Displays 46 (2017) 52–60

Contents lists available at ScienceDirect

Displays

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

Hierarchical recovery for tampered images based on watermark self-embedding ☆

Fang Cao [a,b,*], Bowen An [a,*], Jinwei Wang [b], Dengpan Ye [c], Huili Wang [d]

[a] College of Information Engineering, Shanghai Maritime University, Shanghai 200135, China
[b] School of Computer and Software, Nanjing University of Information Science & Technology, Nanjing 210044, Jiangsu, China
[c] School of Computer, Wuhan University, Wuhan 430072, Hubei, China
[d] School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology, Shanghai 200093, China

ARTICLE INFO

Article history:
Received 15 August 2016
Received in revised form 2 January 2017
Accepted 4 January 2017
Available online 5 January 2017

Keywords:
Self-embedding
Tampering detection
Hierarchical recovery
Reference sharing

ABSTRACT

In this paper, we propose a new self-embedding watermarking scheme with hierarchical recovery capability. The binary bits in the adopted MSB layers are scrambled and individually interleaved with different extension ratios according to their importance to image visual quality. The interleaved data, which are regarded as reference bits for tampering recovery, are segmented into a series of groups corresponding to the divided non-overlapping blocks, and then embedded into the LSB layers of blocks together with authentication bits of tampering detection. Because the extension ratios of MSB-layer bits are based on the hierarchical mechanism, the efficiency of reference bits is increased, and higher MSB layers of tampered regions have greater probabilities to be recovered than lower MSB layers, which can improve the visual quality recovered results, especially for larger tampering rates. Experimental results demonstrate the effectiveness and superiority of the proposed scheme compared with some of state-of-the-art schemes.

1. Introduction

In recent years, the rapid development of multimedia tools and Internet technology brings great convenience for transmitting and downloading multimedia data, which also leads to easier duplication and modification for digital contents than before in the meantime [1,2]. Therefore, how to protect the security and integrity of the multimedia data [3,4], especially the technique of image authentication [5–7], becomes an important research topic nowadays. The traditional image authentication scheme attaches digital signatures with the original image, and then compares the signatures of the received image with that of the original image to authenticate the integrity. However, it cannot locate and further recover the tampered region [8]. In order to solve these problems, fragile watermarking scheme for image authentication with the capability of tampering localization and content recovery has been proposed [9].

In the view of functions, fragile image watermarking schemes can be divided into two types. One type can just locate suspicious regions if the received image is tampered during transmission [10–17]. This type of fragile watermarking schemes usually regards the hash of principal contents retrieved from each image block as its watermark data for embedding, and on the receiver side, the re-calculated hash of the received image is compared with the extracted hash of the image to detect the tampered regions, because tampering operation destroys the matching relationship between the contents of original image and the corresponding watermark data [10,11]. In order to improve the accuracy of tampering detection, some researchers proposed the pixel-wise based fragile watermarking schemes. The watermark data derived from gray values of original pixels were embedded into the original pixels themselves, and then the tampered pixels can be located through the absence of watermark data [12–14]. In the scheme [15], a statistical mechanism was introduced into fragile image watermarking. The watermark data, including the tailor-made authentication data for each pixel and some additional test data, can be used to precisely locate the tampered pixels.

Another type of fragile watermarking schemes can not only locate the faked regions, but also can recover the located, tampered contents [18–34]. In many practical applications, only tampering detection cannot satisfy the requirement, and the reconstruction

☆ This paper was recommended for publication by Pen-Cheng Wang.

* Corresponding authors at: College of Information Engineering, Shanghai Maritime University, No. 1550 Haigang Ave, Shanghai 201306, China.
E-mail addresses: fangcao@shmtu.edu.cn (F. Cao), bwan@shmtu.edu.cn (B. An), wjwei_2004@163.com (J. Wang), yedp@whu.edu.cn (D. Ye), wanghuili2622@163.com (H. Wang).

http://dx.doi.org/10.1016/j.displa.2017.01.001
0141-9382/

for tampered regions is highly desirable. To achieve the self-recovery capability, Fridrich et al. conducted earlier attempt in this field, and they proposed fragile image watermarking scheme, which can realize content recovery after tampering detection [18]. They embedded the watermark of a block into the least significant bits (LSB) of other distant blocks, which was able to resist vector quantization (VQ) attack and collage attack. In order to accurately identify the faked image blocks, a digital watermarking method for image tampering detection and recovery was developed in [19], which was based on a 3-level hierarchical structure. This scheme can not only detect tampered areas accurately but also can deal with high tampering rate with acceptable recovered results. However, the above mentioned methods above cannot recover the tampered blocks whose watermarks embedded in other blocks were also destroyed, which was called as the tampering coincidence problem in Zhang et al.'s scheme [24]. Some watermarking schemes with self-correction capability were free of this problem. In [20], a fragile watermarking scheme with a hierarchical mechanism was presented, which can reconstruct original watermarked image without any error. The pixel-derived and block-derived watermark data were embedded into the LSBs of all pixels. This method had a limitation that the tampering rate must be no greater than 3.2% of the entire image to achieve the perfect restoration. In another work [21], an effective dual watermark scheme for image tampering detection and recovery was proposed by Lee and Lin. They applied two copies of watermark data for each block in the entire image, so it was able to provide the second chance for tampering recovery in case the first copy was damaged. However, the tampering coincidence problem still existed once both two copies of the embedded watermark data for the image block were destroyed. A self-embedding fragile watermarking scheme based on a reference sharing mechanism was proposed in [24], in which the watermark embedded into the three LSB layers of the whole image can be considered as the reference derived from the five most significant bits (MSB) layers of original image and shared by the whole image for further content restoration. As long as the content tampering was not too extensive, the five MSB layers of tampered regions can be perfectly recovered using the sufficient available data scattered in the intact blocks of image. Thus, it can effectively avoid the tampering coincidence problem. However, the way of reference data generation also caused the watermark wasting problem [26]. Huo et al. proposed an alterable-capacity fragile watermarking scheme in [28], which the watermark codes with the alterable-length consisted of three parts and were embedded into other three blocks. On the receiver side, two copies of significant-code were utilized to recover the tampered contents so that the recovery performance can be improved. However, this scheme was poor at dealing with the tampering form of random block missing.

In this work, in order to achieve better performance of visual quality for both watermarked image and recovered image, we propose a self-embedding watermarking scheme for tampering recovery based on hierarchical watermark embedding, which utilizes variable numbers of MSB layers to generate the shared reference data for content recovery and also variable extension ratios between the reference bits for each MSB-layer and the total reference bits for all adopted MSB layers. These parameters can be flexible according to different proportions of the tampered regions to achieve the satisfactory quality of recovered contents. During watermark embedding, the reference data are derived from each MSB layer, whose bits are interleaved and scrambled, and then are combined with the authentication data to form the watermark data to be embedded in the LSBs. Note that the proposed scheme is based upon the reference sharing mechanism and the extension ratio between the reference bits for each MSB-layer and total reference bits is variable. Thus, tampering coincidence problem is effectively avoided and the efficiency of watermark data can also be greatly improved.

The rest of this paper is organized as follows. Section 2 describes the procedure of watermark embedding, including watermark generation and data embedding. Section 3 presents the procedure of content recovery, including tampering detection and content recovery. Experimental results and comparison are given in Section 4. Section 5 concludes the paper.

2. Watermark embedding

The watermark embedding procedure of the proposed scheme consists of the following 3 stages: (1) Select the embedding parameters to generate reference data; (2) Generate authentication data using reference data with the embedding parameters; (3) Embed the watermark data, including reference data and authentication data, into original image to produce watermarked image.

2.1. Watermark generation

Denote the size of original image $\mathbf{I}_o$ as $H \times W$, and $N = H \times W$. In the design of the proposed scheme, the detection of tampered region is based on each non-overlapping image block sized $b \times b$. Thus, for simplicity, H and W are both assumed as the multiples of b. The number of MSB layers used for the generation of reference bits is denoted as m. The $(8 - m)$ LSB layers of original image are used to accommodate the watermark data.

For each non-overlapping block, we allocate h authentication bits for tampering detection and $(8 - m) \cdot b^2 - h$ reference bits for content recovery, respectively. How to generate reference bits and authentication bits is described detailedly in the following steps:

Step 1: Denote the gray value of each pixel in $\mathbf{I}_o$ as $p_i \in [0, 255]$, $i = 1, 2, \ldots, N$, and p_i can be represented by 8 binary bits, i.e., $q_{i,7}$, $q_{i,6}$, $\ldots$, $q_{i,0}$, see Eq. (1).

$$q_{i,k} = \lfloor p_i / 2^k \rfloor \bmod 2, \quad k = 0,\ 1,\ \ldots, 7. \tag{1}$$

Step 2: Collect the N bits of each MSB layer, and then randomly divide them into S subsets and each subset contains u bits, i.e., $u \cdot S = N$. Detailedly, for the x-th MSB layer $\mathbf{C}_x$, its N bits, i.e., $q_{i,8-x}$, $i = 1, 2, \ldots, N$, are collected and divided into S subsets randomly, i.e., $\mathbf{C}_x^{(1)}$, $\mathbf{C}_x^{(2)}$, $\ldots$, $\mathbf{C}_x^{(S)}$.

Step 3: Denote the u MSB bits in the j-th subset $\mathbf{C}_x^{(j)}$ as $c^{(j)}_{x,1}$, $c^{(j)}_{x,2}$, $\ldots$, $c^{(j)}_{x,u}$, and these u MSB bits are transformed into v_x reference bits $\mathbf{R}_x^{(j)}$, i.e., $r^{(j)}_{x,1}$, $r^{(j)}_{x,2}$, $\ldots$, $r^{(j)}_{x,vx}$, $j = 1, 2, \ldots, S$, through Eq. (2):

$$\begin{bmatrix} r^{(j)}_{x,1} \\ r^{(j)}_{x,2} \\ \vdots \\ r^{(j)}_{x,v_x} \end{bmatrix} = \mathbf{H}_x^{(j)} \cdot \begin{bmatrix} c^{(j)}_{x,1} \\ c^{(j)}_{x,2} \\ \vdots \\ c^{(j)}_{x,u} \end{bmatrix} \quad j = 1, 2, \ldots,\ S, \tag{2}$$

where $\mathbf{H}_x^{(j)}$ is the pseudo-random binary matrix sized $v_x \times u$ that is derived from a secret key. Denote the value t_x as the extension ratio between the generated reference bits for the x-th MSB-layer and the total reference bits for all m MSB layers, $x = 1, 2, \ldots, m$, see Eq. (3). Note that the two relationships in Eqs. (4) and (5) should be satisfied:

$$t_x = \frac{S \cdot v_x}{N \cdot [(8 - m) - h/b^2]}, x = 1,\ 2, \ldots, m. \tag{3}$$

$$t_1 \geqslant t_2 \geqslant \cdots \geqslant t_m, \tag{4}$$

$$\sum_{x=1}^{m} t_x = 1. \tag{5}$$

We can find from Eq. (2) that, the v_x reference bits are determined by the u bits that are randomly dispersed in the x-th MSB layer of the entire image.

Step 4: After all m MSB layers are conducted by the above operations, a total of $N \cdot [(8-m) - h/b^2]$ reference bits are obtained. Permute these $N \cdot [(8-m) - h/b^2]$ reference bits through the secret key and divide them into N/b^2 groups with the equal size of $(8-m) \cdot b^2 - h$ bits. In this way, each of the N/b^2 reference-bits groups can be corresponded to each of the N/b^2 non-overlapping image blocks one by one.

Step 5: For each non-overlapping block, collect the $m \cdot b^2$ bits from its m MSB layers and its corresponding $(8-m) \cdot b^2 - h$ reference bits and feed them into a hash function to generate its h authentication bits. Note that the cryptographic property of hash function guarantee that slightly different inputs produce significantly different outputs.

2.2. Data embedding

According above steps in ection 2.1, the $(8-m) \cdot b^2$ watermark bits for each block, including the h authentication bits for tampering detection and the $(8-m) \cdot b^2 - h$ reference bits for content recovery, are obtained. We permute these $(8-m) \cdot b^2$ watermark bits with a secret key and replace the $(8-m)$ LSB layers of each block for data embedding. After all N/b^2 blocks are conducted with data embedding operations, the watermarked image $\mathbf{I}_w$ can be produced.

In the watermark embedding procedure, the m MSB layers of the original image are kept unchanged while the $(8-m)$ LSB layers are replaced with the watermark bits. Note that the MSB bits in the same subset $\mathbf{C}_x^{(j)}$ come from different image regions and the corresponding generated reference bits $\mathbf{R}_x^{(j)}$ are embedded all over the image, which is the keypoint of reference sharing mechanism. Also, the reference bits for content recovery in our scheme are generated according to different importance of MSB layers, which can increase the efficiency of reference bits and improve the visual quality of recovered results.

Because the $(8-m)$ LSB layers of the original image $\mathbf{I}_o$ are substituted with random watermark bits. Therefore, the peak signal-to-noise ratio (PSNR) of watermarked image $\mathbf{I}_w$ with respect to original image $\mathbf{I}_o$ is only dependent upon the value of m. The theoretical value of PSNR for watermarked image with respect to original image is:

$$\mathrm{PSNR}_w(m) = 10 \cdot \log_{10} \frac{255^2}{D_w(m)}. \tag{6}$$

Here, $D_w(m)$ is the average energy of the distortions caused by watermark embedding in the $(8-m)$ LSB layers for each pixel, and its expression is:

$$D_w(m) = \frac{1}{2^{2(8-m)}} \cdot \sum_{\xi_o=0}^{2^{8-m}-1} \sum_{\xi_w=0}^{2^{8-m}-1} (\xi_o - \xi_w)^2 , \tag{7}$$

where ξ_o is the decimal value of the original $(8-m)$ LSBs for a pixel in $\mathbf{I}_o$ and ξ_w is the decimal value of the watermarked $(8-m)$ LSBs for a pixel in $\mathbf{I}_w$. Obviously, both ξ_o and ξ_w belong to $[0, 2^{(8-m)} - 1]$. According to Eqs. (6) and (7), we can easily obtain the theoretical values of PSNR for watermarked image $\mathbf{I}_w$, i.e., PSNR_w, under different parameters m of watermark embedding capacity, see Table 1. In order not to degrade visual quality of watermarked image severely, the parameter m can be set no less than 5.

Table 1
Theoretical PSNR values of watermarked image under different m (unit: dB).

Capacity	$m=3$	$m=4$	$m=5$	$m=6$	$m=7$
$D_w(m)$	170.5	42.5	10.5	2.5	0.5
$\mathrm{PSNR}_w(m)$	25.81	31.85	37.92	44.15	51.14

3. Content recovery

After receiving the suspicious watermarked image, i.e., $\mathbf{I}_w^*$, that may be damaged through the public channel, the receiver should first locate the tampered or missing blocks of $\mathbf{I}_w^*$ using the authentication bits, and then restore the MSBs of each detected, tampered block according to the reference bits and the MSBs retrieved from the intact blocks of the whole image.

3.1. Tampered block detection

For each $b \times b$ block in $\mathbf{I}_w^*$, we segment the $(8-m) \cdot b^2$ bits extracted from its $(8-m)$ LSB layers into two parts, i.e., $(8-m) \cdot b^2 - h$ reference bits and h authentication bits, with the same secret key on the sender side. Then, we feed the $m \cdot b^2$ bits of its m MSB layers and the extracted $(8-m) \cdot b^2 - h$ reference bits into the hash function to re-calculate the h authentication bits. If the re-calculated h authentication bits differ from the extracted h authentication bits, the block is judged as tampered. Otherwise, the block is marked as reserved. Note that a block without being tampered must be correctly judged as reserved, and the probability for a tampered block being mistakenly judged as reserved is only 2^{-h}.

3.2. Tampered content recovery

The m MSBs of all tampered blocks are required for content recovery with the assist of other reserved blocks including the m MSBs and the reference bits embedded in the $(8-m)$ LSBs. Detailed steps about how to recover the tampered image contents are described as follows:

Step 1: After extracting the all $N \cdot [(8-m) - h/b^2]$ reference bits from $(8-m)$ LSBs of $\mathbf{I}_w^*$, with the same secret key, permute and segment these reference bits into m groups. Each group of $t_x \cdot N \cdot [(8-m) - h/b^2]$ reference bits corresponds to the x-th MSB-layer, $x = 1, 2, \ldots, m$.

Step 2: Divide the N bits of the x-th MSB layer $\mathbf{C}_x{}^*$ into S subsets with the equal size of u, i.e., $\mathbf{C}_x{}^{(1)*}$, $\mathbf{C}_x{}^{(2)*}$, …, $\mathbf{C}_x{}^{(S)*}$. Also, divide the corresponding $t_x \cdot N \cdot [(8-m) - h/b^2]$ reference bits into S subsets with the equal size of v_x, i.e., $\mathbf{R}_x{}^{(1)*}$, $\mathbf{R}_x{}^{(2)*}$, …, $\mathbf{R}_x{}^{(S)*}$.

Step 3: Among the v_x reference bits in each subset $\mathbf{R}_x{}^{(j)*}$, $j = 1, 2, \ldots, S$, denote the $v'_{x,j}$ ($\leqslant v_x$) correct bits extracted from the reserved blocks as: $r^{(j)}{}_{x,\lambda(1)}$, $r^{(j)}{}_{x,\lambda(2)}$, …, $r^{(j)}{}_{x,\lambda(v'x,j)}$, which can be used to recover the damaged MSB bits in $\mathbf{C}_x{}^{(j)*}$. This way, construct the relationship between $\mathbf{C}_x{}^{(j)*}$ and $\mathbf{R}_x{}^{(j)*}$ through rewriting Eq. (2):

$$\begin{bmatrix} r^{(j)}_{x,\lambda(1)} \\ r^{(j)}_{x,\lambda(2)} \\ \vdots \\ r^{(j)}_{x,\lambda(v'_{x,j})} \end{bmatrix} = \mathbf{H}_x^{(\mathrm{E}|j)} \cdot \mathbf{C}_x^{(j)*} \tag{8}$$

where $\mathbf{H}_x{}^{(\mathrm{E}|j)}$ is a matrix with $v'_{x,j}$ rows taken from $\mathbf{H}_x{}^{(j)}$ corresponding to the $v'_{x,j}$ correctly extracted reference bits.

Step 4: Parse the u MSB bits in the column vector $\mathbf{C}_x{}^{(j)*}$ into two parts, i.e., $\mathbf{C}_x{}^{(\mathrm{T}|j)}$ and $\mathbf{C}_x{}^{(\mathrm{O}|j)}$, which consist of the $u^*_{x,j}$ damaged bits from tampered blocks and the $u - u^*_{x,j}$ correct bits from reserved blocks, respectively. This way, re-formulate Eq. (8) as:

$$\mathbf{R}_x^{(\mathrm{O}|j)} - \mathbf{H}_x^{(\mathrm{E}|\mathrm{O}|j)} \cdot \mathbf{C}_x^{(\mathrm{O}|j)} = \mathbf{H}_x^{(\mathrm{E}|\mathrm{T}|j)} \cdot \mathbf{C}_x^{(\mathrm{T}|j)}, \tag{9}$$

where $\mathbf{R}_x{}^{(\mathrm{O}|j)}$ denotes the column vector in the left of Eq. (8), i.e., $r^{(j)}{}_{x,\lambda(1)}$, $r^{(j)}{}_{x,\lambda(2)}$, …, $r^{(j)}{}_{x,\lambda(v'x,j)}$, the two matrices $\mathbf{H}_x{}^{(\mathrm{E}|\mathrm{O}|j)}$ and $\mathbf{H}_x{}^{(\mathrm{E}|\mathrm{T}|j)}$ are

sized of $v'_{x,j} \times (u - u^*_{x,j})$ and $v'_{x,j} \times u^*_{x,j}$, and their columns are those in $\mathbf{H}_x^{(\mathrm{E}|j)}$ corresponding to the bits in $\mathbf{C}_x^{(\mathrm{O}|j)}$ and $\mathbf{C}_x^{(\mathrm{T}|j)}$, respectively. Note that as long as Eq. (9) has the unique solution for $\mathbf{C}_x^{(\mathrm{T}|j)}$, it must be the original version of these MSB bits, and $\mathbf{C}_x^{(\mathrm{T}|j)}$ can be successfully recovered. The probability of successful recovery for the $u^*_{x,j}$ damaged bits in $\mathbf{C}_x^{(\mathrm{T}|j)}$ from the subset $\mathbf{C}_x^{(j)*}$ is equivalent to the probability of all $u^*_{x,j}$ column vectors in the random binary matrix $\mathbf{H}_x^{(\mathrm{E}|\mathrm{T}|j)}$ being linearly independent, which is directly proportional to the value of u, and the probability of successful recovery for all damaged bits in the S MSB subsets for the x-th MSB layer is inversely proportional to the value of N/u. But, larger value of u causes heavier computation complexity for solving Eq. (9) due to more unknown MSB bits, thus, to make a tradeoff, the subset length u of MSB bits was set to 512 in our experiments.

Step 5: After all S subsets, i.e., $\mathbf{C}_x^{(1)*}$, $\mathbf{C}_x^{(2)*}$, …, $\mathbf{C}_x^{(S)*}$, are conducted the above operations, all damaged MSB bits of $\mathbf{C}_x^{(\mathrm{T}|1)}$, $\mathbf{C}_x^{(\mathrm{T}|2)}$, …, $\mathbf{C}_x^{(\mathrm{T}|S)}$ can be solved and the x-th MSB layer of $\mathbf{I}^*_{\mathrm{w}}$ can be successfully recovered.

Step 6: After all m MSB layers, i.e., $\mathbf{C}^*_1$, $\mathbf{C}^*_2$, …, $\mathbf{C}_m{}^*$, finish the above steps, the recovered m MSB layers can be obtained. Additionally, In order to further increase the visual quality of recovered image, the post-processing should be conducted, which sets the decimal values of the $(8 - m)$ LSBs for all pixels to 2^{7-m} and obtains the final recovered image $\mathbf{I}_{\mathrm{r}}$.

Under a certain tampering rate, for all m MSB layers $\mathbf{C}^*_1$, $\mathbf{C}^*_2$, …, $\mathbf{C}_m{}^*$ for recovery, statistically speaking, the numbers of their damaged MSB bits are equal. But, since the x-th MSB-layer can generate $t_x \cdot N \cdot [(8 - m) - h/b^2]$ reference bits by Eq. (2), $x = 1, 2, \ldots, m$, thus, with the guarantee of Eqs. (3)–(5), more correct reference bits in Eqs. (8) and (9) can be obtained for higher MSB layers (corresponding to smaller x) that are more important to image visual quality. Because more reference bits can be acquired for higher MSB layers, it means that Eq. (9) has greater probabilities for higher MSB layers to be successfully solved for all S subsets $\mathbf{C}_x^{(1)*}$, $\mathbf{C}_x^{(2)*}$, …, $\mathbf{C}_x^{(S)*}$. That is to say, the higher MSB layers have higher priorities to be recovered than the lower MSB layers, which effectively realizes hierarchical content recovery and improves the visual quality of recovered image, especially for larger tampering rates. Fig. 1 gives theoretical values of recovery probability and PSNR for recovered image under different tampering rates α ($m = 6$). Fig. 1a shows the recovery probability for each subset $\mathbf{C}_x^{(j)*}$ of the x-th MSB layers ($x = 1, 2, \ldots, 6$), i.e., the probability of Eq. (9) with the unique solution, and Fig. 1b shows the PSNR values of recovered image with the hierarchical extension ratios ($t_1 = 1/4$, $t_2 = 1/4$, $t_3 = 1/6$, $t_4 = 1/6$, $t_5 = 1/12$, $t_6 = 1/12$) and the uniform extension ratios ($t_1 = t_2 = t_3 = t_4 = t_5 = t_6 = 1/6$). Hierarchical extension mechanism according to the importance of MSB layers can achieve significantly higher PSNR values of recovered image than uniform extension mechanism for larger tampering rates.

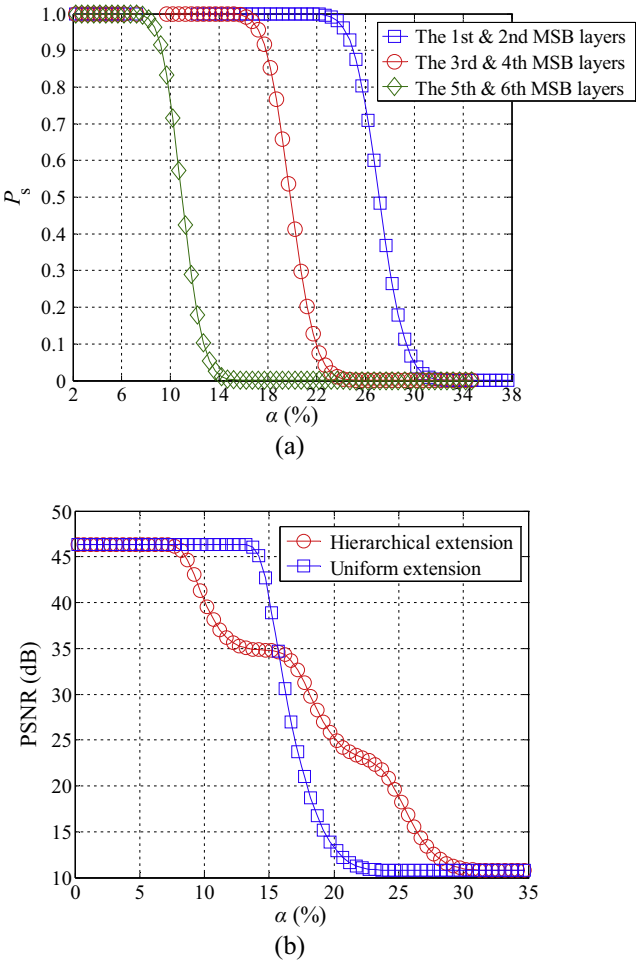

Fig. 1. Recovery probability of m MSB layers and PSNR of recovered image under different tampering rates α ($m = 6$). (a) Recovery probability for each subset $\mathbf{C}_x^{(j)*}$ of the x-th MSB layers ($x = 1, 2, \ldots, 6$), (b) PSNR of recovered image with hierarchical and uniform extension ratios t_x.

4. Experimental results and comparison

All experiments were implemented on a computer with a 3.30 GHz Intel i3 processor, 4.00 GB memory, and Windows 7 operating system, and the programming environment was Matlab R2009b. A large number of test images sized 512×512 are used in our experiments to demonstrate the effectiveness of the proposed scheme. For color images, the luminance components were utilized for testing. In all following experiments, the subset length u of MSB bits for our scheme was set to 512, and the number m of MSB layers used for the generation of reference bits was set to 6, which the 2 LSB layers of original image were used to accommodate the watermark bits produced by 6 MSB layers. Denote the ratio between the number of tampered blocks and the number of all original blocks in the image as the tampering rate α.

4.1. Tampering recovery

Figs. 2(a and b) show the original version of standard test image Lena and its watermarked version, respectively, and the PSNR value of the watermarked image was 44.15 dB. In this experiment, the extension ratios t_x, $x = 1, 2, \ldots, 6$, between the generated reference bits for the x-th MSB-layer and the total reference bits for all 6 MSB layers, are set to be 1/4, 1/4, 1/6, 1/6, 1/12, 1/12, respectively. Fig. 2c shows the tampered version for the watermarked image Lena, in which the face of Lena was replaced by that of a man with tampering rate $\alpha = 6.84\%$. Fig. 2d is the result of tampering detection, in which the white regions denote the detected, tampered blocks and the black regions are the reserved blocks. Fig. 2e shows the recovered image for Fig. 2c, and the PSNR value of the recovered result was 46.06 dB. We can find from the experimental result that, the proposed scheme is effective and as well as with an acceptable performance of tampering recovery.

4.2. Performance with hierarchical extension ratios

In order to demonstrate the superiority of our hierarchical recovery mechanism, the three groups of extension ratios t_x ($x = 1, 2, \ldots, 6$) listed in Table 2 were utilized for experiments, and three groups of t_x correspond to three kinds of trends: varying from small to large, staying the same, and varying from large to

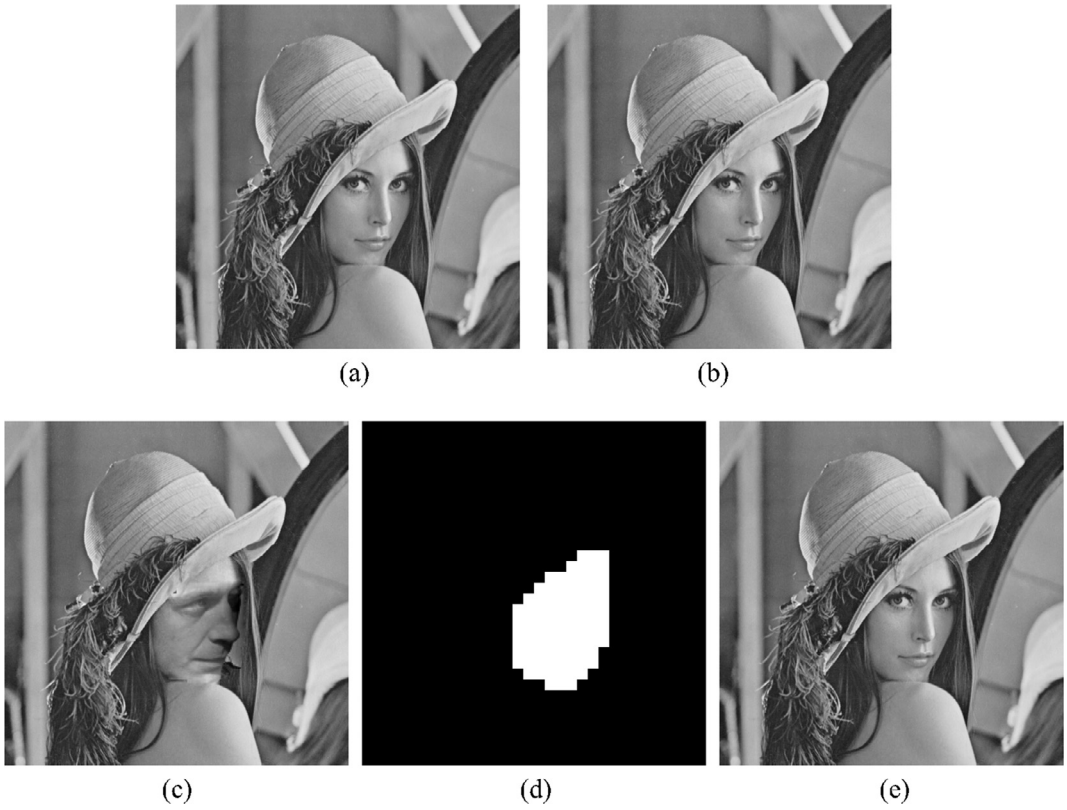

Fig. 2. Tampering recovery results for image Lena. (a) Original image Lena, (b) Watermarked image with PSNR = 44.15 dB, (c) Tampered Lena with $\alpha = 6.84\%$, (d) Tampering detection result, (e) Recovered image with PSNR = 46.06 dB.

Table 2
PSNR values of recovered images for Peppers with different extension ratios (dB).

Extension ratios t_x ($x = 1, 2, \ldots, 6$)	PSNR values of recovered images			
	$\alpha = 5\%$	$\alpha = 10\%$	$\alpha = 15\%$	$\alpha = 20\%$
$t_1 = 1/12$, $t_2 = 1/12$, $t_3 = 1/6$, $t_4 = 1/6$, $t_5 = 1/4$, $t_6 = 1/4$	46.37	20.90	16.07	13.48
$t_1 = t_2 = t_3 = t_4 = t_5 = t_6 = 1/6$	46.37	46.37	32.69	13.43
$t_1 = 1/4$, $t_2 = 1/4$, $t_3 = 1/6$, $t_4 = 1/6$, $t_5 = 1/12$, $t_6 = 1/12$	46.37	42.49	37.00	26.53

small, respectively. Four tampering rates α, i.e., 5%, 10%, 15%, and 20%, were applied to simulate the different missing proportions for image blocks.

Fig. 3a shows the original image Peppers, and Fig. 3(b and d) give the watermarked images under three groups of extension ratios t_x ($x = 1, 2, \ldots, 6$) listed in Table 2, and their corresponding PSNR values all approximated to 44.15 dB due to the same watermark embedding capacity (2 LSB layers), which also conformed to the results in Table 1. The tampered versions of image Peppers under four tampering rates, i.e., $\alpha = 5\%$, 10%, 15%, and 20%, were illustrated in the first row of Fig. 4. The second row of Fig. 4, i.e., subfigures (a2–d2), are the recovered images with $t_1 = 1/12$, $t_2 = 1/12$, $t_3 = 1/6$, $t_4 = 1/6$, $t_5 = 1/4$, $t_6 = 1/4$ for four tampering rates, and their corresponding PSNR values were 46.37 dB, 20.90 dB,

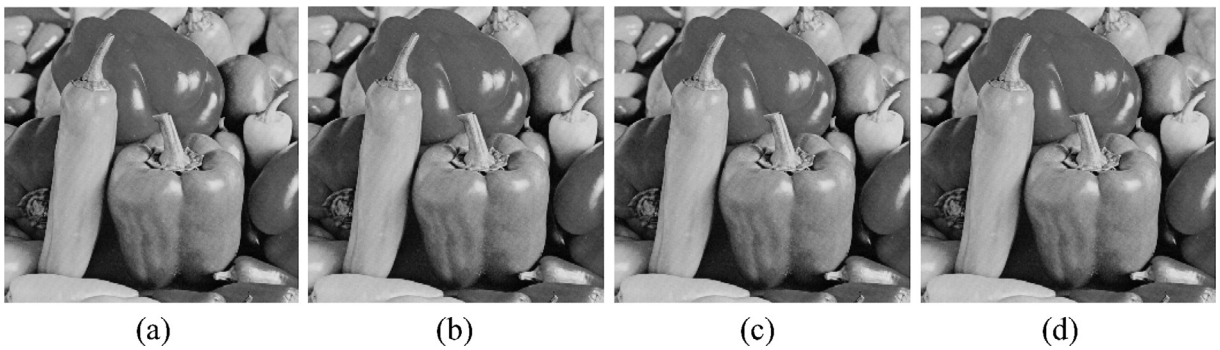

Fig. 3. Original image Peppers and its watermarked versions (PSNR $\approx$ 44.15 dB). (a) Original image Peppers, (b) Watermarked image with $t_1 = 1/12$, $t_2 = 1/12$, $t_3 = 1/6$, $t_4 = 1/6$, $t_5 = 1/4$, $t_6 = 1/4$, (c) Watermarked image with $t_1 = t_2 = t_3 = t_4 = t_5 = t_6 = 1/6$, (d) Watermarked image with $t_1 = 1/4$, $t_2 = 1/4$, $t_3 = 1/6$, $t_4 = 1/6$, $t_5 = 1/12$, $t_6 = 1/12$.

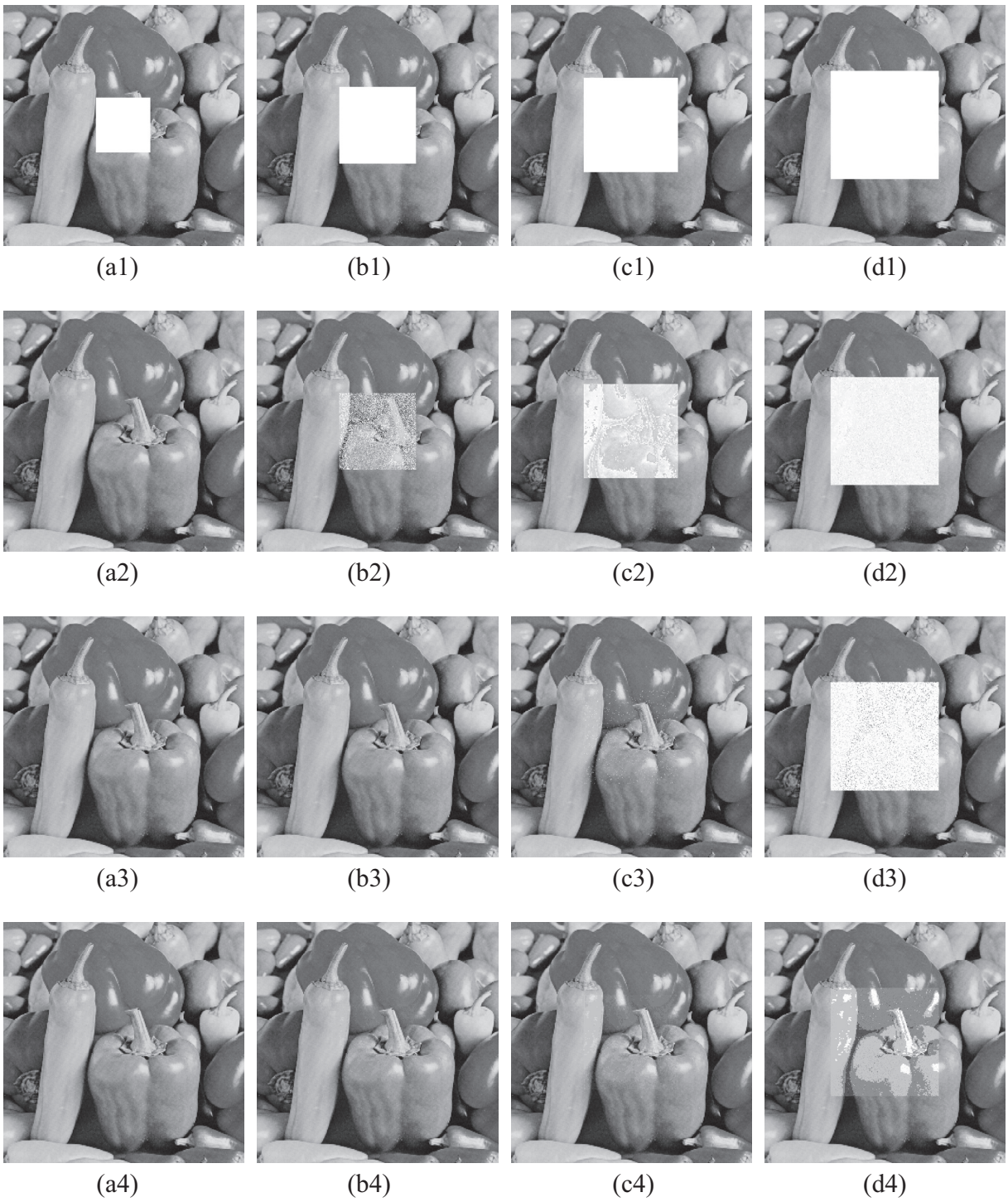

Fig. 4. Recovered results for tampered image Peppers with three groups of extension ratios. (a1–d1) Four tampered images with $\alpha = 5\%$, 10%, 15%, and 20%, (a2–d2) Four recovered images with $t_1 = 1/12$, $t_2 = 1/12$, $t_3 = 1/6$, $t_4 = 1/6$, $t_5 = 1/4$, $t_6 = 1/4$, (a3–d3) Four recovered images with $t_1 = t_2 = t_3 = t_4 = t_5 = t_6 = 1/6$, (a4–d4) Four recovered images with $t_1 = 1/4$, $t_2 = 1/4$, $t_3 = 1/6$, $t_4 = 1/6$, $t_5 = 1/12$, $t_6 = 1/12$.

16.07 dB, and 13.48 dB, respectively. The third row of Fig. 4, i.e., subfigures (a3–d3), are the recovered images with $t_1 = t_2 = t_3 = t_4 = t_5 = t_6 = 1/6$ for four tampering rates, and their corresponding PSNR values were 46.37 dB, 46.37 dB, 32.69 dB, and 13.43 dB, respectively. The fourth row of Fig. 4, i.e., subfigures (a4–d4), are the recovered images with $t_1 = 1/4$, $t_2 = 1/4$, $t_3 = 1/6$, $t_4 = 1/6$, $t_5 = 1/12$, $t_6 = 1/12$ for four tampering rates, and their corresponding PSNR values were 46.37 dB, 42.49 dB, 37.00 dB, and 26.53 dB, respectively. Table 2 presents the PSNR values of recovered images under different tampering rates α. It can be observed from Fig. 4 and Table 2 that, our hierarchical recovery mechanism that the extension ratios of reference bits should be proportional to the importance of the MSB layers (i.e., t_x should be inversely proportional to x), can obtain better overall tampering recovery performance than the other two kinds of settings, which also verifies the conclusion in Section 3.2. In other words, when the extension ratios t_x ($x = 1, 2, \ldots, m$) are set to satisfy the relationship in Eqs. (4) and (5), equivalent performance can be obtained

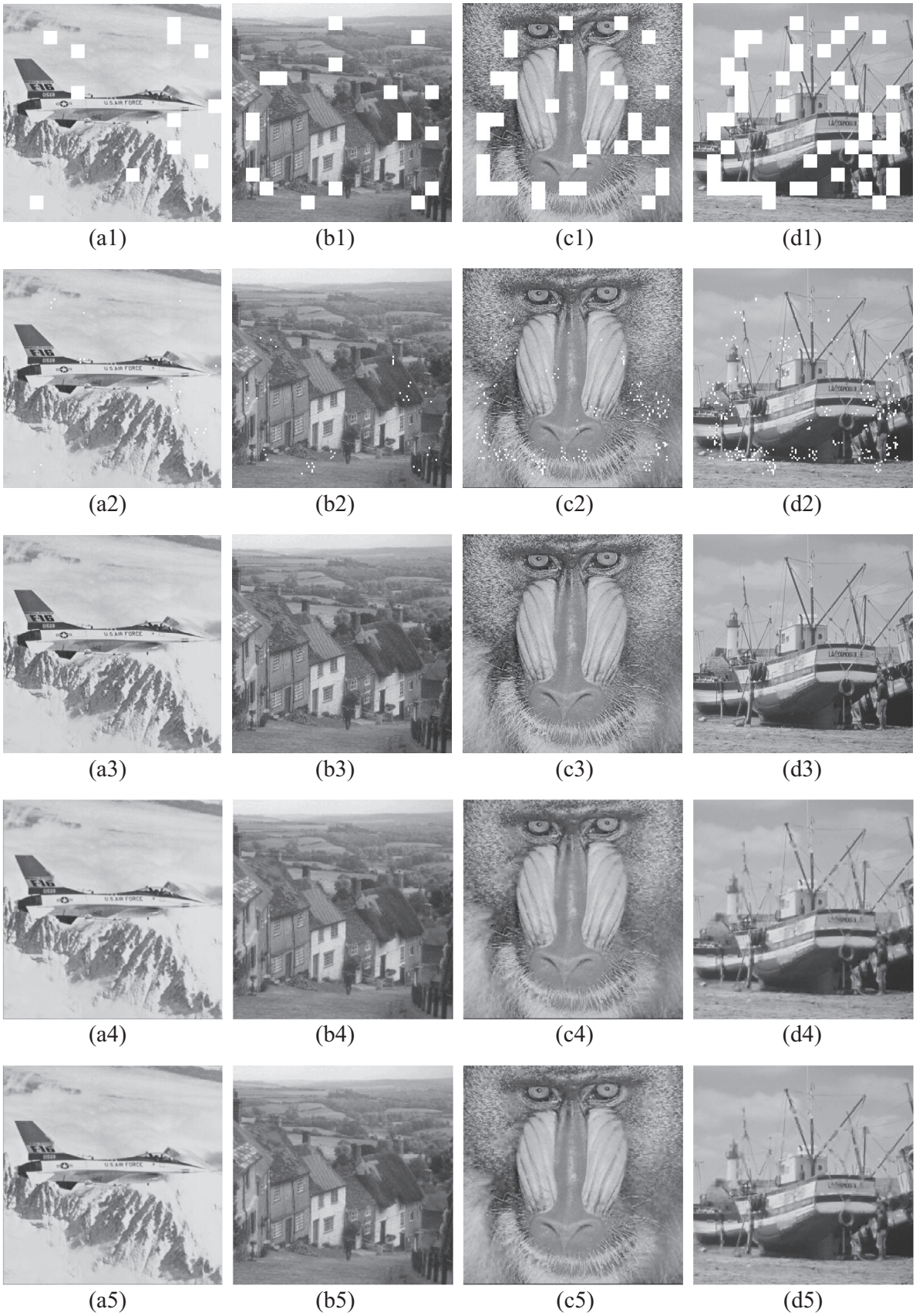

Fig. 5. Comparison results of the schemes [19,24,28] and the proposed scheme. The first row (a1–d1) are the four tampered images with $\alpha = 5\%$, 10%, 15% and 20%, respectively; the second row (a2–d2), the third row (a3–d3) and the fourth row (a4–d4) are the recovered results of [19,24,28], respectively; The last row (a5–d5) are the recovered results of the proposed scheme.

Table 3
Comparison of PSNR values for the proposed scheme and the schemes [19,24,28].

Images	Tampering rate α (%)	{PSNR of watermarked image, PSNR of recovered image}			
		Scheme in [19]	Scheme in [24]	Scheme in [28]	Proposed
Airplane	5	{43.93, 37.60}	{37.96, 35.75}	{43.33, 37.71}	{44.11, 46.34}
Goldhill	10	{44.34, 29.38}	{37.91, 35.70}	{43.43, 35.62}	{44.16, 40.75}
Baboon	15	{44.41, 25.55}	{37.92, 35.73}	{43.72, 25.60}	{44.17, 37.96}
Sailboat	20	{44.48, 21.25}	{37.91, 35.69}	{43.24, 26.93}	{44.11, 36.90}

Table 4
Comparison of SSIM values for the proposed scheme and the schemes [19,24,28].

Images	Tampering rate α (%)	{SSIM of watermarked image, SSIM of recovered image}			
		Scheme in [19]	Scheme in [24]	Scheme in [28]	Proposed
Airplane	5	{0.9958, 0.9846}	{0.9797, 0.9889}	{0.9946, 0.9927}	{0.9951, 0.9974}
Goldhill	10	{0.9983, 0.9706}	{0.9780, 0.9814}	{0.9986, 0.9719}	{0.9980, 0.9939}
Baboon	15	{0.9973, 0.9306}	{0.9885, 0.9883}	{0.9974, 0.8669}	{0.9972, 0.9911}
Sailboat	20	{0.9966, 0.8788}	{0.9834, 0.9892}	{0.9971, 0.9008}	{0.9960, 0.9849}

compared with uniform extension ratios and more desirable visual quality of recovered image can be achieved for larger tampering rate. The optimal allocation of t_x ($x = 1, 2, \ldots, m$) for different tampering rates α can be determined according to dynamic programming.

4.3. Comparison with some of state-of-the-art schemes

In order to demonstrate the superiority of the proposed scheme, we compared our scheme with Lin et al.'s scheme [19], Zhang et al.'s scheme in [24], and Huo et al.'s scheme [28]. The scheme in [19] suffered from the tampering coincidence problem, the scheme in [28] cannot work well under a larger tampering rate, and the scheme in [24] does not consider the unequal importance of different MSB layers during tampering recovery. Fig. 5 shows the recovered results of the proposed scheme and the three schemes [19,24,28] for the images Airplane, Goldhill, Baboon and Sailboat under different tampering rates, which simulated the different missing proportions of image blocks in wireless fading channel. The subfigures (a1–d1) in Fig. 5 are the four tampered images with tampering rates $\alpha = 5\%$, 10%, 15% and 20%, respectively. The subfigures (a2–d2), (a3–d3), and (a4–d4) are the corresponding recovered results of the three schemes [19,24,28], respectively. The watermark embedding capacities of the schemes in [19] and [24] were fixed as 2 LSBs and 3 LSBs, respectively, and the scheme in [28] was alterable. The subfigures (a5–d5) are the recovered results of our scheme with the extension ratios $t_1 = 1/4$, $t_2 = 1/4$, $t_3 = 5/24$, $t_4 = 5/24$, $t_5 = 1/24$, and $t_6 = 1/24$, which are the optimal values of t_x ($x = 1, 2, \ldots, 6$) based on a large number of experimental results.

The PSNR values of watermarked images and recovered images with respect to the original images for the schemes in [19,24,28] and the proposed scheme are listed in Table 3. Also, the values of structural similarity (SSIM) [35] for watermarked images and recovered images are provided in Table 4. The measure of SSIM was developed based on the characteristics of the human visual system (HVS), which integrated the information of structure, luminance and contrast synthetically for image quality assessment. We can observe from Fig. 5 and Tables 3–4, that the scheme [19] cannot recover some tampered blocks for relatively larger tampering rates since there was the tampering coincidence problem, which resulted in unsatisfactory recovery performance. The schemes [24] and [28] cannot work well when tampering rates were relatively larger. Therefore, the proposed scheme based on hierarchical recovery mechanism can achieve better capability of content recovery than the schemes in [19,24,28].

5. Conclusions

In order to achieve better performance of tampering recovery, hierarchical reference-bits capacity according to the importance of image contents is utilized in the proposed scheme. The number of the MSB layers for the generation of the shared reference bits is variable, and the extension ratios between each MSB-layer bits and the total generated reference bits are different so that the efficiency of reference-bits can be increased. Through the hierarchical recovery mechanism, the higher MSB layers of tampered regions have higher priority to be recovered than the lower MSB layers, which can improve the visual quality recovered results, especially for larger tampering rates. In addition, reference sharing mechanism is adopted, thus, the tampering coincidence problem is effectively avoided. A large number of experiments, including the content recovery for meaningful content tampering and image block missing in wireless fading channels, are tested to demonstrate the effectiveness and superiority of our scheme compared with the reported schemes.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (61171126, 61272453, 61672354, 61303203, U1636101, 61401270), Ministry of Transport and Applied Basic Research Projects (2014329810060), the PAPD Fund, and the CICAEET Fund.

References

[1] Z. Xia, X. Wang, X. Sun, Q. Wang, A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data, IEEE Trans. Parallel Distributed Syst. 27 (2016) 340–352.
[2] Z. Fu, K. Ren, J. Shu, X. Sun, F. Huang, Enabling personalized search over encrypted outsourced data with efficiency improvement, IEEE Trans. Parallel Distributed Syst. 27 (2016) 2546–2559.
[3] Z. Xia, X. Wang, X. Sun, Q. Liu, N. Xiong, Steganalysis of LSB matching using differences between nonadjacent pixels, Multimedia Tools Appl. 75 (2016) 1947–1962.
[4] Z. Xia, X. Wang, X. Sun, B. Wang, Steganalysis of least significant bit matching using multi-order differences, Secur. Commun. Networks 7 (2014) 1283–1291.
[5] C. Qin, X. Chen, J. Dong, X. Zhang, Perceptual image hashing with selective sampling for salient structure features, Displays 45 (2016) 26–37.

[6] J. Li, X. Li, B. Yang, X. Sun, Segmentation-based image copy-move forgery detection scheme, IEEE Trans. Inf. Forensics Secur. 10 (2015) 507–518.
[7] C. Qin, X. Zhang, Effective reversible data hiding in encrypted image with privacy protection for image content, J. Visual Commun. Image Represent. 31 (2015) 154–164.
[8] C. Qin, X. Chen, D. Ye, J. Wang, X. Sun, A novel image hashing scheme with perceptual robustness using block truncation coding, Inf. Sci. 361–362 (2016) 84–99.
[9] C.D. Vleeschouwer, J.F. Delaigle, B. Macq, Invisibility and application functionalities in perceptual watermarking: an overview, Proc. IEEE 90 (2002) 64–77.
[10] P.W. Wong, N. Memon, Secret and public key image watermarking schemes for image authentication and ownership verification, IEEE Trans. Image Process. 10 (2001) 1593–1601.
[11] S. Suthaharan, Fragile image watermarking using a gradient image for improved localization and security, Pattern Recognit. Lett. 25 (2004) 1893–1903.
[12] H. Lu, R. Shen, F.L. Chung, Fragile watermarking scheme for image authentication, Electron. Lett. 39 (2003) 898–900.
[13] H. He, J. Zhang, H.M. Tai, A wavelet-based fragile watermarking scheme for secure image authentication, Lecture Notes Comput. Sci. 4283 (2006) 422–432.
[14] S. Liu, H. Yao, W. Gao, Y. Liu, An image fragile watermark scheme based on chaotic image pattern and pixel-pairs, Appl. Math. Comput. 185 (2007) 869–882.
[15] X. Zhang, S. Wang, Statistical fragile watermarking capable of locating individual tampered pixels, IEEE Signal Process. Lett. 14 (2007) 727–730.
[16] P.Y. Lin, J.S. Lee, C.C. Chang, Dual digital watermarking for internet media based on hybrid strategies, IEEE Trans. Circ. Syst. Video Technol. 19 (2009) 1169–1171.
[17] F.D. Martino, S. Sessa, Fragile watermarking tamper detection with images compressed by fuzzy transform, Inf. Sci. 195 (2012) 62–90.
[18] J. Fridrich, M. Goljan, Images with self-correcting capabilities, in: Proc. IEEE Int. Conf. Image Process., 1999, pp. 792–796.
[19] P.L. Lin, C.K. Hsieh, P.W. Huang, A hierarchical digital watermarking method for image tamper detection and recovery, Pattern Recognit. 38 (2005) 2519–2529.
[20] X. Zhang, S. Wang, Fragile watermarking scheme using a hierarchical mechanism, Signal Process. 89 (2009) 675–679.
[21] T.Y. Lee, S.D. Lin, Dual watermark for image tamper detection and recovery, Pattern Recognit. 41 (2008) 3497–3506.
[22] H. He, J. Zhang, F. Chen, Adjacent-block based statistical detection method for self-embedding watermarking techniques, Signal Process. 89 (2009) 1557–1566.
[23] C.W. Yang, J.J. Shen, Recover the tampered image based on VQ indexing, Signal Process. 90 (2010) 331–343.
[24] X. Zhang, S. Wang, Z. Qian, G. Feng, Reference sharing mechanism for watermark self-embedding, IEEE Trans. Image Process. 20 (2011) 485–495.
[25] Z. Qian, G. Feng, X. Zhang, S. Wang, Image self-embedding with high-quality restoration capability, Digital Signal Process. 21 (2011) 278–286.
[26] X. Zhang, Z. Qian, Y. Ren, G. Feng, Watermarking with flexible self-recovery quality based on compressive sensing and compositive reconstruction, IEEE Trans. Inf. Forensics Secur. 6 (2011) 1223–1232.
[27] C. Qin, H. Wang, X. Zhang, X. Sun, Self-embedding fragile watermarking based on reference-data interleaving and adaptive selection of embedding mode, Inf. Sci. 373 (2016) 233–250.
[28] Y. Huo, H. He, F. Chen, Alterable-capacity fragile watermarking scheme with restoration capability, Opt. Commun. 285 (2012) 1759–1766.
[29] C. Qin, C.C. Chang, K.N. Chen, Adaptive self-recovery for tampered images based on VQ indexing and inpainting, Signal Process. 93 (2013) 933–946.
[30] S. Yang, C. Qin, Z. Qian, B. Xu, Tampering detection and content recovery for digital image using halftone mechanism, in: Proc. the 10th Int. Conf. Intelligent Inf. Hiding Multimedia Signal Process., 2014, pp. 130–133.
[31] Y. Huo, H. He, F. Chen, A semi-fragile image watermarking algorithm with two-stage detection, Multimedia Tools Appl. 72 (2014) 123–149.
[32] P. Korus, A. Dziech, Adaptive self-embedding scheme with controlled reconstruction performance, IEEE Trans. Inf. Forensics Secur. 9 (2014) 169–181.
[33] S. Sarreshtedari, M.A. Akhaee, A source-channel coding approach to digital image protection and self-recovery, IEEE Trans. Image Process. 24 (2015) 2266–2277.
[34] X. Qi, X. Xin, A singular-value-based semi-fragile watermarking scheme for image content authentication with tamper localization, J. Visual Commun. Image Represent. 30 (2015) 312–327.
[35] Z. Wang, A.C. Bovik, H.R. Sheikh, E.P. Simoncelli, Image quality assessment: from error visibility to structural similarity, IEEE Trans. Image Process. 13 (2004) 600–612.

Fang Cao received the B.S. degree in applied electronics from Shanghai Normal University, Shanghai, China, in 2002, the M.S. degree in signal and information processing from Shanghai Maritime University, Shanghai, China, in 2004, and the Ph.D. degree in communication and information system from Shanghai University, Shanghai, China, in 2013. Since 2005, she has been with the faculty of the College of Information Engineering, Shanghai Maritime University, where she is currently a Lecturer. Her research interests include image processing, computer vision and multimedia security.

Bowen An received the M.S. degree in signal and information processing from Wuhan University, Hubei, China, in 2004, and the Ph.D. degree in Electronic Science and Technology from Chinese Academy of Sciences, in 2006. Since 2006, he has been with the faculty of the College of Information Engineering, Shanghai Maritime University, where he is currently a Professor. His research interests include remote sensing image processing and signal detection.

Jinwei Wang was born in Inner Mongolia, China, in 1978. He received the Ph.D. degree in information security at Nanjing University of Science & Technology in 2007 and was a visiting scholar in Service Anticipation Multimedia Innovation (SAMI) Lab of France Telecom R&D Center (Beijing) in 2006. He worked as a senior engineer at the 28th research institute, CETC from 2007 to 2010. He worked as a visiting scholar at New Jersey Institute of Technology, NJ, USA from 2014 to 2015. Now he works as an associate professor at Nanjing University of Information Science and Technology. His research interests include multimedia copyright protection, image forensics, image encryption and data authentication. He has published more than 30 papers, hosted and participated in more than 10 research projects.

Dengpan Ye was born in Hubei, China. He received the B.A.Sc in automatic control from SCUT in 1996 and Ph.D degree at NJUST in 2005 respectively. He worked as a Post-Doctoral Fellow in Information System School of Singapore Management University. Since 2012, he has been a professor in the school of computer science at Wuhan University. His research interests include Machine Learning and multimedia security. He is the author or co-author of more than 30 journal and conference papers.

Huili Wang received the B.S. degree in communication engineering from University for Shanghai Science Technology, Shanghai, China, in 2014. She is currently pursuing the M.S. degree in signal and information processing from University of Shanghai for Science and Technology, China. Her research interests include data hiding, digital watermarking, and image authentication.