Multimedia Tools and Applications (2019) 78:12373–12403
https://doi.org/10.1007/s11042-018-6664-3

A restorable fragile watermarking scheme with superior localization for both natural and text images

Omer Hemida[1] · Yaoran Huo[1] · Hongjie He[1] · Fan Chen[1]

Received: 14 February 2018 / Revised: 29 August 2018 / Accepted: 7 September 2018 /
Published online: 24 October 2018

Abstract
In this paper, we present a method for detecting and restoring tampered information in natural and text images. To take the detection ability, invisibility, and recovery quality into account for both natural and text images, this work generates the authentication watermark for each 4×4 block by a hash function and a variable capacity recovery watermark for each 2×2 block by allocating more bits to the textural blocks and fewer bits to the smooth ones. The authentication watermark and the recovery one are embedded in the original image by adopting different strategies based on a secret key. The multi-stage neighbor detection strategy is designed to locate the tampered image blocks accurately. The proposed scheme outperforms in invisibility, with detecting tampered locations and recovery of the tampered regions. The simulation results show that the proposed scheme achieves better recovery quality and invisibility for natural and text images due to a variable-capacity recovery watermark and superior localization. Further, the proposed method computationally is less expensive compared with the existing works.

Keywords Fragile watermarking · Digital image · Multi-stage neighbor detection · A variable length coding

1 Introduction

The development of computer technology and image processing made the possibility of modifying and rigging of digital images more easier without visual detection. This development leads to unexpected systematic errors and even malicious frauds [9, 10, 37]. Significant

✉ Fan Chen
mrchenfan@126.com

Omer Hemida
omerharoun1@yahoo.com

Hongjie He
hjhe@swjtu.cn

[1] Sichuan Key Lab of Signal and Information Processing, Southwest Jiaotong University, Chengdu, Sichuan, China

conditions, such as for evidence in a court of law or insurance a small amount of content modification in digital imaging, can change the judgement. Therefore, in these days the tampered image detection and localization has become important issues. Many researchers have addressed this issue, and they provided many techniques for mitigating the manipulation of the images [18, 30, 31, 33, 41, 43]. The most efficient way used to check the integrity and authenticity of digital contents is the fragile watermarking [3, 28]. The fragile watermarking algorithms can be divided into two types. The first type contains the algorithms that can only authenticate digital image and locate the tampered regions [5, 13, 20, 26], and the other type contains the algorithms that have the ability to recover the destroyed regions using the available information extracted from the whole region of the digital images along with locating the tampered area [2, 6, 40]. However, the tamper detection methods with restoration are desirable for the protection of the content and the integrity of the digital images. Localizing the tampered area along with restoration can make a difference in several profound situations.

Earlier research on self-correction watermarking scheme is proposed in [7]. This method is based on the transformation of 8×8 blocks, hence, utilizing the discrete cosine transform (DCT). They embedded the watermark of the block into the least significant bits (LSB) of other distant blocks. This embedding strategy is mentioned in a self-recovery watermarking scheme. Nevertheless, it is difficult to detect and localize the possible tampering. To localize the tampered regions, Lin et al. [19] utilized a three-level hierarchical structure. He et al. [11] proposed an adjacent-block based on statistical detection method, where the authenticity of each block was determined by comparing the number of dubious blocks in all adjacent blocks corresponding to the mapping blocks. However, these methods in [11, 19] could not recover the tampered blocks whose watermark was embedded in the other destroyed block.

To improve the tamper detection and recovery quality, Lee and Lin [17] proposed a strategy of the dual watermarking scheme. They embedded duplicate copies of the watermark data into three least significant bits (LSB) of the image content. The method proposed in [17] offers a second opportunity for self-recovery in case the primary information is destroyed. The second opportunity for self-recovery can produce a higher quality recovery image. However, the quality of watermarked images decreased due to the watermark embedding payload from 2 bit per pixel (bpp) to 3bpp. Moreover, their proposed scheme is vulnerable to a few security attacks, such as the collage attack [8] and constant-average attack. Yang et al. [42] proposed tampered image recovery by creating an index table of the cover image via vector quantization (VQ). They generated a pseudo-random sequence to determine where to embed the VQ indices of all the blocks. If the watermarked image is tampered, the VQ index table could be reconstructed and used to restore the tampered regions by the VQ code words. However, if all of the embedded copies of the VQ index of the block were damaged, the quality of recovered image using their scheme would not be high enough. Shi et al. [34] proposed a secure variable-capacity self-recovery-watermarking scheme. In their scheme, the recovery watermark includes a basic watermark and additional watermark. The authentication watermarks and recovery watermarks are inserted into the other blocks based on the three-level secret-key. Consequently, the quality of watermarked images decreased due to the increased watermark payload. Zhang et al. [45] proposed a self-embedding watermarking scheme, in which the reference data was generated from the most significant bits (MSB) of the original image. They embedded it into the least signification bits (LSB) of the content image. Moreover, the reference data is extracted from other regions to recover the principal content in the tampered area. However, the quality of the recovered image was degraded when the tampered detection area was enlarged. Zhang et al. [44] also proposed a self-embedding fragile watermarking scheme based on a reference

sharing mechanism. In this scheme, the reference data shared the main contents of different regions in the original image, and then, they are randomly embedded into the cover image for further content restoration. The implementation of this scheme made the quality of the recovered image not good when the tampered area was enlarged.

Singh et al. [35] proposed the self-embedding fragile watermarking scheme with effective image authentication and restorations. In their scheme, the cover image is divided into 2×2 non-overlapping blocks. For each block, 12 bits watermark are generated from the five most significant bits (MSB) of the original cover image. The proposed scheme embedded the watermark into the LSB of the cover image. The validity of the block was determined by comparing the watermark bits with an extracted watermark. However, the tampered detection result is not good enough when the image content and watermark are all tampered. Moreover, the quality of the recovered image by this scheme decreased when tampered detection area is enlarged. This decrease occurs mainly due to the fact that, the fixed recovery watermark capacity of the method provides an insufficient bits for rough blocks, thus restricting the recovery quality. In another work, Singh et al. [36] proposed a fragile watermarking scheme for multilevel tamper detection and recovery based on the dynamic domain. The original image is divided into small sized 1×2 non-overlapping blocks. Here, four recovery watermark bits are generated from the five most significant bits of the content image. It is embedded into two least significant bit positions of each DCT coefficient of the block, and three authentication bits are generated for each pixel value based on its content, location, and neighborhood. Additionally, one-bit information is generated to identify the recovery generation method used for particular blocks. This bit is called recovery method identification bit. It is embedded alternatively into the first LSB of the first or second pixel of the block depending upon whether the block is odd or even. Three bits were used for authentication and the other one bit used for identifying the recovery method for each block. They were embedded into the three least significant bits (3 LSBs) of each pixel of the non-overlapping block. However, the quality of watermarked images decreased due to the watermark embedding payload increasing from 2 bit per pixel (bpp) to 4(bpp). Qin et al. [32] proposed self-embedding fragile image watermarking scheme for tampering recovery based on reference data interleaving mechanism and adaptive selection of embedding mode. In this scheme, the embedding modes of the proposed approach were categorized as overlapping-free embedding and overlapping embedding. It is related to variable numbers of the MSB layers and LSB layers that are used during watermark embedding. The MSB bits that represent the principal content of the image blocks are interleaved to generate the reference bits and then embedded into the LSBs. Both numbers of the MSB and LSB layers are used for influencing the quality of the watermarked images, thus affecting the probability of perfect recovery as well as the quality of the recovered images. However, this scheme was vulnerable to collage attack [8], as the authentication watermark was independent of the content of the cover image. Henceforth, the quality of the recovered image is decreased as long as there is an increasement in the tampered detection region.

Zhang et al. [46] proposed a watermarking scheme based on DCT coefficients encoding. The DCT coefficients of 2×2 blocks were encoded into different numbers of bits, and the watermark information bits were embedded into another block of the cover image for improving tamper localization and recovery. However, the quality of recovered images was decreased when the tampered area is enlarged. Tong et al. [38] proposed chaos-based fragile watermarking for image tampering detection and self-recovery. The proposed algorithm scrambles the original image by utilizing chaotic maps and divides the image into 2×2 non-overlapping blocks. The watermark bits are generated from a most significant

bit of the cover image and then embedded into the least significant bit (LSB) of the corresponding mapping block. However, the quality of the recovered image was low, when the tampered detection area was enlarged. Niu et al. [25] proposed a self-embedding watermarking scheme based on the Maximum Distance Separable (MDS) codes. In this scheme, the reference-bits are generated by encoding the main content of the image blocks. The watermark bits, which include the reference-bit and authentication bits, are randomly embedded into the mapping blocks based on a secret key. Meanwhile, the tampering detection performance is not good, and the quality of the recovered image is imperfect. Ji et al. [15] proposed a self-embedding watermarking scheme based on Absolute Moment Block Truncation Code (AMBTC). The sharing reference bits were generated from the AMBTC algorithm. Then, they were applied to the original image with a reference sharing mechanism, for the aim of content restoration. By implementing this scheme, the original image can be retrieved when the tampered area was not large. As long as tampered area is smaller, the quality of recovered images is better.

The text images are important. The text images has various features such as symbols, lines, and dots, sizes, styles of letters. Even one small feature is interrupted, the meaning can be misleading. The research on text images watermarking is started in 1993. Brassil et al. [4] proposed three invisible techniques for encoding information in a text document image to protect copyright and compared three different watermark embedding methods. These work rested the establishment for the further research on text image watermarking. Atallah et al. [1] proposed several methods of natural language watermarking, which radiated a new trail in this field. Some progress on content authentication of text document image has been made in [16, 29]. Puhan et al. [29] proposed a tamper restoration technique using erasable watermarks in conjunction with error control coding techniques. In this method, an erasable watermark is embedded in each block of a text document image for the restoration of the original character sequence. Huazheng et al. [14] proposed a fragile watermarking method to preserve the authenticity of the digital Holy Quran. This scheme works on wavelet and spatial domains of digital Quran images. The authentication bits are embedded into each block of wavelet transformed image. Then the least Significant bits of pixels are considered to embed another authentication bits. Olanrewaju et al. [27] proposed a text watermarking scheme for text document image authentication. This scheme syndicates the features of the text image with the user data as a watermark, which is embedded into the converted text image itself to verify the integrity and the authentication of the text image through the blind detection technique. However, this scheme is vulnerable to the college attack. Kurniawan et al. [16] proposed fragile watermarking for validating and protecting the integrity of the digital Holy Quran in Portable Document Format (PDF). This scheme used 2 and 4 level Discrete Wavelet Transform (DWT) to protect and detect the authenticity of a digital Holy Quran. In this scheme, DWT is carried out on it following the watermark image embedding process on different trials. The inverse DWT is then carried out to obtain the watermarked Quran PDF. However, these methods in [16, 27] could not recover the tampered image. The text image has various features such as symbols, lines, and dots, sizes, styles of letters. Feature extraction in learning schemes extends over the use of a sensor to discover a set of characteristics in build motions, poses, shape, color and so on that can appropriately describe human actions. These actions are represented by a set of descriptive features extracted from the sensors. Some associated work in this area includes [21] and [22] , where hard activities are recognized from sensor data and smartphone accelerometer. In their works, they recognized temporal patterns between actions for activity representation as well as boosting scheme. The conception of feature leaning spans to real-life scenarios that have a direct influence on humans life, such as in [24] where the author presents the techniques of

expecting the quality of urban water supply through multi-task multi-view learning scheme. The author extracts meteorological feature, hydraulic features and time of day features from temporal data of each station. They also extract Points of Interests (POIs) features and road network features from each stations spatial data. Then they are working multi-view based prediction to capture the local information from both combined features. Also in [23], the author extracted demographics, user topics and LIWC (a psychological analysis tool) feature from the users social media profiles for the goal of forecasting an individuals career path.

In this work, we proposed a restorable fragile image watermarking scheme. The main objective of this algorithm is to achieve good tamper detection and recovery performance for the potential tampered natural objects, characters and numbers in the image. The proposed scheme also takes into account the invisibility and time efficiency. In order to achieve the above goals, this paper adopts the following innovation strategy: (1) the image block sizes of the authentication watermark and the restoration watermark are different. The size of blocks generating the authentication watermark is 4×4 pixels and the size of blocks generating the recovery watermark is 2×2 pixels. This strategy can adopt the structure of each block to generate appropriate watermark for better tamper detection and recovery performance. (2) The variable-length recovery watermark generation method generates the recovery watermark according to the complexity of image content adaptively. The original image is divided into blocks with a size of 2×2 pixels. For each block, the DCT (discrete cosine transform) is implemented to generate a variable-codes bit. For different blocks, a variable-capacity recovery watermark can be generated by allocating more bits to the textural blocks and fewer bits to the smooth blocks to encode the block content. (3) The multi-stage neighbor detection strategy is designed to improve the performance of tamper detection. This detection strategy adopts both the authentication watermark and recovery watermark to detect different types of tampering. The neighborhood method can reduce the probability of false acceptance (PFA) and the probability of false rejection (PFR) in tamper detection. The experimental results show that the proposed scheme allows image recovery with acceptable visual quality (peak signal-to-noise ratio (PSNR)) 26 dB with the tampering ratio up to 60% of natural image. For the sensitive information (numbers, text, etc.) in the text images, under different attacks, such as general tampering, collage attack, content-only and hybrid attack, the recovery performance of the proposed method is better.

The remaining section of this paper is organized as follows. Section 2 describes the proposed watermark generation, watermark embedding, watermark extraction, tamper detection, tamper recovery. Experimental results are given in Section 3, and Section 4 finally concludes the paper.

2 The proposed fragile watermarking scheme

This section describes in detail the proposed fragile watermarking method. A variable-capacity recovery watermark is proposed to enhance the quality of the watermarked image. Tamper detection based on multi-stage neighbor detection strategy is designed to improve the performance of tamper detection. The variable-capacity recovery watermark and superior localization method can improve the recovery quality. The proposed algorithm is described through six stages: authentication watermark generation, variable-capacity recovery watermark generation, watermark embedding, watermark extraction, multi-stage tamper detection and tamper recovery.

2.1 Authentication watermark generation

The proposed scheme generates the authentication watermark by using a hash function. The authentication watermark is used to identify any modification made to the authenticated image. For authentication watermark generation, the host image P is divided into 4×4 blocks $P = \{p_l | l = 1, 2, ..., M\}$. Where $M(M = N_1 \times N_2/16)$ is the total number of blocks. Each 4×4 block P_l is expressed as

$$P_l = \begin{pmatrix} p_{l1} \cdots p_{l4} \\ \vdots \ddots \vdots \\ p_{l13} \cdots p_{l16} \end{pmatrix}, l = 1, 2, 3, ..., M. \quad (1)$$

For each 4×4 block P_l , the 4-bit authentication watermark $A_l = a_{lk} | k = 1, 2, 3, 4$ is computed as

$$A_l = H(P_l, k_1) \quad (2)$$

Where, $H(.)$ is the hash function, A_l is a hash code, and K_1 is a secret key. The secret key K_1 is used to generate authentication watermark.

2.2 A variable-capacity recovery watermark generation

The proposed scheme generates the variable-capacity recovery watermark by encoding the significant DCT coefficients. The variable-capacity recovery watermark is used for tamper detection and restore the blocks, which have been tampered. The following steps can do a variable-capacity recovery watermark generation procedure. The flowchart of a variable-capacity recovery watermark generation of the proposed scheme shown in Fig. 1.

Step 1. Blocking For removing the 4LSB and reduce the range of pixels-value, the host image P of size $N_1 \times N_2$ is partitioned into non-overlapping 2×2 pixel blocks.$p_s(i, j)$ denotes the pixel. Where, $1 \leq s \leq N/4, 1 \leq i \leq 2, 1 \leq j \leq 2$ and $N(N = N_1 \times N_2/4)$ is the total number of blocks. For each block, the original pixel values are quantized by removing four LSB to reduce the range gray level from [0,255] to [0,15]. Denote the new pixel-value as $g_s(i, j)$.

$$g_s(i, j) = \left\lfloor p_s(i, j)/2^4 \right\rfloor \quad (3)$$

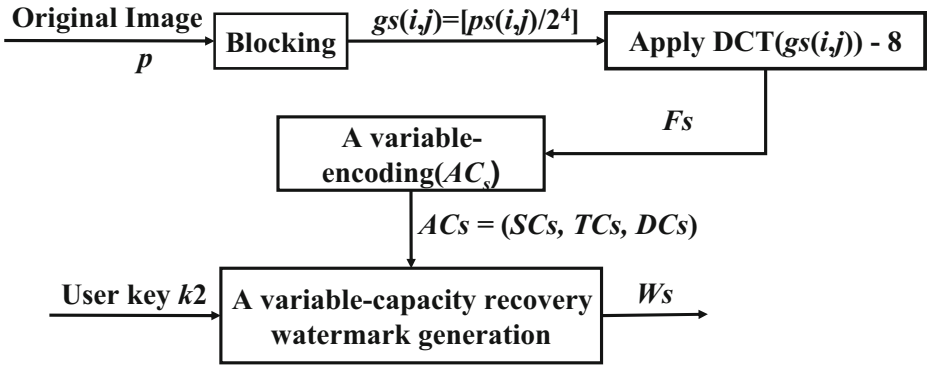


Fig. 1 Flowchart of variable- capacity recovery watermark generation of the proposed scheme

Step 2. Apply DCT DCT is often utilized in images, especially for lossy data compression because it has a strong energy compaction property. The DCT has the characteristic property that most of the significant information of the image is concentrated in just a few low-frequency coefficients of the DCT. To generate the DCT coefficients, the DCT transform is applied on each block after subtracting half the maximum possible values, i.e., eight. The DCT coefficients are used to generate the variable encoding bits.

$$F_s(u,v) = \frac{c(u)c(v)}{2}\sum_{i=1}^{2}\sum_{j=1}^{2}[g_s(i,j)-8]\times cos\left(\frac{\pi u(2i-1)}{4}\right)\times cos\left(\frac{\pi v(2j-1)}{4}\right)$$
$$1 \le s \le N/4, \quad 1 \le u \le 2, \quad 1 \le v \le 2 \tag{4}$$

where

$$c(z) = \begin{cases} 1/\sqrt{2}, & z = 1 \\ 1, & z > 2 \end{cases} \tag{5}$$

Where, F_s is the DCT matrix of s^{th} block.

By using all experimental results, it has been observed that the second row f_{s3} and f_{s4} of F_s will be zero or negligible.

Step 3. A variable-encoding AC_S For a variable-length encoding, the proposed scheme uses the first row (f_{s1} and f_{s2}) in the matrix F_s to generate the codes bits. The length of codes bits is not more than 10 bits and not less than 6 bits. The code structure of each block including significant code SC_s , Type-code TC_s, and detail-code DC_s are shown in Fig. 2.

1. Significant-code $SC_s = \{sc_{sk} | k = 1, ..., 5\}$ is generated for the smooth and textural block by converting the f_{s1} coefficient into the binary sequence of 5bits.
2. Block Type-code TC_s is generated to determine the type of block if the block is the smooth block denoted as 0. Otherwise, the type-code is textual block denoted as 1 as follows:

$$TC_s = \begin{cases} 0, iff_{s2} = 0 \\ 1, otherwise \end{cases} \tag{6}$$

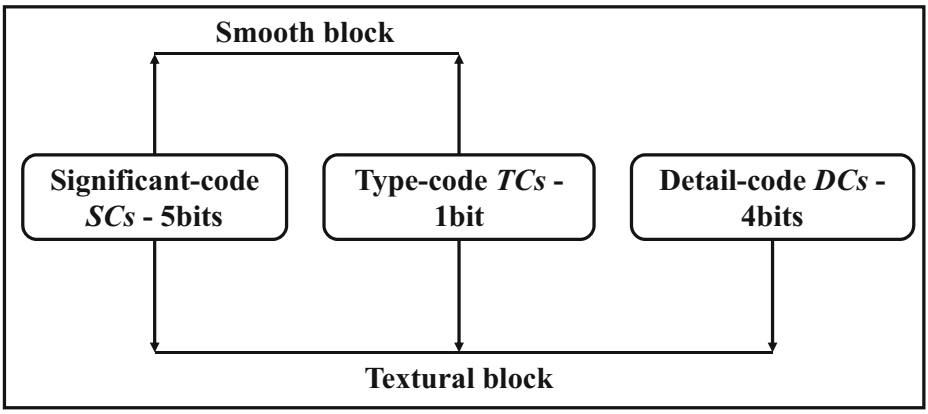


Fig. 2 Codes structure of each block

3. Detail-code $DC_s = \{dc_{sk} | k = 1, ..., 4\}$ is generated only for those textural blocks by converting the coefficient f_{s2} into the binary sequence of 4bits. The variable-encode $AC_s = AC_{s1}, AC_{sv}$ can be obtained by:

$$AC_s = \begin{cases} [TC_s, SCs], & if\ TC_s = 0 \\ [TC_s, SC_s, DC_s], & otherwise \end{cases} \tag{7}$$

Where, $TC_s$is the type-code, SC_s is the significant-code, DC_s is the detailed-code, and $v = 10$ or 6 is the length of codes.

Step 4 A variable-capacity recovery watermark: To ensure the security of a varible-capcity recovery watermark, a binary pseudo-random sequence $E_s = \{e_{sj} | j = 1, 2, ..., v_s\}$ with a secret key k_2 is generated to encrypt the variable codes and a variable- capacity recovery watermark $W_s = \{w_{sj} | j = 1, 2, ..., v_s\}$ is obtained by:

$$w_{sj} = AC_{sj} \oplus E_{sj},\ j = 1, ..., v_s \tag{8}$$

where, AC_{sj} is the variable-code, E_{sj} is random binary sequence generated by the key k_2 and $\oplus$ denotes the bit by bit exclusive OR operation. The secret key k_2 is used to generate the random binary sequence, which is used to encrypt a variable code and improve the security of recovery watermark

2.3 Watermark embedding

In watermark embedding, we need to consider the performances of fragile watermarking, such as invisibility, detection ability, and so on. To take into consideration the trade-off between watermark payload and invisibility, the proposed watermark embedding process is illustrated in Fig. 3. The details are described as follows:

1. Block Division: the host image P of size $2m \times 2n$ pixels is divided into N non–overlapping 2×2 blocks $P = \{p_i | i = 1, 2, ..., N\}$
2. Block mapping. A block mapping is used for watermark embedding. According to the secret key k_3, a random sequence $Z = (z_1, z_2, ..., z_N)$ is generated. An ordered index sequence $Q = (q_1, ..., q_i, ..., q_N)$ such that $z_{q1} \leq z_{q2}, ..., \leq z_{qN-1} \leq Z_{qN}$ is obtained by sorting Z. Let the index of mapping block P_j be $j = h_i, i = 1, 2, ..., N$.

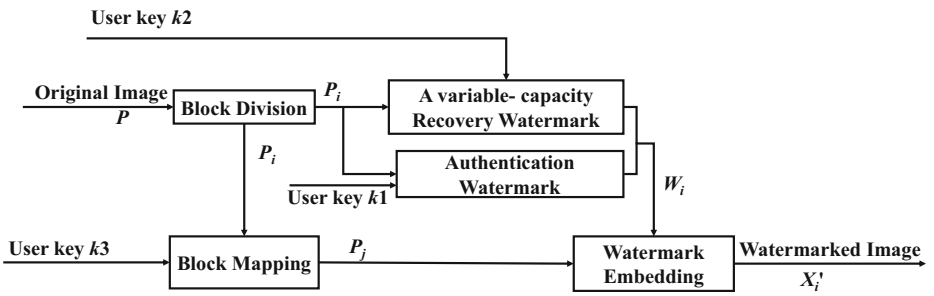


Fig. 3 Flowchart of watermark embedding of the proposed scheme

3. Watermark embedding. In the watermark generation process, a variable-capacity recovery watermark of a 2×2 block and authentication watermark of 4×4 block are generated. We embed the variable- capacity recovery watermark in 2×2 mapping block P_j and insert the authentication watermark in the same 4×4 block in host image based on the secret key, respectively. Each 2×2 block is used as an example for embedding. In each 2×2 block, there are 1bit authentication watermark and corresponding a variable-capacity recovery watermark, which is denoted as $W_i^{'} = \left\{ w_{ij}^{'} | j = 1, 2, ..., v_i + 1 \right\}$. The watermarked block $X_j = \left\{ x_{jb} | , b = 1, 2, 3, 4 \right\}$ is obtained by one of the following two cases. If $v_i = 10$,

$$X_{jb} = \begin{cases} 8 \left\lfloor p_{jb}/8 \right\rfloor + 4w_{i(3b)}^{'} + 2w_{i(3b-1)}^{'} + w_{i(3b-2)}^{'}, & b = 1, 2, 3 \\ 4 \left\lfloor p_{jb}/4 \right\rfloor + 2w_{i(10)}^{'} + w_{i(11)}^{'}, & b = 4. \end{cases} \tag{9}$$

$if\ v_i = 6$

$$X_{jb} = \begin{cases} 4 \left\lfloor p_{jb}/4 \right\rfloor + 2w_{i(2b)}^{'} + w_{i(2b-1)}^{'}, & b = 1, 2, 3 \\ 4 \left\lfloor p_{jb}/4 \right\rfloor + w_{i(7)}^{'}, & b = 4. \end{cases} \tag{10}$$

The watermarked image $X_j = \left\{ x_{jb} | b = 1, 2, 3, 4, i = 1, 2, ..., N \right\}$ can be generated if all the watermarks are embedded in the mapping blocks using (9) and (10).

2.4 Watermark extraction

Watermark extraction can be considered as the reverse process of watermark embedding. Let X^* represents the test image, which can be a tampered watermarked image or untampered one.

Step 1. Authentication watermark extraction. The extracted authentication watermark A_l from tested X_l^* can be obtained by

$$A_l = mod(x_{l(b-1)}^*, 2), b = 1, 2, 3, 4 \tag{11}$$

Step 2. A variable- capacity recovery watermark extraction. The extracted recovery watermark E_i from tested X_i^* can be achieved by:

$$E_i = \begin{cases} mod(x_{i(b-1)}^*, 2), & b = 1, 2, 3, 4 \\ mod(\left\lfloor x_{i(b-5)}^*/2 \right\rfloor, 2), & b = 5, 6, 7, 8 \\ mod(\left\lfloor x_{i(b-9)}^*/4 \right\rfloor, 2), & b = 9, 10 \end{cases} \tag{12}$$

Step 3. Inconsistent map generation: The inconsistency map of authentication data matching $D^A = \left\{ d_l^A | l = 1, 2, ..., M \right\}$ and the recovery data match-matrix $D = \left\{ d_i^A | i = 1, 2, ..., N \right\}$ are calculated by

$$d_i^A = \begin{cases} 0, if\ C_l = A_l \\ 1, otherwise \end{cases} \tag{13}$$

$$d_i = \begin{cases} 0, if\ \varphi_i = E_i \\ 1, otherwise \end{cases} \tag{14}$$

where, C_l is the reconstructed authentication watermark of the block X_l^*, φ_i is the reconstructed recovery watermark of the block $X_{i'}^*$, $E_{i'}$ is the extracted recovery watermark from the tested X_i^* and A_l is the extracted authentication watermark from the tested Y_l^*.

2.5 Multi-stage neighbor tamper detection

In the receiving or detection side, the received image might be tampered with by potential attackers. To detect and locate the tampered regions accurately, the multi-stage neighbor detection strategy is designed to improve the performance of tamper detection in the proposed method. Let X^* represent the test image, which can be a tampered watermarked image or untampered one. The $T = \{t_i | i = 1, 2, ..., M\}$ called the tamper detection Mark (TDM) is used to localize the tamper blocks. Where, $t_i = 0$ signifies a valid block and $t_i = 0$ signifies an invalid block. The flowcharts of multi-stage tamper detection and tamper recovery of the proposed scheme are shown in Fig. 4. The tamper detection procedure includes the following steps. **Step 1.** The authentication data $T^A = \{t_l^A | l = 1, 2, ..., M\}$ is obtained by comparing block neighborhood characterization of D^A for removing the unmatched blocks.

$$t_l^A = \begin{cases} 1, & if(d_l^A = 0)\&(\Psi_l^{t^A} \geq 4) \\ 0, & otherwise \end{cases} \tag{15}$$

where, $\Psi_l^{t^A}$ denotes the number of nonzero pixels in the eight neighborhood of the l^{th} pixels in D^A. To make the validity of block X_l^* in test image, the authentication data matching TDM $T^m = \{t_i^m | i = 1, 2, ..., M\}$ is obtained. The value of t_i^m equals to that of t_l^A if the 2×2 block X_i^* belongs to the 4×4 block X_i^*. **Step 2.** The recovery data TDM $U = \{u_i | i = 1, 2, ..., N\}$ is obtained by comparing block neighborhood tampering characterization method proposed in [12].

$$u_i = \begin{cases} 1, & if(d_i = 1)\&(d_{i'} = 1)\&(\Psi_i^D \geq \Psi_{i'}^D) \\ 0, & if(d_i = 1)\&(d_{i'} = 1)\&(\Psi_i^D) < \Psi_{i'}^D) \\ d_i, & otherwise \end{cases} \tag{16}$$

where $\Psi_i^D and\ \Psi_{i'}^D < a$ denote the number of nonzero pixels in the eight neighborhood of the i^{th} pixel and its mapping pixel in D. To further remove the unmatched blocks, the neighborhood characterization of U is used to obtain the recovery data TDM $T^R = \{t_i^R | i = 1, 2, ..., N\}$,

$$t_i^R = \begin{cases} 1, & if(u_i = 1)\&(\Psi_i^{t^R} \geq 3) \\ 1, & if(u_i = 0)\&(\Psi_i^{t^R} \geq 4) \\ 0, & if(u_i = 1)\&(\Psi_i^{t^R} < 3) \\ u_i, & otherwise \end{cases} \tag{17}$$

where, $\Psi_i^{t^R}$ denotes the number of nonzero pixels in the eight neighborhood of the i^{th} pixel in D. Step 3. Final detection result: After the above steps, the main tampered region can be

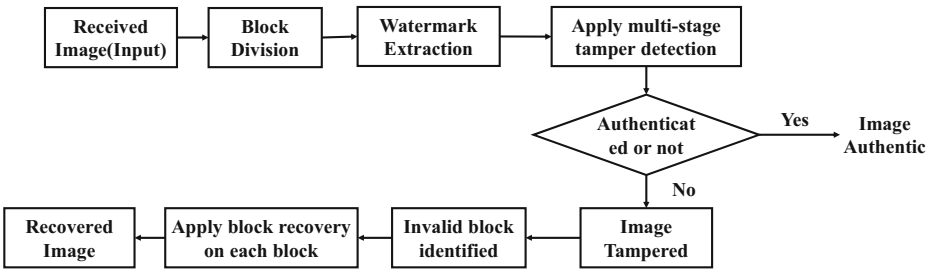


Fig. 4 Flowchart of tamper detection and recovery of the proposed scheme

localized. However, there are some dark spots, in T^m and T^R. The tamper detection Mark TDM $T^0 = \{t_i^0 | i = 1, 2, ..., N\}$ is further processed as shown in (18).

$$t_0 = \begin{cases} 1, & if(t_i^m = 1)\ or\ (t_i^R = 1) \\ 0, & otherwise \end{cases} \tag{18}$$

The tamper detection Mark (TDM) T is obtained by

$$t_i = \begin{cases} 1, & if(t_i^0 = 1)\&(\Psi_i^{t^0} \geq 4) \\ 0, & if(t_i^0 = 1)\&(\Psi_i^{t^0} < 3) \\ t_i^0, & otherwise \end{cases} \tag{19}$$

where, $\Psi_i^{t^0}$ is the number of nonzero pixels in the eight neighborhood of the i^{th} pixels in TDM T^0.

2.6 Tamper recovery

After the multi-stage tamper detection, all 2×2 blocks in the tested image are marked as either valid or invalid. If all blocks in the tested image are marked as valid, it indicates that the test image is authentic and the tamper recovery step will not be executed. If some blocks in the tested image are considered as tampering, the tamper recovery step will be excited. The recovery procedure is only for the invalid blocks by extracted watermark to recovers the invalid blocks. In the block recovery method, a matrix V of size 2×2 is generated for each invalid block G_n. The five most significant bits of the invalid block G_n is filled with binary values generated from the entry of matrix V. Next; three 0s are added in the least significant bits of each pixel of block G_n to convert the gray values in the range [0,255]. After the completion of recovery of the invalid block G_n, make it as a valid block. These processes are contiguous to all invalid blocks and in finally, apply function in tampered regions of the recovered image. Details of the recovery procedure are described in [35].

3 Experimental results

This section conducts numerous experiments to illustrate the efficiency of the proposed method and compare with [35] and [32] methods. The performance of test images includes 1) Invisibility and watermark capacity. Where, the invisibility is measured by the PSNR and the structural similarity index (SSIM) [39], and watermark capacity is measured by bits per pixel (bpp). 2) Tamper detection and recovery performance: the tamper detection is accomplished by tamper ratio (TR) [11], the probability of false acceptance (PFA) [11] and the probability of false rejection (PFR) [11]. The tamper detection performance is better with lower PFA and PFR. Tamper recovery performance is measured by PSNR between the recovered image and the watermarked one. 3) Time complexity: Run-time for information embedding, tamper detection, and image recovery.

3.1 Watermark capacity and invisibility

A total of sixty images including grayscale and text images sized 512×512, which were either smooth or rough, are used for comparison. The watermark capacity and invisibility of watermarked images are reported in the proposed scheme, [35] and [32] methods. The statistical results are shown in Fig. 5. The watermark capacity of [35] and [32] methods are fixed as 3bpp. The watermark capacity of proposed method alters according to the complexity

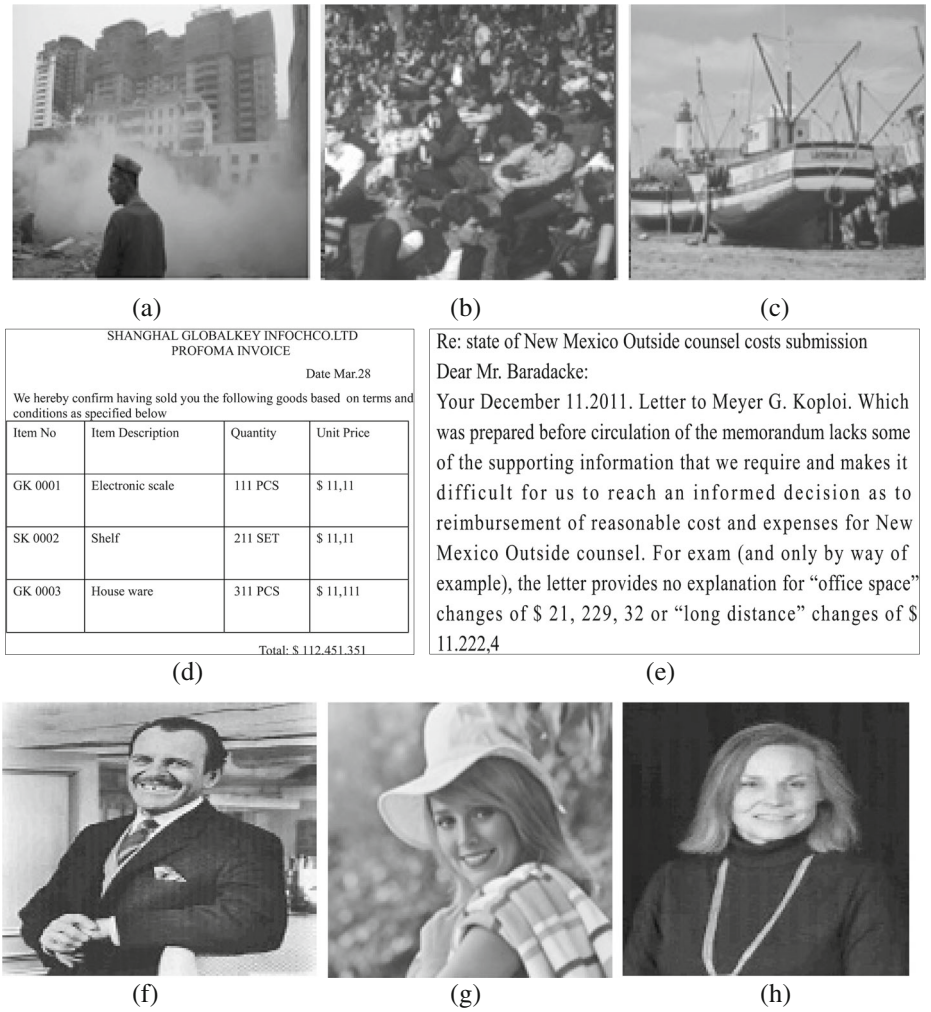


Fig. 5 Test Cover Images used in the Experiment **a** Old man **b** Couple **c** Boat **d** Invoice **e** Text **f** Man **g** Elaine **h** Woman

of the images, and it ranges from 1.66 bpp up to 2.30 bpp. The watermark capacity of the proposed method is much lower than [35] and [32] methods. Correspondingly, the invisibility of the proposed scheme is better than [35], [32] methods, as depicted in Fig. 6. The proposed method obtained PSNR range from 40 dB to 45 dB. Our scheme is higher with 3 dB to 5 dB as compared to [35] and [32], where their obtained PSNRs are from 37 dB to 40dB. In addition to PSNR values, the SSIM values of the proposed scheme are higher than [35] and [32] methods, as shown in Fig. 7. This is due to the available capacity of recovery watermark.

3.2 Tamper detection and recovery

There are numerous watermarked images tampered by general tampering, content-only tampering, collage attack and hybrid attack. This section has been implemented by performing

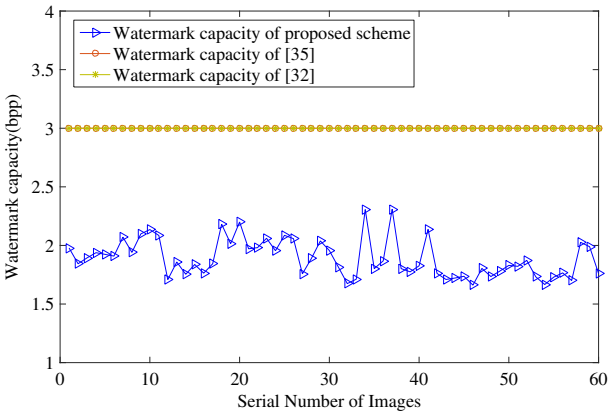


Fig. 6 Watermark capacity of the proposed scheme, [35] and [32]

a comparison of tamper detection and recovered the image quality among the proposed scheme, [35] and [32] methods. In the statistical results, a selected watermarked image is tampered fifty times randomly for each tamper ratio and the average statistic value is calculated as the final result. Simulations are done using a set of grayscale and text test cover images of size 512 × 512 as shown in Fig. 8.

3.2.1 General tampering

General tampering means that the image content and watermark are all tampered together. Figures 9 and 10 give the tamper detection and recovery performance for general tampering. The text image sized 512 × 512 is used as the cover image for general tampering and

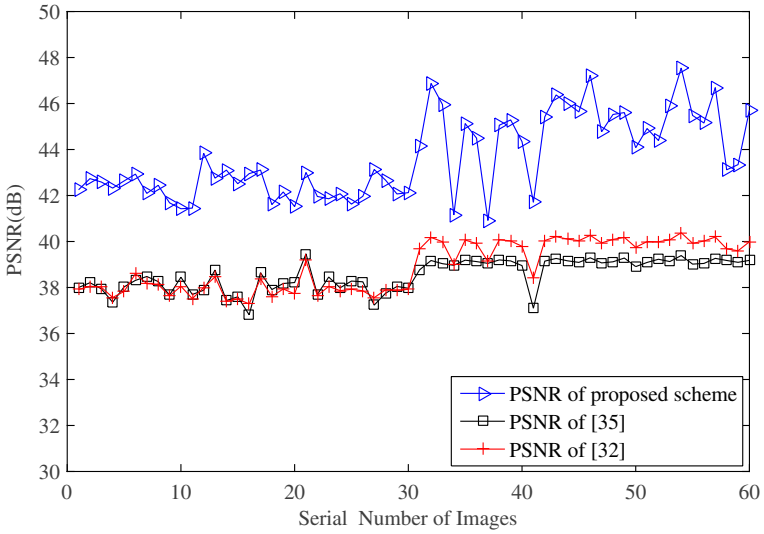


Fig. 7 PSNR of the proposed scheme, [35] and [32]

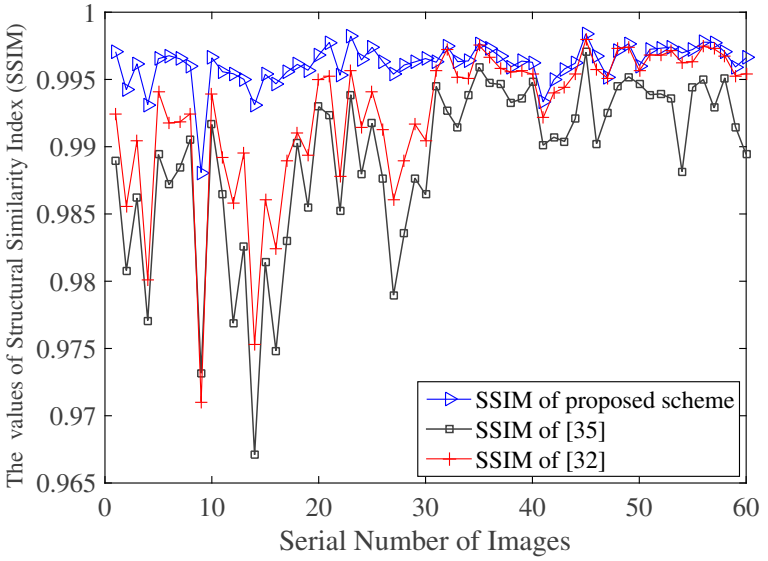


Fig. 8 SSIM of the proposed scheme, [35] and [32]

recovery. Figure 9a shows the watermarked text image that is generated by the proposed scheme. Figure 9b illustrates the tampered text image which was a modification and multiple tampers with a watermarked text image changing the meaning of the text image in the column of quantity and the column of unit price from 111 PCS, 211SET,311PCS and 11.1,11,11.11,11.11 to 989 PCS, 898 SET,868 PCS and 8888, 8989,9896 sequentially. The detection results of the proposed scheme, [35] and [32] methods are shown in Fig. 9d, e and f respectively. The detection result of the [35] method is shown in Fig. 9e. The black dots in the tampered region of the [35] methods indicates that the method of [35] is affecting to detect the general tampering blocks whose mapping blocks fall into the tampered region. Therefore, the scheme in [35] authenticates the tampered block with higher PFA and PFR as 0.417 and 0.020 consecutively. The detection result of the [32] method is shown in Fig. 9f. It resists the general tampering with higher PFR and lowers PFA as 0.534 and 0.0 . In contrast, the proposed method resist the general tampering with lower PFR and PFA as 0.0071 and 0.004 respectively. The proposed method obtained a better tamper detection result due to the multi-stage neighbor detection strategy.

The recovered text image results in Fig. 9c delivered by the proposed scheme and other methods [35] and [32] are presented in Fig. 10a-c, respectively. The quality of recovered text image by the proposed scheme shown in Fig. 10a and scheme in [32] displayed in Fig. 10c exhibit much better tamper recovery performance compared with [35] scheme. The PSNR of the recovered image was done by the proposed scheme is 34.51 dB, which is about 10 dB higher than [35] scheme of 24.44 dB. The main reasons that made the recovery images of the proposed method higher than its counterpart are due to the available capacity of recovery watermark and the detection results of proposed scheme have a significant impact on the quality of the recovered image. This demonstrates that the variable capacity watermark provides more available information about the original image for the recovery process and the proposed scheme can effectively resist the general tampering attack.

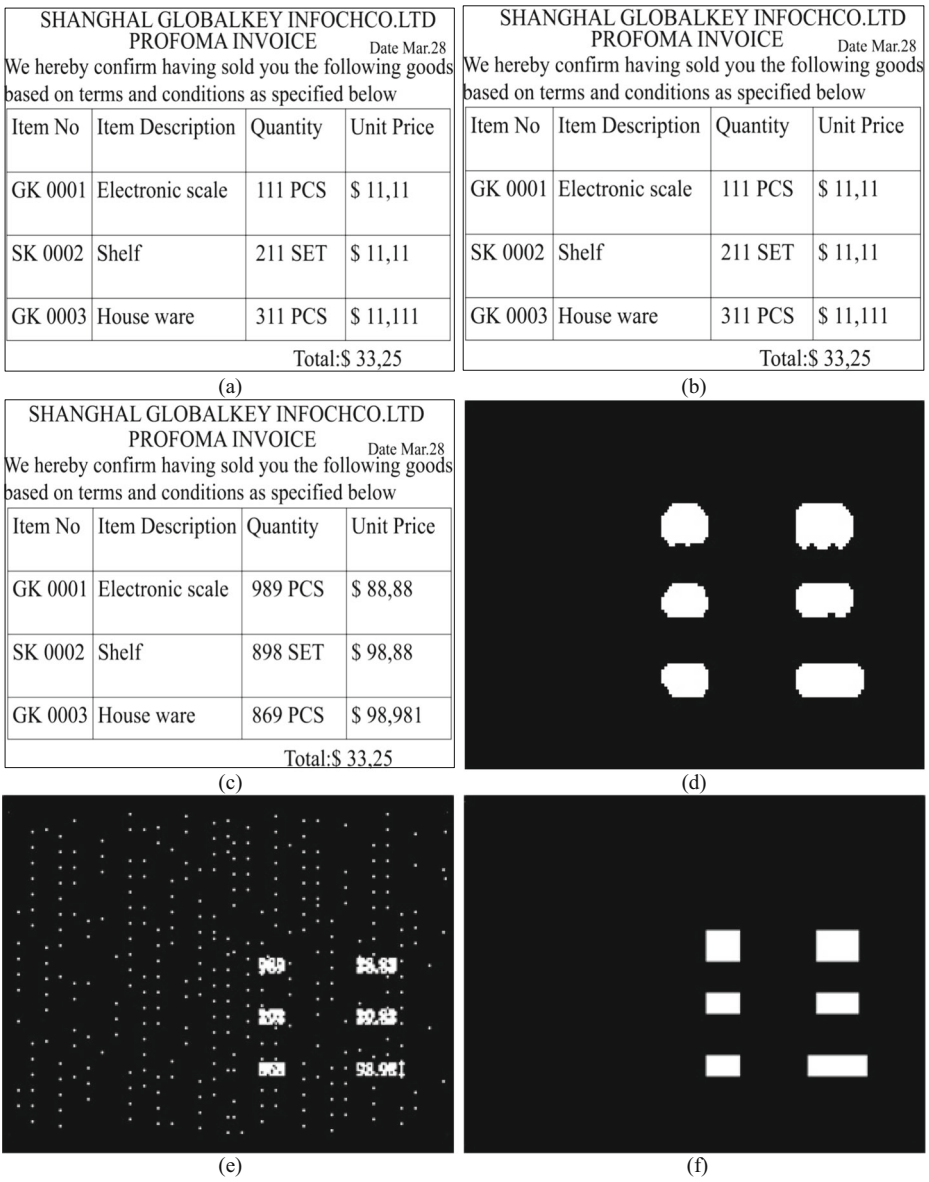
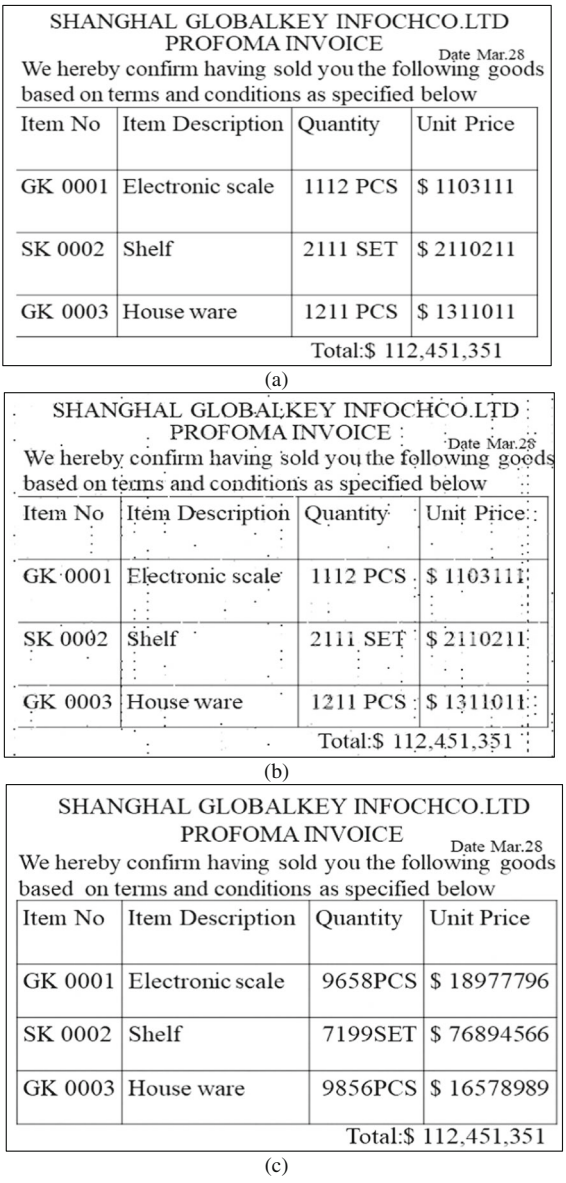


Fig. 9 Tampered detection under general tamper **a** Original image **b** watermarked image **c** Tampered image, detection results **d** by proposed scheme, **e** by [35] and **f** by [32]

To show the tamper detection performance severely under general tampering, the watermarked image Boat is used for calculating the statistical results. The statistical PFA and PFR of the proposed scheme and other schemes [35] and [32] are shown in Fig. 11. The tamper ratio is from 0% to 80%. As shown in Fig. 11, the PFA of the scheme in [35] is higher and large than 0.01. When the tamper ratio is larger than 30%, PFA of the scheme in [35] is about 0.015. However, the PFA of the proposed scheme and [32] method are zero. From Fig. 11b,


SHANGHAL GLOBALKEY INFOCHCO.LTD
PROFOMA INVOICE
Date Mar.28
We hereby confirm having sold you the following goods based on terms and conditions as specified below

Item No	Item Description	Quantity	Unit Price
GK 0001	Electronic scale	1112 PCS	$ 1103111
SK 0002	Shelf	2111 SET	$ 2110211
GK 0003	House ware	1211 PCS	$ 1311011
		Total:$ 112,451,351	

(a)

SHANGHAL GLOBALKEY INFOCHCO.LTD
PROFOMA INVOICE
Date Mar.28
We hereby confirm having sold you the following goods based on terms and conditions as specified below

Item No	Item Description	Quantity	Unit Price
GK 0001	Electronic scale	1112 PCS	$ 1103111
SK 0002	Shelf	2111 SET	$ 2110211
GK 0003	House ware	1211 PCS	$ 1311011
		Total:$ 112,451,351	

(b)

SHANGHAL GLOBALKEY INFOCHCO.LTD
PROFOMA INVOICE
Date Mar.28
We hereby confirm having sold you the following goods based on terms and conditions as specified below

Item No	Item Description	Quantity	Unit Price
GK 0001	Electronic scale	9658PCS	$ 18977796
SK 0002	Shelf	7199SET	$ 76894566
GK 0003	House ware	9856PCS	$ 16578989
		Total:$ 112,451,351	

(c)

Fig. 10 Recovered image under general tamper, recovered results **a** by proposed scheme, **b** by [35] and **c** by [32]

it can be concluded that PFR of the scheme in [32] is almost zero. On the other hand, in [35] the PFR increase linearly with the increase of tamper ratio. In summary, antecedes the existing schemes under general tampering due to the multi-stage neighbor detection strategy method. Figure 12 shows the performance of the statistical recovery results under general tampering with various tamper ratio by the proposed, [35] and [32] methods. The recovery quality of the proposed scheme is better than that of [35] and [32] methods. As seen in Fig. 12, these results indicate that the tampered image can be recovered by the proposed scheme with an acceptable visual quality, even the tamper ratio is up to 70% of the host image.

3.2.2 Collage attack

(a) Collage attack for text image

This subsection gives more consideration to the effect of the collage attack for text imge. Collage attack introduced in [8] is a special attack for the watermarking method based on the

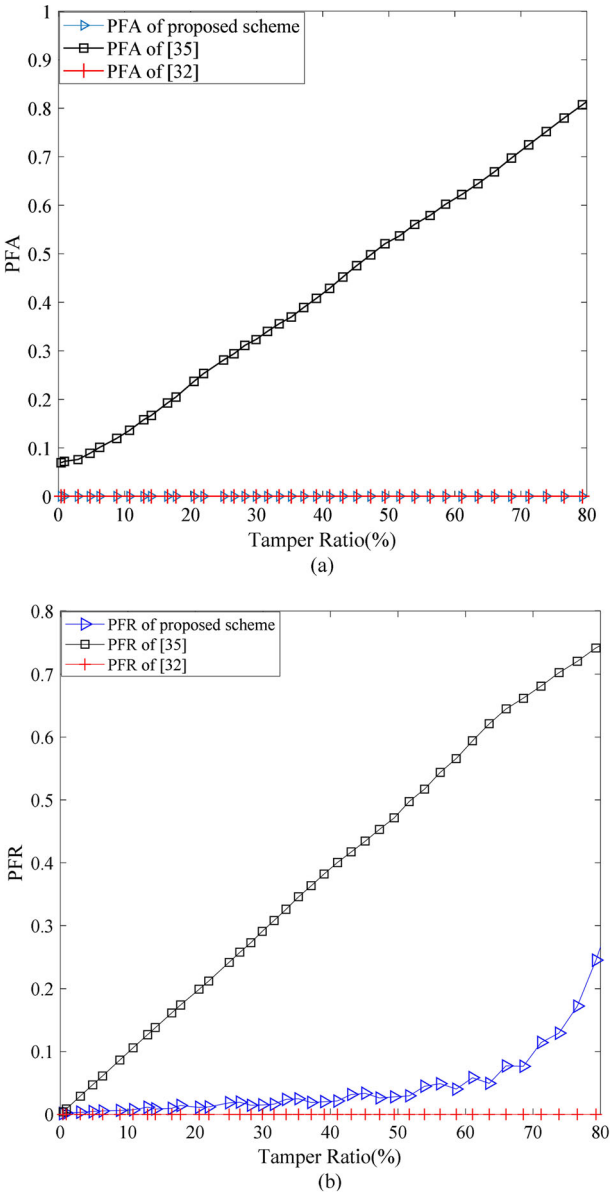


Fig. 11 Statistic detection results of the proposed scheme compared with [35] and [32] under general tampering **a** PFA and **b** PFR

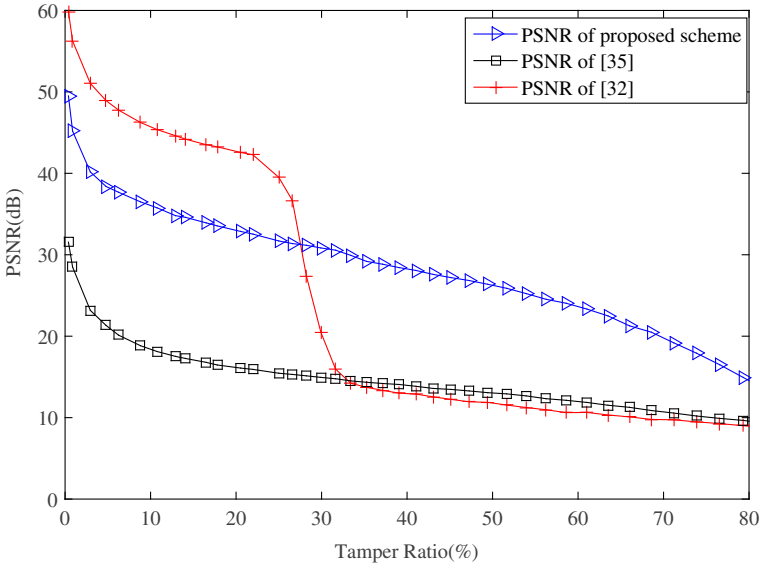


Fig. 12 Statistical recovery results of PSNR under general tampering with different tampering ratios

block-independent. Figures 13 and 14 give the tamper detection and recovery performance for collage attack. Two sized 512 × 512 watermarked text images invoice1 and text invoce2 are generated by the proposed scheme with the same key, as shown in Fig. 13a and b. The collage attack tampered image shown in Fig. 13c is generated by copying the content of the text image in the column of quantity and the column of unit price from Fig. 13a and pasted it into Fig. 13b without changing the relative spatial locations. The tamper detection results by the proposed scheme and another scheme [35] and [32] are presented in Fig. 13d–f, respectively. The detection result in Fig. 13d indicates that the proposed method can resist the collage attack and locate the splicing area successfully. The detection results of scheme [35] in Fig. 13e effects to resist the collage attack because there are some black dots whose mapping blocks fall into the tampered region. The detection results in Fig. 13e indicate that the method [32] does not resist the collage attack. The reason is that the method proposed in [32] does not break the block-independent characteristic during watermark generation and embedding processes. The recovered text image results in Fig. 13c carried out by the proposed scheme, and other methods [35] and [32] are presented in Fig. 14a–c, respectively. The quality of the recovered text image by the proposed scheme tops other schemes with the PSNR of 30.35 dB compared to the 28.65 dB by scheme [35], 24.45 dB by scheme [32]. The watermarking method in [32] cannot recovery the tampered regions because the collage attack has been survived from the detection process. This is mainly due to the fact that the detection results have a signification impact on the quality of the recovered image. This demonstrates that the proposed scheme can effectively resist the collage attack.

(b) Collage Attack for natural image

This sub-section gives more consideration to the effect of the collage attack on natural image. Figure 15 gives the tamper detection and recovery performance for collage attack. Here, two cover images sized 512 × 512, man as shown in Fig. 15a and woman as shown in Fig. 15b, are used for the simulation. These two images are watermarked with the same key

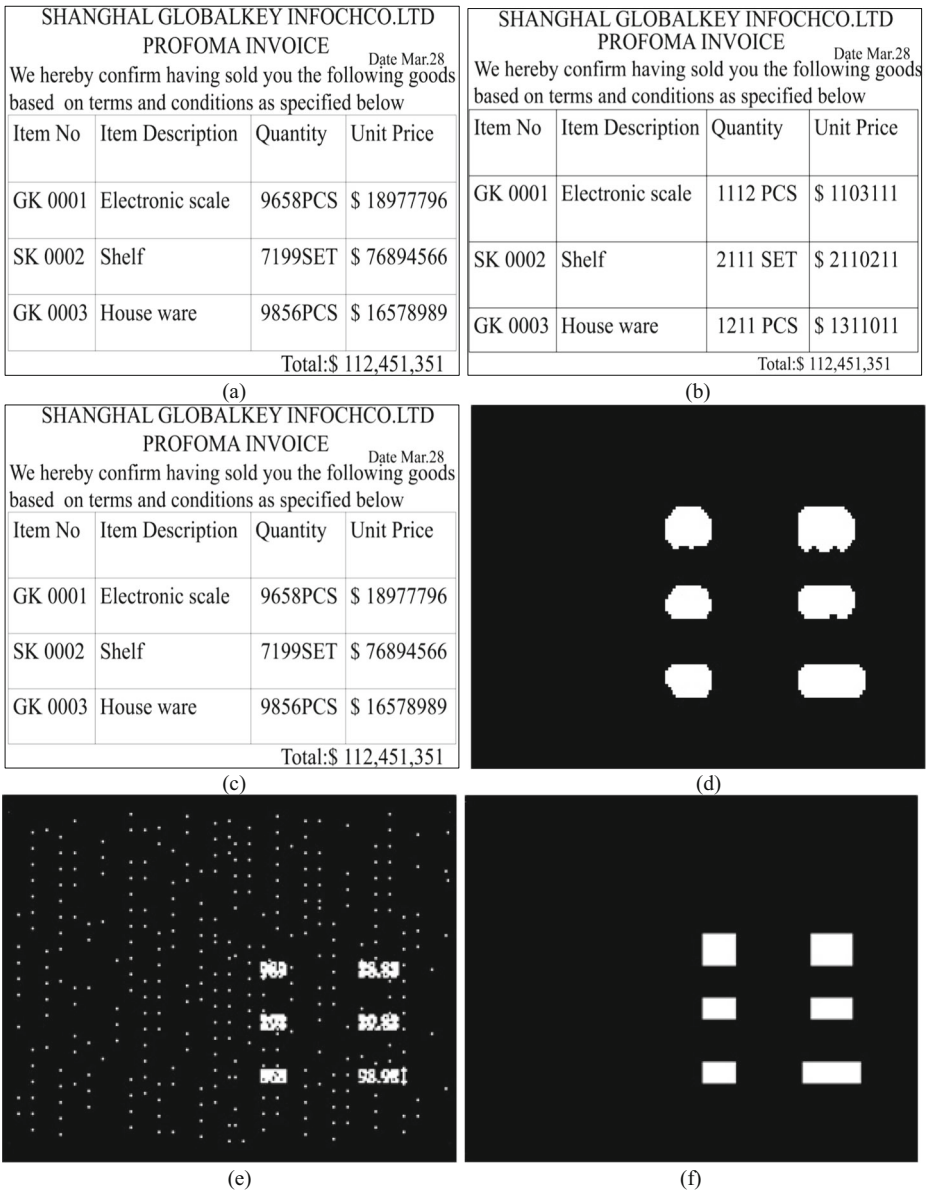


Fig. 13 Tampered detection under collage attack **a** Watermarked image **b** Watermarked image, **c** Tampered image, detection results **d** by proposed scheme, **e** by [35] and **f** by [32]

using the proposed, [35] and [32] methods. Then the tampered image in Fig. 15c were constructed by copying the face in the woman image and then pasting it into the watermarked man image without changing its relative location with tamper ratio 25%. The white region is deemed as tamper area as shown in Fig. 15d, e and f. The tampered detection result that was done by [35] is shown in Fig. 15e. The black dots in the collaged region in Fig. 15e indicated that the scheme in [35] fails to detect the collaged blocks whose mapping blocks fall into the

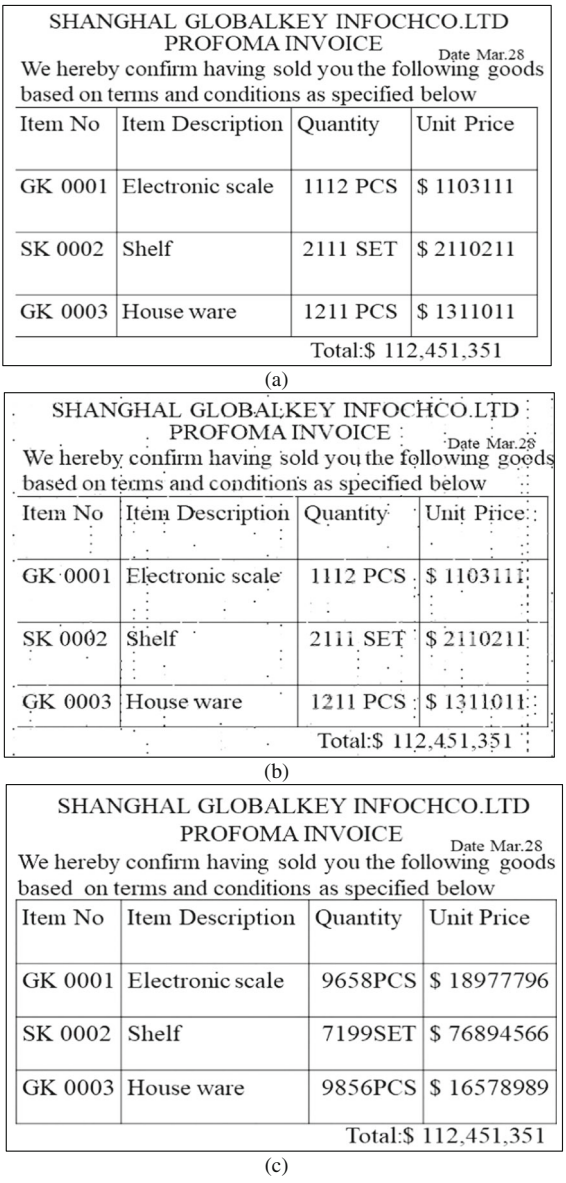


Fig. 14 Recovered text image under collage attack, recovered results **a** by proposed scheme, **b** by [35] and **c** by [32]

collage region. This failure made the PFA and PFR of [35] increased to 0.2599 and 0.3062 respectively. The tampered detection result of the [32] scheme as shown in Fig. 15f cannot detect the full tampered blocks under collage attack; this is because the [32] scheme cannot resist the collage attack due to the block-wise independence characteristic during watermark generation and embedding process. The condition of unresisting the collage attack made the PFA and PFR of [32] increases to 1 and 0.0055 respectively. In contrast, the proposed method as shown in Fig. 15d is effectively resisting the collage attack. Thus the RFA of the proposed scheme is lower to 0.0, which suggests a better tamper detection result. The multi-stage neighbor detection strategy reduced the number of black spots in collage region

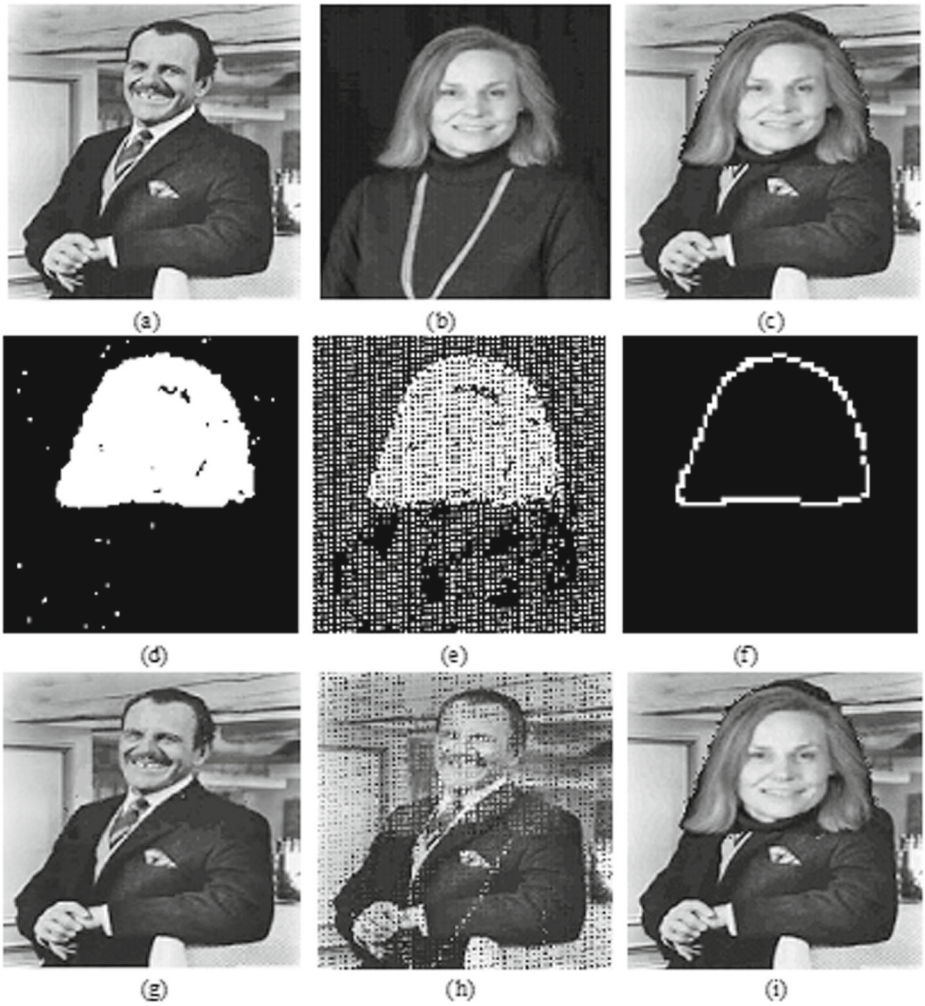


Fig. 15 Tampered detection and recovered image under collage attack **a** Watermarked image 'Man' **b** Watermarked -image 'Woman' **c** Tampered image, detection results **d** by proposed scheme, **e** by [35] and **f** by [32], recovered results **g** by proposed scheme, **h** by [35] and **i** by [32]

significantly. The recovered image results for Fig. 15c carried out by the proposed scheme and other schemes [35] and [32] are presented in Fig. 15g–h, respectively. The PSNR of the recovered image by the proposed scheme is 32.71 dB, which is higher than 16 dB for [35] with (PSNR= 16.16 dB) and 16 dB for [32] with (PSNR = 16.65 dB). This is mainly due to the fact that the detection results have significant role on the quality of the recovered image. This demonstrates that the proposed scheme can effectively resist the collage attack.

To show the statistic detection and recovery results under collage attack, the watermarked image Boat is used for the statistical experiment. The statistical PFA and PFR of the proposed scheme, and other methods [35] and [32] are shown in Fig. 16a and b. Where, the tamper ratio ranges from 0 to 45%. As the analysis in instruction, the scheme in [32] cannot resist collage attack. Then the PFA of the method in [32] is 1 and PFR is 0 as shown in

Fig. 16a and b. The PFA of the scheme [35] is about 0.5. The PFR of the proposed scheme is lower than the scheme [32] and the PFA of proposed scheme higher than [32] when the tamper ratio is larger than 15%, PFA of the proposed scheme is much lower than the scheme in [35]. In a word, the tamper detection performance of the proposed scheme is better than the existing schemes under collage attack. Figure 17 shows the performance of statistical recovery results under collage attack with various tamper ratios by the proposed scheme,

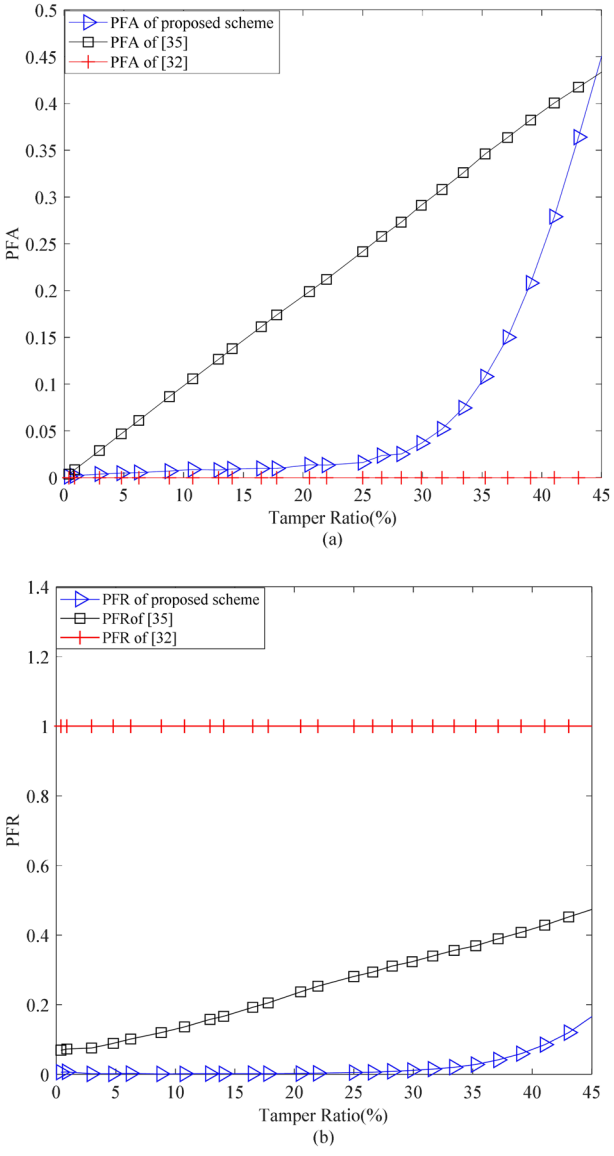


Fig. 16 Statistic detection results of the proposed scheme compared with [35] and [32] under the collage attack **a** PFA and **b** PFR

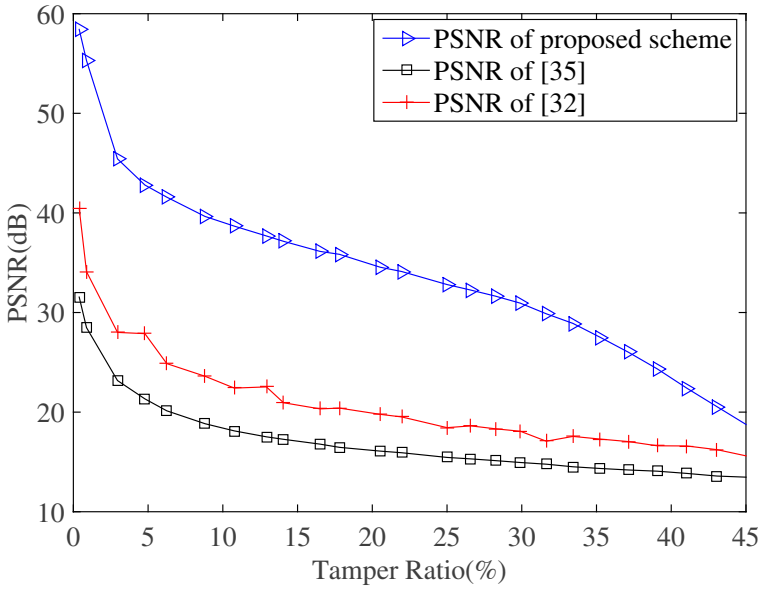


Fig. 17 Statistical recovery results of PSNR under collage attack with different tampering ratios

[35] and [32]. The quality of recovered images by the proposed scheme is better than that of [35] and [32] methods as seen in Fig. 17.

3.2.3 Content-only tampering

The third testing is content-only attack. The content-only attack is another special attack that is commonly used in fragile watermarking. In some watermarking schemes with recovery ability, the authentication bits of a block are entirely irrelevant to the image content. The characteristic feature of alterations is that the embedded watermark in the LSB planes of the original image is intact. In this case, the quality of the recovered image would not be strictly disgraced if the authentic blocks are falsely recovered. On the other hand, if the tampered blocks are undetected, the quality of the recovered image would be strictly disgraced. Hence, the essential for high- quality recovered image under content-only tampering is a low PFA. The text image sized 512×512 is used as the cover image for image content tampering and recovery, Fig. 18a displays the original text image and Fig. 18b illustrates the watermarked text image generated by the proposed scheme, [35] and [32] methods. Figure 18c shows text image that are modified by changing the meaning of the text image in the watermarked image from (Bardacke to Rahdahe Mohammed Adam, 11.2011 to 09.2014 , Meyer to Weelid, us to we, we to us, 21.229.32 to 37.338.92, 11 222.4 to 77.888.978912546) and (from our account in the bank of Sudan) is an insertion . The tampered detection result that is achieved by the proposed method is shown in Fig. 18d and the method in [35] is displayed in Fig. 18f, which can resist the content-only tampering. Therefore the PFA and RFR of proposed scheme decrease to 0 and 0.02 and the PFA and RFR of [32] method it is 0 and 0.030, respectively. The good detection result of the proposed scheme is due to the multi-stage neighbor detection strategy. The scheme in [35] which is shown in Fig. 18e has black dots in the content region. The resistance of the content only tampering affects

it. Therefore the PFA and PFR of [35] were increased to 0.0317 and 6.699, consecutively. The recovery results for Fig. 18c delivered by the proposed scheme, [35] and [32] methods are presented in Fig. 19a, b and c respectively. The quality of recovered text images that were performed by the proposed scheme highly depends on the tampered accuracy and a variable-capacity of the recovery watermark. Then, The PSNR of the proposed method got

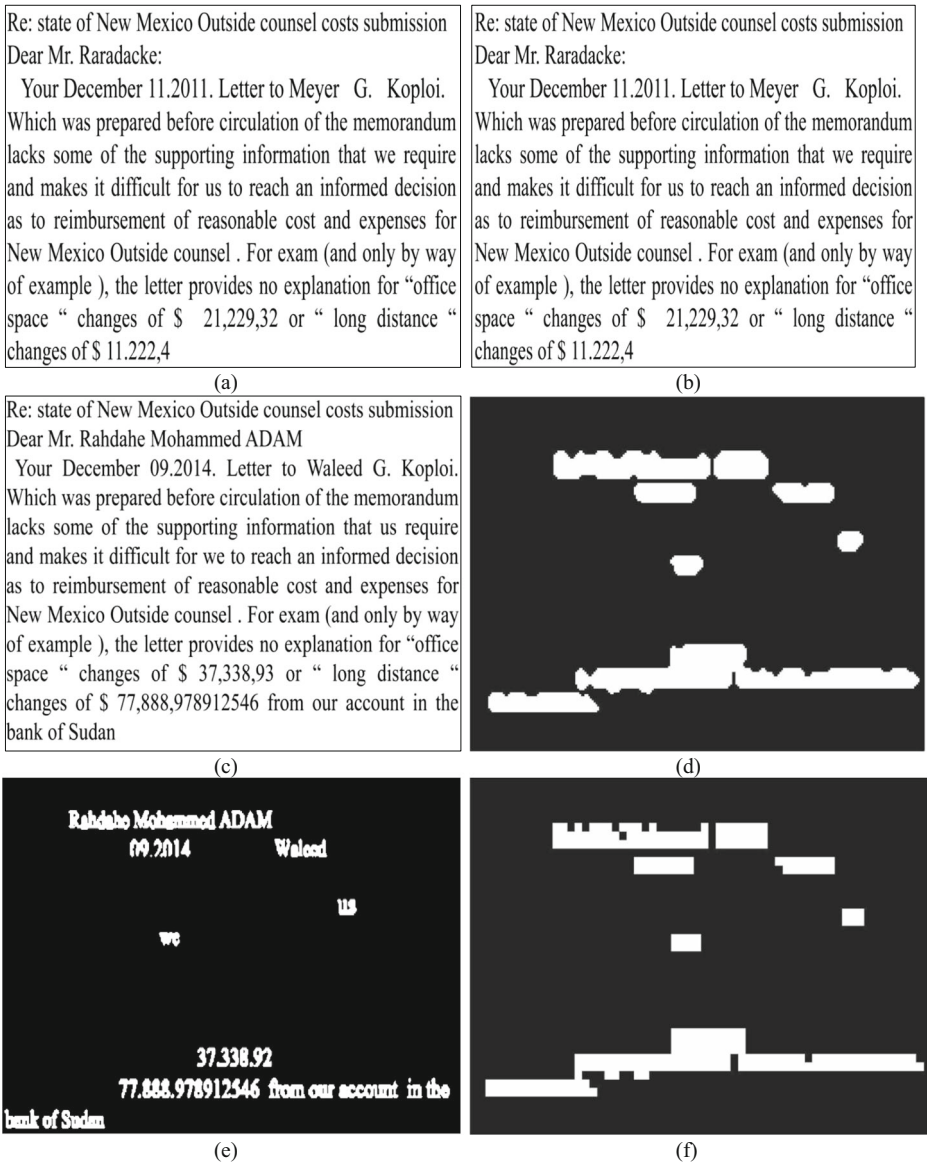
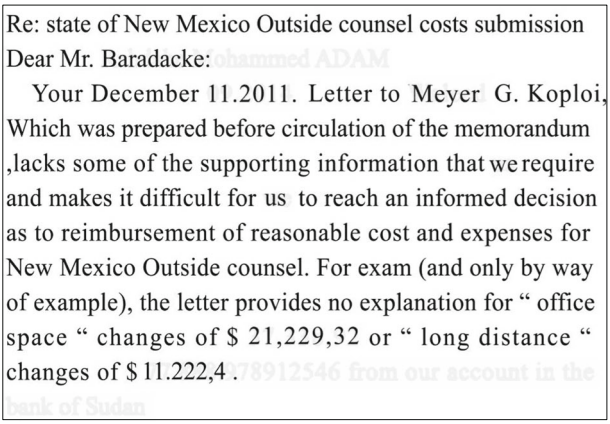
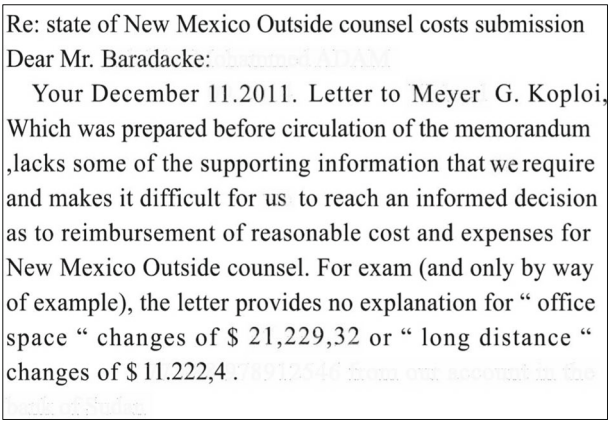


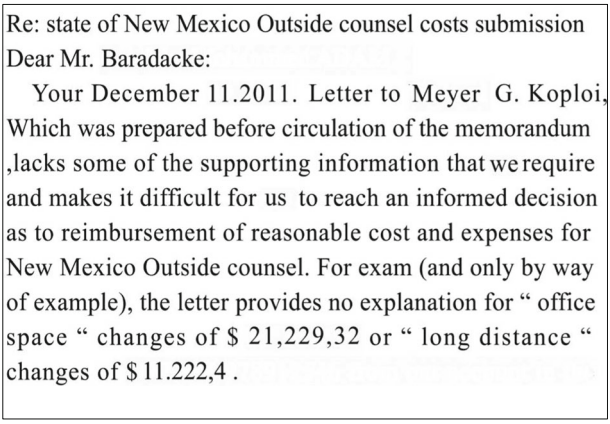
Fig. 18 Tampered detection under content-only tampering **a** Original text image **b** watermarked text image **c** tampered text image, detection results **d** by the proposed scheme, **e** by [35] and **f** by [32]


Re: state of New Mexico Outside counsel costs submission
Dear Mr. Baradacke:
Your December 11.2011. Letter to Meyer G. Koploi, Which was prepared before circulation of the memorandum ,lacks some of the supporting information that we require and makes it difficult for us to reach an informed decision as to reimbursement of reasonable cost and expenses for New Mexico Outside counsel. For exam (and only by way of example), the letter provides no explanation for " office space " changes of $ 21,229,32 or " long distance " changes of $ 11.222,4 .

(a)


Re: state of New Mexico Outside counsel costs submission
Dear Mr. Baradacke:
Your December 11.2011. Letter to Meyer G. Koploi, Which was prepared before circulation of the memorandum ,lacks some of the supporting information that we require and makes it difficult for us to reach an informed decision as to reimbursement of reasonable cost and expenses for New Mexico Outside counsel. For exam (and only by way of example), the letter provides no explanation for " office space " changes of $ 21,229,32 or " long distance " changes of $ 11.222,4 .

(b)


Re: state of New Mexico Outside counsel costs submission
Dear Mr. Baradacke:
Your December 11.2011. Letter to Meyer G. Koploi, Which was prepared before circulation of the memorandum ,lacks some of the supporting information that we require and makes it difficult for us to reach an informed decision as to reimbursement of reasonable cost and expenses for New Mexico Outside counsel. For exam (and only by way of example), the letter provides no explanation for " office space " changes of $ 21,229,32 or " long distance " changes of $ 11.222,4 .

(c)

Fig. 19 Recovered text image under content-only tampering recovered results **a** by the proposed scheme, **b** by [35] and **c** by [32]

up to 33.21 dB, which is lower than [35] (PSNR = 37.06 dB) and [32] (PSNR=47.50 dB), because our recovery scheme restores any effects in the tampered area.

3.2.4 Hybrid attack

In this section, the hybrid attack consists of general tampering and collage attack simultaneously in the image. Figure 20 shows the algorithm performance comparisons for hybrid attack. The watermarked images 'Couple' and 'Old man' are used to implement the hybrid attack as shown in Fig. 20a, b and c represents the tampered image under the hybrid attack. The Old man is attacked by collage attack using watermarked Couple and Old man while the English words are attacked by general tampering attacks. Figure 20e represent the tamper detection result of [35]. The black dots in Fig. 20e showed that the scheme in [35] detect the hybrid attack. Figure 20f represent the tamper detection result of [32]. It provided a better detection result of the general tampering region. However, the tampered region under collage attack cannot be localized satisfactorily. As seen in Fig. 20f, the tampered Old man cannot be localized That is because it can not resist to the collage attack. The PFA and PFR of [32] increased from 0.62 and 0.04 respectively. In contrast, the result of proposed method

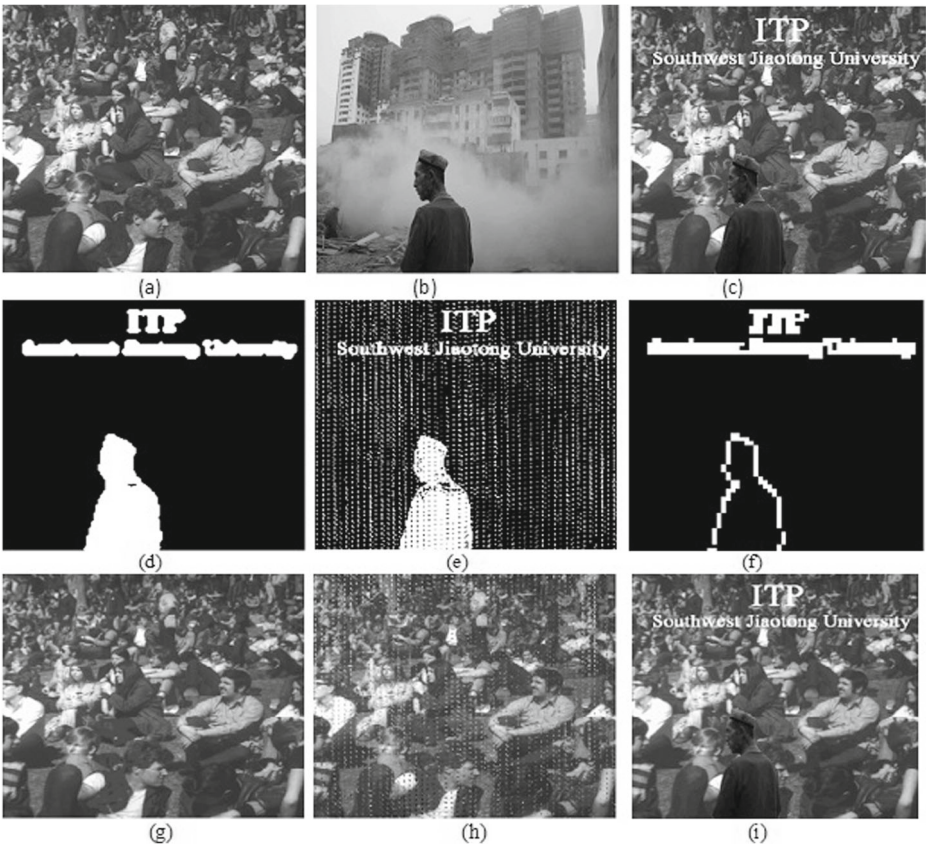


Fig. 20 Tampered detection and recovered image under hybrid attack **a** Watermarked image **b** Watermarked image, **c** Tampered image, detection results **d** by proposed, **e** by [35] and **f** by [32], recovered results **g** by proposed, **h** by [35] and **i** by [32]

Table 1 Time complexity (Seconds) of watermark embedding and tamper detection and recovery

Time	Embedding	Tamper detection and recovery		
		TR=5%	TR=15%	TR=20%
Proposed scheme	31.3	47.5	49.1	50.6
[35]	48.2	60.0	61.4	67.5
[32]	12	95.4	235.5	324.4

as displayed in Fig. 20d shows that the tampered regions under general tampering and collage attack are detected more accurately than its counterparts, due to use of the multi-stage neighbor detection strategy.

The recovered results for Fig. 20c delivered by the proposed scheme and other schemes [35] and [32] are presented in Fig. 20g, h and i respectively. The quality of recovered image of the proposed scheme with PSNR of 36.32 dB is better than which schemes. Where, the PSNR of [35] (as shown in Fig. 20h) is 20.71dB and [32] (as shown in Fig. 20k is 17.71 dB were significantly lower. This is mainly due to the fact that a variable recovery watermark and the detection results have significantly impact on the quality of the recovered image.

3.3 Time complexity

The time complexity of the proposed scheme and the other methods [35] and [32] will be tested using a grayscale image of size 512 × 512 pixels. The test environment is on Acer computer using Matlab 2015a, CPU (Central processing unit) frequency is 1.80 GHz, and RAM (Random Access Memory) is 2G. The run-times of the watermarking embedding, tamper detection and recovery were tested in the different tamper ratio (TR) and the experimental results are shown in Table 1. As can be seen from Table 1, the time-consuming of the watermark embedding in [32] is about 12 seconds, and that in the proposed scheme is about 31 seconds which is lower than 48 seconds of [35]. Although the watermark embedding time in [32] is less expensive, the time for tamper detection and recovery is longer and it increases rapidly as the TR increases. The time-consuming of the proposed tamper detection and recovery for the different tamper ratio TR=5 %, 15%, and 30% is about 47.5, 49.1 and 50.6 seconds, respectively is much smallest than that of schemes in [35] is about 60.0, 61.4, 67.5 and [32] is about 95.4, 235.5, 324.4 seconds, respectively. From the results, we can see that the computational times for embedding and tampering detection and recovery at different tampering ratio of the proposed scheme are smaller than the existing schemes. However, the proposed scheme should be further improved to realize real-time.

4 Conclusions

This work proposed a restorable fragile watermarking scheme based on DCT for both natural and text images. A variable-capacity recovery watermark is generated by allocating more bits to the textural blocks and fewer bits to the smooth ones. The authenticity of each size 4 × 4 block is generated with the hash function and embedded in the original block. A variable-capacity recovery watermark and authentication watermark are embedded in the original block based on a secret key, which improves the quality of watermarked image. The multi-stage neighbor detection strategy is designed to improve the tamper detection

performance under various attacks including general tampering, content-only attack, collage attack and hybrid attack. The proposed scheme outperforms in invisibility, detecting tampered locations and recovery of the tampered information. The simulation results show that the proposed scheme achieves better recovery quality and invisibility due to the variable -capacity recovery watermark and superior localization. Further, the proposed method computationally is less expensive compared with the existing works. The Future work focuses on improving the recovery quality using the advanced image processing methods.

Acknowledgements This work is supported by National Natural Science Foundation of China (NSFC) Under grants (61872303,61461047), and Technology Innovation Talent Program of Science & Technology Department of Sichuan Province(2018RZ0143).

References

1. Atallah MJ, Raskin V, Hempelmann CF, Karahan M, Sion R, Topkara U, Triezenberg KE (2002) Natural language watermarking and tamperproofing. In: International workshop on information hiding, pp 196–212
2. Benrhouma O, Hermassi H, Belghith S (2015) Tamper detection and self-recovery scheme by dwt watermarking. Nonlinear Dyn 79(3):1817–1833
3. Betancourth GP (2012) Fragile watermarking scheme for image authentication. In: 2012 5th international conference on human system interactions (HSI), pp 168–174
4. Brassil JT, Low S, Maxemchuk NF (1999) Copyright protection for the electronic distribution of text documents. Proc IEEE 87(7):1181–1196
5. Chang CC, Hu YS, Lu TC (2006) A watermarking-based image ownership and tampering authentication scheme. Pattern Recogn Lett 27(5):439–446
6. Dadkhah S, Manaf AA, Hori Y, Hassanien AE, Sadeghi S (2014) An effective svd-based image tampering detection and self-recovery using active watermarking. Signal Process Image Commun 29(10):1197–1210
7. Fridrich J, Goljan M (1999) Images with self-correcting capabilities. In: Proceedings of 1999 international conference on image processing, 1999. ICIP 99, vol 3, pp 792–796
8. Fridrich J, Goljan M, Memon ND (2002) Cryptanalysis of the yeung-mintzer fragile watermarking technique. J Electron Imaging 11(2):262–275
9. Han SH, Chu CH (2010) Content-based image authentication: current status, issues, and challenges. Int J Inf Secur 9(1):19–32
10. Haouzia A, Noumeir R (2008) Methods for image authentication: a survey. Multimed Tools Appl 39(1):1–46
11. He HJ, Zhang JS, Chen F (2009) Adjacent-block based statistical detection method for self-embedding watermarking techniques. Signal Process 89(8):1557–1566
12. He HJ, Zhang JS, Tai HM (2009) Self-recovery fragile watermarking using block-neighborhood tampering characterization. In: International workshop on information hiding, pp 132–145
13. Hu YC, Choo KKR, Chen WL (2017) Tamper detection and image recovery for btc-compressed images. Multimed Tools Appl 76(14):15435–15463
14. Huazheng X, Xingming S, Chengliang T (2006) A new fragile watermarking scheme for text documents authentication. Wuhan Univ J Nat Sci 11(6):1661–1666
15. Ji P, Qin C, Tang Z (2016) Fragile watermarking with self-recovery capability via absolute moment block truncation coding. In: International conference on cloud computing and security, pp 104–113
16. Kurniawan F, Khalil MS, Khan MK, Alginahi YM (2014) Dwt+ lsb-based fragile watermarking method for digital quran images. In: 2014 international symposium on biometrics and security technologies (ISBAST), pp 290–297
17. Lee TY, Lin SD (2008) Dual watermark for image tamper detection and recovery. Pattern Recogn 41(11):3497–3506

18. Li C, Wang Y, Ma B, Zhang Z (2011) A novel self-recovery fragile watermarking scheme based on dual-redundant-ring structure. Comput Electr Eng 37(6):927–940
19. Lin PL, Hsieh CK, Huang PW (2005) A hierarchical digital watermarking method for image tamper detection and recovery. Pattern Recognit 38(12):2519–2529
20. Lin CC, Huang Y, Tai WL (2017) A novel hybrid image authentication scheme based on absolute moment block truncation coding. Multimed Tools Appl 76(1):463–488
21. Liu Y, Nie L, Han L, Zhang L, Rosenblum DS (2015) Action2activity: recognizing complex activities from sensor data. In: IJCAI, vol 2015, pp 1617–1623
22. Liu Y, Nie L, Liu L, Rosenblum DS (2016) From action to activity: sensor-based activity recognition. Neurocomputing 181:108–115
23. Liu Y, Zhang L, Nie L, Yan Y, Rosenblum DS (2016) Fortune teller: predicting your career path. In: AAAI, vol 2016, pp 201–207
24. Liu Y, Zheng Y, Liang Y, Liu S, Rosenblum DS (2016) Urban water quality prediction based on multi-task multi-view learning
25. Niu D, Wang H, Cheng M, Zhou L (2015) Self-embedding watermarking scheme based on mds codes. In: International workshop on digital watermarking, pp 250–258
26. Nyeem H, Boles W, Boyd C (2016) Modelling attacks on self-authentication watermarking. Multimed Tools Appl 75(23):15849–15880
27. Olanrewaju RF, Fajingbesi FE, Ishak NAB (2016) Watermarking in protecting and validating the integrity of digital information: a case study of the holy scripture. In: 2016 6th international conference on information and communication technology for the Muslim World (ICT4M), pp 222–227
28. Piper A, Safavi-Naini R (2013) Scalable fragile watermarking for image authentication. IET Inf Secur 7(4):300–311
29. Puhan NB, Ho AT (2005) Restoration in secure text document image authentication using erasable watermarks. In: International conference on computational and information science, pp 661–668
30. Qian Z, Feng G, Zhang X, Wang S (2011) Image self-embedding with high-quality restoration capability. Digital Signal Process 21(2):278–286
31. Qin C, Chang CC, Chen KN (2013) Adaptive self-recovery for tampered images based on vq indexing and inpainting. Signal Process 93(4):933–946
32. Qin C, Wang H, Zhang X, Sun X (2016) Self-embedding fragile watermarking based on reference-data interleaving and adaptive selection of embedding mode. Inf Sci 373:233–250
33. Rosales-Roldan L, Cedillo-Hernandez M, Nakano-Miyatake M, Perez-Meana H, Kurkoski B (2013) Watermarking-based image authentication with recovery capability using halftoning technique. Signal Process Image Commun 28(1):69–83
34. Shi H, Wang X, Li M, Bai J, Feng B (2017) Secure variable-capacity self-recovery watermarking scheme. Multimed Tools Appl 76(5):6941–6972
35. Singh D, Singh SK (2017) Dct based efficient fragile watermarking scheme for image authentication and restoration. Multimed Tools Appl 76(1):953–977
36. Singh P, Agarwal S (2016) An efficient fragile watermarking scheme with multilevel tamper detection and recovery based on dynamic domain selection. Multimed Tools Appl 75(14):8165–8194
37. Sreenivas K, Prasad VK (2018) Fragile watermarking schemes for image authentication: a survey. Int J Mach Learn Cybern 9(7):1193–1218
38. Tong X, Liu Y, Zhang M, Chen Y (2013) A novel chaos-based fragile watermarking for image tampering detection and self-recovery. Signal Process Image Commun 28(3):301–308
39. Wang Z, Bovik AC, Sheikh HR, Simoncelli EP (2004) Image quality assessment: from error visibility to structural similarity. IEEE Trans Image Process 13(4):600–612
40. Wang X, Zhang D, Guo X (2013) A novel image recovery method based on discrete cosine transform and matched blocks. Nonlinear Dyn 73(3):1945–1954
41. Wang H, Ho AT, Li S (2014) A novel image restoration scheme based on structured side information and its application to image watermarking. Signal Process Image Commun 29(7):773–787
42. Yang CW, Shen JJ (2010) Recover the tampered image based on vq indexing. Signal Process 90(1): 331–343
43. Zhang X, Qian Z, Ren Y, Feng G (2011) Watermarking with flexible self-recovery quality based on compressive sensing and compositive reconstruction. IEEE Trans Inf Forensics Secur 6(4):1223–1232
44. Zhang X, Wang S, Qian Z, Feng G (2011) Reference sharing mechanism for watermark self-embedding. IEEE Trans Image Process 20(2):485–495
45. Zhang X, Wang S, Qian Z, Feng G (2011) Self-embedding watermark with flexible restoration quality. Multimed Tools Appl 54(2):385–395
46. Zhang J, Zhang Q, Lv H (2013) A novel image tamper localization and recovery algorithm based on watermarking technology. Optik-Int J Light Elect Opt 124(23):6367–6371

Omer Hemida received the B.S. degree from the University of Kordofan and M.S. degree from Sudan University of Science and technology, Sudan. Currently, he is pursuing Ph.D. from Southwest Jiaotong University, Chengdu, China. His research interests are in the areas of digital watermarking and multimedia security.

Yaoran Huo is pursuing the doctor degree in Southwest Jiaotong University, China. His research interesting includes single-pixel imaging and image forensics.

Hongjie He is a professor in the School of Information Science and Technology at the Southwest Jiaotong University of Chengdu in China. She received the B.S. degree in Computer Science and Technology from Henan Normal University, Xinxiang, China, the Ph.D. degrees in Signal and Information Processing from Southwest Jiaotong University. Her research interests are in the areas of Multimedia Security, Information Hiding and image processing and forensics.

Fan Chen received the M.S. degree in Computer Software and Theory from Chengdu Branch, Chinese Academy Sciences. Currently, he is an associate professor of Southwest Jiaotong University, Chengdu, China. His research interests include multimedia security and digital watermarking.