Information Sciences 373 (2016) 233–250

Contents lists available at ScienceDirect

Information Sciences

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

Self-embedding fragile watermarking based on reference-data interleaving and adaptive selection of embedding mode

Chuan Qin[a,*], Huili Wang[a], Xinpeng Zhang[b], Xingming Sun[c]

[a] *Shanghai Key Lab of Modern Optical System, and Engineering Research Center of Optical Instrument and System, Ministry of Education, University of Shanghai for Science and Technology, Shanghai 200093, China*
[b] *School of Communication and Information Engineering, Shanghai University, Shanghai 200072, China*
[c] *School of Computer and Software, Nanjing University of Information Science & Technology, Nanjing 210044, Jiangsu, China*

ARTICLE INFO

Article history:
Received 13 April 2016
Revised 28 August 2016
Accepted 1 September 2016
Available online 3 September 2016

Keywords:
Fragile watermarking
Self-embedding
Embedding mode
Tampering detection
Content recovery

ABSTRACT

In this paper, we propose a novel self-embedding fragile image watermarking scheme for tampering recovery based on reference-data interleaving mechanism and adaptive selection of embedding mode. During watermark embedding, reference bits are derived from the interleaved, scrambled MSB bits of original image, and then are combined with authentication bits to form the watermark bits for LSB embedding. Different with the reported schemes with the fixed embedding mode, the proposed scheme not only has two types of embedding modes, i.e., overlapping-free embedding and overlapping embedding, but also utilizes the adaptively flexible numbers of MSB and LSB layers to achieve satisfactory performances for different tampering rates. Also, detailed analyses are given to provide the theoretical values of watermarked-image quality, perfect recovery probability, and recovered-image quality, which are used to conclude the optimal choice of embedding modes. Experimental results show the effectiveness and superiority of the proposed scheme compared with some state-of-the-arts schemes.

1. Introduction

In the past two decades, with the development of the Internet and multimedia processing tools, the transmission, duplication, and modification of digital contents have become much easier than before [34,5]. As a result, protecting the intellectual property contained in the multimedia data has become an important challenge [8]. In addition to properly identifying ownership [14], determining the authenticity of multimedia data and protecting their integrity also are important current issues that must be solved [21,38,16]. When the traditional cryptographic technique is used to authenticate multimedia data by attaching digital signatures, it cannot locate suspicious regions if the multimedia data that are received have been tampered during transmission [18]. Also, the computation burden associated with digital signatures for multimedia data is extremely heavy, and additional storage space is required to attach the signatures. Thus, in order to deal with these problems effectively, in recent years, researchers have proposed the technique of fragile watermarking for the authentication of multimedia data [31]. In this paper, we mainly focus on the authentication of digital images.

[*] Corresponding author at: School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology, No. 516 Jungong Road, Shanghai 200093, China. Fax: 86 21 55272982.
E-mail addresses: qin@usst.edu.cn (C. Qin), wanghuili2622@163.com (H. Wang), xzhang@shu.edu.cn (X. Zhang), sunnudt@163.com (X. Sun).

http://dx.doi.org/10.1016/j.ins.2016.09.001
0020-0255/© 2016 Elsevier Inc. All rights reserved.

One category of reported fragile watermarking schemes focused on integrity authentication and tampering detection for digital images, which are sensitive to any modifications of the images and can effectively identify locations where tampering has occurred [33,29,22,35,2,41,10,23,3,20]. The embedded watermark data for this category of fragile watermarking schemes usually are the hash of principal contents retrieved from each image pixel or block [33,29,22,35]. Since tampering manipulations destroy the matching relationship between the contents of the original image and the corresponding watermark data, the tampered regions can be detected. Chang et al. proposed a fragile watermarking scheme for image ownership and tampering authentication [2]. The aim of their scheme was to protect the rightful ownership and detect malicious manipulations of embedded images using the authentication data inserted in adaptive least significant bits (LSB) of the original pixels. Zhang and Wang proposed a statistical scheme of fragile watermarking to locate tampered regions with pixel-wise accuracy [41]. The watermark data of this scheme consisted of tailor-made authentication data for each pixel and some additional test data that can be used to reveal the exact pattern of the tampered contents. However, in many real applications, just detecting tampering is not enough, and it is highly desirable to recover the original content from the tampered regions. Therefore, many researchers have investigated ways of recovering the original content after tampering has been detected [4,17,24,15,12,6,26,25,19,40,37,7,28,13,42,36,43,39,11].

Fridrich and Goljan developed a fragile watermarking scheme with self-recovery capability, which encoded the DCT coefficients of each block into 64 or 128 bits and embedded them into the LSBs of other distant blocks [4]. This embedding strategy made the scheme can resist the collage attack. When the tampered blocks were detected, the quantized DCT coefficients were extracted from the intact regions and decoded to recover the original contents of the tampered image. In [17], Lin et al. presented a fragile watermarking method for detecting image tampering and recovering the original content, which was based on a 3-level hierarchical structure to ensure the accuracy of tampering localization. The scheme can deal with high tampering rates and obtain acceptable recovery results. However, these schemes had the problem of not being able to recover original content of the tampered regions if the hidden reference information used for the recovery also was destroyed. This situation is referred to as a tampering coincidence problem [42]. To solve this problem, Lee and Lin proposed an effective dual watermark scheme for image tampering detection and recovery in [19]. Their scheme provided two copies of watermark data for each non-overlapping block in the entire image, thereby providing a second chance for tampering recovery in case the first copy of the watermark was damaged. In [40], a tailor-made watermark consisting of reference-bits and check-bits was hidden in the original image using a reversible data hiding method [9]. On the receiver side, the extracted and calculated check-bits can be used to locate tampered image blocks. The original image can be reconstructed exactly by the reliable reference-bits extracted from other blocks. If the tampering rate is less than 3.2%, this scheme can restore the information about the original image with no errors, but, in this scheme, the visual quality of the watermarked image is relatively low. The scheme [37] reduced the encoding length of block features by establishing an index table for the original image via vector quantization (VQ). In this scheme, several copies of the VQ indices for all image blocks were embedded into the original image as watermark data according to a pseudo-random sequence. The tampered image can be recovered by the decoded VQ codewords. However, if all of the copies of the embedded watermark for the image block were damaged, the visual quality of recovered result was not very good. A self-embedding fragile watermarking scheme based on a reference sharing mechanism was proposed in [42]. In this scheme, the shared reference bits derived from the five most significant bit (MSB) layers of original image were scrambled and then embedded into the three LSB layers of the entire image. As long as the area where tampering occurred was not too extensive, sufficient available data scattered in the intact regions of image can be retrieved to recover the five MSB layers of tampered regions, effectively avoiding the tampering coincidence problem. However, the fixed embedding capacity of this scheme made the usage efficiency of watermark bits lower when dealing with variable tampering rates, and the way of reference-bits generation also caused the watermark wasting problem [39].

In this work, in order to achieve better visual quality of watermarked images and recovered images, we propose a novel, self-embedding, fragile watermarking scheme, which integratedly considers visual quality of watermarked image and recovered image from different tampering rates based on the reference-data interleaving mechanism. Different from earlier schemes, our scheme utilizes flexible numbers of the MSB layers to generate the interleaved reference bits for content recovery, and it also uses variable numbers of LSB layers to accommodate watermark bits. The embedding modes of the proposed scheme can be categorized as overlapping-free embedding and overlapping embedding. Detailed analysis and calculation of the theoretical PSNR values of the watermarked/recovered images, as well as the probability of the perfect recovery of tampered images, are given so that the optimal choice of embedding modes can be made for different tampering rates. To the best of our knowledge, our work is the first to present the relationship for the overall performance of self-embedding scheme, the embedding modes that are used, and the ranges of tampering rates. The experimental results show the effectiveness and superiority of our scheme compared with some state-of-the-art schemes.

The rest of this paper is organized as follows. Section 2 describes the proposed scheme including the procedures of watermark embedding, tampering detection and content recovery. Section 3 presents the theoretical performance analysis of our scheme. Experimental results and comparisons are given in Section 4. Section 5 concludes the paper.

2. Proposed scheme

In the proposed self-embedding scheme, there are two main procedures: (1) watermark embedding procedure, which embeds watermark bits (including authentication bits and reference bits) derived from MSBs of the original image into LSBs;

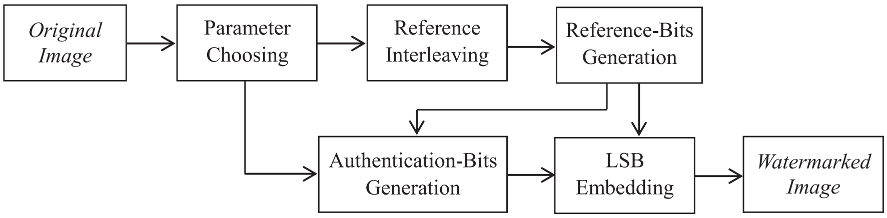

Fig. 1. Flowchart of watermark embedding procedure.

(2) tampering detection and content recovery, which can be achieved by the extracted authentication bits and reference bits together with the received MSBs. The details of the two procedures are described as follows.

2.1. Watermark embedding

For the convenience of descriptions, we denote the number of MSB layers for the generation of reference bits as m and denote the number of LSB layers for the accommodation of reference bits and authentication bits as l. In our general self-embedding framework, authentication bits and reference bits are used to detect and recover tampered regions, respectively, and the choices of m and l are related with watermarked image quality, estimated tampering rate, and recovered image quality. The flowchart of watermark embedding procedure is illustrated in Fig. 1.

In the design of the proposed scheme, the detection of the tampered region is based on each non-overlapping image block sized $b \times b$, and we allocate L_a authentication bits to each block for tampering detection ($L_a < l \cdot b^2$). Denote the size of original image $\mathbf{I}_o$ as $N_1 \times N_2$, and $N = N_1 \times N_2$. For simplicity, N_1 and N_2 are both assumed to be the multiples of b. Therefore, in the l LSBs of the image, in addition to the $L_a \cdot N/b^2$ authentication bits for detecting tampering, there are $l \cdot N - L_a \cdot N/b^2$ bits that can be assigned to reference bits for the recovery of content in the future. In the following, we describe how to generate reference bits and authentication bits detailedly.

The gray value of each pixel in $\mathbf{I}_o$ is denoted as $p_i \in [0, 255]$, where $i = 1, 2, \ldots, N$, 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).

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

The m MSBs of each pixel p_i, i.e., $q_{i,7}, q_{i,6}, \ldots, q_{i,8-m}$, in $\mathbf{I}_o$ are collected and then permuted with a secret key to form a set $\mathbf{C}$ consisting of $m \cdot N$ bits. We divide these $m \cdot N$ bits in $\mathbf{C}$ into S subsets, i.e., $\mathbf{C}_1, \mathbf{C}_2, \ldots, \mathbf{C}_S$, and each subset contains u bits, i.e., $u \cdot S = m \cdot N$. Denote the u bits in the jth subset $\mathbf{C}_j$ as $c_{j,1}, c_{j,2}, \ldots, c_{j,u}, j = 1, 2, \ldots, S$. Using Eq. (2), the u bits in each subset $\mathbf{C}_j$ of m MSBs are transformed into v reference bits $\mathbf{R}_j$, i.e., $r_{j,1}, r_{j,2}, \ldots, r_{j,v}$.

$$\begin{bmatrix} r_{j,1} \\ r_{j,2} \\ \vdots \\ r_{j,v} \end{bmatrix} = \mathbf{H}_j \cdot \begin{bmatrix} c_{j,1} \\ c_{j,2} \\ \vdots \\ c_{j,u} \end{bmatrix}, \tag{2}$$

where $\mathbf{H}_j$ is the pseudo-random binary matrix with the size of $v \times u$ that is derived from a secret key. As mentioned above, there are a total of $l \cdot N - L_a \cdot N/b^2$ bits in l LSBs that can be assigned to reference bits, therefore, the value of v in Eq. (2) should satisfy the relationship:

$$v \cdot S = v \cdot \frac{m \cdot N}{u} = l \cdot N - L_a \cdot N/b^2. \tag{3}$$

In other words, after all S subsets, i.e., $\mathbf{C}_1, \mathbf{C}_2, \ldots, \mathbf{C}_S$, are conducted with the transform of interleaving in Eq. (2), we can obtain the $l \cdot N - L_a \cdot N/b^2$ reference bits. It can be observed from Eq. (2) that each reference bit in $\mathbf{R}_j$ is related to all u bits in $\mathbf{C}_j$ that are dispersed in the entire image and that all v reference bits in $\mathbf{R}_j$ are related to each bit in $\mathbf{C}_j$. Then, we permute the obtained $l \cdot N - L_a \cdot N/b^2$ reference bits and divided them into N/b^2 equal-size groups, i.e., each group contains $l \cdot b^2 - L_a$ bits.

We divide the original image $\mathbf{I}_o$ into N/b^2 non-overlapping blocks with sizes of $b \times b$, so each of the N/b^2 groups of reference bits can be easily corresponded to each of the N/b^2 blocks one by one. Denote the minimum of the two values m and $8-l$ as m'. For each $b \times b$ block, the $m' \cdot b^2$ bits of its m' MSB layers are collected and then fed into a hash function together with its corresponding $l \cdot b^2 - L_a$ reference bits to generate its L_a authentication bits. Note that the cryptographic property of the hash function is that slightly different inputs produce significantly different outputs. Thus, the $l \cdot b^2$ watermark bits, including the $l \cdot b^2 - L_a$ reference bits and the L_a authentication bits, can be obtained for each $b \times b$ block. We permute the $l \cdot b^2$ watermark bits of each block with a secret key and use them to replace the l LSB layers of each block for watermark embedding. After all of the N/b^2 image blocks are conducted by the above operations, the watermarked image $\mathbf{I}_w$ can be produced. The proposed watermark embedding algorithm is summarized in Algorithm 1.

Algorithm 1
Watermark Embedding Procedure of Proposed Scheme.

```
Input: Original image $\mathbf{I}_o$ sized $N_1 \times N_2$, the number $m$ of MSB layers used for the reference-bits generation, the number $l$ of LSB layers used for the
       watermark-bits accommodation.
Output: Watermarked image $\mathbf{I}_w$.
1) Divide $\mathbf{I}_o$ into $N/b^2$ non-overlapping blocks sized $b \times b$ ($N = N_1 \times N_2$);
2) Permute the $m \cdot N$ bits in $m$ MSB layers of $\mathbf{I}_o$ and divide them into $S$ subsets;
3) Generate $l \cdot N - L_a \cdot N/b^2$ reference bits using Eqs. (2-3) for all $S$ subsets and divide the permuted reference bits into $N/b^2$ groups;
4) for each block do
     a) Generate $L_a$ authentication bits using the $m' \cdot b^2$ bits of its $m'$ MSB layers and the corresponding $l \cdot b^2 - L_a$ reference bits with hash function;
     b) Permute the $l \cdot b^2$ watermark bits, including $l \cdot b^2 - L_a$ reference bits and $L_a$ authentication bits, and use them to replace $l$ LSB layers of the block;
   end
Result: Obtain the watermarked image $\mathbf{I}_w$.
```

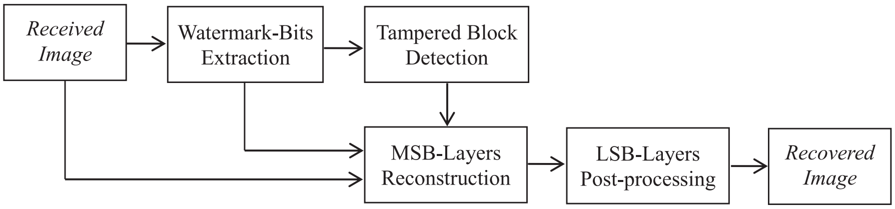
Received Image
Watermark-Bits Extraction
Tampered Block Detection
MSB-Layers Reconstruction
LSB-Layers Post-processing
Recovered Image

Fig. 2. Flowchart of the procedure for tampering detection and content recovery.

Obviously, larger l means that more embedded watermark bits can be utilized for tampering detection and recovery, and that lower visual quality of watermarked image is caused meanwhile. On the other hand, larger m means that more MSB layers are involved to form reference bits, and that higher visual quality of recovered image can be achieved if the tampered region can be successfully recovered. In addition, tampering recovery performance of the self-embedding based scheme is closely related with the tampering rate, i.e., the percentage of tampered/missing blocks in the watermarked image. Therefore, rather than directly adopt the fixed values of m and l for watermark embedding, the choices of m and l should be synthetically considered based on the different tampering rates and the visual quality of watermarked image and recovered image. The detailed discussions for the optimal choice of m and l are presented in Section 3.

2.2. Tampering detection and 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 recover the MSBs of each detected, tampered block according to the reference bits and the MSBs retrieved from the intact blocks of the whole image. The flowchart of the procedure for tampering detection and content recovery is illustrated in Fig. 2.

As a general self-embedding framework, the two parameters m and l in the proposed scheme can be variable and correspond to different embedding modes, thus, we describe the procedure of tampering detection and content recovery according to two different conditions of m and l, i.e., $m + l \le 8$ (named as overlapping-free embedding) and $m + l > 8$ (named as overlapping embedding).

2.2.1. Tampering recovery for overlapping-free embedding

(1) *Tampered Block Detection:* For each $b \times b$ block in $\mathbf{I}_w^*$, we use the same secret key to segment the $l \cdot b^2$ bits extracted from its l LSB layers into two parts, i.e., L_a authentication bits and $l \cdot b^2 - L_a$ reference bits, and then we feed the $m \cdot b^2$ bits of its m MSB layers and the extracted $l \cdot b^2 - L_a$ reference bits into the hash function to recalculate the L_a authentication bits. If the recalculated L_a authentication bits differ from the extracted L_a authentication bits, the block is judged as having been tampered. Otherwise, the block is marked as intact. Note that a block that has not been tampered must be correctly judged as intact, and the probability for a tampered block's being falsely judged as intact is 2^{-L_a}.

(2) *Tampered Content Recovery:* The m MSBs of all tampered blocks are required for content recovery with the assist of the m MSBs and the reference bits in the l LSBs of other intact blocks. Similar to the operation of Eq. (2) on the sender side, we also can construct the subset $\mathbf{C}_j^*$ of m MSBs and the corresponding reference bits $\mathbf{R}_j^*$, $j = 1, 2, \ldots,$ S. Note that both the u bits in $\mathbf{C}_j^*$ and the v bits in $\mathbf{R}_j^*$ may contain some damaged bits that come from the blocks judged as tampered. Thus, all damaged bits in $\mathbf{C}_j^*$ of MSBs are required for recovery, and only the reference bits extracted from the intact blocks can be used. We denote that there are v_j' correct reference bits in $\mathbf{R}_j^*$, i.e., $r_{j,\lambda(1)}$,

$r_{j,\lambda(2)}, \ldots, r_{j,\lambda(v_j')}$, that are extractable from the intact blocks ($v_j' \le v$), see Eq. (4).

$$\begin{bmatrix} r_{j,\lambda(1)} \\ r_{j,\lambda(2)} \\ \vdots \\ r_{j,\lambda(v_j')} \end{bmatrix} = \mathbf{H}_j^{(\mathrm{E})} \cdot \begin{bmatrix} c_{j,1}^* \\ c_{j,2}^* \\ \vdots \\ c_{j,u}^* \end{bmatrix}, \tag{4}$$

where $\mathbf{H}_j^{(\mathrm{E})}$ is a matrix with v_j' rows taken from $\mathbf{H}_j$ corresponding to the v_j' extractable reference bits, and $c_{j,1}^*$, $c_{j,2}^*$, … , $c_{j,u}^*$ are the u bits in the jth subset $\mathbf{C}_j^*$ of MSBs. We denote the column vector $\mathbf{C}_j^*$ in Eq. (4) as two parts, i.e., $\mathbf{C}_j^{(\mathrm{T})}$ and $\mathbf{C}_j^{(\mathrm{O})}$, which consist of the u_j^* damaged bits and the $u-u_j^*$ intact bits in $\mathbf{C}_j^*$, respectively. In other words, the $u-u_j^*$ bits in $\mathbf{C}_j^{(\mathrm{O})}$ from intact blocks are known, and the u_j^* bits in $\mathbf{C}_j^{(\mathrm{T})}$ coming from tampered blocks are unknown and required for recovery. Therefore, we can reformulate Eq. (4) as:

$$\mathbf{R}_j^{(\mathrm{O})} - \mathbf{H}_j^{(\mathrm{E,O})} \cdot \mathbf{C}_j^{(\mathrm{O})} = \mathbf{H}_j^{(\mathrm{E,T})} \cdot \mathbf{C}_j^{(\mathrm{T})}, \tag{5}$$

where $\mathbf{R}_j^{(\mathrm{O})}$ denotes the column vector of $r_{j,\lambda(1)}$, $r_{j,\lambda(2)}$, … , $r_{j,\lambda(v_j')}$, the two matrices $\mathbf{H}_j^{(\mathrm{E,O})}$ and $\mathbf{H}_j^{(\mathrm{E,T})}$ have the sizes of $v_j' \times (u-u_j^*)$ and $v_j' \times u_j^*$, respectively, and their columns are those in $\mathbf{H}_j^{(\mathrm{E})}$ that correspond to the bits in $\mathbf{C}_j^{(\mathrm{O})}$ and $\mathbf{C}_j^{(\mathrm{T})}$, respectively. It can be observed that Eq. (5) consists of v_j' equations with u_j^* unknowns of $\mathbf{C}_j^{(\mathrm{T})}$ to be solved. Therefore, as long as Eq. (5) has a unique solution for $\mathbf{C}_j^{(\mathrm{T})}$, it must be the original version of these MSB bits, and $\mathbf{C}_j^{(\mathrm{T})}$ can be successfully recovered. The necessary and sufficient condition for the existence of the unique solution to Eq. (5) is that the rank of the $v_j' \times u_j^*$ -size matrix $\mathbf{H}_j^{(\mathrm{E,T})}$ should be u_j^*, i.e., the u_j^* column vectors of $\mathbf{H}_j^{(\mathrm{E,T})}$ should be linearly independent. The theoretical analysis of the probability of the existence of a unique solution in Eq. (5) is given in Subsection 3.2.

We can find that, in the intact blocks of $\mathbf{I}_\mathrm{w}^*$, both the reference bits $\mathbf{R}_j^{(\mathrm{O})}$ extracted from their l LSB layers and the bits $\mathbf{C}_j^{(\mathrm{O})}$ derived from their m MSB layers can contribute to tampering recovery, because the information of all MSB bits and all reference bits in the corresponding subsets are shared with each other through Eq. (2) during watermark embedding procedure. After all corresponding S subsets $\mathbf{C}_j^*$ and $\mathbf{R}_j^*$ are conducted the above operations ($j=1, 2, \ldots, S$), the recovery procedure for all of the damaged MSB bits in $\mathbf{I}_\mathrm{w}^*$ is finished.

2.2.2. Tampering recovery for overlapping embedding

(1) *Tampered Block Detection:* For each $b \times b$ block of $\mathbf{I}_\mathrm{w}^*$, after segmenting the $l \cdot b^2$ bits of its l LSB layers into L_a authentication bits and $l \cdot b^2 - L_\mathrm{a}$ reference bits, different with the tampering detection for the overlapping-free embedding, we enter the $(8-l) \cdot b^2$ bits of its $(8-l)$ MSB layers (instead of $m \cdot b^2$ bits of m MSB layers) and the extracted $l \cdot b^2 - L_\mathrm{a}$ reference bits into the hash function to recalculate the L_a authentication bits. The following process for comparing the recalculated/extracted authentication bits and for judging tampered/intact blocks is the same as that for the overlapping-free embedding.

(2) *Tampered Content Recovery:* Similar to the content recovery for the overlapping-free embedding, the subset $\mathbf{C}_j^*$ of m MSBs and the corresponding reference bits $\mathbf{R}_j^*$, $j=1, 2, \ldots, S$, also are constructed, and the bits in $\mathbf{C}_j^*$ and $\mathbf{R}_j^*$ that come from the tampered blocks are denoted as damaged. In addition, it should be noted that, due to the overlapping embedding ($m+l>8$), the bits in the first ($m+l$–8) layers of m MSBs diffused in the S subsets of $\mathbf{C}_j^*$ also are damaged, irrespective of whether they come from intact or tampered blocks. Therefore, when we transform Eq. (4) into Eq. (5) for content recovery of overlapping embedding, the item $\mathbf{C}_j^{(\mathrm{T})}$ that must be solved consists of all damaged bits in $\mathbf{C}_j^*$ caused by both tampering and overlapping embedding. The subsequent process for solving Eq. (5) to recover the damaged MSB bits in $\mathbf{I}_\mathrm{w}^*$ is the same as that for overlapping-free embedding.

For both scenarios of overlapping-free embedding and overlapping embedding, when all damaged bits in $\mathbf{C}_j^*$ ($j=1, 2, \ldots, S$) can be solved by Eq. (5), we claim that the *perfect recovery* for $\mathbf{C}_j^*$ is achieved, and the recovery is completely dependent on the correct MSBs and the embedded reference bits from the intact blocks. Additionally, In order to further increase the visual quality of recovered image, the post-processing should be conducted. Denote the minimum of the two values l and $8-m$ as l' . Because the l' LSBs of the image are substituted with random watermark bits during embedding procedure, thus, we set the decimal values of l' LSBs for all pixels to $2^{l'-1}$ and obtain the final recovered image $\mathbf{I}_\mathrm{r}$. The proposed tampering recovery algorithm is summarized in Algorithm 2.

Under the same embedding parameter m of MSB layers, due to the larger watermark embedding capacity l, more extractable reference bits for overlapping embedding can be obtained for content recovery than overlapping-free embedding. On the other hand, under the same parameter of embedding capacity l, due to the larger embedding parameter m, the number of recoverable MSB layers for overlapping embedding is more than that of overlapping-free embedding if the perfect recovery can be achieved, which leads to higher visual quality of recovered image. However, for overlapping embedding, because the embedding of watermark bits destroys a portion of MSB bits, thus, the maximum of its tolerable tampering area must be smaller than that of overlapping-free embedding under the conditions of perfect recovery and the same embedding capacity l.

Algorithm 2
Tampering Recovery Procedure of Proposed Scheme.

```
Input: Suspicious watermarked image $\mathbf{I}_\mathrm{w}^*$.
Output: Recovered image $\mathbf{I}_\mathrm{r}$.
1) Divide $\mathbf{I}_\mathbf{w}$* into $N/b^2$ non-overlapping blocks sized $b\times b$;
Tampered Block Detection:
2) for each block do
    a) Parse the $l\cdot b^2$ watermark bits extracted from $l$ LSB layers of the block into $L_\mathrm{a}$ authentication bits and $l\cdot b^2-L_\mathrm{a}$ reference bits;
    b) Feed the $m'\cdot b^2$ bits of $m'$ MSB layers and the extracted $l\cdot b^2-L_\mathrm{a}$ reference bits into hash function to re-calculate the $L_\mathrm{a}$ authentication bits;
    c) Compare the re-calculated $L_\mathrm{a}$ authentication bits with the extracted $L_\mathrm{a}$ authentication bits (if equal, the block is judged as intact; otherwise, the
       block is marked as tampered);
  end
Tampered Content Recovery:
3) Permute the $m\cdot N$ bits in $m$ MSB layers of $\mathbf{I}_\mathrm{w}^*$ and divide them into $S$ subsets;
4) Establish the interleaving relationship among the $v_j$' correct reference bits, the $u-u_j^*$ intact MSB bits and the $u_j^*$ damaged MSB bits for each subset
     using Eqs. (4–5);
5) Solve the damaged MSB bits of $\mathbf{C}_j^{(\mathrm{T})}$ in Eq. (5) with the assist of the reference bits $\mathbf{R}_j^{(\mathrm{O})}$ extracted from $l$ LSB layers and the bits $\mathbf{C}_j^{(\mathrm{O})}$ derived from $m$
     MSB layers;
Post-processing:
6) Set the decimal values of $l'$ LSB layers for all the pixels to $2^{l'-1}$ ($l'$ is the minimum of the two values $l$ and $8-m$);
Result: Obtain the recovered image $\mathbf{I}_\mathrm{r}$.
```

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

Capacity	$l=1$	$l=2$	$l=3$	$l=4$	$l=5$
$D_\mathrm{w}(l)$	0.5	2.5	10.5	42.5	170.5
$\mathrm{PSNR}_\mathrm{w}(l)$	51.14	44.15	37.92	31.85	25.81

3. Theoretical analysis

In this section, we conduct theoretical analysis for the performance of the proposed scheme from four aspects: (1) PSNR of watermarked image, (2) Probability of perfect recovery, (3) PSNR of recovered image, and (4) Optimal choice of embedding modes.

3.1. PSNR of watermarked image

As described in Section 2, in our scheme, the embedding capacity of watermark bits for the whole image is $l\cdot N$ bits, that is to say, the l LSB layers of original image $\mathbf{I}_\mathrm{o}$ are substituted with random watermark bits. Therefore, the PSNR of watermarked image $\mathbf{I}_\mathrm{w}$ with respect to original image $\mathbf{I}_\mathrm{o}$ is only dependent upon the value of l.

Denote the decimal value of the original l LSBs for a pixel in $\mathbf{I}_\mathrm{o}$ as ξ_o and the decimal value of the watermarked l LSBs for a pixel in $\mathbf{I}_\mathrm{w}$ as ξ_w. Obviously, both ξ_o and ξ_w belong to $[0, 2^l-1]$. Thus, the average energy of the distortions caused by watermark embedding in l LSBs for each pixel is:

$$D_\mathrm{w}(l)=\frac{1}{2^{2l}}\cdot\sum_{\xi_\mathrm{o}=0}^{2^l-1}\sum_{\xi_\mathrm{w}=0}^{2^l-1}(\xi_\mathrm{o}-\xi_\mathrm{w})^2. \tag{6}$$

Then, the theoretical value of PSNR for watermarked image $\mathbf{I}_\mathrm{w}$ with respect to original image $\mathbf{I}_\mathrm{o}$ can be calculated as:

$$\mathrm{PSNR}_\mathrm{w}(l)=10\cdot\log_{10}\frac{255^2}{D_\mathrm{w}(l)}. \tag{7}$$

According to Eqs. (6–7), we can easily obtain the theoretical values of PSNR, i.e., PSNR_w, for watermarked image under different parameters l of watermark embedding capacity, see Table 1. In order not to degrade visual quality of watermarked image severely, we often set the parameter l no greater than 3.

3.2. Probability of perfect recovery

As described in Section 2.2, the necessary and sufficient condition of perfect recovery for all damaged MSB bits in $\mathbf{C}_j^{(\mathrm{T})}$ derived from each subset $\mathbf{C}_j^*$ is that the u_j^* column vectors of $\mathbf{H}_j^{(\mathrm{E,T})}$ must be linearly independent, $j=1, 2, \ldots, S$. For a random binary matrix sized $x\times y$, we denote the probability of its y column vectors being linearly dependent as $\varphi(x, y)$.

Then, the following relationships for $\varphi(x, y)$ can be acquired using linear algebra:

$$\varphi(x,\ y) = \begin{cases} \frac{1}{2^x}, & \text{if } y = 1, \\ \left(1 - \frac{2^y}{2^x}\right) \cdot \varphi(x, y-1) + \frac{2^y}{2^x}, & \text{if } 2 \le y \le x, \\ 1, & \text{if } y > x. \end{cases} \tag{8}$$

As we know, $\mathbf{H}_j^{(\mathrm{E,T})}$ is a random binary matrix sized $v_j' \times u_j^*$, where v_j' denotes the number of correct reference bits, that are extracted from the intact blocks, among the v bits of $\mathbf{R}_j^*$, and u_j^* denotes the number of damaged MSB bits, that come from the tampered blocks, among the u bits of $\mathbf{C}_j^*$. We define the ratio between the number of tampered blocks and the total number of blocks as the tampering rate, i.e., α. Therefore, the number v_j' of correct reference bits extracted from intact blocks can be represented by a binomial distribution:

$$P_{v'}(x) = \binom{v}{x} \cdot (1-\alpha)^x \cdot \alpha^{v-x}, \quad x = 0,\ 1, \ldots,\ v. \tag{9}$$

On the other hand, the number u_j^* of damaged MSB bits coming from tampered blocks also can be represented by a binomial distribution, but the probability of damage to each MSB bit in $\mathbf{C}_j^*$ is α' rather than α, which is related to m and l, i.e., the utilization of overlapping-free embedding or overlapping embedding, see Eq. (10).

$$\alpha' = \begin{cases} \alpha, & \text{if } m+l \le 8, \\ \frac{8-l}{m} \cdot \alpha + \frac{m+l-8}{m}, & \text{if } m+l > 8, \end{cases} \tag{10}$$

Thus, the distribution of u_j^* can be obtained as:

$$P_{u^*}(y) = \binom{u}{y} \cdot (\alpha')^y \cdot (1-\alpha')^{u-y}, \quad y = 0,\ 1, \ldots,\ u. \tag{11}$$

After obtaining the distributions of v_j' and u_j^*, we can calculate the probability P_{sr} of all u_j^* column vectors in the random binary matrix $\mathbf{H}_j^{(\mathrm{E,T})}$ being linearly independent, see Eq. (12).

$$P_{\mathrm{sr}} = 1 - \sum_{x=0}^{v} \sum_{y=0}^{u} \varphi(x, y) \cdot P_{v'}(x) \cdot P_{u^*}(y). \tag{12}$$

where P_{sr} is also the probability of perfect recovery for all damaged bits in each MSB subset $\mathbf{C}_j^*$. Therefore, the probability P_{SR} of perfect recovery for all damaged bits in all S MSB subsets, i.e., the probability for recovering all m MSB layers of $\mathbf{I}_{\mathrm{w}}^*$ exactly to those of $\mathbf{I}_{\mathrm{o}}$, can be calculated:

$$P_{\mathrm{SR}} = (P_{\mathrm{sr}})^S = (P_{\mathrm{sr}})^{m \cdot N/u}. \tag{13}$$

We can find from Eqs. (8–13) that, the tampering rate α, the embedding mode (m, l), the subset lengths u and v of MSB bits and reference bits, and the total pixel number N of the image are related with the perfect recovery probabilities P_{sr} and P_{SR} for each MSB subset and the whole image $\mathbf{I}_{\mathrm{w}}^*$. Actually, in the proposed self-embedding scheme, the image block size $b \times b$ and the length L_{a} of authentication bits for each block are often set to the fixed values, i.e., 8×8 and 32, to ensure the accuracy of tampering detection, thus, the value of v is only related with m, l, and u according to Eq. (3). As a result, it can be concluded that, the probability P_{sr} is dependent on α, m, l, and u, and the probability P_{SR} is dependent on α, m, l, u, and N. Obviously, the probabilities P_{sr} and P_{SR} of perfect recovery are inversely proportional to the tampering rate α. It can also be easily observed from Eqs. (8-13) that, the probability P_{sr} is directly proportional to the value of u, and the probability P_{SR} is inversely proportional to the value of N/u.

In order to show the relationship between perfect recovery probabilities (P_{sr} and P_{SR}) and embedding parameters (m and l), different embedding modes are utilized for demonstration, see Figs. 3–4. Fig. 3(a-b) show the probability P_{sr} of perfect recovery for each MSB subset with the length u of 512 under different tampering rates α. The six groups of embedding parameters m and l in the two subfigures have three cases, i.e., $m+l < 8$, $m+l=8$, and $m+l > 8$. Fig. 4(a-b) show the probability P_{SR} of perfect recovery for a whole image sized 512×512 corresponding to Fig. 3(a-b), respectively. For a given tampering rate α, the following conclusions about the performances with different embedding modes (m, l) can be generally drawn. For the scenario of overlapping-free embedding ($m+l \le 8$), under the same watermark embedding capacity, i.e., l LSBs, smaller value of m leads to greater probabilities of P_{sr} and P_{SR}; on the other hand, under the same number m of MSB layers for reference-bit generation, larger value of l leads to greater probabilities of P_{sr} and P_{SR}. For the scenario of overlapping embedding ($m+l > 8$), under the same value of l, smaller value of m (in other words, smaller number $m+l-8$ of the destroyed MSB layers caused by LSB embedding) leads to greater probabilities of P_{sr} and P_{SR}; similarly, under the same value of m, smaller value of l leads to greater probabilities of P_{sr} and P_{SR}. Also, for both scenarios of overlapping-free and overlapping embedding, under the same value of $m+l-8$, larger value of l leads to greater probabilities of P_{sr} and P_{SR}.

Obviously, when the probability P_{sr} is equal to 1, P_{SR} must equal 1 and it also means that all damaged MSB bits in the image $\mathbf{I}_{\mathrm{w}}^*$ can be definitely recovered to their original versions without relevance to image size N. Here, we define $\alpha_{\max}$ as

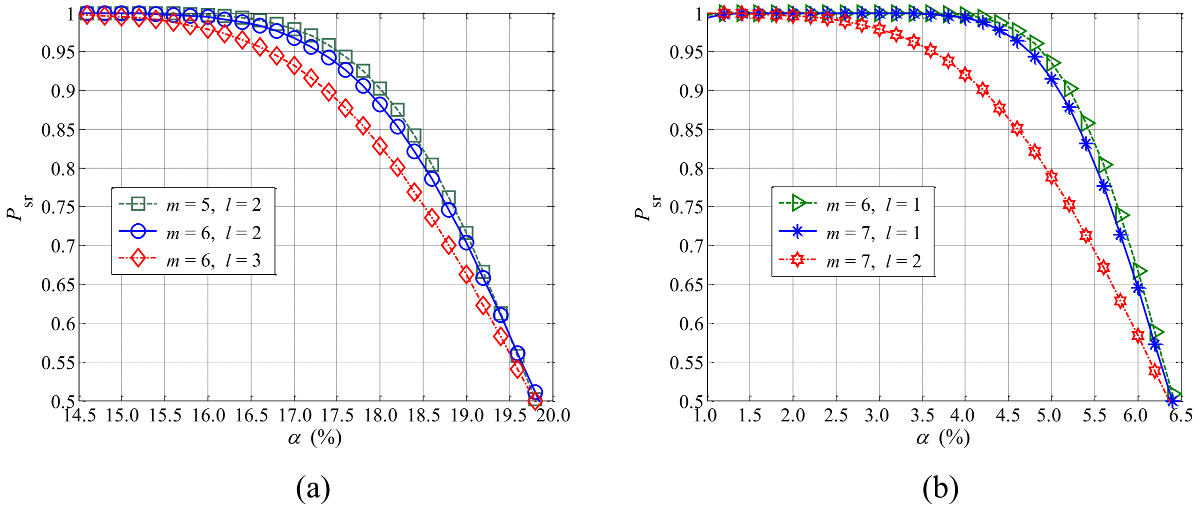

Fig. 3. The probability P_{sr} under different tampering rates α ($u = 512$).

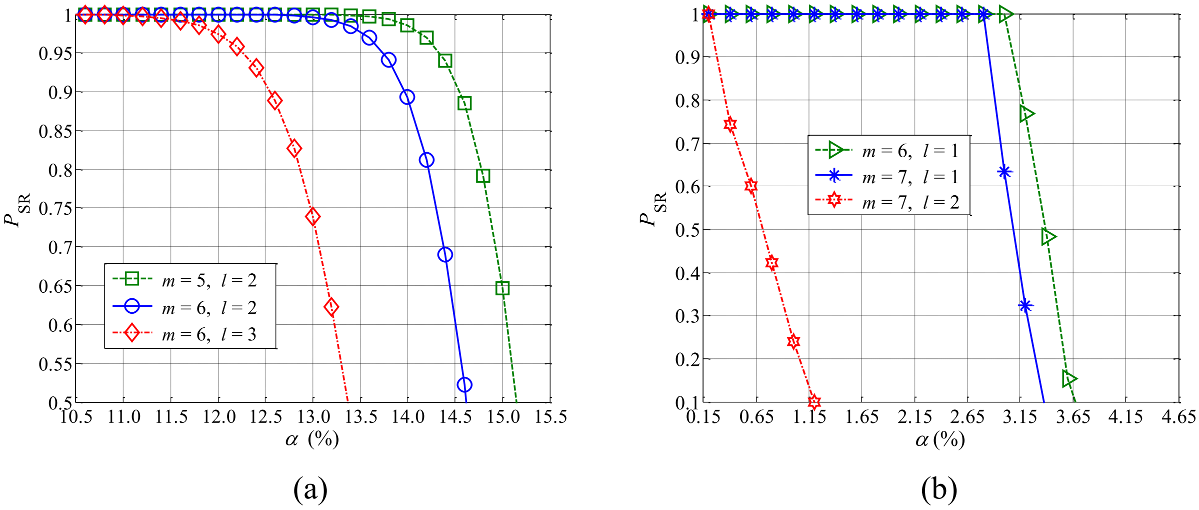

Fig. 4. The probability P_{SR} under different tampering rates α ($u = 512$, $N = 512 \times 512$).

Table 2
The values of α_{max} under different embedding modes (m, l).

		$m=4$	$m=5$	$m=6$	$m=7$
$u=512$	$l=1$	3.8%	3.4%	3.0%	2.8%
	$l=2$	13.6%	12.6%	11.8%	0.2%
	$l=3$	25.4%	24.2%	9.8%	0.02%
$u=1024$	$l=1$	3.8%	3.6%	3.2%	3.0%
	$l=2$	15.4%	14.8%	14.2%	0.4%
	$l=3$	27.8%	27.0%	12.8%	0.04%

the maximum of tolerable tampering rates that can make P_{sr} equal 1 under certain values of m, l, and u. In other words, as long as tampering rate α is no greater than α_{max}, the perfect recovery for all damaged MSB bits in $\mathbf{I}_w{}^*$ can always be guaranteed with $P_{SR} = 1$. Table 2 shows the values of α_{max} under different embedding modes (m, l) and MSB subset lengths u. It should be noted that, if the probability P_{sr} is not equal to 1, all damaged MSB bits can still be perfectly recovered with the probability of P_{SR} (<1). In other words, in practice, the perfect recovery may be achieved on tampered image with tampering rate α larger than α_{max}.

Table 3
Theoretical values of PSNR_w, PSNR_r and $\alpha_{\max}$ under different embedding modes (m, l).

Embedding mode	(m, l)						
	(7, 2)	(7, 1)	(6, 3)	(6, 2)	(6, 1)	(5, 3)	(5, 2)
$\alpha_{\max}$ (%)	0.2	2.8	9.8	11.8	3.0	24.2	12.6
PSNR_w (dB)	44.15	51.14	37.92	44.15	51.14	37.92	44.15
PSNR_r (dB)	51.14	51.14	46.37	46.37	50.65	40.73	44.16

3.3. PSNR of recovered image

In this Subsection, we give the analysis for the recovered image quality of our proposed scheme with different embedding modes. As described in Subsection 2.2, after the damaged bits in all S subsets derived from m MSBs are perfectly recovered, the decimal values of l' LSBs for all pixels are set to $2^{l'-1}$, where l'=min(l, 8 − m), and the final recovered image $\mathbf{I}_\text{r}$ can be obtained.

For the conditions that $m+l>8$ and $m+l=8$, the distortions of the recovered image $\mathbf{I}_\text{r}$ compared with the original image $\mathbf{I}_\text{o}$ are caused by the l' LSBs; for the condition of $m+l<8$, the distortions of $\mathbf{I}_\text{r}$ are caused by the $(8-m)$ LSBs, which include l' LSBs and the higher $(8-m-l')$ bit layers. Note that, although these $(8-m-l')$ bit layers higher than l' LSBs are not embedded with watermark bits, they may also be damaged due to tampering operations. Therefore, the theoretical value of PSNR for recovered image $\mathbf{I}_\text{r}$ with respect to original image $\mathbf{I}_\text{o}$ can be calculated through Eqs. (14–16):

$$D_\text{r}(m,\ l) = \frac{1}{2^{l'}} \cdot \sum_{\xi_\text{o}=0}^{2^{l'}-1} \left(\xi_\text{o} - 2^{l'-1}\right)^2, \quad \text{where } l' = \min(l,\ 8-m), \tag{14}$$

$$D_\text{t}(m,\ l) = \alpha \cdot 2^{(l-2\mu)} \cdot \sum_{\xi_\text{o}=0}^{2^\mu-1} \sum_{\xi_\text{d}=0}^{2^\mu-1} (\xi_\text{o} - \xi_\text{d})^2, \quad \text{where } \mu = 8-m-l', \tag{15}$$

$$\text{PSNR}_\text{r}(m,\ l) = \begin{cases} 10 \cdot \log_{10} \dfrac{255^2}{D_\text{r}(m,\ l)}, & \text{if } m+l \geq 8\,, \\ 10 \cdot \log_{10} \dfrac{255^2}{D_\text{r}(m,\ l) + D_\text{t}(m,\ l)}, & \text{if } m+l < 8\,, \end{cases} \tag{16}$$

where $D_\text{r}(m, l)$ denotes the distortions caused by the l' LSBs, $D_\text{t}(m, l)$ denotes the distortions of the higher, non-embedded $(8-m-l')$ bit layers caused by tampering operations, and $\text{PSNR}_\text{r}(m, l)$ is the theoretical PSNR value of $\mathbf{I}_\text{r}$ under different embedding modes.

3.4. Optimal choice of embedding modes

According to the analysis in Sections 3.1–3.3, we can easily calculate the theoretical values for PSNR of watermarked image (PSNR_W), PSNR of recovered image (PSNR_r), and the maximum of tolerable tampering rate ($\alpha_{\max}$) under different embedding modes (m, l), as listed in Table 3.

We can conclude the optimal choice of embedding modes based on the theoretical values in Table 3 as follows. When the tampering rate α belongs to (0, 2.8%], the six embedding modes, i.e., (5, 2), (5, 3), (6, 1), (6, 2), (6, 3) and (7, 1), can all achieve perfect recovery with $P_\text{SR}=1$. With respect to PSNR of watermarked image and recovered image, the embedding mode (7, 1) has better performances than the other five embedding modes. Therefore, when $\alpha \in$ (0, 2.8%], the optimal embedding mode (m, l) should be (7, 1). When α belongs to (2.8%, 3.0%], the embedding modes of (5, 2), (5, 3), (6, 1), (6, 2) and (6, 3) can achieve perfect recovery with $P_\text{SR}=1$, and the embedding mode (6, 1) has both better results of PSNR_W and PSNR_r compared with the modes of (5, 2), (5, 3), (6, 2) and (6, 3). Therefore, when $\alpha \in$ (2.8%, 3.0%], the optimal embedding mode (m, l) should be (6, 1). When α belongs to (3.0%, 9.8%], the embedding modes of (5, 2), (5, 3), (6, 2) and (6, 3) can all achieve perfect recovery with $P_\text{SR}=1$. With respect to PSNR_W and PSNR_r, the embedding mode (6, 2) has better performances than the other three embedding modes of (5, 2), (5, 3) and (6, 3). When α belongs to (9.8%, 11.8%], the three embedding modes of (5, 2), (5, 3) and (6, 2) can achieve perfect recovery with $P_\text{SR}=1$, and the embedding mode (6, 2) can also have better performances of both PSNR_W and PSNR_r than the modes of (5, 2) and (5, 3). Therefore, when $\alpha \in$ (3.0%, 11.8%], the optimal embedding mode (m, l) should be (6, 2). When α belongs to (11.8%, 12.6%], only the two embedding modes of (5, 2) and (5, 3) can achieve perfect recovery with $P_\text{SR}=1$, and the embedding mode (5, 2) has better performances of both PSNR_W and PSNR_r than the mode (5, 3). Therefore, the optimal embedding mode (m, l) should be (5, 2) when $\alpha \in$ (11.8%, 12.6%]. When α belongs to (12.6%, 24.2%], only the embedding mode (5, 3) can achieve perfect recovery with $P_\text{SR}=1$. Therefore, when $\alpha \in$ (12.6%, 24.2%], the optimal embedding mode (m, l) is just (5, 3). When α is greater than 24.2%, all embedding modes of the proposed scheme ($l \leq 3$) can not guarantee the definitely perfect recovery, thus, no optimal embedding mode

Table 4
Theoretical optimal embedding modes with $P_{SR} = 1$ for different ranges of α.

Range of α (%)	(0, 2.8]	(2.8, 3.0]	(3.0, 11.8]	(11.8, 12.6]	(12.6, 24.2]
Optimal embedding mode (m, l)	(7, 1)	(6, 1)	(6, 2)	(5, 2)	(5, 3)

Fig. 5. Original image Lena and its watermarked versions. (a) Original image Lena, (b) Watermarked image with embedding mode (6, 2) and $\text{PSNR}_w = 44.16$ dB.

(m, l) can be theoretically provided under this scenario. Based on the above analysis, we can summarize the conclusions of optimal choice for embedding modes in Table 4.

In the scenario of image transmission through the wireless fading channel, the information of a portion of image blocks may be missing or be contaminated. Consequently, on the receiver side, the decoded image may be visually degraded compared with original image. We can naturally analogize the noise strength of the fading channel with the tampering rate of the self-embedding problem. Also, by using the existing techniques of channel estimation, the noise strength of the fading channel, i.e., the analogized tampering rate α, can be easily estimated. Therefore, in order to effectively recover the missing contents of degraded images on the receiver side, before transmitting the image, the optimal mode can be chosen for watermark self-embedding according to the estimated α and their relationship in Table 4.

4. Experimental results and comparisons

Experiments were conducted on a large number of test images to demonstrate the effectiveness of the proposed scheme. For color images, the luminance components were utilized for testing. 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. The subset length u of MSB bits in our scheme was set to 512 in the experiments. The forms of the tampering operations in our experiments included both intentional tampering and inadvertent tampering, which can correspond to the malicious modification by an adversary and the image block missing in the fading transmission channel, respectively.

Figs. 5–6 show the original versions of two standard test images both sized 512 × 512, i.e., Lena and Lake, and their corresponding watermarked versions. PSNR value of the watermarked image for Lena with embedding mode (6, 2) was 44.16 dB, and PSNR value of the watermarked image for Lake with embedding mode (7, 1) was 51.14 dB The visual distortions caused by watermark embedding were imperceptible. Two kinds of meaningful tampering operations for Lena and Lake are illustrated in Fig. 7(a) and (b), in which the face of Lena was replaced with that of a man ($\alpha = 6.84\%$) and one more sailboat was added on the surface of lake ($\alpha = 1.86\%$), respectively. Figs. 8–9(a) show the results of tampering detection for the two tampered images in Fig. 7, in which all tampered blocks were localized and marked with the white color. Figs. 8–9(b) show the corresponding recovered results, and the embedding mode (6, 2) for Lena and the embedding mode (7, 1) for Lake both completed perfect recovery. PSNR values of recovered images Lena and Lake were 46.37 dB and 51.14 dB, respectively, which achieved satisfactory visual quality.

As we describe in Section 3.2, as long as the tampering rate α is no greater than the theoretical maximum of tolerable tampering rates $\alpha_{\max}$, the perfect recovery for all damaged MSB bits can always be achieved with the probability $P_{SR} = 1$. Actually, in practical applications, the perfect recovery that recovers all damaged MSB bits in a tampered image may be achieved with the probability of $P_{SR} < 1$, which means the practical maximum of tolerable tampering rates under the condition of perfect recovery for a tampered image, i.e., $\alpha'_{\max}$, may be greater than the theoretical value $\alpha_{\max}$. Therefore, in order to obtain the practical maximum $\alpha'_{\max}$, the well-known uncompressed color image database (UCID) [30] that contains 1338 various natural images was utilized. For each image in UCID, the practical maximum of tolerable tampering rates for perfect

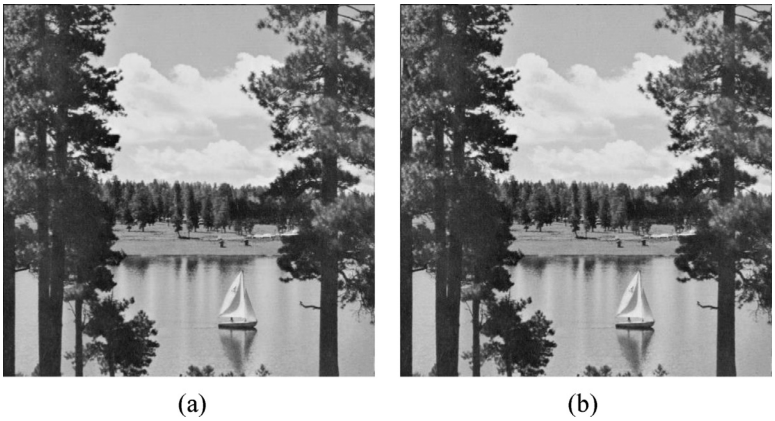

Fig. 6. Original image Lake and its watermarked versions. (a) Original image Lake, (b) Watermarked image with embedding mode (7, 1) and $\mathrm{PSNR_w} = 51.14$ dB.

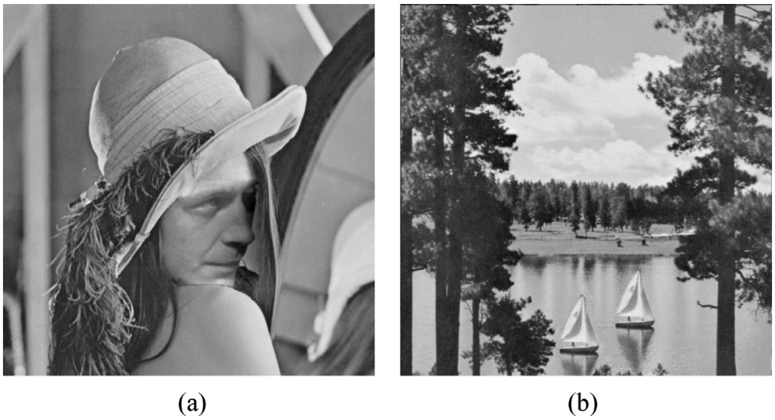

Fig. 7. Two tampered, watermarked images of Lena and Lake. (a) Lena with tampering rate $\alpha = 6.84\%$, (b) Lake with tampering rate $\alpha = 1.86\%$.

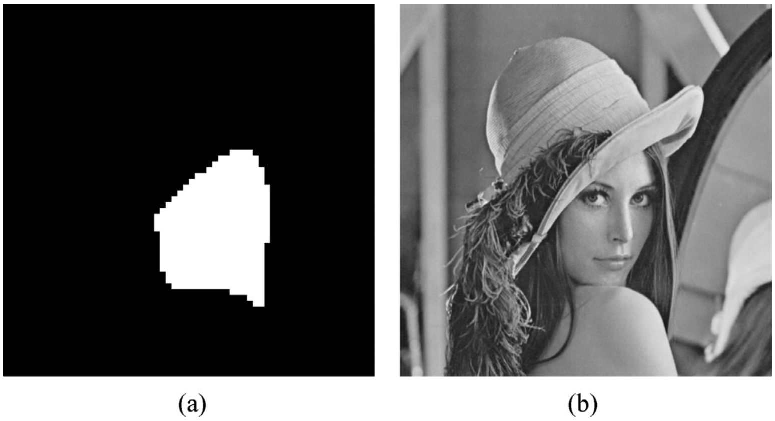

Fig. 8. Results of tampering detection and content recovery for Lena. (a) Tampering detection result, (b) Recovered image of embedding mode (6, 2) and $\mathrm{PSNR_r} = 46.37$ dB

recovery was calculated, and the average value of the practical maximums for these 1338 images was obtained as $\alpha'_{\max}$. Table 5 gives the practical optimal embedding modes corresponding to different ranges of tampering rates α, which were based on the experimental statistics of $\alpha'_{\max}$ for the image database UCID. We can find from Tables 4 and 5 that, their order of corresponding relationship between α and (m, l) is consistent, and compared with theoretical optimal embedding modes, the ranges of the tolerable tampering rates for practical optimal embedding modes are extended.

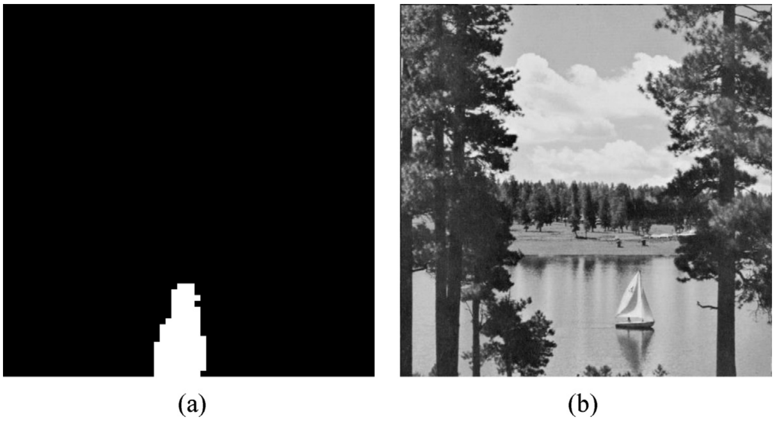

Fig. 9. Results of tampering detection and content recovery for Lake. (a) Tampering detection result, (b) Recovered image of embedding mode (7, 1) and $\text{PSNR}_\text{r} = 51.14\,\text{dB}$

Table 5
Practical optimal embedding modes from experimental statistics of UCID for different ranges of α.

Optimal embedding mode (m, l)	(7, 1)	(6, 1)	(6, 2)	(5, 2)	(5, 3)
α'_{max} (%)	3.1	3.4	14.6	17.3	28.0
Range of α (%)	(0, 3.1]	(3.1, 3.4]	(3.4, 14.6]	(14.6, 17.3]	(17.3, 28.0]

Besides the meaningful tampering, the meaningless tampering that simulated the missing of image blocks in wireless fading channel was also conducted for testing, see Fig. 10. The five embedding modes listed in Table 5 were utilized for tampering recovery, and six tampering rates α, i.e., 3.0%, 3.4%, 6.0%, 16.0%, 20.0% and 30.0%, were applied to simulate the six kinds of different missing percentages for image blocks sized 8 × 8, as shown the damaged, watermarked image Crowd sized 512 × 512 in subfigures (a1-c1) and (a3-c3) of Fig. 10. The subfigures (a2-c2) and (a4-c4) in Fig. 10 are the corresponding recovered images with practical optimal embedding modes (7, 1), (6, 1), (6, 2), (5, 2), (5, 3) and (5, 3), respectively. When α was equal to 3.0%, i.e., Fig. 10(a1), all five modes (7, 1), (6, 1), (6, 2), (5, 2) and (5, 3) can complete perfect recovery, and the corresponding PSNR values of recovered images were 51.15 dB, 50.93 dB, 46.58 dB, 45.86 dB and 40.75 dB, respectively. When α was equal to 3.4%, i.e., Fig. 10(b1), the four modes (6, 1), (6, 2), (5, 2) and (5, 3) can complete perfect recovery, and the corresponding PSNR values of recovered images were 50.90 dB, 46.58 dB, 45.77 dB and 40.75 dB However, the mode (7, 1) can not realize perfect recovery, because there are not enough correct MSB bits and extracted reference bits from intact blocks under the condition of this embedding mode for larger tampering rate. Consequently, some damaged MSB bits for the mode (7, 1) can not be solved by Eq. (5). In order to remedy this problem, after recovering some tampered blocks with the solvable MSB bits, the technique of image inpainting [27,1] can be further utilized to repair the remaining unsolvable blocks. In the experiments, we adopted a typical image inpainting method based partial differential equation (PDE) with the fluid dynamics model [1]. This inpainting method analogized the inpainting process as the fluid flowing and imitated the practice of a traditional art professional in manual retouching, thus, the structural and geometric information of the unsolvable tampered blocks can be approximately repaired through propagating the intact and recovered information in neighboring blocks along the isophote direction. PSNR value of the recovered image with assist of inpainting for the mode (7, 1) was 50.89 dB When α was equal to 6.0%, i.e., Fig. 10(c1), the modes (6, 2), (5, 2) and (5, 3) can complete the perfect recovery, and PSNR values of recovered images were 46.58 dB, 45.23 dB and 40.75 dB The modes (7, 1) and (6, 1) can not realize perfect recovery, and the PSNR values of their recovered images with assist of inpainting were 34.06 dB and 38.68 dB, respectively. When α was equal to 16.0%, i.e., Fig. 10(a3), the two modes (5, 2) and (5, 3) can complete the perfect recovery, and PSNR values of recovered images were 43.52 dB and 40.75 dB The modes (7, 1), (6, 1) and (6, 2) can not realize the perfect recovery, and the PSNR values of their recovered images with assist of inpainting were 27.65 dB, 29.43 dB and 41.51 dB, respectively. When α was equal to 20.0%, i.e., Fig. 10(b3), only the mode (5, 3) can complete the perfect recovery, and PSNR value of recovered image was 40.75 dB The other four modes (7, 1), (6, 1), (6, 2) and (5, 2) can not realize perfect recovery, and the PSNR values of their recovered images with assist of inpainting were 26.65 dB, 27.22 dB, 29.57 dB and 37.58 dB, respectively. When α was equal to 30.0%, i.e., Fig. 10(c3), none of the five modes (7, 1), (6, 1), (6, 2), (5, 2) and (5, 3) can realize perfect recovery, and the PSNR values of their recovered images with assist of inpainting were 24.82 dB, 25.13 dB, 25.49 dB, 26.36 dB and 33.79 dB, respectively. Table 6 lists the PSNR values of both watermarked images and recovered images, i.e., P_W and P_r, under different tampering rates α, which also verify the results of theoretical analysis and experimental statistics for the optimal choice of embedding modes given in Section 3 and Table 5.

To demonstrate the superiority of the proposed scheme, we compared our scheme with Yang and Shen's scheme [37], Huo et al.'s scheme [7], and Yang et al.'s scheme [36]. Fig. 11 illustrates the recovered results of the proposed scheme and the other schemes [37,7,36] for Airplane, Goldhill, Baboon and Sailboat, all sized 512 × 512 with different tampering rates

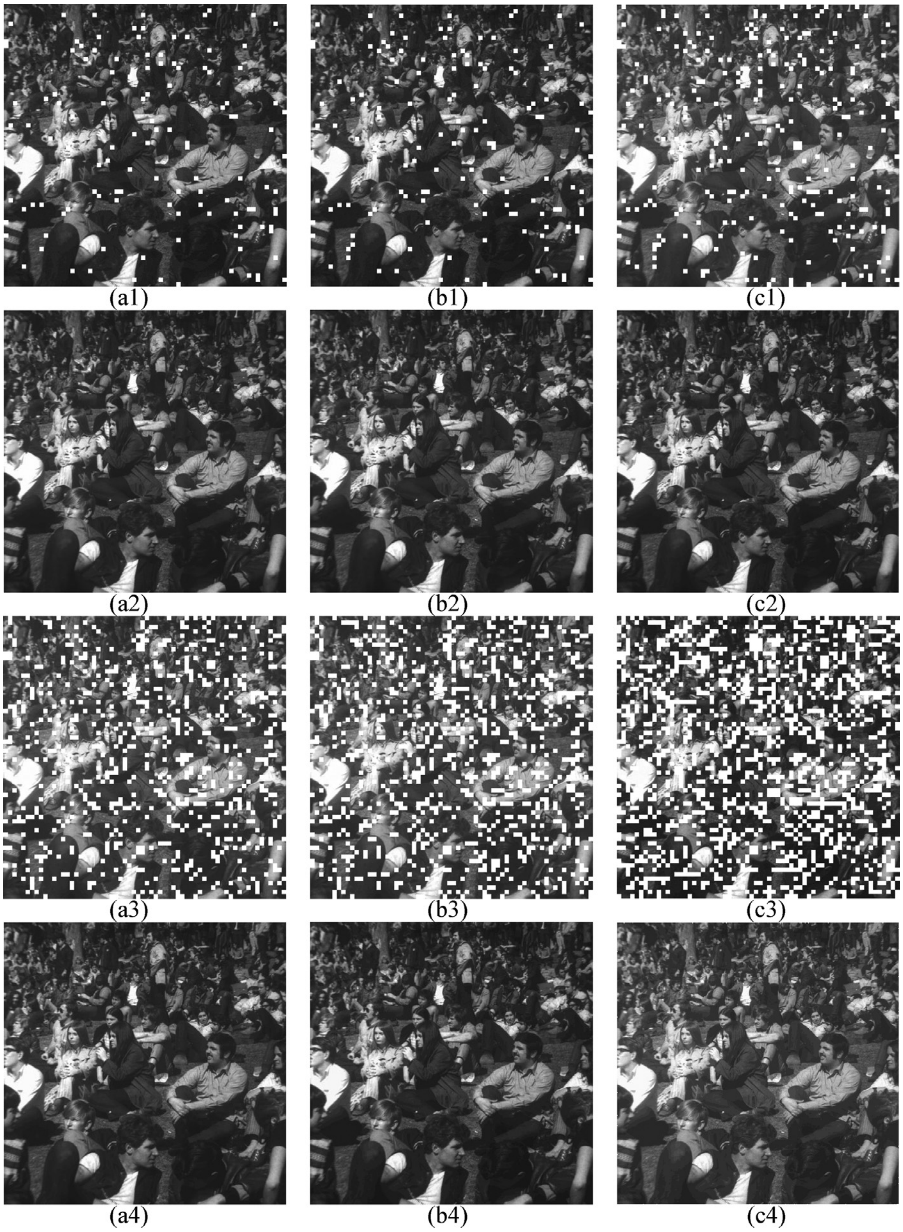

Fig. 10. Results of content recovery for tampered image Crowd. (a1) $\alpha = 3.0\%$, (b1) $\alpha = 3.4\%$, (c1) $\alpha = 6.0\%$, (a3) $\alpha = 16.0\%$, (b3) $\alpha = 20.0\%$, (c3) $\alpha = 30.0\%$, (a2) Recovered image for (a1) with embedding mode (7, 1) and $\text{PSNR}_r = 51.15$ dB, (b2) Recovered image for (b1) with embedding mode (6, 1) and $\text{PSNR}_r = 50.90$ dB, (c2) Recovered image for (c1) with embedding mode (6, 2) and $\text{PSNR}_r = 46.58$ dB, (a4) Recovered image for (a3) with embedding mode (5, 2) and $\text{PSNR}_r = 43.$ 52 dB, (b4) Recovered image for (b3) with embedding mode (5, 3) and $\text{PSNR}_r = 40.75$ dB, (c4) Recovered image with inpainting for (c3) under embedding mode (5, 3) and $\text{PSNR}_r = 33.79$ dB

(i.e., the missing percentages of image blocks sized 32 × 32 in the wireless fading channel). The first row of Fig. 11 shows the four tampered images with $\alpha = 3\%$, 10%, 15% and 20%, respectively. The second, third, and fourth rows are the corresponding recovered results of the three schemes [37,7,36], respectively. The watermark embedding capacities of schemes [37] and [36] were fixed as 3 LSBs and 1 LSB, respectively, and scheme [7] had variable capacities. The last row shows the recovered results of our scheme with unfixed embedding modes (7, 1), (6, 2), (5, 2) and (5, 3), which individually correspond to the optimal modes for the different tampering rates α in Table 5. Table 7 presents the PSNR values of watermarked images and recovered images with respect to the original images for the proposed scheme and schemes [37,7,36]. In addition to PSNR values, the values of structural similarity (SSIM) [32] for watermarked images and recovered images are given in Table 8. 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. Also, we conducted

Table 6
PSNR values of watermarked and recovered images for image Crowd (dB)[a].

Embedding mode (m, l)		(7, 1)	(6, 1)	(6, 2)	(5, 2)	(5, 3)
$\alpha = 3.0\%$	P_w	51.13	51.14	44.18	44.17	37.84
	P_r	51.15	50.93	46.58	45.86	40.75
$\alpha = 3.4\%$	P_w	51.13	51.14	44.18	44.17	37.84
	P_r	50.89^*	50.90	46.58	45.77	40.75
$\alpha = 6.0\%$	P_w	51.13	51.14	44.18	44.17	37.84
	P_r	34.06^*	38.68^*	46.58	45.23	40.75
$\alpha = 16.0\%$	P_w	51.13	51.14	44.18	44.17	37.84
	P_r	27.65^*	29.43^*	41.51^*	43.52	40.75
$\alpha = 20.0\%$	P_w	51.13	51.14	44.18	44.17	37.84
	P_r	26.65^*	27.22^*	29.57^*	37.58^*	40.75
$\alpha = 30.0\%$	P_w	51.13	51.14	44.18	44.17	37.84
	P_r	24.82^*	25.13^*	25.49^*	26.36^*	33.79^*

[a] The superscript symbol $*$ denotes that the recovered result of the corresponding embedding mode was assisted with image inpainting.

Table 7
Comparisons of PSNR values for the proposed scheme and the schemes [37,7,36].

Images	Tampering rate α (%)	{PSNR of watermarked image, PSNR of recovered image}			
		Scheme in [37]	Scheme in [7]	Scheme in [36]	Proposed scheme
Airplane	3	{36.68, 37.13}	{43.33, 37.51}	{51.10, 38.67}	{51.15, 51.14}
Goldhill	10	{36.71, 36.96}	{43.43, 35.62}	{51.10, 37.78}	{44.14, 46.36}
Baboon	15	{36.74, 34.39}	{43.72, 25.60}	{51.10, 33.12}	{44.17, 43.33}
Sailboat	20	{36.69, 33.40}	{43.24, 26.93}	{51.10, 31.20}	{37.91, 40.72}
Average	12	{36.71, 35.47}	{43.43, 31.42}	{51.10, 35.19}	{44.34, 45.39}

Table 8
Comparisons of SSIM values for the proposed scheme and the schemes [37,7,36].

Images	Tampering rate α (%)	{SSIM of watermarked image, SSIM of recovered image}			
		Scheme in [37]	Scheme in [7]	Scheme in [36]	Proposed scheme
Airplane	3	{0.9839, 0.9828}	{0.9966, 0.9921}	{0.9982, 0.9831}	{0.9991, 0.9995}
Goldhill	10	{0.9934, 0.9727}	{0.9986, 0.9719}	{0.9962, 0.9823}	{0.9980, 0.9990}
Baboon	15	{0.9896, 0.9780}	{0.9974, 0.8669}	{0.9981, 0.9660}	{0.9972, 0.9965}
Sailboat	20	{0.9869, 0.9728}	{0.9971, 0.9008}	{0.9949, 0.9580}	{0.9834, 0.9914}
Average	12	{0.9885, 0.9766}	{0.9974, 0.9329}	{0.9969, 0.9724}	{0.9944, 0.9966}

performance comparisons between the proposed scheme and schemes [37,7,36] for the 1338 images in the image database of UCID, see Tables 9-10. It can be observed from Fig. 11 and Tables 7–10 that, the proposed scheme can achieve better visual quality of recovered images than the reported schemes [37,7,36] under the different tampering rates.

5. Conclusions

In this work, we propose a general image self-embedding scheme for tampering recovery. Different from the reported schemes that used a fixed embedding mode, the embedding modes of the proposed scheme can be categorized into overlapping-free embedding and overlapping embedding, which are related with variable numbers of the MSB layers and LSB layers that are used during watermark embedding. Based on the reference interleaving mechanism, the MSB bits that represent the principle contents of the image blocks are interleaved to generate reference bits, and then, are embedded

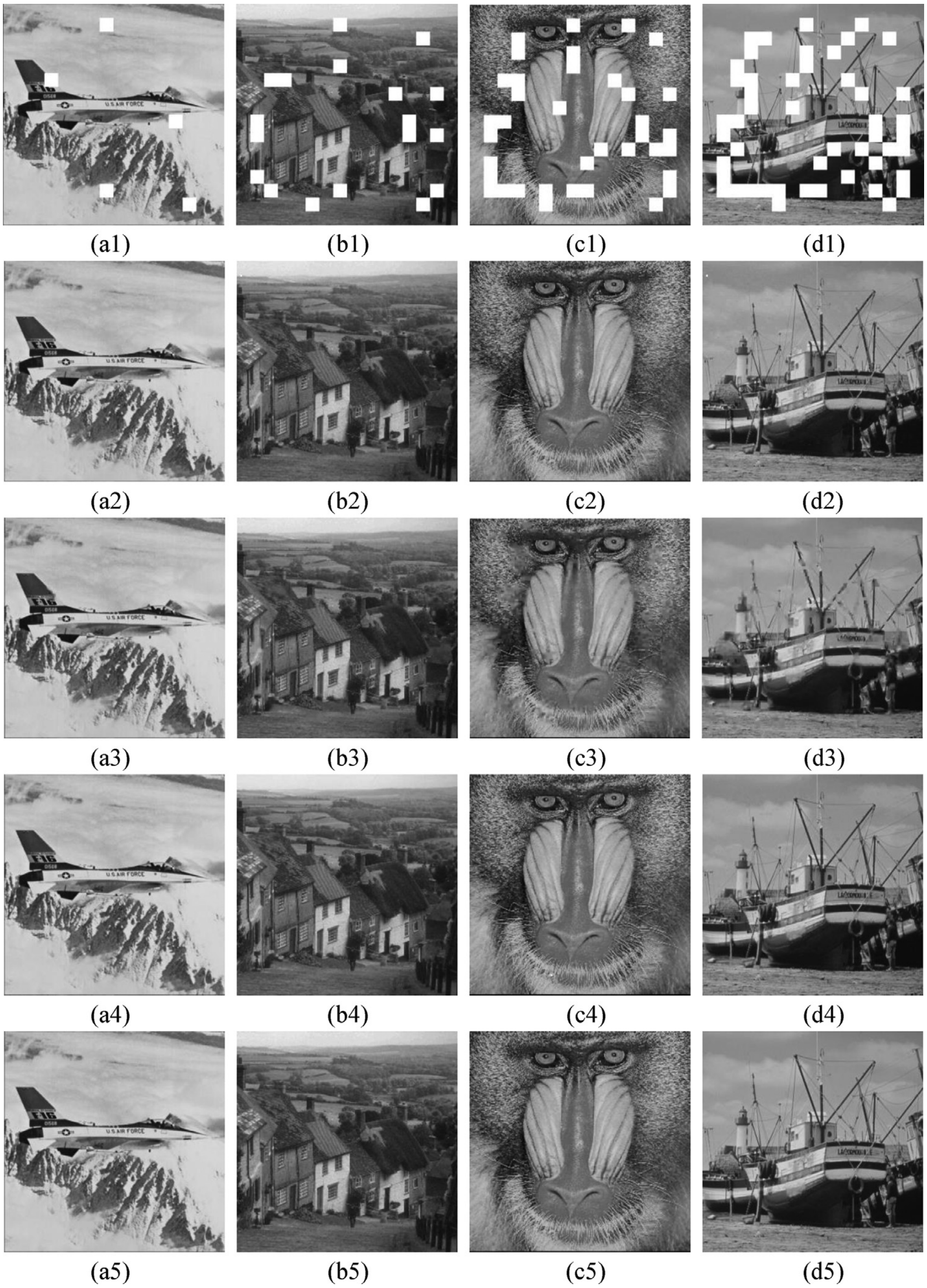

Fig. 11. Recovered results of the schemes [37,7,36] and the proposed scheme. The first row (a1-d1) are the four tampered images with $\alpha = 3\%$, 10%, 15% and 20%, respectively; the second row (a2-d2), the third row (a3-d3) and the fourth row (a4-d4) are the recovered results of [37,7,36], respectively; The last row (a5-d5) are the recovered results of the proposed scheme.

into the LSBs. Because both the numbers of the MSB layers and LSB layers that are used influence the quality of the watermarked images, affect the probability of perfect recovery, and the quality of the recovered images, detailed analyses are given to provide the theoretical values and present the optimal choice of embedding modes. Also, many experiments, including content recovery for intentional tampering and inadvertent tampering of block missing in the wireless fading channels, are simulated to demonstrate the effectiveness and superiority of our scheme compared with the reported schemes.

Table 9
Comparison results of PSNR values for the 1338 images in UCID.

Images	Tampering rate α (%)	{PSNR of watermarked image, PSNR of recovered image}			
		Scheme in [37]	Scheme in [7]	Scheme in [36]	Proposed scheme
UCID	3	{38.12, 37.44}	{43.47, 37.12}	{51.12, 38.67}	{51.14, 51.12}
	10	{38.12, 36.10}	{43.47, 35.07}	{51.12, 37.98}	{44.15, 46.40}
	15	{38.12, 34.24}	{43.47, 25.39}	{51.12, 33.19}	{44.15, 43.40}
	20	{38.12, 33.74}	{43.47, 24.71}	{51.12, 30.80}	{37.92, 40.75}
Average	12	{38.12, 35.38}	{43.47, 30.57}	{51.12, 35.16}	{44.34, 45.42}

Table 10
Comparison results of SSIM values for the 1338 images in UCID.

Images	Tampering rate α (%)	{SSIM of watermarked image, SSIM of recovered image}			
		Scheme in [37]	Scheme in [7]	Scheme in [36]	Proposed scheme
UCID	3	{0.9876, 0.9845}	{0.9968, 0.9911}	{0.9962, 0.9871}	{0.9994, 0.9996}
	10	{0.9876, 0.9717}	{0.9968, 0.9720}	{0.9962, 0.9523}	{0.9970, 0.9983}
	15	{0.9876, 0.9305}	{0.9968, 0.8698}	{0.9962, 0.9360}	{0.9970, 0.9956}
	20	{0.9876, 0.8915}	{0.9968, 0.8792}	{0.9962, 0.9380}	{0.9874, 0.9931}
Average	12	{0.9876, 0.9446}	{0.9968, 0.9280}	{0.9962, 0.9534}	{0.9952, 0.9967}

Acknowledgments

This work was supported by the National Natural Science Foundation of China (61672354, 61303203), the Innovation Program of Shanghai Municipal Education Commission (14YZ087), the Open Project Program of Shenzhen Key Laboratory of Media Security, the Open Project Program of the National Laboratory of Pattern Recognition (201600003), Shanghai Engineering Center Project of Massive Internet of Things Technology for Smart Home (GCZX14014), Hujiang Foundation of China (C14001, C14002), the PAPD Fund, and the CICAEET Fund.

References

[1] M. Bertalmio, G. Sapiro, V. Caselles, C. Ballester, Image inpainting, in: Proceedings of 27th International Conference on Computer Graphics and Interactive Techniques, New Orleans, LA, USA, Jul. 2000, p. 417–424.
[2] C.C. Chang, Y.S. Hu, T.C. Lu, A watermarking-based image ownership and tampering authentication scheme, Pattern Recognit. Lett. 27 (5) (2006) 439–446.
[3] R. Chamlawi, A. Khan, Digital image authentication and recovery: employing integer transform based information embedding and extraction, Inf. Sci. 180 (24) (2010) 4909–4928.
[4] J. Fridrich, M. Goljan, Images with self-correcting capabilities, in: Proceedings of IEEE International Conference on Image Processing, 1999, pp. 792–796.
[5] Z. Fu, X. Sun, Q. Liu, L. Zhou, J. Shu, Achieving efficient cloud search services: multi-keyword ranked search over encrypted cloud data supporting parallel computing, IEICE Trans. Commun. E98-B (1) (2015) 190–200.
[6] H. He, F. Chen, H.M. Tai, T. Kalker, J. Zhang, Performance analysis of a block-neighborhood-based self-recovery fragile watermarking scheme, IEEE Trans. Inf. Forensics Secur. 7 (1) (2012) 185–196.
[7] Y. Huo, H. He, F. Chen, Alterable-capacity fragile watermarking scheme with restoration capability, Opt. Commun. 285 (7) (2012) 1759–1766.
[8] F. Hartung, M. Kutter, Multimedia watermarking techniques, Proc. IEEE vol. 87 (7) (1999) 1079–1107.
[9] Y. Hu, H.K. Lee, K. Chen, J. Li, Difference expansion based reversible data hiding using two embedding directions, IEEE Trans. Multimedia 10 (8) (2008) 1500–1512.
[10] H. He, J. Zhang, H.M. Tai, A wavelet-based fragile watermarking scheme for secure image authentication, Lect. Notes Comput. Sci. 4283 (2006) 422–432.
[11] P. Korus, J. Bialas, A. Dziech, Towards practical self-embedding for JPEG-compressed digital images, IEEE Trans. Multimedia 17 (2) (2015) 157–170.
[12] P. Korus, A. Dziech, Adaptive self-embedding scheme with controlled reconstruction performance, IEEE Trans. Inf. Forensics Secur. 9 (2) (2014) 169–181.
[13] P. Korus, A. Dziech, Efficient method for content reconstruction with self-embedding, IEEE Trans. Image Process. 22 (3) (2013) 1134–1147.
[14] X. Kang, J. Huang, W. Zeng, Improving robustness of quantization-based image watermarking via adaptive receiver, IEEE Trans. Multimedia 10 (6) (2008) 953–959.
[15] K.C. Liu, Colour image watermarking for tamper proofing and pattern-based recovery, IET Image Proc. 6 (5) (2012) 445–454.
[16] J.C. Lee, C.P. Chang, W.K. Chen, Detection of copy-move image forgery using histogram of orientated gradients, Inf. Sci. 321 (15) (2015) 250–262.
[17] P.L. Lin, C.K. Hsieh, P.W. Huang, A hierarchical digital watermarking method for image tamper detection and recovery, Pattern Recognit. 38 (12) (2005) 2519–2529.
[18] C.S. Lu, H.Y.M. Liao, Structural digital signature for image authentication: an incidental distortion resistant scheme, in: Proceedings of ACM Workshops on Multimedia, 2000, pp. 115–118.
[19] T.Y. Lee, S.D. Lin, Dual watermark for image tamper detection and recovery, Pattern Recognit. 41 (11) (2008) 3497–3506.
[20] P.Y. Lin, J.S. Lee, C.C. Chang, Dual digital watermarking for internet media based on hybrid strategies, IEEE Trans. Circuits Syst. Video Technol. 19 (8) (2009) 1169–1171.
[21] J. Li, X.L. Li, B. Yang, X.M. Sun, Segmentation-based image copy-move forgery detection scheme, IEEE Trans. Inf. Forensics Secur. 10 (3) (2015) 507–518.
[22] H. Lu, R. Shen, F.L. Chung, Fragile watermarking scheme for image authentication, Electron. Lett. 39 (12) (2003) 898–900.
[23] 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 (2) (2007) 869–882.
[24] F.D. Martino, S. Sessa, Fragile watermarking tamper detection with images compressed by fuzzy transform, Inf. Sci. 195 (15) (2012) 62–90.
[25] C. Qin, C.C. Chang, K.N. Chen, Adaptive self-recovery for tampered images based on VQ indexing and inpainting, Signal Process. 93 (4) (2013) 933–946.
[26] C. Qin, C.C. Chang, P.Y. Chen, Self-embedding fragile watermarking with restoration capability based on adaptive bit allocation mechanism, Signal Process. 92 (4) (2012) 1137–1150.

[27] C. Qin, C.C. Chang, Y.P. Chiu, A novel joint data-hiding and compression scheme based on SMVQ and image inpainting, IEEE Trans. Image Process. 23 (3) (2014) 969−978.
[28] Z. Qian, G. Feng, X. Zhang, S. Wang, Image self-embedding with high-quality restoration capability, Digit. Signal Process. 21 (2) (2011) 278–286.
[29] S. Suthaharan, Fragile image watermarking using a gradient image for improved localization and security, Pattern Recognit. Lett. 25 (16) (2004) 1893–1903.
[30] G. Schaefer, M. Stich, UCID – an uncompressed color image database, in: Proceedings of SPIE in Storage and Retrieval Methods and Applications for Multimedia, vol. 5307, 2004, pp. 472–480.
[31] C.D. Vleeschouwer, J.F. Delaigle, B Macq, Invisibility and application functionalities in perceptual watermarking: an overview, Proc. IEEE 90 (1) (2002) 64–77.
[32] 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 (4) (2004) 600−612.
[33] P.W. Wong, N. Memon, Secret and public key image watermarking schemes for image authentication and ownership verification, IEEE Trans. Image Process. 10 (10) (2001) 1593–1601.
[34] Z. Xia, X. Wang, X. Sun, Q. Wang, A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data, IEEE Trans. Parallel Distrib. Syst. 27 (2) (2015) 340−352.
[35] H. Yang, A.C. Kot, Binary image authentication with tampering localization by embedding cryptographic signature and block identifier, IEEE Signal Process Lett. 13 (12) (2006) 741–744.
[36] S. Yang, C. Qin, Z. Qian, B. Xu, Tampering detection and content recovery for digital images using halftone mechanism, in: Proceedings of the 10th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Kitakyushu, Japan, Aug. 2014, p. 130−133.
[37] C.W. Yang, J.J. Shen, Recover the tampered image based on VQ indexing, Signal Process. 90 (1) (2010) 331–343.
[38] F. Zou, Y. Chen, J. Song, K. Zhou, Y. Yang, N. Sebe, Compact image fingerprint via multiple kernel hashing, IEEE Trans. Multimedia 17 (7) (2015) 1006−1018.
[39] 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 (4) (2011) 1223–1232.
[40] X. Zhang, S. Wang, Fragile watermarking with error-free restoration capability, IEEE Trans. Multimedia 10 (8) (2008) 1490−1499.
[41] X. Zhang, S. Wang, Statistical fragile watermarking capable of locating individual tampered pixels, IEEE Signal Process Lett. 14 (10) (2007) 727–730.
[42] X. Zhang, S. Wang, Z. Qian, G. Feng, Reference sharing mechanism for watermark self-embedding, IEEE Trans. Image Process. 20 (2) (2011) 485–495.
[43] X. Zhang, Y. Xiao, Z. Zhao, Self-embedding fragile watermarking based on DCT and fast fractal coding, Multimedia Tools Appl. 74 (15) (2015) 5767−5786.

Chuan Qin received the B.S. degree in electronic engineering and the M.S. degree in signal and information processing from Hefei University of Technology, Anhui, China, in 2002 and 2005, respectively, and the Ph.D. degree in signal and information processing from Shanghai University, Shanghai, China, in 2008. Since 2008, he has been with the faculty of the School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology, where he is currently an Associate Professor. He was with Feng Chia University at Taiwan as a Postdoctoral Researcher and Adjunct Assistant Professor from July 2010 to July 2012. Dr. Qin is also a visiting researcher with Shenzhen Key Laboratory of Media Security, Shenzhen University, Shenzhen 518,060, China. His research interests include image processing and multimedia security. He has published more than 70 papers in these research areas.

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.

Xinpeng Zhang received the B.S. degree in computational mathematics from Jilin University, China, in 1995, and the M.E. and Ph.D. degrees in communication and information system from Shanghai University, China, in 2001 and 2004, respectively. Since 2004, he has been with the faculty of the School of Communication and Information Engineering, Shanghai University, where he is currently a Professor. He was with the State University of New York at Binghamton as a visiting scholar from January 2010 to January 2011, and Konstanz University as an experienced researcher sponsored by the Alexander von Humboldt Foundation from March 2011 to May 2012. His research interests include multimedia security, image processing, and digital forensics. He has published more than 180 papers in these areas. Currently, he is an Associate Editor for the IEEE Transactions on Information Forensics and Security.

Xingming Sun is currently a Professor with the College of Computer and Software, Nanjing University of Information Science and Technology, Nanjing, China. He was a Professor with the College of Computer and Communication, Hunan University, Changsha, China. He was a Visiting Professor with University College London, London, U.K., and the University of Warwick, Coventry, U.K. He received the B.S. degree in mathematics from Hunan Normal University, Changsha, in 1984, the M.S. degree in computing science from the Dalian University of Science and Technology, Dalian, China, in 1988, and the Ph.D. degree in computer science from Fudan University, Shanghai, China, in 2001. His research interests include network and information security, digital watermarking, cloud computing security, and wireless network security.