Multimedia Tools and Applications (2023) 82:45503–45518
https://doi.org/10.1007/s11042-023-15261-9

Blind Dual Image Watermarking for Copyright Protection, Tamper Proofing and Self-Recovery

MingQuan Fan[1]

Received: 24 March 2022 / Revised: 20 June 2022 / Accepted: 6 April 2023 /
Published online: 4 May 2023

Abstract
In this paper, a blind dual image watermarking scheme for copyright protection, tamper proofing and self-recovery is proposed. For purpose of copyright protection, we use binary handwritten signature, a high correlative biometric to owner as robust watermark, and embed it into hybrid domain constructed by dual tree complex wavelet transform (DT-CWT) and discrete cosine transform (DCT). For purpose of tamper proofing and self-recovery, source encoding output bits generated by set partitioning in hierarchical trees (SPIHT) encoding are embedded into image based on least significant bits (LSB) replacement, moreover, in order to enhance the robustness of self-recovery, repeated encoding technique is adopted, and hash-based check bits are used for tamper proofing. Experimental results indicate the proposed watermarking mechanism can withstand various image processing attacks, accurately locate and recover the tampered area of an image, especially it has the ability of tamper discrimination that other existing schemes do not have. It can find application for joint ownership and content authentication synchronously.

Keywords Dual watermarking · Copyright protection · Tamper discrimination · Set partitioning in hierarchical trees(SPIHT) · Dual tree complex wavelet transform (DT-CWT)

1 Introduction

The digital image resources on the Internet are increasing daily due to the age of sharing. It greatly promotes interaction for people's lives. However, problems including copyright protection and integrity verification, etc., also have attracted many eyes from academia and industry. Digital watermarking as an effective countermeasure has been greatly developed and is now becoming the main mechanism to overcome these issues in digital image world [7, 13, 21, 26].

Traditionally, most image watermarking schemes only focus on one purpose, such as digital rights management (DRM) [3, 8, 22] or integrity verification [11, 12, 19]. In digital watermarking schemes used for DRM, a predefined string such as name of

✉ MingQuan Fan
1147955679@qq.com

[1] Southwest China Research Institute of Electronic Equipment, Chengdu, China

author or logo is adopted for robust watermark, research focus is whether the watermark could undergo various attacks, such as noise attack [2], synchronous attack [5], scraping attack [24], confusion attack [17], IBM attack [29], StirMark attack [18], etc. In digital watermarking schemes used for integrity verification, the early fragile watermarks mainly focus on the localization ability of tampered area, as well as the tampering localization precision [23], later fragile watermarks aim to accomplish both tasks of tampering localization and recovering the media information in the lost area [19]. Fewer image watermarking schemes aim to accomplish both tasks of DRM and integrity verification. It is hardly any research work carries out using dual watermarking strategy for multipurpose goals.

Liu et al. [20] used a combination of invisible watermarks to establish the owner's right to the image and detect the intentional and unintentional tampering of image. Chen et al. [6] proposed a novel general non-negative matrix factorization based digital watermarking scheme with one watermark, which could be used for both synchronous image authentication and copyright protection. In [1], authenticity and copyright of printed images are verified via image hashing and digital watermarking technique, and it is resilient against print-scan process distortions. Ayesha et al. [4] used the instability property of playfair cipher to achieve data authentication and ownership authentication in next generation wireless technology 5G. In [15], the copyright protection of media is taken care of by embedding a robust watermark using an efficient inter-block coefficient differencing algorithm, the authentication of the content has been ensured by embedding a fragile watermark in spatial domain. Ansari et al. [3] proposed non-blind dual watermarking for image authentication and copyright protection. To sum up, the present multipurpose watermarking schemes used for copyright protection and content authentication have given resolutions to the following technical difficulties: Malicious falsification can be detected effectively, and the tampered position of image can be located precisely. However, the current multipurpose image watermarking schemes have some shortcomings as follows: 1) Most schemes have no ability of tamper discrimination [1, 3, 15, 20]. 2) Almost all schemes do not have ability of tamper recovery [1, 3, 4, 6, 15, 20]. These shortcomings are not conducive to practical applications.

Aim to resolve these problems, we propose a blind dual image watermarking scheme for copyright protection, tamper proofing and self-recovery in this paper. For traditional predefined string such as name of author or logo has some limitations including less meaningful, intuitive for easily identifying and low correlative to owner for authentication [30], we use biometric of handwritten signature as robust watermark to enhance the credibility of conventional watermarking. Besides, refer to our recent work [10, 11], the fragile watermark includes three parts, the first part is composed of source encoder output bits used for image content self-recovery, the second part is composed of parity bits used for correcting the error of source encoder output bits, the last part is composed of check bits used for detecting tampered area of image. Experimental results demonstrate the effectiveness of the proposed watermarking scheme.

This paper proceeds as follows. Section 2 gives the robust watermark embedding, fragile watermark generation and embedding decision procedure. This is followed by fragile watermark extraction and content authentication, robust watermark extraction. We then give experimental results and security analysis in Section 4. Finally, we draw the conclusions.

2 Watermark embedding decision procedure

In this paper, we use dual watermarks for the goals of copyright protection, tamper proofing and self-recovery, etc. One is the binary biometric of handwritten signature used as robust watermark, the other is fragile watermark, generated from image itself and composed of three parts. The two watermarks embedding decision procedure are described as following.

Suppose $I = \{I(s,t)|1 \le s \le M, 1 \le t \le N\}$ represents the host image, and the handwritten signature is denoted as $W = \{W(m,n)|1 \le m \le M_1, 1 \le n \le N_1\}$, here, M, M_1, N, and N_1 are as the number of pixels for every column and row, respectively. The handwritten signature watermark embedding process is illustrated in Fig. 1. Details of embedding are elaborated as following:

Step1. Divide into blocks. First, the two LSB planes of host image I are set to zero, and denote the 6 MSB image content as I'. Then I' is equally split into non-overlapping blocks with size of $B_l \times B_l$, denoted as $I'_1(j,k)$, $j = 1,2,\cdots,M/B_l$, $k = 1,2,\cdots,N/B_l$, and $(M \times N/B_l^2) \ge M_1 \times N_1$.

Step2. DT-CWT. Perform the DT-CWT on each image block with T level to obtain the low frequency sub-band, denoted as $I'_2(j,k)$, $j = 1,2,\cdots,M/B_l$, $k = 1,2,\cdots,N/B_l$.

$$I'_2(j,k) = \text{DT-CWT}(I'_1(j,k), T) \tag{1}$$

Step3. DCT. Perform DCT on each low frequency sub-band to obtain hybrid domain coefficients, denoted as $I'_3(j,k)$, $j = 1,2,\cdots,M/B_l$, $k = 1,2,\cdots,N/B_l$.

Step4. Chaotic sequence. Based on key K_1, use Logistic map to generate pseudo-random sequence $Q = \{Q(r)|r = 1,2,\cdots,M_1 \times N_1\}$ with length of $M_1 \times N_1$, here, K_1 is the initial value of the adopted chaotic system.

Step5. Address sequence. The elements of Q are sorted in descending order, just as Eq. (2) shows:

$$\{Q_{a(1)},\cdots,Q_{a(r_0)},\cdots,Q_{a(M_1 \times N_1)}\} = \text{descend}\{Q(1),\cdots,Q(r),\cdots,Q(M_1 \times N_1)\} \tag{2}$$

where $a(r_0)$ is the address index of the sorted chaotic sequence, $1 \le a(r_0) \le M_1 \times N_1$.

Step6. Encrypt. According to the address sequence, the scrambled handwritten signature image W_e is obtained as follows:

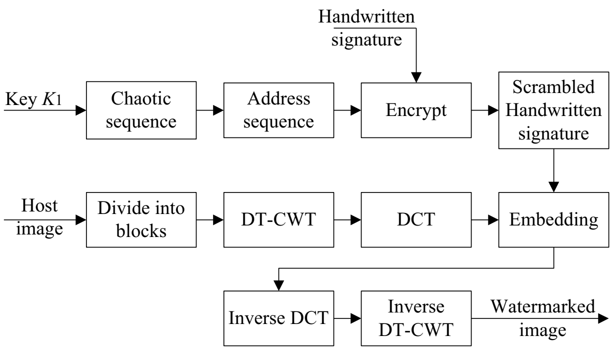


Fig. 1 Diagram of robust watermark embedding

$$W_e(p_1, q_1) = W(m, n) \tag{3}$$

where,

$$p_1 = \begin{cases} \lfloor a(r_0)/N_1 \rfloor, & if \quad \mod (a(r_0), N_1) = 0 \\ \lfloor a(r_0)/N_1 \rfloor + 1, & if \quad \mod (a(r_0), N_1) \neq 0 \end{cases} \tag{4}$$

$$q_1 = \begin{cases} N_1, & if \quad \mod (a(r_0), N_1) = 0 \\ a(r_0) - \lfloor a(r_0)/N_1 \rfloor \times N_1, & if \quad \mod (a(r_0), N_1) \neq 0 \end{cases} \tag{5}$$

and $r_0 = (m-1) \times N_1 + n, m = 1, 2, \cdots, M_1, n = 1, 2, \cdots, N_1$.

Step7. Embedding. Use odd–even quantization method to embed one scrambled distorted bit into DC current. Suppose F denotes the DC current, w is one scrambled distorted bit, F' denotes the modified DC current. Details of embedding are described as Eq. (6) shows. Where, $temp = \lfloor F/\Delta \rfloor$, Δ is the odd–even quantization step. The robustness of the watermark is improved as Δ increases. However, a larger Δ causes higher distortion. So there is a trade-off between robustness and imperceptibility in choosing the size of Δ.

$$F' = \begin{cases} (temp + 0.5) \times \triangle \ if \ w = \mod (temp, 2) \\ (temp - 0.5) \times \triangle \ if \ w \neq \mod (temp, 2) \ and \ F < (temp + 0.5) \times \triangle \\ (temp + 1.5) \times \triangle \ if \ w \neq \mod (temp, 2) \ and \ F \geq (temp + 0.5) \times \triangle \end{cases} \tag{6}$$

Step8. Inverse transforms. Inverse DCT and DT-CWT are orderly implemented on the watermarked coefficients to get watermarked image I_w.

Refer to our recent work [11], the fragile watermark generation and embedding process are illustrated in Fig. 2, details are elaborated as following.

Step9. Source Coding (SPIHT). We first simply divide image I_w into four non-overlapping blocks, denoted as IB_i, $i = 1, 2, 3, 4$. Then each image block IB_i is further divided into non-overlapping sub-blocks with size of $B \times B$, denoted as IB_{ij}, $i = 1, 2, 3, 4$, $j = 1, \cdots, T_0, T_0 = M \times N/(4B^2)$. Finally, the compression algorithm SPIHT is applied

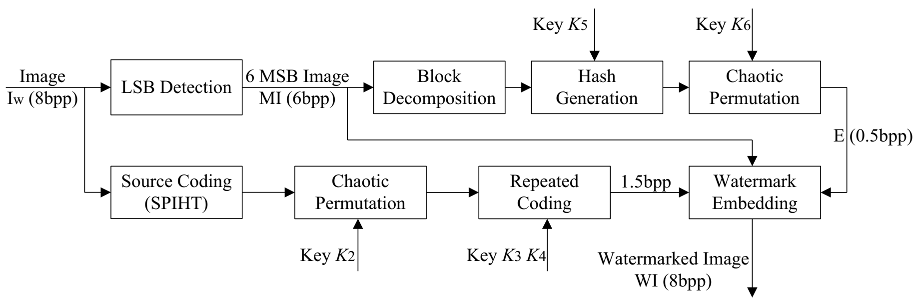


Fig. 2 The generic block diagram of the proposed fragile watermark generation and embedding using two LSB

on each image sub-block IB_{ij} rather than the whole image [25] with compression rate of 0.75 bpp (bit per pixel), we denote the source coding output bits of four image blocks as $S_{ij}(k), i = 1, 2, 3, 4, j = 1, \cdots, T_0, k = 1, \cdots, T_1, T_1 = 0.75 \times B^2$.

Step10. Chaotic Permutation (K_2). Based on key K_2, according to Step4 and Step5, get chaotic address index sequence $b = \{b(k_0)\}, 1 \le b(k_0) \le T_1, k_0 = 1, \cdots, T_1$. Then, scramble S_{ij} with address sequence, and denote the scrambled source encoder output bits as S'_{ij}, we have $S'_{ij}(k_0) = S_{ij}(b(k_0))$, here, K_2 is the initial value of the adopted chaotic system.

Step11. Repeated Coding. In order to correct the errors of source encoder output bits, we not only embed the source encoder output bits of one image sub-block into its own LSB image, but also embed it into LSB image of other image sub-block as parity bits. Take an example, for image sub-block IB_{1j_1}, we embed S'_{1j_1} and S'_{4j_4} into it, where, S'_{4j_4} belongs to image sub-block IB_{4j_4}. Here, $j_1 = (i-1) \times N/(2B) + j$, $j_4 = (c(i)-1) \times N/(2B) + d(j)$, $i = 1, \cdots, M/(2B)$, $j = 1, \cdots, N/(2B)$, $c = \{c(i) | 1 \le c(i) \le M/(2B)\}$ and $d = \{d(j) | 1 \le d(j) \le N/(2B)\}$ are the address indexes of the sorted chaotic sequences based on key K_3 and K_4, respectively. In this way, each image sub-block needs to be embedded with source encoder output bits and parity bits, they are in total 1.5 bpp.

Step12. LSB Detection and Block Decomposition. The two LSB planes of image I_w are set to zero, and the 6 MSB image is denoted as MI. Then the 6 MSB image MI is equally divided into non-overlapping image blocks with size of $B_0 \times B_0$, and each image block is denoted as $M_b(i,j), i = 1, \cdots, M/B_0, j = 1, \cdots, N/B_0$.

Step13. Hash Generation. The pseudo-code of this step is illustrated as follows:

```
Use Logistic map to generate pseudo-random sequence PS_1 based on key K_5
for k = 1 to MN/2
  if ps_1(k) ≥ 0.5
    ps_2(k) = 1
  else
    ps_2(k) = 0
  end
end
for i = 1 to M/B_0
  for j = 1 to N/B_0
    Perform Hash operation: {h_1 h_2 h_3 ··· h_j ··· h_n}_2 = hash{M_b(i,j), i, j}
    Obtain XOR value of each image block:
    H(p) = (h_1 h_2 ··· h_{n/n_1}) ⊕ (h_{n/n_1+1} h_{n/n_1+2} ··· h_{2n/n_1}) ⊕ ··· ⊕ (h_{n-n/n_1+1} h_{n-n/n_1+2} ··· h_n)
  end
end
Obtain check bits of whole image: D = {H(1) || H(2) || ··· || H(p)} ⊕ PS_2
```

where, $PS_1 = \{0 < ps_1(k) < 1 | k = 1, \cdots, MN/2\}$,$K_5$ is the initial value of the adopted chaotic system, $PS_2 = \{ps_2(k) \in \{0, 1\} | k = 1, \cdots, MN/2\}$, $\{h_1 h_2 h_3 \cdots h_j \cdots h_n\}_2$ is the output of Hash function, and $h_j \in \{0, 1\}$. The n-bit Hash value is equally divided into n_1 groups, and the length of each group is n/n_1. $p = 1, 2, \cdots, MN/{B_0}^2$, and $n/n_1 = {B_0}^2/2$, $D = \{D(k) \in \{0, 1\} | k = 1, \cdots, MN/2\}$.

Step14. Chaotic Permutation (K_6). In order to make the proposed scheme have ability of tampering discrimination, the check bits must be scrambled before being embedded into image. Based on key K_6, use method of Step10 to generate chaotic address sequence with length of $MN/2$, then check bits sequence D is permuted, and its scrambled version is denoted as $E = \{E(k) \in \{0, 1\} | k = 1, \cdots, MN/2\}$.

Step15. Watermark Embedding. For each image sub-block IB_{ij}, $i = 1, 2, 3, 4$, $j = 1, \cdots, T_0$, its own scrambled source encoder output bits S'_{ij} (0.75 bpp), parity bits (0.75 bpp) and check bits (0.5 bpp) are concatenated to replace the 2 LSB planes of cover image. In this way, we get the watermarked image WI.

3 Watermark Extraction Decision Procedure

The fragile watermark extraction and authentication process have no use for the cover image (LSB Embedding), and the watermark extraction is almost the reverse of watermark embedding process. The overall flowchart is shown in Fig. 3, and details are described as follows.

Step1. According to Step12 and Step13 in Section 2, based on key K_5, we get the compressed hash bits $H_2 = H_2(1)||H_2(2)|| \cdots ||H_2(p)$, $p = 1, 2, \cdots, MN/{B_0}^2$.

Step2. Watermark Decomposition. The two LSB planes of received image R are extracted, denoted as L. Then divide the LSB image L into four non-overlapping blocks, denoted as IL_i, $i = 1, 2, 3, 4$. In succession, each block IL_i is further divided into non-overlapping sub-blocks with size of $B \times B$, denoted as IL_{ij}, $i = 1, 2, 3, 4$, $j = 1, \cdots, T_0$, $T_0 = M \times N/(4B^2)$. Finally, extract source encoder output bits, parity bits and check

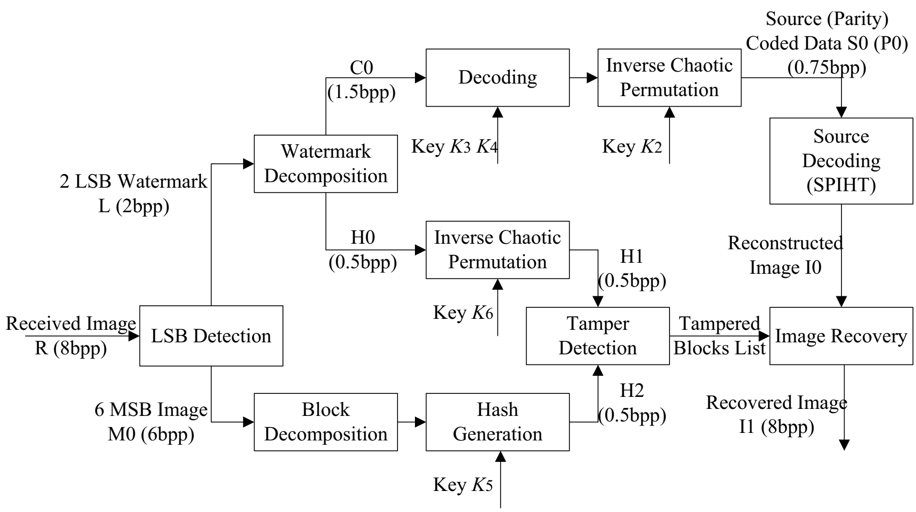


Fig. 3 Diagram of fragile watermark extraction and content authentication

bits from each sub-block, the source encoder output bits and parity bits are denoted as $C_0 = \{S_{11} + P_{11}, \cdots, S_{ij} + P_{ij}, \cdots, S_{4T_0} + P_{4T_0}\}$, and the check bits are denoted as $H_0 = \{H_{11}, \cdots, H_{ij}, \cdots, H_{4T_0}\}$.

Step3. Decoding. According to Step11 in Section 2, based on key K_3 and K_4, generate chaotic address sequences c and d, and extract source encoder output bits and parity bits from C_0, respectively. The source encoder output bits are denoted as S_0, and the parity bits are denoted as P_0.

Step4. Inverse Chaotic Permutation. Based on key K_6, use method of Step10 in Section 2 to generate chaotic address sequence with length of $MN/2$, and perform inverse permutation on H_0. Then we get the positive compressed hash bits $H_1 = H_1(1)||H_1(2)|| \cdots ||H_1(p), p = 1, 2, \cdots, MN/{B_0}^2$.

Step5. Tamper Detection. Use the reconstructed compression hash bits H_2 and the extracted compression hash bits H_1 to authenticate integrity of the received image.

Define the authentication sequence $Au = \{Au(r) \in \{0, 1\}\}$, $r = 1, 2, \cdots, MN/{B_0}^2$, and Au is obtained as follows:

$$Au(r) = \begin{cases} 0 \sum H_1(p) \oplus H_2(p) = 0 \\ 1 \sum H_1(p) \oplus H_2(p) \neq 0 \end{cases} \tag{7}$$

where $Au(r) = 1$ represents that the r th image block with size of $B_0 \times B_0$ is tampered, and $Au(r) = 0$ represents that the r th image block with size of $B_0 \times B_0$ is not tampered.

Step6. Image Recovery. If the r th image block with size of $B_0 \times B_0$ is tampered, then we can use corresponding source encoder output bits from S_0 to recover the tampered image content; if it unsuccessfully recovers the tampered image content by using source encoder output bits from S_0, we can use the corresponding parity bits from P_0 to recover the tampered image content.

The handwritten signature extraction process also does not need the original host image, and the overall flowchart is shown in Fig. 4, details are described as follows.

Step7. According to Steps 1–3 in Section 2, we get the low frequency sub-band hybrid domain coefficients. Suppose F^* denotes the DC current, w^* is the corresponding scrambled distorted bit, then $w^* = \text{mod}(\lfloor F^*/\Delta \rfloor, 2)$, in this way, scrambled binary image W_1 is obtained.

Step8. According to Steps 4–6 in Section 2, we get the address index sequence to restore original binary image W^* from the scrambled binary image W_1.

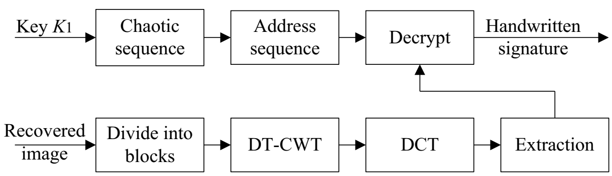


Fig. 4 Diagram of robust watermark extraction

(a) (b) (c)

Fig. 5 Cover images. (**a**) Cameraman. (**b**) Lena. (**c**) Boats

4 Experimental Results and Analysis

In our experiments, three 512×512 standard images "Cameraman", "Lena" and "Boats" are used as cover images to report results, shown in Fig. 5. A binary handwritten signature image with size of 54×75 is used as the robust watermark, shown in Fig. 6a. Let $B = 32$, $B_0 = 8$, $n_1 = 4$, $K_1 \sim K_6$ are the initial values of Logistic map, their range is $(0, 1)$.

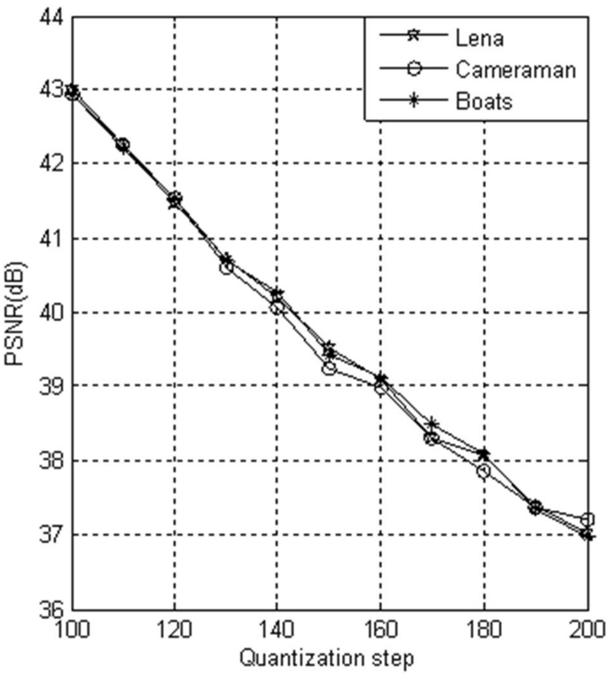
4.1 Select Suitable Quantization Step

Using the cover images as host image, a series of experiments have been performed to test the imperceptibility of watermarked image. Figure 7 shows the PSNR [9] values under various quantization steps, and it is known that the PSNR value is improved as quantization step Δ decreases. As a rough estimation, distortion of modified image with PSNR lower than 36 dB is noticeable to human visual system (HVS). From Fig. 7, it can be found that $[100, 200]$ is the suitable value range. When $\Delta = 120$, the PSNR values of the watermarked images "Cameraman", "Lena" and "Boats" are 39.5889 dB, 39.57 dB and 39.61 dB, respectively, and they are shown in Fig. 8. And as an example, Fig. 9 shows the reconstructed "Cameraman" images using source encoder output bits and parity bits, respectively. It can be seen that the reconstructed images are practicable. Figure 6b shows the extracted handwritten signature from watermarked Lena. Figure 6c shows the extracted handwritten signature from recovered Lena using source coding output bits.

(a) (b) (c)

Fig. 6 Binary handwritten signature. (**a**) Original handwritten signature. (**b**) Extracted handwritten signature from watermarked Lena. (**c**) Extracted handwritten signature from recovered Lena using source coding output bits

Fig. 7 The PSNR values under various quantization steps



4.2 Robustness Against Common Image Processing Operations

Robustness against common image processing operations is another important requirement of watermarking technique used for copyright protection. The robustness against common image processing operations means its ability to correctly detect the watermark from polluted watermarked image. Table.1 lists the BER [9] values under various common image processing operations, including median filtering(3×3) (I), wiener filtering(5×5) (II), supplement image (III), salt & pepper noise(0.003) (IV), adjustment of brightness(75) & contrast(50) (V), adjustment of brightness(150) & contrast(100) (VI). It can be found that the proposed scheme is robust against common image processing operations. Table.2 lists the BER values under JPEG compression with different quality factors, except quality factor as 10, other

(a) (b) (c)

Fig. 8 Watermarked images. (**a**) Cameraman. (**b**) Lena. (**c**) Boats

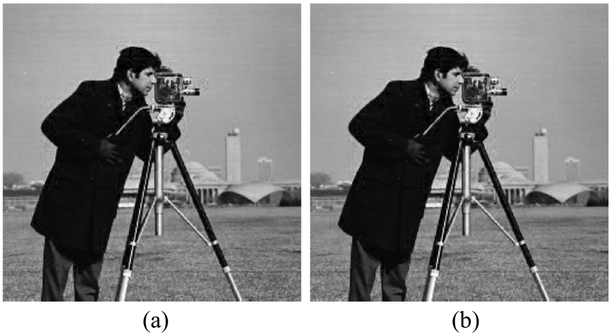


Fig. 9 **a** Reconstructed image using source encoder output bits. b Reconstructed image using parity bits

results are satisfactory. The results are compared with [9, 16], it is clear that our proposed scheme achieves great robustness against JPEG compression than existing excellent schemes.

4.3 Ability of Tampering Discrimination

In the proposed scheme, we use chaotic sequence to permutate check bits, in this way our proposed scheme can discriminate whether only the image content being tampered, or only the fragile watermark being changed, or they both being modified, while the scheme proposed in [25] does not have this ability. Figure 10a shows a tower is added in the watermarked image, the MSB image content and corresponding watermark bits are all changed; Fig. 10b shows only the watermark bits of the corresponding modification position in Fig. 10a are altered; Fig. 10c shows only the MSB image content is changed, while the corresponding watermark bits are all invariant. Figure 11a-c depict the detection results of check bits examination, they are corresponding to Fig. 10a-c. Figure 12 and Fig. 13 show the similar results with standard image "Lena" as test image. It can be found that when the MSB image content and watermark bits are all tampered, the difference image presents block areas and random dots, just as Fig. 11a and Fig. 13a, when only the watermark bits are tampered, the difference image presents only random dots, just as Fig. 11b and Fig. 13b, when only the MSB image content is tampered, the difference image only presents block areas, just as Fig. 11c and Fig. 13c.

4.4 Robustness Against Parity Bits Modification Attack

Compared with [25], in the proposed scheme, we perform SPITH on image blocks rather than the whole image. Hence, even if part of source encoder output bits are modified, it will not lead to the unsuccessful reconstruction of the whole image [25]. Besides, we use repeated coding method instead of RS coding [25], and embed source encoder output bits of one image block into other image block. With the center of image as the origin, we build a rectangular coordinate system, then the two image blocks belong to different quadrants.

Table 1 BER values under six attacks

	I	II	III	IV	V	VI
Cameraman	0.0348	0.0585	0	0.0277	0	0.0138
Lena	0.0067	0.0279	0	0.0200	0	0.0323
Boats	0.0200	0.0635	0.0062	0.0393	0.0079	0.0422

Table 2 BER values under JPEG attacks with different quality factor ($\Delta = 200$)

	JPEG(90)	JPEG(80)	JPEG(70)	JPEG(60)	JPEG(50)	JPEG(40)	JPEG(30)	JPEG(20)	JPEG(10)
Cameraman	0	0	0	0	0.0012	0.0017	0.0151	0.1148	0.4793
Boats	0.0064	0.0069	0.0067	0.0072	0.0064	0.0074	0.0101	0.1405	0.4696
Lena	0	0	0	0	0	0	0.0035	0.0407	0.3370
Lena[9]	0	0	0	0	0.0010	0.1553	0.2432	0.5010	0.5010
Lena[16]	0	0	0	0.007	0.007	0.02	0.15	0.38	0.62

The distance between two image blocks may ensure when one image block is maliciously tampered, the other image block is invariant, which enhances the possibility of successfully reconstructing image content. In this way, we not only enhance the protection of source encoder output bits, but also the parity bits, while scheme in [25] has no protection of parity bits. Figure 14a depicts the maliciously tampered image, Fig. 14b demonstrates the detection results of check bits examination, Fig. 14c demonstrates the reconstructed image, Fig. 14d demonstrates the recovered image. It can be found from Fig. 14b that only using source encoder output bits or using parity bits, it can not successfully reconstruct image content. Only simultaneously using source encoder output bits and parity bits, we can successfully reconstruct image content, just as Fig. 14c shows.

4.5 Security of Resisting Key Exhaustion Attack

In our scheme, we use chaotic sequences to select image blocks for repeated coding (K_3,K_4), permutate binary sequences (K_2,K_6) and encrypt binary sequence (K_1,K_5). The keys $K_1 \sim K_6$ are the initial conditions of Logistic map. Because these keys possess real-valued numbers, so a large number of non-periodic noise-like chaotic sequences can be generated. Let $10^{-\sigma}$ represent a micro-change of chaotic key value, then the key space is $1/10^{-\sigma} = 10^{\sigma}$. Here, $\sigma \in Z^{+}$ is a negative logarithm of changing the chaotic key. As an example, the chaotic sequence x_n is generated by K_1, and another chaotic sequence x'_n is generated by $\left(K_1 + 10^{-\sigma}\right)$. The function $\beta = \sum_{n=0}^{N-1} \left| x_n - x'_n \right| / N$ represents an average distance of two chaotic sequences with a tiny change of K_1, which is used to test the key space. The curve of β is shown in Fig. 15. We can

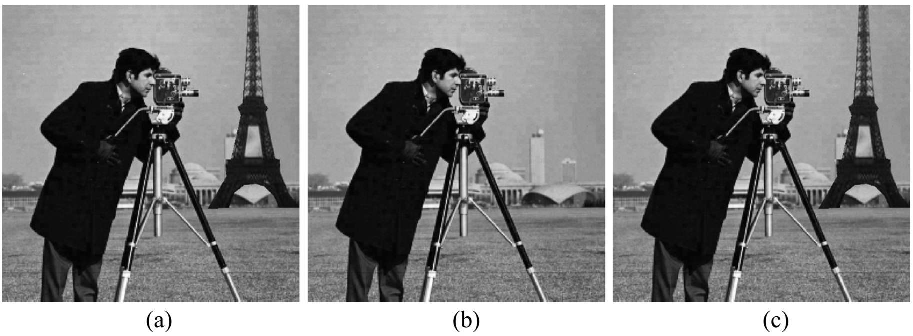


Fig. 10 **a** The maliciously tampered watermarked image “Cameraman” with MSB image content and watermark bits both being modified. **b** The watermarked image “Cameraman” with only the watermark bits being modified compared with Fig. 10a. **c** The watermarked image “Cameraman” with only MSB image content being modified compared with Fig. 10a

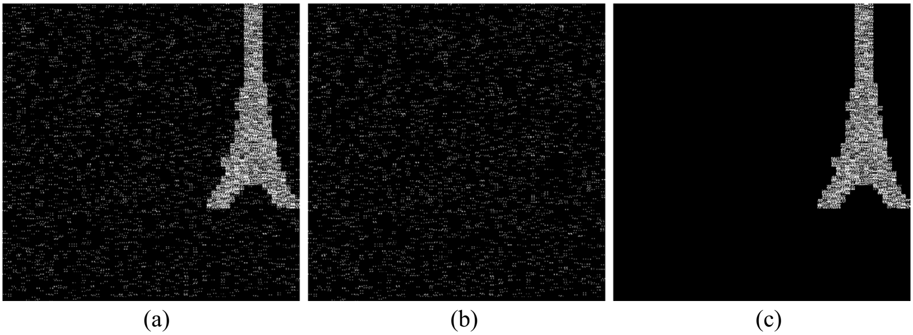


Fig. 11 **a** Detection result corresponding to Fig. 10a. **b** Detection result corresponding to Fig. 10b. **c** Detection result corresponding to Fig. 10c

Fig. 12 **a** The maliciously tampered watermarked image "Lena" with MSB image content and watermark bits both being modified. **b** The watermarked image "Lena" with only the watermark bits being modified compared with Fig. 12a. **c** The watermarked image "Lena" with only MSB image content being modified compared with Fig. 12a

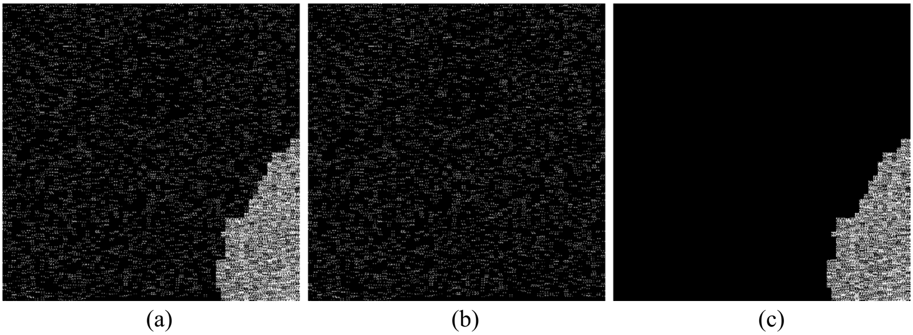


Fig. 13 **a** Detection result corresponding to Fig. 12a. **b** Detection result corresponding to Fig. 12b. **c** Detection result corresponding to Fig. 12c

easily see that when the tiny change of $K_1 \sim K_6$ is equal to 10^{-19}, β value is gradually approach zero, which means there are part of chaotic initial parameters can result in the same chaotic sequences. So we know that the key spaces of $K_1 \sim K_6$ are all 10^{19}, and the whole key space of the watermarking scheme is 10^{114}, it is large enough to ensure the security.

4.6 Comparisons with other Existing Multipurpose Watermarking Schemes

The dual watermarking scheme contains both robust watermarking and fragile watermarking is proposed to address four objectives: copyright/ownership protection, tamper localization, self-recovery, and tamper discrimination. To the best knowledge of authors, it is the multipurpose watermarking scheme that addresses the most objectives. The multipurpose nature makes it be useful for different applications at the same time. In this section, the

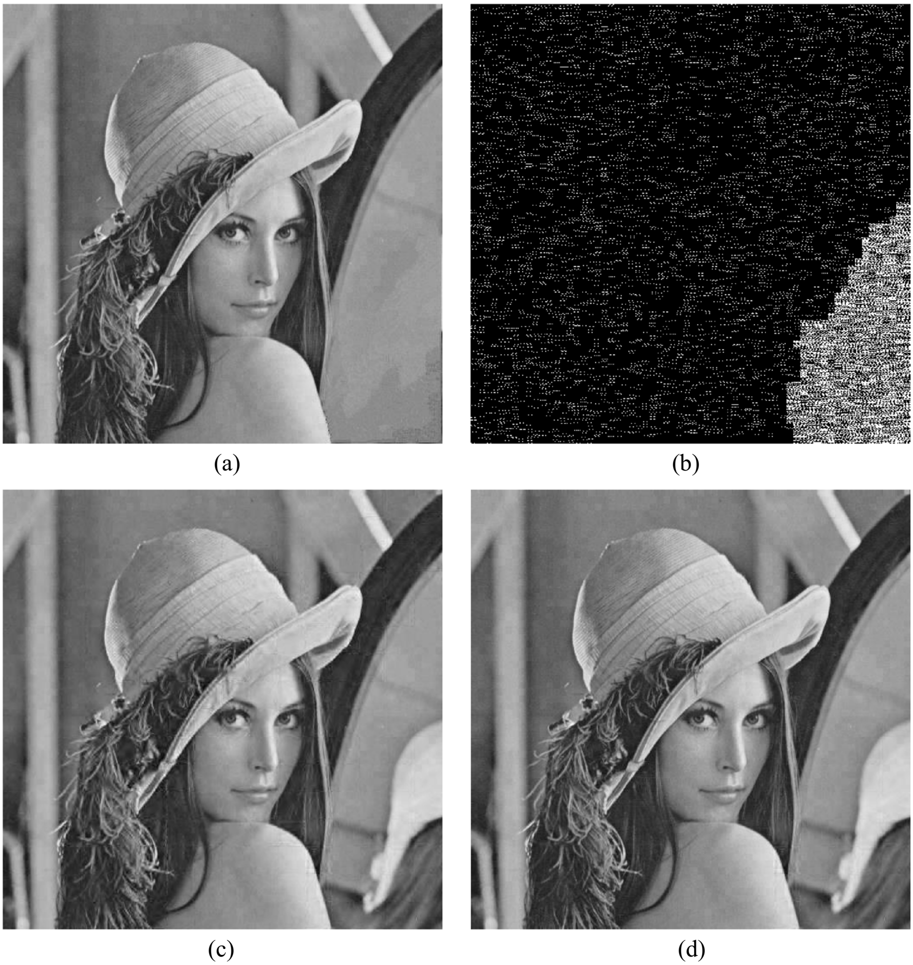


Fig. 14 **a** The maliciously tampered watermarked image with MSB image content and watermark bits both being modified. **b** Detection result corresponding to Fig. 14a. **c** Reconstructed image using source encoder output bits and parity bits. **d** The recovered tampered image content

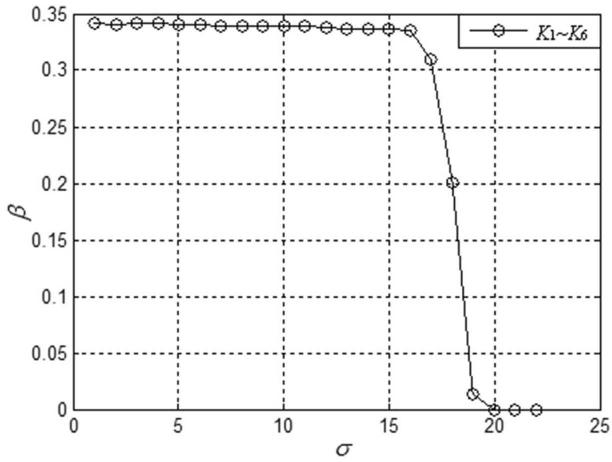


Fig. 15 Key space of keys K_1 ~ K_6

superior performance of the proposed scheme is demonstrated by comparing its functionality with that of the related well-known dual watermarking mechanisms [6, 14, 20, 27, 28]. Table.3 illustrates the different functionalities of the multipurpose mechanisms.

The first difference between the six schemes is that scheme [6] is non-blind and it only uses one watermark, whereas other schemes use dual watermarks, and the PSNR of our scheme belongs to range (37, 43). In Table.3, "~" means approximately, the robustness and security become strong with the large number of "☆". In our scheme, the security relies on system keys, and the keyspace is large enough to ensure that the security of our scheme is better than other schemes. On the other hand, our scheme is robust against most common image processing operations, especially the JPEG compression, it can obtain four stars. Besides, our scheme has ability of tamper discrimination ability, whereas all current other excellent schemes do not have. Thus, after considering the global functionality, our proposed scheme is demonstrably superior.

Table 3 Comparisons between the proposed scheme and other multipurpose schemes

Functionality	Ref. [20]	Ref.[6]	Ref [27]	Ref.[14]	Ref.[28]	This work
Nature	Blind	Non-blind	Blind	Blind	Blind	Blind
Embedding Domain	Transform Spatial	Transform	Transform Spatial	Transform Transform	Transform Spatial	Transform Spatial
Visibility	Invisible Invisible	Invisible	Invisible Invisible	Invisible Invisible	Invisible Invisible	Invisible Invisible
Watermark Type	Robust Fragile	Semi-fragile	Robust Fragile	Robust Semi-fragile	Robust Fragile	Robust Fragile
PSNR	~40	~36	~30	~38	~41	(37,43)
Robustness	☆☆☆	☆☆☆	☆☆☆☆	☆☆☆	☆☆☆☆	☆☆☆☆
Copyright Protection	Yes	Yes	Yes	Yes	Yes	Yes
Image Authentication	Yes	Yes	Yes	Yes	Yes	Yes
Image Restoration	No	No	Yes	No	Yes	Yes
Tamper Discrimination	No	No	No	No	No	Yes
Security	☆☆	☆☆	☆☆☆	☆☆	☆☆☆☆	☆☆☆☆☆
Host Image	Color	Gray	Gray	Gray	Gray	Gray

5 Conclusions

In this correspondence, we present a blind dual image watermarking scheme for copyright protection, tamper proofing and self-recovery. We use binary handwritten signature as robust watermark, and embed it into hybrid domain constructed by DT-CWT and DCT, experimental results show its robustness against common image processing operations, especially the robustness against JPEG compression is better than current excellent schemes. Furthermore, we adopt SPHIT, repeated coding and hash to generate three parts of fragile watermark. Compared with Sarreshtedari's work, we perform SPIHT on image blocks rather than the whole image, in this way, even if part of source encoder output bits are modified, it can not lead to the unsuccessful reconstruction of the whole image. Besides, the adoption of repeated coding method can protect both source encoder output bits and the parity bits, while Sarreshtedari's work only emphasized the protection of source encoder output bits. Moreover, the employment of chaotic system in the proposed scheme makes it have the ability of tampering discrimination. Experimental results show the effectiveness of our proposed scheme. However, our proposed scheme also has limitation of poor robustness performance against rotational attack, future work will focus on this problem and extend our scheme for color images.

Data Availability The raw data required to reproduce the above finding cannot be shared at this time as the data also forms part of an ongoing study.

Declarations

Conflict of interests The author declares that there are no conflict of interests, and does not have any possible conflicts of interest. Furthermore, the datasets generated during and/or analysed during the current study are available from the corresponding author on reasonable request.

References

1. Ahmad F, Cheng LM (2018) Authenticity and copyright verification of printed images. Signal Processing, pp 322–335
2. Ahmaderaghi B, Kurugollu F, Rincon JMD et al (2018) Blind image watermark detection algorithm based on discrete shearlet transform using statistical decision theory. IEEE Trans Comput Imag 4:46–59
3. Ansari IA, Pant M (2017) Multipurpose image watermarking in the domain of DWT based on SVD and ABC. Pattern Recogn Lett 94:228–236
4. Ayesha SK, Masilamani V (2018) A novel digital watermarking scheme for data authentication and copyright protection in 5G networks. Comput Electri Engin, pp 589–605
5. Chen Y, Jia ZG, Peng Y, et al. A new structure-preserving quaternion QR decomposition method for color image blind watermarking, Signal Proc. https://doi.org/10.1016/j.sigpro.2021.108088
6. Chen ZG, Peng HP, Liu YH et al (2018) A novel digital watermarking based on general non-negative matrix factorization. IEEE Trans Multimed 20:1973–1986
7. Chen B, Lu W, Huang JW et al (2022) Secret sharing based reversible data hiding in encrypted images with multiple data-hiders. IEEE Trans Dependable Secure Comput 19:978–991
8. Divya Shivani JL, Senapati RK (2017) Robust image embedded watermarking using DCT and listless SPIHT. Future Internet, 33. p1–16
9. Ernawan F, Kabir MN (2018) A robust image watermarking technique with an optimal DCT-psycho visual threshold. IEEE Access 6:20464–20480
10. Fan MQ (2019) A source coding scheme for authenticating audio signal with capability of self-recovery and anti-synchronization counterfeiting attack. Multimed Tools Appli. https://doi.org/10.1007/s11042-019-08095-x

11. Fan MQ, Wang HX (2018) An enhanced fragile watermarking scheme to digital image protection and self-recovery. Sig Proc: Image Comm 66:19–29
12. Faranak T, Manoranjan P, Mohammad RH (2021) Detection and recovery of higher tampered images using novel feature and compression strategy. IEEE Access 9:57510–57528
13. Guo YF, Au OC, Wang R et al (2018) Halftone image watermarking by content aware double-sided embedding error diffusion. IEEE Trans Image Proc 27:3387–3402
14. Haghighi B, Taherinia AH, Harati A et al (2021) WSMN: an optimized multipurpose blind watermarking in shearlet domain using MLP and NSGA-II. Appl Soft Comput 101:1–23
15. Hurrah NN, Parah SA, Loan NA (2019) Dual watermarking framework for privacy protection and content authentication of multimedia, Future Generation Computer Systems, pp 654–673
16. Jamali M, Rafiee S, Soroushmehr SMR et al. Adaptive blind image watermarking using fuzzy inference system based on human visual perception, arXiv:1709.06536
17. Khaled L, Ahmed R, Khalil Z (2017) Ambiguity attacks on robust blind image watermarking scheme based on redundant discrete wavelet transform and singular value decomposition. J Electri Syst Inform Technol 4:359–368
18. Khushwant S, Samriddhi R, Ashutosh M et al (2021) Robust and secure digital image watermarking technique using Arnold transform and memristive chaotic oscillators. IEEE Access 9:72465–72483
19. Laouamer L, Tayan O (2018) Performance evaluation of a document image watermarking approach with enhanced tamper localization and recovery. IEEE Access 6:26144–26166
20. Liu XL, Lin CC, Yuan SM (2018) Blind dual watermarking for color images' authentication and copyright protection. IEEE Trans Circuits Syst Video Technol 28:1047–1055
21. Loan NA, Hurrah NN, Parah SA et al (2018) Secure and robust digital image watermarking using coefficient differencing and chaotic encryption. IEEE Access 6:19876–19897
22. Magdy M, Neveen IG, Said G et al (2022) Multiple zero-watermarking of medical images for internet of medical things. IEEE Access 10:38821–38831
23. Nandhini S, Omar E, Somaya A et al (2021) Image steganography: a review of the recent advances. IEEE Access 9:23409–23423
24. Rudman K, Bonenfant M, Celik M et al (2016) Toward real-time detection of forensic watermarks to combat piracy by live streaming. SMPTE Motion Imag J 125:34–41
25. Saeed S, Mohammad AA (2015) A source-channel coding approach to digital image protection and self-recovery. IEEE Trans Image Proc 24:2266–2277
26. Shehab A, Elhoseny M, Muhammad K et al (2018) Secure and robust fragile watermarking scheme for medical images. IEEE Access 6:10269–10278
27. Singh P, Agarwal S (2017) A self recoverable dual watermarking scheme for copyright protection and integrity verification. Multimed Tools Appli 76:6389–6428
28. Sinhal R, Ansari IA (2022) Multipurpose image watermarking: ownership check, tamper detection and self-recovery. Circuits Syst Signal Proc 41:3199–3221
29. Su QT, Liu DC, Yuan ZH et al (2019) New rapid and robust color image watermarking technique in spatial domain. IEEE Access 7:30398–30409
30. Wu YD, Weng J, Wang ZX, et al. Attacks and countermeasures on privacy-preserving biometric authentication schemes, IEEE Trans Dependable Sec Comput. https://doi.org/10.1109/TDSC.2022.3162623