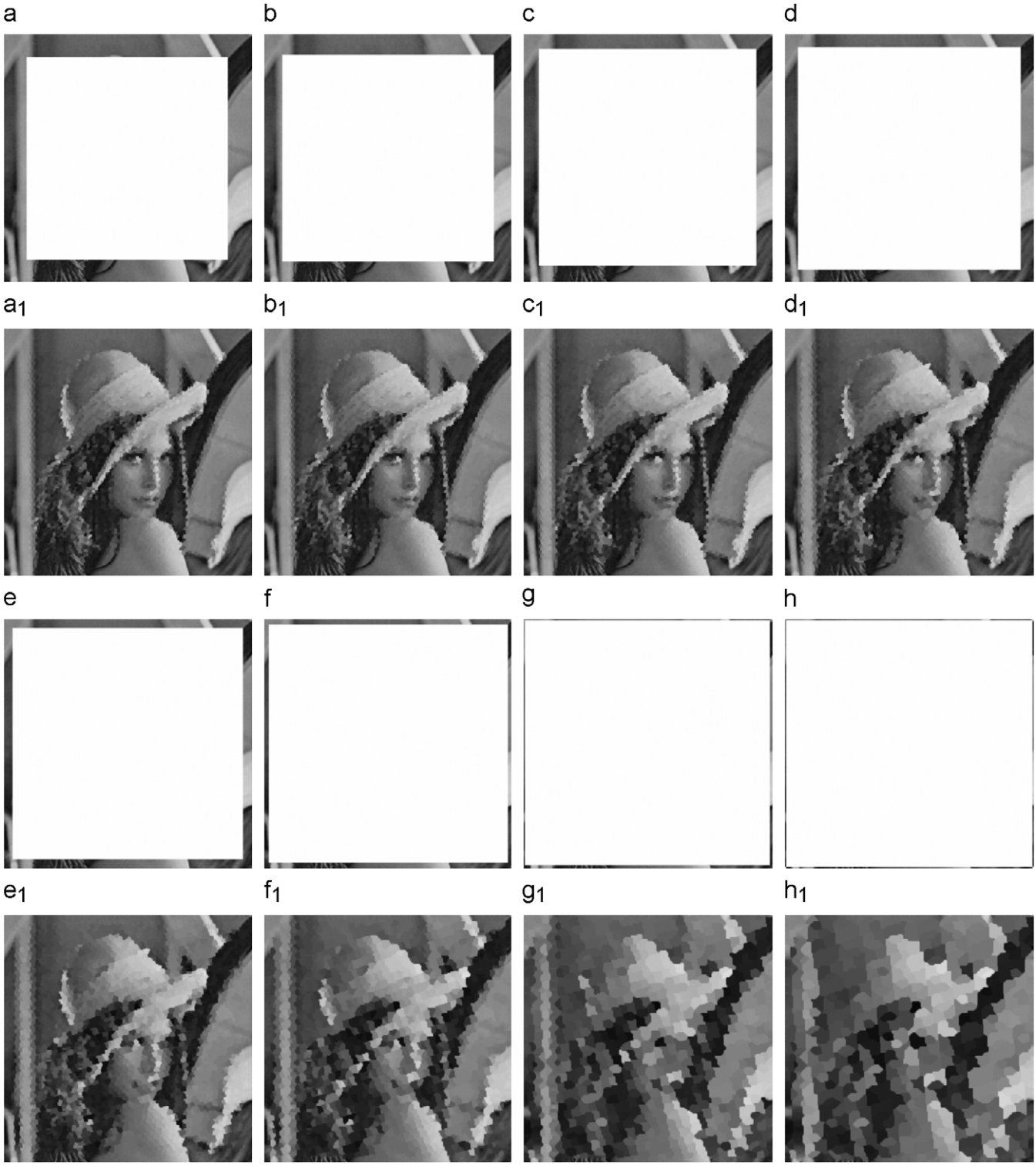

Fig. 9. (a) 65% cropped; (a_1) recovered image of (a), PSNR = 24.57 dB; (b) 70% cropped; (b_1) recovered image of (b), PSNR = 24.16 dB; (c) 75% cropped; (c_1) recovered image of (c), PSNR = 23.43 dB; (d) 80% cropped; (d_1) recovered image of (d), PSNR = 22.55 dB; (e) 85% cropped; (e_1) recovered image of (e), PSNR = 21.28 dB; (f) 90% cropped; (f_1) recovered image of (f), PSNR = 19.86 dB; (g) 95% cropped; (g_1) recovered image of (g), PSNR = 18.05 dB; (h) 97% cropped; (h_1) recovered image of (h), SNR = 16.87 dB.

Stage-2 recovery: Recover the remaining invalid blocks after stage-1 recovery with the pixels surrounding them as shown in Fig. 7. The central block B in Fig. 7 is the block being processed, blocks $N_1 \sim N_8$ are B's 3×3 neighboring blocks. Only the darker pixels surrounding block B are used for stage-2 recovery.

3. Experimental results

Three quantities are evaluated for the performance of the proposed algorithm. The first one is the quality of the recovered image after various sizes and types of image manipulation. The second one

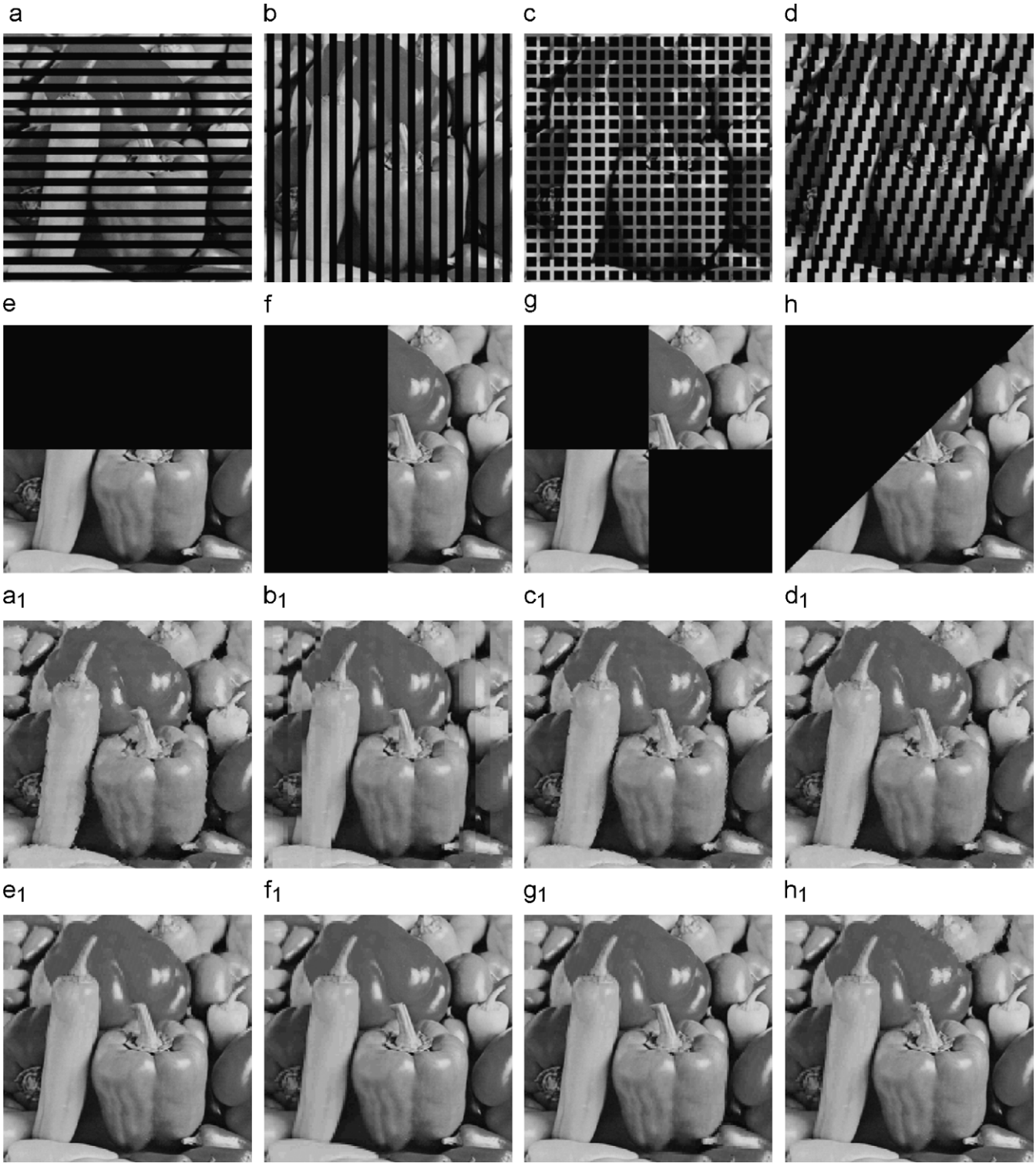

Fig. 10. (a)–(h) Eight different types of tampering distribution which are all 50% tampered; (a_1) recovered image of (a), PSNR = 27.35 dB; (b_1) recovered image of (b), PSNR = 26.22 dB; (c_1) recovered image of (c), PSNR = 29.20 dB; (d_1) recovered image of (d), PSNR = 29.01 dB; (e_1) recovered image of (e), PSNR = 30.69 dB; (f_1) recovered image of (f), PSNR = 30.96 dB; (g_1) recovered image of (g), PSNR = 31.14 dB; (h_1) recovered image of (h), PSNR = 29.91 dB.

is the percentage of the tampered blocks not recovered after stage-1 tamper recovery. The last one is the quality of the watermarked image. The performance of the proposed technique is compared with some existing methods [14–16].

Fig. 8(a) is the original Elvis. In Fig. 8(a_1), the facial features of Elvis are all cropped. Lin's method [14] results in a stained and confused man with grim look on his face as shown in Fig. 8(a_2). On the contrary, our technique results in a clear Elvis with much better quality than Lin's method as shown in Fig. 8(a_3). Fig. 8(b) is the original sailboat. In Fig. 8(b_1), the sailboat has been wiped out from the scene. Wang's method [16] results in poor resolution as shown in Fig. 8(b_2), yet we got a pellucid sailboat with the quality more than 10 dB better than

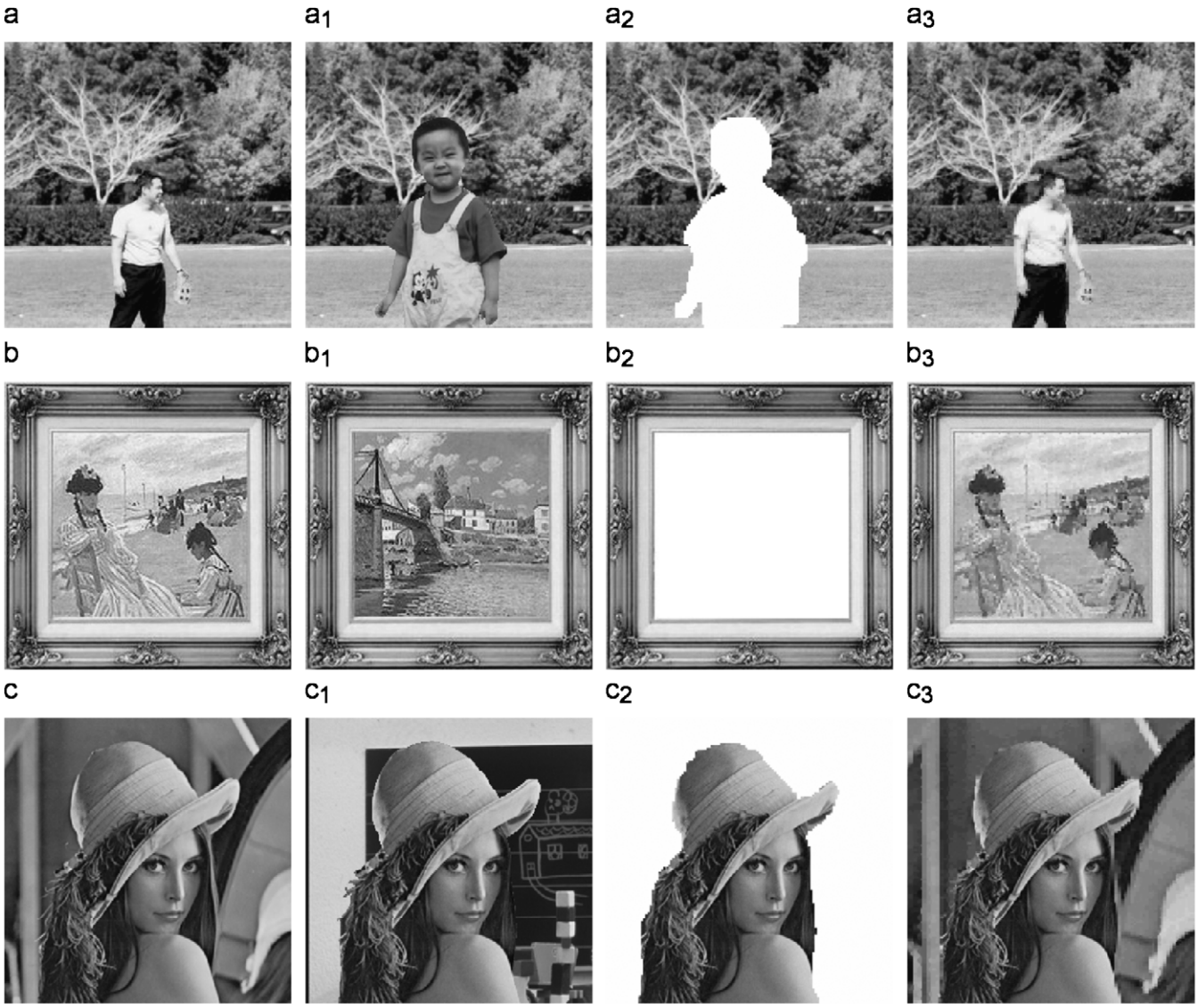

Fig. 11. (a)–(c) Original images; (a_1) the tampered image of (a) (21% tampered); (b_1) the tampered image of (b) (43% tampered); (c_1) the tampered image of (c) (55% tampered); (a_2)–(c_2) the detected tampered regions of (a_1)–(c_1) which are displayed in white; (a_3) recovered image of (a_1), PSNR = 29.53 dB; (b_3) recovered image of (b_1), PSNR = 25.41 dB; (c_3) recovered image of (c_1), PSNR = 26.89 dB.

Wang's method as shown in Fig. 8(b_3). Fig. 8(c) is the original Lena. In Fig. 8(c_{11}), the image is 61% cropped and the head of Lena is fully sheltered. Lin's method results in an extremely blurred image which is impossible to be recognized as shown in Fig. 8(c_{12}). However, as shown in Fig. 8(c_{13}), our technique results in a still clear Lena with the quality more than 5 dB better than Lin's method. In Fig. 8(c_{21}), a decoration is put on Lena's hat. Wang's method results in a blurred image as shown in Fig. 8(c_{22}), yet we got a clear Lena with the quality more than 13 dB better than Wang's method as shown in Fig. 8(c_{23}).

Furthermore, we expand the cropping size from 65% to 97% as shown in Figs. 9(a)–(h) to see the outstanding performance of restoration of the proposed algorithm. The quality of the recovered image degrades from Figs. 9(a_1)–(h_1) as the cropping size increases. Fig. 9(d) is 80% cropped, yet we can still recognize Lena's eyebrows, eyes, nose, lips, etc., in Fig. 9(d_1). In Fig. 9(f), the image is 90% cropped but we still know it is Lena in the recovered image as shown in Fig. 9(f_1). In Fig. 9(g), although the remaining valid information is only 5%, the contour of Lena can still be recognized as shown in Fig. 9(g_1). The experimental results demonstrate that as long as the image is not totally destroyed, we can restore the image to a certain extent. And the quality of the recovered image is still acceptable even if the tampered area is really large.

Eight different types of tampering distribution are applied to simulate cropping attacks in Fig. 10. We simply black out 50% of the test image at various locations as shown in Figs. 10(a)–(h). The experimental results show that the performance of our algorithm for the chunk-distribute tampering (Figs. 10(e)–(h), with PSNR around 30 dB) is better than the spread-distribute tampering (Figs. 10(a)–(d), with PSNR less than 30 dB). The worst case is the longitudinal spread-distribute tampering as shown in Fig. 10(b). The quality of the recovered image is degraded to 26.22 dB and the blocky effect is obvious as shown in Fig. 10(b_1). The whole-column moving phenomenon, which is inherent in the 1-D transformation block mapping scheme, accounts for the degradation of the image quality for longitudinal spread-distribute tampering. If column A and its mapping column in the image are tampered concurrently, we lose the information of column A forever. According to our algorithm, each block in column A will be recovered with the surrounding pixels in its 3×3

Table 3
The percentage of blocks not recovered after stage-1 tamper recovery (test image: Lena)

Tampered (%)	Location	5	10	15	20	30	40	50	70
Lin et al.	–	0	2	2.2	4.8	7.5	14	20	39
Proposed	Center	0	0	0	0	0	0	0	25.57
Proposed	Top/bottom	0	0	0	0	0	0	0	28.56
Proposed	Left/right	0	0	0	0	0	0	0	40.63

neighboring blocks and consequently bring about blocky effect and degrade the image quality. However, the blocky effect that arose in our algorithm is much less obvious than in Lin's method [14]. Lin et al. recovered such block with the average intensity of its 3×3 neighboring block values that resulted in serious blocky effect, and hence severely degraded the quality of the recovered image as shown in Fig. 8(c_{12}).

Notice that Fig. 10(f) can also be viewed as longitudinal tampering distribution; yet the quality of its recovered image is more than 4 dB better than Fig. 10(b). It is because the push-aside operation applied in our algorithm and the information of the cropped left half region can be entirely restored by the information hidden in the right half region. Fig. 11 illustrates three kinds of malicious manipulations that are concerned with covering and replacing attacks. The tampered regions are all well detected and recovered by the proposed algorithm.

Table 3 lists the percentage of blocks not recovered after stage-1 tamper recovery for both Lin's [14] and our algorithm. The stage-1 recovering rate of our technique is 100% when the rate of tampering is less than or equal to 50% for single-chunk tampering distribution. That is to say, we can restore almost all tampered blocks by the information hidden in the image even if the image is half tampered. Table 4 lists the PSNR of the recovered image relative to various tampered sizes and locations. When the tampered region is small, the performance of Lin's method [14] is a little better than ours. But when the tampered region grows gradually, Lin's performance falls behind ours, especially when the tampered region is really large. In Lin's method, when the image is 61% tampered, the quality of the recovered image is 19.47 dB. Nevertheless, the quality of the recovered image is 19.86 dB for our technique even if the image is 90% tampered.

The quality of the watermarked image is around 44.4 dB for Lin's method [14] which uses two LSBs of each pixel for watermark embedding. Li et al. [13] uses only one bit (the fourth bit from the last) and the quality of their watermarked image is around 42.3 dB. Three lower bits of each pixel are used in Wang's method [16] which gives the quality of the watermarked image around 33.3 dB. In our approach, we use the three LSBs of each pixel in the image for watermark embedding. The quality of our watermarked image is around 40.7 dB which is acceptable and the distortion is imperceptible to human eyes. Comparing with these methods, ours has much better capability of tamper recovery especially when the tampered area is large.

4. Conclusions

In this paper, an effective dual watermark scheme for image tamper detection and recovery has been proposed. This scheme provides the ability to hierarchically detect the tampered regions and dual chance for tamper recovery. Experimental results demonstrate that the proposed method has resilience for cropping, covering, removing and replacing attacks. Our scheme is efficient because we only use parity-check for tamper detection, a secret key and a public chaotic mixing algorithm for tamper recovery, and there is no need of the original image.

Table 4
The PSNR of the recovered image relative to the tampered size and location (test image: Lena)

Tampered size	Tampered %	Location	Lin et al. (dB)	Proposed (dB)
6×256	2.34	Top	48.97	48.09
40×40	2.4	Center	39.96	39.48
70×75	8.01	Corner	42.32	41.42
80×80	9.7	Center	36.24	35.17
256×64	25.0	Left	31.60	33.45
85×256	34.0	Top	27.37	33.01
164×164	40.1	Center	23.97	27.97
200×200	61.0	Center	19.47	25.20
206×206	65.0	Center	–	24.57
214×214	70.0	Center	–	24.16
222×222	75.0	Center	–	23.43
230×230	80.0	Center	–	22.55
236×236	85.0	Center	–	21.28
244×244	90.0	Center	–	19.86
250×250	95.0	Center	–	18.05

Our scheme is superior to the compared techniques in two aspects. First, our scheme is less sensitive to error pixels and introduces much less false alarms. Second, we use dual watermark technique to provide a second chance for block recovery that results in better image resolution. It gives outstanding performance, especially when the tampered area is really large. Based on the advantages described above, in conclusion, our scheme is really efficient and effective for image tamper detection and recovery.

References

[1] G.L. Friedman, The trustworthy digital camera: restoring credibility to the photographic image, IEEE Trans. Consum. Electron. 39 (1993) 905–910.
[2] M.M. Yeung, F. Mintzer, An invisible watermarking technique for image verification, in: Proceedings of ICIP' 97, Santa Barbara, California, 1997, pp. 680–683.
[3] P.W. Wong, A watermark for image integrity and ownership verification, in: Proceedings of the IS&T PIC. Conference, Portland, USA, May 1998.
[4] C.W. Wu, D. Coppersmith, F.C. Mintzer, C.P. Tresser, M.M. Yeung, Fragile imperceptible digital watermark with privacy control, in: Proceedings of the SPIE Security Watermarking Multimedia Contents, vol. 3657, 1999, pp. 79–84.
[5] D. Kundur, D. Hatzinakos, Digital watermarking for telltale tamper proofing and authentication, Proc. IEEE 87 (7) (1999) 1167–1180.
[6] G.J. Yu, C.S. Lu, H.Y.M. Liao, Mean quantization-based fragile watermarking for image authentication, Opt. Eng. 40 (7) (2001) 1396–1408.
[7] C.Y. Lin, S.F. Chang, Semi-fragile watermarking for authenticating JPEG visual content, in: SPIE International Conference on Security and Watermarking of Multimedia Contents II, vol. 3971, no. 13, EI '00, San Jose, USA, January 2000.
[8] J. Fridrich, A hybrid watermark for tamper detection in digital images, in: International Symposium on Signal Processing and Its Applications, vol 1, 1999, pp. 301–304.
[9] J. Zhao, E. Koch, Embedding robust labels into images for copyright protection, in: Intellectual Property Rights New Technologies, Proceedings of KnowRight'95 Conference, 1995, pp. 242–251.
[10] M.D. Swanson, B. Zhu, A.H. Tewfik, Robust data hiding for images, in: Proceedings of the IEEE Digital Signal Processing Workshop (DSP 96), Loen, Norway, September 1996, pp. 37–40.
[11] I.J. Cox, J. Kilian, T. Leighton, T. Shamoon, Secure spread spectrum watermarking for multimedia, IEEE Trans. Image Process. 6 (1997) 1673–1687.
[12] C.S. Lu, S.K. Huang, C.J. Sze, H.Y.M. Liao, Cocktail watermarking for digital image protection, IEEE Trans. Multimedia 2 (2000) 209–224.
[13] K.-F. Li, T.-S. Chen, S.-C. Wu, Image tamper detection and recovery system based on discrete wavelet transform, in: IEEE Pacific Rim Conference on Communications, Computers and Signal Processing, vol. 1, August 2001, pp. 164–167.
[14] P.-L. Lin, P.-W. Huang, A.-W. Peng, A fragile watermarking scheme for image authentication with localization and recovery, in: IEEE Sixth International Symposium on Multimedia Software Engineering, 13–15 December 2004, pp. 146–153.
[15] P.-L. Lin, C.-K. Hsieh, P.-W. Huang, A hierarchical digital watermarking method for image tamper detection and recovery, Pattern Recognition 38 (2005) 2519–2529.
[16] C.-L. Wang, R.-H. Hwang, T.-S. Chen, H.-Y. Lee, Detecting and restoring system of tampered image based on discrete wavelet transformation and block truncation coding, in: 19th International Conference on Advanced Information Networking and Applications, 2005.

About the Author—TIEN-YOU LEE is a PhD student at the Department of Computer Science and Information Engineering of National Dong Hwa University. His research interests include digital watermark and medical image processing. He received his MS degree in Computer Science from the Utah State University.

About the Author—SHINFENG D. LIN is a professor at the Department of Computer Science and Information Engineering of National Dong Hwa University. His research interests include digital watermark, signal/image processing, image/video compression and information security. He received his PhD degree in electrical engineering from the Mississippi State University.