Blind Dual Watermarking Scheme Using Stucki Kernel and SPIHT for Image Self-Recovery

QIYUAN ZHANG, XIAOCHEN YUAN, (Member, IEEE), AND TONG LIU
Faculty of Applied Sciences, Macao Polytechnic University, Macau 853, China
Corresponding author: Xiaochen Yuan (xcyuan@mpu.edu.mo)

This work was supported by the Research Project of the Macao Polytechnic University under Project RP/ESCA-03/2021.

ABSTRACT In this paper we propose a blind dual watermarking scheme using Set Partitioning in Hierarchical Trees (SPIHT) and Stucki Kernel halftone technique for the tamper detection and image self-recovery. The watermark consists of authentication bits for tampering area location and recovery bits for image restoration. We generate two recovery bits to ensure the high-quality recovery of the tampered image. The primary recovery bit is generated by the SPIHT encoding, and the secondary recovery bit is generated by the Stucki Kernel halftone technique. Then the authentication bit is generated based on the recovery bits. Before embedding the watermark, we shuffle the watermark bits through Arnold cat mapping and diagonal mapping to improve the security and quality of the restored image. LSB-based watermarking technique is used to embed the watermark into the original image to ensure the invisibility of the watermarked image. Experiments have been conducted on two datasets, BOW2 and USC-SIPI, and results show that the proposed scheme can achieve high restoration quality. Comparison with the existing works demonstrate the good performance and superiority of the proposed scheme.

INDEX TERMS Set partitioning in hierarchical trees (SPIHT), Arnold cat map, image self-recovery, Stucki Kernel halftone technique, authentication bit.

I. INTRODUCTION

Nowadays we can save and share the digital image by convenient storage and transmission throughout the Internet. The multimedia is a vehicle for information transmission. However, the digital images can be simply copied and modified maliciously through various image processing software. It is difficult for people to distinguish the integrity and authenticity of images after processing, so that how to avoid tampering digital images has become a serious problem. The watermarking techniques can be classified into different categories: fragile watermarking, which is designed to detect every possible change in the watermarked image, and it is very sensitive, thus suitable for verifying the integrity of the data. Semi-fragile watermark, which enables the embedded information to withstand acceptable operations such as compression, slight noise, filtering, A/D or D/A conversion, thus it is often used for robustness checks. Reversible watermarking, which is also known as lossless watermarking, fully extracts the embedded information and fully restores the original image. And robust watermarking, which is to ensure the integrity and security of the watermark information under various attacks.

In recent years, watermarking scheme for self-recovery has become an important research topic. In the authentication process, the watermark is extracted and compared with the content information of the original image, to determine whether the content of the image has been tampered. It can not only judge tampered image and its tampered area, but also restore the tampered area. The researches focus on ensuring the invisibility of watermarked image and improving the localization of tampered area and performance of image self-recovery. In these works, the watermark is generated from the host image and then embedded. By extracting the watermark information, the tampered region can be detected and located by the authentication bits. On this basis, the detected region can furtherly be recovered by recovered bits. Therefore, these schemes can be classified as fragile watermarking.

The idea of restoring fragile image watermarking algorithm was first proposed in [1]. The purpose of the
self-recovery fragile watermarking algorithm is to restore the tampered part of the image. Watermark generation, embedding location selection and tamper detection performance can ensure the effective recovery of tampered image, and the quality of the image depends on the way to restore the watermark. Therefore, the scholars have put forward different schemes that have focused on generating watermark, embedding location and tamper recovery performance.

Watermark generation can be divided into two types: authentication watermark generation and recovery watermark generation. Dadkhah et al. [2] introduced the two $2 \times 2$ image blocks with high 5-bit mean value which was used to generate and recover watermarks, and 2-bit authentication watermarks were obtained through XOR operation, so that 12 bits of watermark information was generated in total. Kang et al. [3] detected tampering by generating additional authentication. The additional generation of authentication watermark increases the embedding capacity and reduces the invisibility of watermarked images. However, because it needs more embedding capacity, the watermark image after embedding has high distortion. Lee et al. [4], [5] showed a 6-bits recovery watermark based on the average of the height of 6-bits in $2 \times 2$ image blocks. Qin et al. [6] showed two kinds of recovery watermarks of different lengths by using VQ coding of $4 \times 4$ image block. Variable length recovery watermarks were generated according to image block texture features combined with Discrete Wavelet Transform (DWT) transformation, 7-bit recovery watermarks were generated from smooth blocks, and 12-bit recovery watermarks were generated from texture blocks as embedded mapping blocks. Qin et al. [7] introduced an image hash method with folding operation to generate authentication bits. The low-frequency components of non-sub-sampling contour transform (NSCT) coefficients are used to encode the recovered bits of each block through an adaptive bit allocation mechanism. In order to reduce the embedding capacity of watermark, Ansari et al. [8], [9] introduced a method to compress watermark information and decode it after extraction. However, the efficiency of this algorithm became lower.

Generally speaking, the traditional methods of embedding watermark data into host image may cause some distortion to the original image. But it also brings the capability of self-recovery. For example, Roy et al. [10] introduced a hardware implementation of a digital watermarking system that can insert invisible, semi-fragile watermark information into compressed video streams in real time. The watermark embedding was performed in the Discrete Cosine Transform (DCT) domain. It showed that the Peak-Signal-to-Noise-Ratio (PSNR) was above 35dB. Molina et al. [11] introduced a digital watermarking method based on Daubechies DWT, halftoning and Quantization Index Modulation (QIM). Although it is resistant to attacks of JPEG compression with the quality factor above 75, its PSNR is only 35dB. Zhang et al. [12] proposed a tamper detection, localization, and recovery scheme for encrypted images using DWT and compressed sensing. If the watermark or low frequency parts are tampered, the recovery accuracy is 100%. Bravo et al. [13] introduced a receiver that used authentication bits to locate changed blocks of pixels and then performed an iterative recovery mechanism to compute the original values of the watermarked pixels. In this method, it embeds reference bits and some authentication bits to the 3 Least Significant Bit (LSB) planes of the image. Therefore, based on the premise of being less perceptible and resistant to attacks, we choose to use the method of watermark embedding to LSB. Haghighi et al. [14] presented a fragile blind quad watermarking scheme, which was proposed for image tamper detection and recovery based on wavelet transform and genetic algorithm. This scheme introduced two techniques called Mirror-aside and Partner-block, and it can achieve the average PSNR and Structural Similarity Index (SSIM) values of the watermarked image of about 46 dB and 1. Su et al. [15] proposed an effective self embedding fragile watermarking scheme for medical images. The self-recovery information and verification code of each block were pre-generated, and then embedded into other blocks with the help of tortoise shell and embedded table. The simulation results showed that the accuracy of tamper detection can reach 99.83%, and the average PSNR of the restored image can reach 42.11 dB. Hamid et al. [16] introduced a method of extracting local features in DCT domain, where the positions of three DCT peaks were checked to distinguish 13 texture contours with different number of edges, edge directions, and combinations of the two. Sinhal et al. [17] proposed a blind fragile watermarking scheme for color images which can provide effective image tamper detection and self-recovery. The pseudo-random binary sequence based on the key was used as a watermark for tamper detection. Experimental results showed that the scheme achieved nearly 99% accurate tamper detection and significant tamper image restoration. Shehab et al. [18] proposed a new image authentication and self-recovery scheme for medical applications based on fragile watermarking. Singular value decomposition (SVD) is used to calculate the transformation in the original image by inserting the trajectory of block level SVD into the LSB of image pixels. We summarize the existing works in Table 1. It can be seen that most of the algorithms have the problems of low PSNR of recovered images and small attack resistance area.

In order to further improve the accuracy of tamper detection and ensure the quality of self-recovery, in this paper we propose a blind dual watermarking scheme using Set Partitioning in Hierarchical Trees (SPIHT) and Stucki Kernel halftone technique for the tamper detection and image self-recovery. The SPIHT-based recovery bit is used to recover the tampered area as an image digest, while the halftone-based recovery bit can provide a second chance of recovery and additional information for authentication. At the same time, we improve security by permuting the coefficients of
the recovery bits. In this proposed scheme, we generate two recovery bits to ensure the high-quality recovery of the tampered image. The primary recovery bit is generated by the SPIHT encoding, while the secondary recovery bit is generated by the Stucki Kernel halftone technique [19], [20], [21]. On this basis, we then generate the authentication bit by applying the logical operation. Furthermore, we employ the Arnold’s Cat Map (ACM) [22], [23] and diagonal mapping [26] during embedding to improve the security and tamper recovery rate. Then, we concatenate all the watermark bits after ACM scramble. Finally, the watermark is embedded into the original image by LSB technique. Compared to the traditional image digests which are obtained based on averaging pixels or MSBs planes, the proposed method for generating recovery bits can achieve better quality.

### A. GENERATING AND EMBEDDING WATERMARK

There are two types of watermarks that make up this embedded part. The watermark bits for recovery, which are for the purpose of recovering the tampered regions, and the watermark bits for authentication, which are for the purpose of tampering localization, are created and embedded into the host image. In this work, we propose to generate the recovery watermark using the Stucki kernel and SPIHT, on the basis that SPIHT can be used as image digests, thus to recover the tampered regions, while the Stucki kernel can provide a second chance for recovery and can also be used as authentication information. Additionally, we propose to apply ACM and Diagonal Mapping to shuffle and encrypt the coefficients in each block, which in order to increase security. The process of generating and embedding the watermark is shown in Figure 1. After producing the recovery bits, we use a logical operation between the two recovery bits to generate the authentication bits, providing a detecting method with high precision and credibility. Afterwards, we concatenate the recovery bits and the authentication bits after shuffling them by ACM. Finally, the watermark composed of recovery bits and authentication bits is embedded into the LSB planes of the host image.

To generate the recovery bits, the SPIHT and Stucki kernel are respectively applied to the host image respectively, to generate the primary recovery bits $W_{Rec1}$ and the secondary primary bits $W_{Rec2}$. The SPIHT is widely used as embedded-compression algorithm in digital signals compression. SPIHT can generate a wavelet transform coefficients bitstream at our desired rate and can be used to reconstruct the image even the received bit stream is interrupted anywhere with good progressive transmission. Therefore, in our method, we employ the SPIHT for generation of the primary recovery bits $W_{Rec1}$.

The SPIHT sorts the rounded multi-resolution wavelet transform coefficients according to their magnitudes and transmits them based on significant bit order for higher quality because the quality of reconstruction depends on the output rate exploited [24], [25]. The same process will be used available to the decoder inversely as well. These similarities can be found through wavelet transform spatial orientation trees as shown in Figure 2. To satisfy our requirement, we set the compressing rate as 1.5 bpp, and the length of bit stream is $393172$, given the host image be $512 \times 512$. As a result, the SPIHT matrix of $256 \times 256$ will be generated after zero-paddiing and resizing.

Then we propose to apply the mapping to the generated matrix, to improve the security of the watermarked image and furtherly quality of the recovered image. In this work, we employ the ACM and diagonal mapping to shuffle the result. The specific steps are: divide the matrix into four equal columns from left to right, denoting as p1, p2, p3, and p4. If the position of the coefficients that generated by ACM is p1, then we shuffle it to p3, so as p2 and p4. And the same operation will be applied to right side of the matrix. In this

### II. PROPOSED APPROACH FOR DIGITAL IMAGE SELF-RECOVERY

The goal of the scheme is to detect the tampered region and then recover them to its original form. To achieve this goal, in this work, we propose the fragile and blind dual watermarking scheme using Stucki kernel and SPIHT. The proposed approach consists of two main stages: (1) generate and embed the watermark, and (2) detect and recover the tampered regions. The sub-sections II.A and II.B respectively explain the two stages in detail.

### TABLE 1. Comparison of related works and methods.

| Authors         | Method’s digests | Recovered images (dB) | Limitations                  |
|-----------------|------------------|-----------------------|------------------------------|
| Dadkhah et al.  | SVD              | PSNR>45               | Cannot sustain collage attack |
| Qin et al. [7]  | DWT, VQ          | PSNR>41               | Small attack area            |
| Roy et al. [10] | DCT              | PSNR>35               | Low self-recovery            |
| Molina et al. [11] | DWT, QIM       | PSNR>35               | Low self-recovery            |
| Zhang et al. [12] | DWT            | PSNR>36               | Low self-recovery            |
| Bravo et al. [13] | LSB,            | PSNR>37               | Low self-recovery            |
| Haghighi et al. [14] | Blind-quad      | PSNR>46               | Small attack area            |
| Su et al. [15]  | TSDH, LSB        | PSNR>42               | Small attack area            |
| Hamid et al. [16] | DCT             | PSNR>41               | Small attack area            |
| Sinhal et al. [17] | Randomized binary fragile | PSNR>36               | Low self-recovery            |
| Shehab et al. [18] | SVD             | PSNR>38               | Low self-recovery            |
way, all the coefficients of the matrix can be shuffled by ACM. Figure 3 shows the example of mapping generation of a $8 \times 8$ matrix by ACM and diagonal mapping. Specifically, when the tampered regions are on the left or right side of the original image, the recovery bits can be retained and that can be used to recover the tampered regions. Therefore, the mapping operation can help to make the proposed approach resist copy-move attack and vector quantization attack.

On the other hand, in order to improve the quality of the restoration, the halftoning technique is used to compress the original image into its half size, thus generating the secondary recovery bits $W_{Rec2}$. Halftone refers that a continuous tone image is quantized into image with only a few colors, and the quantized image looks like the original image. In our scheme, the Stucki kernel is employed and we can get the secondary recovery bits after diagonal mapping.

With the generated primary recovery bits $W_{Rec1}$, and secondary recovery bits $W_{Rec2}$, the authentication bits are then calculated accordingly. Given the host image of size $M \times N$, firstly the blocking is applied to the host image to generate blocks of $b \times b$, from each of which one authenticate bit will be calculated. In the following experiments, we use $b = 2$ in the proposed scheme. That means, one bit will be generated as authenticate bit in each $2 \times 2$ block. By representing the generated primary recovery bits $W_{Rec1}$ in its binary form,
W_{Rec1} can be denoted as $c_{i,j}^k, c_{i,j}^{k-1}, \ldots, c_{i,j}^0$, then the $Num_{i,j}$ can be calculated by (1).

$$Num_{i,j} = \sum_{n=0}^{k} c_{i,j}^n$$

where $c_{i,j}$ represents the coefficients, and $k$ represents the number of bits.

And then the corresponding $Flag_{matrix}$ can be calculated by (2):

$$Flag_{matrix} = [Num_{i,j} \mod 2]$$

Finally, the authentication bits $W_{Auth}$ can be obtained by applying the logical operation using (3)

$$W_{auth} = Flag_{matrix} \oplus W_{Rec2}$$

After generating the recovery bits $W_{Rec1}$ which is of 6 bits per block (bpb), $W_{Rec2}$ which is of 1 bpb, and authentication bits $W_{Auth}$ which is of 1 bpb, the watermark information can be generated by concatenating $W_{Rec1}$, $W_{Rec2}$, and $W_{Auth}$. Then the watermark information will be embedded into the two LSB planes of the host image. Figure 4 shows the demonstration of watermark embedding in one block of $2 \times 2$. In order to resist attack of copy-move, we propose to apply the ACM into the watermark information as well before being embedded.

B. DETECTING AND RECOVERING TAMPERED REGIONS

In order to detect and recover the tampered regions, the watermark information is extracted from the received watermarked image. The ACM will be used to generate the recovery bits and authentication bits, same to how watermark generation was mentioned above. Once the recovery bits have been retrieved, the authentication bits may be computed, much like with the watermark generation process. We can identify the tampered regions by comparing the computed authentication bits with the extracted authentication bits. On basis of that, the extracted recovery bits can be employed for the recovery of the tampered regions. Figure 5 shows the procedures of detecting and recovering the tampered regions.

Similar as described in Section II.A, firstly, the received image is blocked into $2 \times 2$ blocks, from each of which, the watermark information is extracted by extracting the 2 LSBs of each pixel. After permuting and decrypting the extracted information by ACM, eight bits can be obtained from each block. In each block, the first six bits are the primary recovery bits, notated as $W_{Ext,Rec1}$, while the seventh bit is the secondary recovery bit, notated as $W_{Ext,Rec2}$, and the eighth bit is the extracted authentication bit, notated as $W_{Ext,Auth}$. From the extracted recovery bits, the corresponding authentication bits $W_{Cal,Auth}$ can be calculated using Eq. (1), (2), and (3). From $W_{Ext,Auth}$ and $W_{Cal,Auth}$, the tampered regions can be detected by (4). It is noted that the morphology operations such as closing operations should be applied to the $Tamp_{region}$ for higher tamper detection rate.

$$Tamp_{region}(i,j) = W_{Ext,Auth}(i,j) \oplus W_{Cal,Auth}(i,j)$$

After locating the tampered regions, the recovery bits are then used to recover the tampered regions. Due to a series of mapping operations have been applied to increase the security of the watermark information, we should de-map the watermark by ACM and diagonal mapping. On one hand, from the watermarked image, 6 bits of each block that represent the coefficients of SPIHT are retrieved. In the stage of watermark generation and embedding, in order to satisfy the capacity requirements, we put zeros into the spare bits. Therefore, in order to obtain the initial bitstream, we should resize the matrix and extract the significant bits.

After that, we can apply the SPIHT decoding and reconstruct the image from SPIHT coefficients. On the other hand, we apply the Stucki Kernel [26] algorithm to $W_{Ext,Rec2}$ and
thus to reconstruct the halftone image accordingly. With the SPIHT decoded image and the halftone image, the detected tampered region can be recovered and then constructed into the input image, thus generating the reconstructed image.

### III. EXPERIMENTAL RESULTS AND DISCUSSIONS

In this section, we choose the BOW2 and USC-SIPI image database to evaluate the performance of the proposed method. The metrics Precision, Recall and F1score as defined in Eq. (5) ~ (7) are calculated to evaluate the tampering detection results. The Precision reflects the proportion of pixels actual tampered in those labeled as tampered, the Recall reflects the ability to detect tampered pixels correctly, while F1score combines the Precision and Recall, which can reflect the comprehensive performance of the detecting algorithm. To measure the quality of recovered images, the Peak Signal to Noise Ratio (PSNR) [27] and Structural similarity (SSIM) [28] are calculated using (8) and (10) respectively. PSNR is an image quality evaluation index and it can evaluate the quality of the recovered image; the higher the PSNR is, the more similar between the original image and the recovered one. SSIM is used to measure the similarity of images based on three comparative measures: luminance, contrast,
where MSE means the Mean Square Error obtained by formula (9), and $a \times b$ is the size of image.

$$SSIM = \frac{(2\mu_1\mu_2 + c_1)(2\sigma_{12} + c_2)}{(\mu_1^2 + \mu_2^2 + c_1)(\sigma_1^2 + \sigma_2^2 + c_2)}$$

where $\mu_1, \mu_2, \sigma_1$, and $\sigma_2$ are the mean and variance values for two images, respectively. The $\sigma_{12}$ is the covariance between two images. The $c_1$ and $c_2$ are constant values.

**A. PERFORMANCE OF THE PROPOSED SCHEME**

Figure 6 shows demonstration of the proposed scheme with examples from BOW2 dataset: ‘japan tower’, ‘hedge’, ‘barrier’, ‘statue’, and ‘three hundred’. The 1st row shows the host images of different texture; 2nd row shows the corresponding watermarked images, which are acceptable by human vision system and are close to the host image; 3rd row shows the tampered images, where the tampered regions are highlighted in red circle, and it can be seen that different kinds of tampering and different tampering sizes are included; 4th row shows the ground truth, 5th row shows the detected results, and 6th row shows the recovered images. The results show the good performance of the proposed scheme in both tamper detection and image recovery. In addition to the subjective evaluation, the performance is also evaluated with objective metrics. The quality of watermarked images and recovered images are evaluated in terms of PSNR and SSIM, while the tamper detection results are evaluated in terms of Precision, Recall, and...
FIGURE 6. Demonstration of the results of the proposed scheme. 1st row: (A1)–(E1) the original images, 'japan tower', 'hedge', 'barrier', 'statue', 'three hundred'; 2nd row: (A2)–(E2) the watermarked image; 3rd row: (A3)–(E3) tampered images; 4th row: (A4)–(E4) the ground truth; 5th row: (A5)–(E5) the detected tampered results; 6th row: (A6)–(E6) the corresponding recovered images.
FIGURE 7. Performance of proposed scheme under tampering of various rates and positions. 1st row: (A1)∼(F1) 50% tampering at top of image; 2nd row: (A2)∼(F2) 50% tampering at top of image; and 3rd row: (A3)∼(F3) 40% tampering at middle of image. 1st column: (A1)(A2)(A3) original images; 2nd column: (B1)(B2)(B3) watermarked images; 3rd column: (C1)(C2)(C3) tampered images; 4th column: (D1)(D2)(D3) ground truth; 5th column: (E1)(E2)(E3) detected tampered regions; and 6th column: (F1)(F2)(F3) recovered images, \( \text{PSNR, SSIM} = \{35.8368\, \text{dB}, 0.9293\}, \{35.5718\, \text{dB}, 0.9492\}, \{28.7048\, \text{dB}, 0.9273\} \).

FIGURE 8. Performance of proposed scheme under multiple tampering and splicing tampering. 1st row: (A1)∼(F1) multiple tampering; 2nd row: (A2)∼(F2) splicing tampering. 1st column: (A1)(A2) original images; 2nd column: (B1)(B2) watermarked images; 3rd column: (C1)(C2) tampered images; 4th column: (D1)(D2) ground truth; 5th column: (E1)(E2) detected tampered regions; and 6th column: (F1)(F2) recovered images, \( \text{PSNR, SSIM} = \{38.1778\, \text{dB}, 0.9713\}, \{46.2621\, \text{dB}, 0.9904\} \).

\( \text{F1score} \), as shown in Table 2. The results indicate the excellent performance of the proposed scheme. The \( \text{PSNR} \) values of watermarked image are over 49dB, that means that the similarity of the watermarked images and original images are out of the range of human vision system. The \( \text{PSNR} \) and \( \text{SSIM} \) values of recovered image are respectively over 30dB and 0.95, which indicate the high quality of the recovered image. High \( \text{Precision, recall and F1score} \) results reflect the comprehensive good performance of the detection algorithm.
To show the performance of the proposed scheme, we give examples from USC-SIPI image dataset under tampering of different rates and positions, as shown in Figure 7, where the 1st row shows the example of ‘Lena’ when tampered at top of image with tampering rate of 50%, the 2nd row shows the example of ‘Pepper’ when tampered at left of image with tampering rate of 50%, and the 3rd row shows the example of ‘Elaine’ when tampered at middle of image with tampering rate of 40%. The detected tampered regions are shown in the 5th column, by comparing with the ground truth in the 4th column, it can be easily seen that the proposed scheme can detect the tampered regions correctly. Based on the tampering detection results, the recovered results are then shown in the final column, with the corresponding PSNR and SSIM values respectively calculated as 35.8368dB and 0.9293 for ‘Lena’, 35.5718dB and 0.9492 for ‘Pepper’, and 28.7048dB and 0.9273 for ‘Elaine’. Additionally, in Figure 8, we give examples under multiple tampering and splicing tampering. The corresponding PSNR and SSIM values of the recovered images are respectively calculated as 38.1778dB and 0.9713 for the multiple tampered ‘Pepper’, and 46.2621dB and 0.9904 for splicing tampered ‘F16’. The results demonstrate the good quality of the recovered images in different situations.
B. PERFORMANCE OF THE PROPOSED SCHEME

In this section, we compare performance of the proposed scheme with the existing work TRLH [29] using examples from USC-SIPI dataset: ‘Baboon’, ‘Barbara’, ‘Lena’, ‘Pepper’, ‘Gril’, ‘Lake’, and ‘F16’. The PSNR and SSIM values of watermarked images for TRLH [29] and our method is shown in Table 3. The color images and grayscale images are used as host images respectively, and the results are calculated respectively. The best results are highlighted in bold and it explicitly show that the proposed scheme can obtain better quality of the watermarked images than the existing TRLH [29]. Figure 9 shows the comparison results of TRLH [29] and the proposed scheme under different tampering rates, varying from 10% to 90%. The 1st column, (A1) and (B1), show the results of color images, and the 2nd column, (A2) and (B2), show the results of grayscale images. It can be seen that our method achieves better results for both color images and grayscale images.

IV. CONCLUSION

In this work, we propose a tamper detection and self-recovery scheme for digital images using SPIHT and Stucki Kernel halftone technique. The SPIHT and Stucki Kernel halftone technique can provide a better recovery digest compared to the various compression method. The authentication bits are then calculated according to the recovered bits. Furthermore, we employ the ACM and diagonal mapping to make the watermark bits have better security and unpredictability. Numerous experiments have been conducted on the two public datasets, BOW2 and USC-SIPI, and the results indicate that the proposed scheme can achieve excellent performance in tampering detection and tampered regions recovery. The proposed scheme can detect the tampered regions in some indistinguishable circumstances for human vision system, and the recovered images can get high similarity to the original image. The PSNR values of watermarked images are high and that helps to maintain the good invisibility. By comparing with the existing method, the superiority of the proposed scheme can be demonstrated even when under high tampering rates. Although the proposed scheme can achieve a satisfactory performance according to the experimental results, there are some issues to be improved. When the host image is relatively smooth, the detected region will be larger than the ground truth, that might be caused by the authentication bits. Therefore, in our future work, we will continue to work on improvement on authentication bits generation.

REFERENCES

[1] J. Fridrich, “Protection of digital images using self-embedding,” in Proc. Symp. Content Secur. Data Hiding Digit. Media. New Jersey Institute of Technology, May 1999.
[2] S. Dadkhah, A. A. Manaf, Y. Hori, A. E. Hassanien, and S. Sadeghi, “An effective SVD-based image tampering detection and self-recovery using active watermarking,” Signal Process., Image Commun., vol. 29, no. 10, pp. 1197–1210, 2014.
[3] Q. Kang, K. Li, and H. Chen, “An SVD-based fragile watermarking scheme with grouped blocks,” in Proc. 2nd Int. Conf. Inf. Technol. Electron. Commerce, Dec. 2014, pp. 172–179.
[4] T.-Y. Lee and S. D. Lin, “Dual watermark for image tamper detection and recovery,” Pattern Recognit., vol. 41, no. 11, pp. 3497–3506, 2008.
[5] Y. Chang and W. Tai, “A block-based watermarking scheme for image tamper detection and self-recovery,” Opto-Electron. Rev., vol. 21, no. 2, pp. 182–190, Jan. 2013.
[6] C. Qin, C.-C. Chang, and P.-Y. Chen, “Self-embedding fragile watermarking with restoration capability based on adaptive bit allocation mechanism,” Signal Process., vol. 92, no. 4, pp. 1137–1150, 2012.
[7] C. Qin, P. Ji, X. Zhang, J. Dong, and J. Wang, “Fragile image watermarking based on pixil wise recovery and grouped block DCT encoding strategy,” Signal Process., vol. 138, pp. 280–293, Sep. 2017.
[8] C. Qin, C.-C. Chang, and K.-N. Chen, “Adaptive self-recovery for tampered images based on VQ indexing and inpainting,” Signal Process., vol. 93, no. 4, pp. 933–946, Apr. 2013.
[9] I. Ansari, M. Patra, and C. W. Ahn, “SVD based fragile watermarking scheme for tamper localization and self-recovery,” Int. J. Mach. Learn. Cybern., vol. 7, no. 6, pp. 1225–1239, Dec. 2016.
[10] S. D. Roy, X. Li, Y. Shoshan, A. Fish, and O. Yadid-Pecht, “Hardware implementation of a digital watermarking system for video authentication,” IEEE Trans. Circuits Syst. Video Technol., vol. 23, no. 2, pp. 289–301, Feb. 2013.
[11] J. Molina-Garcia, R. Reyes-Reyes, V. Ponomaryov, and C. Cruz-Ramos, “Watermarking algorithm for authentication and self-recovery of tampered images using DWT,” in Proc. 9th Int. Kharkiv Symp. Phys. Eng. Microw., Millim. Submillimeter Waves (MSMW), 2016, pp. 1–4.
[12] R. Zhang, D. Xiao, and Y. Chang, “A novel image authentication with tamper localization and self-recovery in encrypted domain based on compressive sensing,” Secur. Commun. Netw., vol. 2018, Mar. 2018, Art. no. 1591206.
[13] S. Bravo-Solorio, F. Calderon, C.-T. Li, and A. K. Nandi, “Fast fragile watermark embedding and iterative mechanism with high self-restoration performance,” Digit. Sig. Process., vol. 73, pp. 83–92, Feb. 2018.
[14] B. Bolourian Haghighi, A. H. Taherinia, and A. H. Mohajerzadeh, “TRLG: Fragile blind quad watermarking for image tamper detection and recovery by providing compact digests with optimized quality using LWT and GA,” Inf. Sci., vol. 486, pp. 204–230, Jun. 2019.
[15] G.-D. Su, C.-C. Chang, and C.-C. Lin, “Effective self-recovery and tampering localization fragile watermarking for medical images,” IEEE Access, vol. 8, pp. 160840–160857, 2020.
[16] M. Hamid and C. Wang, “Adaptive image self-recovery based on feature extraction in the DCT domain,” IEEE Access, vol. 6, pp. 67156–67165, 2018.
[17] R. Sinhal, I. A. Ansari, and C. W. Ahn, “Blind image watermarking for localization and restoration of color images,” IEEE Access, vol. 8, pp. 200157–200169, 2020.
[18] A. Shehab, M. Elhoseny, K. Muhammad, A. K. Sangaih, P. Yang, H. Huang, and G. Hou, “Secure and robust fragile watermarking scheme for medical images,” IEEE Access, vol. 6, pp. 102578–102588, Oct. 2018.
[19] P. E. Axelson, “Quality measures of halftoned images (a review),” Institutionen für Technik Och Natuervetenskap, p. 81, Jan. 2003.
[20] S. H. Soleymani and A. H. Taherinia, “High-capacity image steganography on sparse message of scanned document image (SMSDI),” Multimedia Tools Appl., vol. 76, no. 20, pp. 20847–20867, Oct. 2017.
[21] J. F. Jarvis, C. N. Judice, and W. Ninke, “A survey of techniques for the display of continuous tone pictures on bilevel displays,” Comput. Graph. Image Process., vol. 5, no. 1, pp. 13–40, 1976.
[22] I. Arnold and A. Avez, Ergodic Problems of Classical Mechanics. Redwood City, CA, USA: Addison-Wesley, 1989, p. 17.
[23] M. Ali, C. W. Ahn, and M. Pant, “A robust image watermarking technique using SVD and differential evolution in DCT domain,” Optik Int. J. Light Electron Opt., vol. 125, no. 1, pp. 428–434, 2014.
[24] S. Sarreshshadi and M. A. Akhhae, “A source-channel coding approach to digital image protection and self-recovery,” IEEE Trans. Image Process., vol. 24, no. 7, pp. 2266–2277, Jul. 2015.
[25] T. Liu and X. Yuan, “A dual-tamper-detection method for digital image authentication and content self-recovery,” Multimedia Tools Appl., vol. 80, no. 19, pp. 29805–29826, Aug. 2021.
[26] Z. Xiong, M. T. Orchard, and K. Ramchandran, “Wavelet-based approach to inverse halftoning,” Proc. SPIE, vol. 3018, pp. 89–100, Apr. 1997.
[27] A. H. Obaid, “Information hiding techniques for steganography and digital watermarking,” Hum.-Comput. Interact., vol. 73, no. 4, pp. 63, 2015.
[28] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, “Image quality assessment: From error visibility to structural similarity,” IEEE Trans. Image Process., vol. 13, no. 4, pp. 600–612, Apr. 2004.
[29] B. Bolourian Haghighi, A. H. Taherinia, and A. Harati, “TRLH: Fragile and blind dual watermarking for image tamper detection and self-recovery based on lifting wavelet transform and halftoning technique,” J. Vis. Commun. Image Represent., vol. 50, pp. 49–64, Jan. 2018.
QIYUAN ZHANG received the B.Sc. degree in electronic information technology from the Macau University of Science and Technology, in 2019, and the M.Sc. degree in electronic communication and computer engineering from the University of Nottingham, in 2021. He is currently pursuing the Ph.D. degree in computer applied technology with the Faculty of Applied Sciences, Macau Polytechnic University. His research interests include speech recognition, digital signal processing, and fragile watermarking for image tamper detection and recovery.

XIAOCHEN YUAN (Member, IEEE) received the B.Sc. degree in electronic information technology from the Macau University of Science and Technology, in 2008, and the M.Sc. degree in e-commerce technology and the Ph.D. degree in software engineering from the University of Macau, in 2010 and 2013, respectively. From 2014 to 2015, she was a Postdoctoral Fellow at the Department of Computer and Information Science, University of Macau. From 2016 to 2021, she was an Assistant Professor and an Associate Professor with the Faculty of Information Technology, Macau University of Science and Technology. She is currently an Associate Professor with the Faculty of Applied Sciences, Macau Polytechnic University. Her research interests include digital multimedia processing, digital watermarking, multimedia forensics, tampering detection and self-recovery, acoustic processing and diagnosis, and deep learning techniques and applications.

TONG LIU received the B.Sc. degree in communication engineering from the Communication University of Zhejiang, in 2018, and the M.S. degree in computer information science from the Macau University of Science and Technology, in 2020. She is currently pursuing the Ph.D. degree in computer applied technology with the Faculty of Applied Sciences, Macau Polytechnic University. From 2021 to 2022, she was a Research Assistant at the Department of Computer and Information Science, University of Macau. Her research interests include digital image forensics, digital watermarking, tampering detection and self-recovery, and deep learning techniques and applications.