Circuits, Systems, and Signal Processing (2022) 41:3199–3221
https://doi.org/10.1007/s00034-021-01926-z

Multipurpose Image Watermarking: Ownership Check, Tamper Detection and Self-recovery

Rishi Sinhal[1] · Irshad Ahmad Ansari[1]

Received: 12 June 2021 / Revised: 29 November 2021 / Accepted: 30 November 2021 /
Published online: 20 January 2022

Abstract

In the present digital scenario, false ownership claims and tampering with digital data have become serious concerns for users. There have been a very few schemes proposed in the past that can provide solutions for the three major requirements (ownership proof, tamper detection and self-recovery) in an efficient way. This paper presents a blind multipurpose image watermarking scheme for copyright/ownership protection, image authentication, and image restoration. Two different watermarking strategies (robust and fragile) are used to achieve the multipurpose nature. For Robust watermark insertion, an encrypted watermark is inserted into the host image using IWT (Integer wavelet transform). Afterward, a 9-base notation-based least significant bit replacement approach is used to embed the fragile sequence along with recovery information in a controlled randomized manner. During the testing phase, high imperceptibility, decent robustness, and good self-recovery are noticed against different types of attack. The scheme provides nearly 99.8% accurate tamper localization and can significantly recover even a severely tampered (up to 80%) image. The performance comparison with other existing watermarking schemes confirms the superiority of the proposed scheme. The multipurpose nature of the scheme makes it versatile and practical for the current scenario of digital technologies and era of internet.

Keywords Multipurpose image watermarking · Integer wavelet transform · Copyright protection · Image authentication · Image restoration

✉ Irshad Ahmad Ansari
irshad@iiitdmj.ac.in

Rishi Sinhal
rishi.sinhal.jec@gmail.com

[1] Electronics and Communication Engineering, PDPM Indian Institute of Information Technology Design and Manufacturing, Jabalpur, MP 482005, India

1 Introduction

With the advancement in digital technologies, the use of social media becomes very common in our day to day life. The uploading of images on social media platforms is one of the primary ways for information sharing in the present time. These images need to be protected against wrongful ownership claims. At the same time, they must have the ability to detect tampering and self-recovery (in case attackers modifies the content) [23]. Images are main communication medium over the social media. Therefore, the safe communication of digital images needs to be assured by using highly secured digital technologies. The copyright protection [29], image authentication [30], and the recovery of the altered portion of the image [28] are some of the imperative matters that need serious attention with the increase in the digital industry. The security of digital images against attacks is an important research area among researchers, which results in a wide verity of solutions like digital watermarking [27], steganography [14], and cryptography [5]. Watermarking provides many advantages over other methods including key-based verification and access control [18].

Digital image watermarking is the process of inserting watermark data (e.g., digital data) into the image [4]. The watermark data are extracted from the watermarked image at the time of extraction. Digital watermarking can be divided into different categories. The watermarking schemes are widely used in healthcare, secure communication, and other areas [4, 5, 18]. Digital watermarking offers verification of ownership/copyright and image integrity, which is mandatory in the current era of digital media communication. Let us suppose, a person (owner) uploads an image on a social media platform. If the image is publically available (this is mostly the case), attacker can easily modify, tamper, and claim false ownership of the image. If a proper watermarking protection is provided (before upload), the owner can verify the ownership (using secret key), prove its authenticity and recover the tampered regions. Figure 1 represents this same process graphically.

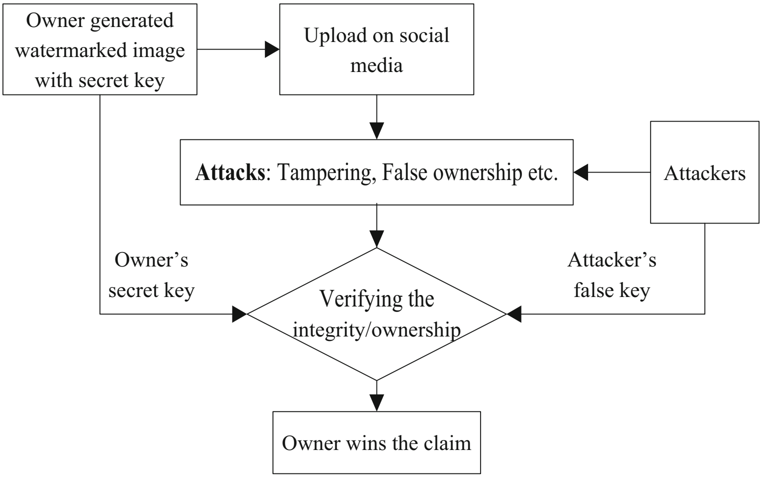

Owner generated watermarked image with secret key
Upload on social media
Attacks: Tampering, False ownership etc.
Attackers
Owner's secret key
Verifying the integrity/ownership
Attacker's false key
Owner wins the claim

Fig. 1 Image security/verification using digital image watermarking

The rapid development of digital era demands more advanced watermarking methods; having multipurpose nature for various applications. Multipurpose watermarking schemes help to achieve multiple objectives simultaneously, which make it more convenient for practical applications [16]. In the literature, many multipurpose image watermarking methods have been proposed [1, 2, 6, 7, 10, 11, 15–17, 19, 24–26, 32–35], but very limited work has been done on methods that can simultaneously solve three main objectives: ownership proof, tamper detection, and tamper recovery [2, 24]. In addition, solving three objectives with blind nature and good imperceptibility is still the most challenging task in watermarking domain. Therefore, a multipurpose image watermarking is proposed in this work to address three objectives (copyright/ownership protection, tamper localization, and self-recovery) in an efficient and blind manner with good imperceptibility. The main contributions of this work are as follows:

1. To the best knowledge of authors, first blind multipurpose (with three objectives) scheme with imperceptibility ~ 41 dB.
2. Even after multipurpose nature, excellent image restoration even for severely tampered images (up to 80% tampered).
3. Average tamper localization is found to be around 99.8%.
4. Very good robustness even after multipurpose nature.

2 Literature Review

Generally, the robust watermarking schemes are used for copyright/ownership verification. Mostly transform domain schemes (i.e., Fourier Transform (FT), Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), Lifting Wavelet Transform (LWT), Integer Wavelet Transform (IWT), etc.) have been preferred over spatial domain approaches to get high robustness [2, 15, 24]. IWT maps integer values to integers with no rounding-off error. Thus, it reduces the loss of information due to round-off errors and performs efficiently as compare to counterpart transforms [3, 13, 36]. The fragile watermarking detects tamper/forged region and authenticate the image [35]. Some of the advanced fragile schemes also offer self-recovery of the image by inserting the recovery data with the fragile watermark during embedding [32–35]. Multipurpose schemes fulfill two or more requirements at the same time. Normally, robust and fragile mechanisms are combined in a single scheme to get the multipurpose nature [2, 24].

To the best knowledge of authors, Lu and Liao [16] presented first ever multipurpose watermarking scheme in 2001 that can be used for image authentication and copyright protection. The watermark embedding was based on the quantization of wavelet coefficients. The scheme has blind nature and acceptable results to a certain limit. However, the discussion on the security issues and feature of image restoration were not provided. Zhu et al. [35] offered a semi-fragile scheme for image watermarking to provide image authentication and restoration. In this scheme, the Pinned Sine Transform (PST) was used to embed authentication watermark and restoration of image was considered as an irregular sampling issue. The repetitive projections onto convex were used to reconstruct the tampered blocks. However, the performance was limited to low tampering rate. Zhang and Wang [32] introduced a fragile image watermarking method for authentication and restoration of the image. The embedding process was based on differential expansion (DE). The image restoration was limited to the tampering rate less < 3.2% (very low). Additionally, the visual quality of the watermarked image was also low (approx. 28 dB). Zhang et al. [33] offered two fragile image watermarking methods using the reference sharing mechanism for digital images. The first method performed efficiently for very low tampering rate (i.e., < 24%). The second scheme used adaptive restoration along with the reference sharing to get efficient results for the tampering rate < 66%.

Zhang et al. [34] presented a watermarking scheme for tamper localization and self-recovery. The method was based on compressive sensing, DCT, and Composite reconstruction. The imperceptibility of the scheme was significant, but the image restoration was limited to a tampering rate of less than 60%. Ansari et al. [1] presented a watermarking technique for tamper localization and self-recovery of the tampered regions. It was based on the spatial domain, block-wise division, singular value decomposition (SVD), and LSB bit replacement. The scheme has given significant results. However, the scheme's ability to restore the image has been limited to the tampering rate of 50%. Mehta et al. [17] offered a watermarking scheme based on LWT, QR decomposition, and LSVR (Lagrangian Support Vector Regression) for protecting ownership/copyright. The robust watermark has been secured by using AT (Arnold Transform). Acceptable experimental outcomes in terms of robustness have been achieved but the scheme has only robust nature, and therefore, it could not be used for tamper detection and self-recovery. Liu et al. [15] proposed a multipurpose watermarking scheme to offer copyright protection and image authentication. The scheme was based on DWT, luminance quantization, and an efficient LSB replacement procedure. Results showed the effectiveness of the scheme but it was not secured against block-based attacks due to lack of organized randomness in fragile sequence, and block-based self-authentication. Furthermore, it lacked in restoring the tampered images. Singh and Agarwal [24] offered a multipurpose scheme that can be used for copyright protection, image authentication, and self-recovery. The chaotic map and DCT were used to provide security and quantization, respectively. The scheme provided high robustness but the imperceptibility was poor ($\leq$ 30 dB). Even the image restoration was limited to a tampering rate of less than 50%. Ansari and Pant [2] established a non-blind multipurpose watermarking for gray images using DWT, SVD. The scheme had acceptable results to protect copyright and check authenticity, along with significant imperceptibility. Yet the considerable image restoration can be attained only for a tampering rate < 50%. Also, the non-blind mechanism made it impractical. Islam and Laskar [10] introduced an image watermarking technique using LWT and SVD. To extract the watermark, SVM (support vector machine)-based binary classification process was applied. Experimental outcomes proved that significance in terms of robustness and imperceptibility, but the embedding capacity (payload) was low. Additionally, the scheme was unable to provide tamper detection and self-recovery features. Singh and Singh [25] presented a BTC (block truncation coding)- and quantization-based fragile watermarking technique for digital images, which can be used for tamper localization and image recovery. Results demonstrated effective authentication and recovery, but the significant image restoration was possible only for the tampering of less than 50%.

Qin et al. [19] offered a novel fragile image watermarking method using non-uniform watermark sharing and OIBTC (optimal iterative block truncation coding). Although the results showed significant outcomes in terms of tamper detection and image recovery but similarly to [1] and [25], the restoration condition required tampering rate $\leq$ 50%. Islam et al. [11] proposed a watermarking scheme for copyright protection of digital images based on LWT. To extract the robust watermark, SVM classifier has been employed. The scheme gave considerable results; however, the embedding payload (capacity) of the scheme was significantly low and multipurpose nature was also not there. Haghighi et al. [7] offered a blind multipurpose image watermarking method based on Shearlet transform using MLP and NSGA-II algorithms. The embedding threshold and blocks got selected using an optimization approach for watermarking. The method provided good results for copyright protection/image authentication to a certain limit against attacks. However, the method did not provide image restoration capability. Daneshmandpour et al. [6] introduced a fragile scheme for tamper detection and self-recovery of gray images. The detection of tampering in the images was based on the cyclic redundancy check (CRC), whereas the image recovery process was based on Embedded Zero Block Coding (EZBC), bit streaming and rate allocation. Although a multi-scale recovery process provides acceptable results, the scheme can't tolerate tampering more than 72%. Additionally, the scheme used the block size of 8 × 8 for watermarking, which reduces the detection accuracy significantly.

With reference to the above discussed literature, it is quite evident that the multipurpose watermarking is still an open and challenging research area. Existing schemes are unable to provide an acceptable solution for ownership protection, image authentication, and image restoration simultaneously. Even though a few existing schemes such as [24] and [2] fulfill all three purposes, yet they have other serious limitations. For example, [24] has poor imperceptibility and [2] has a non-blind mechanism that required the original host for the extraction process. The proposed work offers a blind multipurpose scheme to provide effective solutions for the mentioned issues without compromising the performance.

3 Proposed Scheme

The proposed scheme has four main parts: (1) Watermark preparation, (2) Watermark embedding, (3) Watermark extraction (for ownership and tamper check), and (4) Image self-recovery. Robust watermark is embedded in the transform domain using IWT after double layers of encryptions (using Arnold Transform (AT) [31] and XOR key). Encryption provides extra security to the robust watermark. Fragile watermark is embedded using 9-base notation-based least significant bit replacement [15]. Each part of the proposed framework is explained in detail as follows:

3.1 Watermark Preparation

In the proposed scheme, the pseudo-random binary sequences are used for robust watermark encryption (XOR-based) and fragile watermarking. In context to digital image watermarking, the pseudo-random binary representation helps to secure the watermarking system against illegal reach. Further, it improves the robust watermarking results against cropping, content removal, and other common attacks. In terms of fragile watermarking, it improves the authentication results in an effective manner against copy-move, copy-paste, and other types of tampering attacks. Moreover, it ensures the authenticity and safety of the digital data because no one can decrypt or access the data in its actual form without the knowledge of the secret key. Thus, the pseudo-random binary sequences can be effective in order to get better results with added security in digital watermarking schemes. Mersenne Twister (MT) is one of the widely used PRNG (pseudo-random number generation) algorithms [12, 21]. The sequence obtained by PRNG generator remains deterministic in nature and can be reproduced by using the initial value (i.e., seed value). A variant of MT algorithm known as SFMT (SIMD-Oriented Fast Mersenne Twister) is used in this work because of its faster speed and improved equi-distribution feature [22]. SFMT generates floating-point numbers ranging between 0 and 1, each element ($\mathrm{Num}_{\mathrm{val}}$) of the sequence is converted into $\mathrm{Bin}_{\mathrm{val}}$ (i.e., binary value 0 or 1) using Eq. (1).

$$\mathrm{Bin}_{\mathrm{val}} = \begin{cases} 0 \text{ if } \mathrm{Num}_{\mathrm{val}} < 0.5 \\ 1 \text{ if } \mathrm{Num}_{\mathrm{val}} \geq 0.5 \end{cases} \tag{1}$$

This generated $\mathrm{Bin}_{\mathrm{val}}$ is used in robust as well as fragile watermark preparation for different purposes, which are discussed in following sections.

3.1.1 Robust Watermark Preparation

The robust watermark W_{robust} (i.e., binary image of size 32 × 32) is encrypted to get better security against unauthorized access. At first, AT transform is applied on the robust watermark for K_1 (secret key-1) times. It converts W_{robust} to scrambled noisy form W_{AT}. Next, a random binary sequence $W_{\mathrm{ran\_1}}$ is produced using K_2 (secret key-2) with the help of SFMT generator of length 32 × 32. Next, XOR operation is performed between corresponding bits of $W_{\mathrm{ran\_1}}$ and W_{AT}, which generates $W_{\mathrm{encrypted}}$ (of size 32 × 32). The process of robust watermark preparation and encrypted robust watermark are shown in Fig. 2a, b, respectively. Only correct keys (K_1 and K_2) can decrypt the robust watermark to original form.

3.1.2 Fragile Watermark Preparation

The host image is divided into 2 × 4 size non-overlapping blocks (total blocks = TB).A random binary sequence $W_{\mathrm{ran\_2}}$ is produced using K_3 (secret key-3) with the help of SFMT generator of length 6 × TB. The average blocks intensities of every 2 × 4 are converted into 8-bit binary representation. 6 MSB (most significant bit) of these

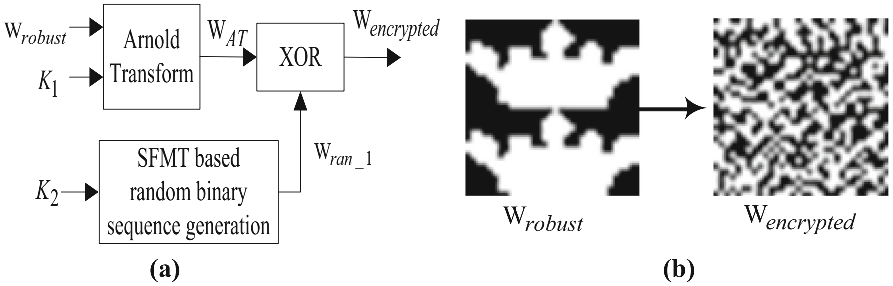


Fig. 2 **a** Robust watermark preparation. **b** The robust watermark and its encrypted watermark

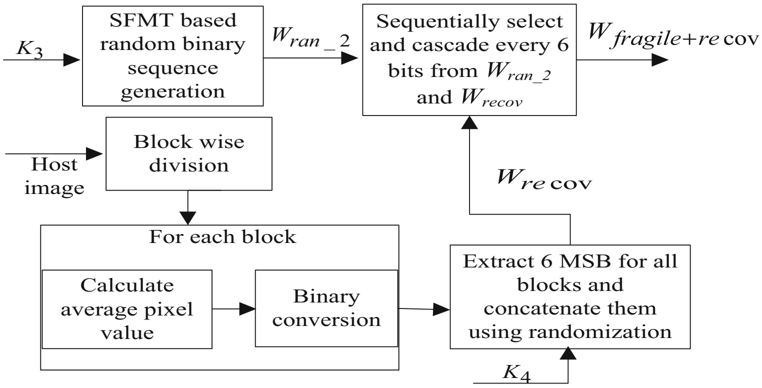

K_3
SFMT based random binary sequence generation
W_ran_2
Sequentially select and cascade every 6 bits from W_ran_2 and W_recov
W_fragile+recov
Host image
Block wise division
W_recov
For each block
Calculate average pixel value
Binary conversion
Extract 6 MSB for all blocks and concatenate them using randomization
K_4

Fig. 3 Fragile watermark preparation in order to preserve the recovery data along with the authentication data

8 bits are concatenate in a controlled randomized manner using K_4 (secret key-4) to generate recovery watermark data (W_{recov}). Now, Every 6 bits from both sequences (i.e., $W_{\text{ran\_2}}$ and W_{recov}) and cascaded. Finally, the combined watermark $W_{\text{fragile+recov}}$ is obtained from this cascading. Figure 3 presents the process of generating the watermark $W_{\text{fragile+recov}}$.

3.2 Watermark Embedding

The watermark insertion (Robust and Fragile) process is described as follows.

3.2.1 Robust Embedding

The following steps show the embedding of the robust watermark (i.e., $W_{\text{encrypted}}$) into the host image.

Step-1 Divide the host image into 16 × 16 size non-overlapping blocks.

Step-2 Apply IWT transform on the first block to get LL, LH, HL, and HH bands. Again apply IWT on the LH band to get LL1, LH1, HL1, and HH1.

Step-3 Calculate modification coefficients using Eq. (2).

$$M_{\text{coeff-1}} = {}^{\{\alpha - (\text{HL1}_{\text{avg}} - \text{LH1}_{\text{avg}})\}}\!/_{2} \text{ and } M_{\text{coeff-2}} = {}^{\{\alpha - (\text{LH1}_{\text{avg}} - \text{HL1}_{\text{avg}})\}}\!/_{2} \quad (2)$$

Here, α is the embedding parameter, LH1_{avg} and HL1_{avg} denote average value of pixels of LH1 and HL1, respectively.

Step-4 Embed first bit of $W_{\text{encrypted}}$ by updating the LH1 and HL1 coefficients using Eq. (3) and Eq. (4).

$$\text{LH1}(x, y) = \begin{cases} \text{LH1}(x, y) - M_{\text{coeff-1}} & \text{if } w\_\text{bit} = 1 \text{ and } \text{HL1}_{\text{avg}} - \text{LH1}_{\text{avg}} < \alpha \\ \text{LH1}(x, y) + M_{\text{coeff-2}} & \text{if } w\_\text{bit} = 0 \text{ and } \text{LH1}_{\text{avg}} - \text{HL1}_{\text{avg}} < \alpha \\ \text{LH1}(x, y) & \text{otherwise} \end{cases} \quad (3)$$

$$\text{HL1}(x, y) = \begin{cases} \text{HL1}(x, y) + M_{\text{coeff-1}} & \text{if } w\_\text{bit} = 1 \text{ and } \text{HL1}_{\text{avg}} - \text{LH1}_{\text{avg}} < \alpha \\ \text{HL1}(x, y) - M_{\text{coeff-2}} & \text{if } w\_\text{bit} = 0 \text{ and } \text{LH1}_{\text{avg}} - \text{HL1}_{\text{avg}} < \alpha \\ \text{HL1}(x, y) & \text{otherwise} \end{cases} \quad (4)$$

Step-5 Perform inverse IWT operation twice to get the robust watermarked block.

Step-6 Repeat steps 2, 3, 4, and 5 for each block to embed each bit of $W_{\text{encrypted}}$ in blocks sequentially.

Step-7 Finally combine the blocks to generate the robust watermarked image (Watermarked_r).

3.2.2 Fragile Embedding

The following steps show the embedding of the watermark ($W_{\text{fragile+recov}}$) into the image (Watermarked_r).

Step-1 Divide the *image* (Watermarked_r) into 2 × 4 size of non-overlapping blocks. Then, sequentially select 12 bits of watermark data from $W_{\text{fragile+recov}}$ for each block.

Step-2 Choose the first block and consider that each column is representing a pixel unit (with 2 pixels). Thus, each 2x4 size block has four units (e.g., U1, U2, U3, and U4).

Step-3 Convert 12-bit watermark into 9-base number Wat_9 in such a way that it has four digits (e.g., Wat_9 = d1d2d3d4).

Step-4 Modify pixels of U1 using **d1** as per the given steps.

- Compute digit F_{embed} as shown in Eq. (5). Here, P_k is the k$^{\text{th}}$ pixel of unit U.

$$F_{\text{embed}} = \left\{ \sum_{k=1}^{n} 3^{k-1} P_k . \right\} \bmod 3^n \quad \text{where } n = 2 \quad (5)$$

- Calculate x as given in Eq. (6).

$$x = \left(d - F_{\text{embed}} + \left\lfloor \frac{3^n - 1}{2} \right\rfloor \right) \bmod 3^n \quad (6)$$

- Change x into $x^{'}$ by converting into 3-base number as $x^{'} = y_1 y_2 \ldots . y_n$, where y_i denotes the ith digit of $x^{'}$ for $1 \le i \le n$. Next, get $x^{"}$=$z_1 z_2 \ldots . z_n$, where $z_i = y_i - 1$.
- Add digits of $x^{"}$ to the pixels of unit U to get the updated pixels as shown in Eq. (7).

$$P\_\mathrm{new}_k = P_k + z_i \text{ where } \begin{cases} 1 \le k \le n \\ i = n - k + 1 \end{cases} \tag{7}$$

- Repeat the steps with U2, U3, and U4 to embed d2, d3, and d4, respectively.

Step-5 Repeat step 2, 3, and 4 for each block to get the dual watermarked image W_img.

3.3 Watermark Extraction

The attacker can modify the watermarked image (W_img) considering that the owner may have uploaded it on a public platform. In such a situation, robust watermark can be used to check the ownership and fragile watermark can be used for content verification and self-recovery.

3.3.1 Robust Watermark Extraction (Ownership Check)

During simulation, common signal processing attacks have been used to check the performance of the scheme. Following steps show the extraction process from the attacked image:

Step-1 Divide the attacked image into blocks (i.e., 16 × 16 size) that are uniform and non-overlapping.

Step-2 Get LL, LH, HL, and HH by applying IWT on the first block. Next, perform IWT on LH band to get LH1 and HL1.

Step-3 Calculate average values $\mathrm{LH1}_{\mathrm{avg}}$ and $\mathrm{HL1}_{\mathrm{avg}}$, and extract the bit as per Eq. (8).

$$\mathrm{Ext}_{\mathrm{bit}} = \begin{cases} 0 \text{ if } \mathrm{HL1}_{\mathrm{avg}} \le \mathrm{LH1}_{\mathrm{avg}} \\ 1 \text{ if } \mathrm{HL1}_{\mathrm{avg}} > \mathrm{LH1}_{\mathrm{avg}} \end{cases} \tag{8}$$

Step-4 Repeat step 2 and 3 on each block to extract all bits from the attacked watermarked image.

Step-5 Reshape the extracted bits and decrypt it via reversing the encryption process to get the extracted watermark $W_{\mathrm{extracted}}$.

3.3.2 Fragile Watermark Extraction (Tamper Check)

The following steps show the authentication process to check the tampering:

Step-1 Divide the attacked watermarked image into 2 × 4 size blocks and extract the four digits (F_{ext}) using Eq. (5) from each block.

Step-2 Convert the four digit 9-base number (i.e., $F_{\mathrm{ext\_1}} F_{\mathrm{ext\_2}} F_{\mathrm{ext\_3}} F_{\mathrm{ext\_4}}$) into binary (i.e., 12 bit size). Similarly, extract 12-bit number from each block.

Step-3 Get $\mathrm{EW}_{\mathrm{ran\_2}}$ by concatenating initial 6-bits concerning each block. Likewise, get $\mathrm{EW}_{\mathrm{recov}}$ by cascading last 6 bits related to each block.

Step-4 Generate binary sequence W_{ran_2} using K_3-based SFMT process and Eq. (1). Further, compare the corresponding bits of $\mathrm{EW}_{\mathrm{ran\_2}}$ and $W_{\mathrm{ran\_2}}$ to authenticate the image. If the bits are different, then the concerning block is marked as tampered.

Step-5 Apply the block-neighborhood approach to smoothen the resultant of Step 4. For smoothing, eight neighborhood blocks (except corner positions) of each block is considered. If majority of the blocks (out of these nine blocks) are tampered/non-tampered, the block is also marked as tampered/non-tampered.

3.4 Image Self-recovery

The authenticated image (after tamper localization) can be divided into tampered blocks and non-tampered blocks. Further, the tampered blocks can also be classified into two types. (1) Reserved feature blocks: The tampered blocks, whose mapping blocks are not tampered. (2) Ruined feature blocks: The tampered blocks, whose mapping blocks are also tampered.

At first, reserved feature blocks are recovered with the help the mapping. The recovery information from the mapped block is extracted (6 MSB) using K_4 and padded with "00" to make it 8 bit. This 8 bit (after decimal conversion) is used to replace pixel values of reserved feature block. Then after, Ruined feature blocks are recovered through the adaptive neighborhood block averaging (ANBA) process. Figure 4 represents the ANBA process for the recovery for the tampered block 'T'.

Here, average intensity "μ" is calculated for each valid (non-tampered or recovered) neighbor block. Next, the average (X) of all valid "μ" values is obtained as shown in Fig. 4. At last, X is substituted on all pixel positions of tampered block "T". In the same way, repeat the process for every tampered block. Afterward, the ANBA

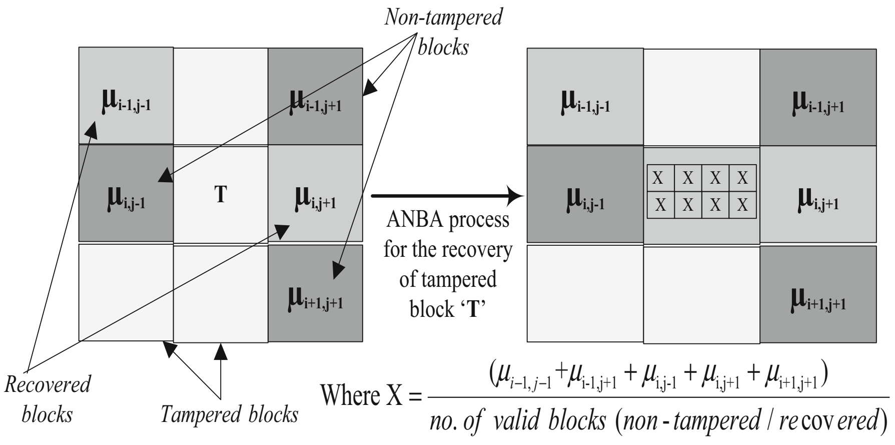

Non-tampered blocks
$\mu_{i-1,j-1}$
$\mu_{i-1,j+1}$
$\mu_{i,j-1}$
T
$\mu_{i,j+1}$
$\mu_{i+1,j+1}$
ANBA process for the recovery of tampered block 'T'
X X X X
X X X X
Recovered blocks
Tampered blocks
Where $X = \frac{(\mu_{i-1,j-1} + \mu_{i-1,j+1} + \mu_{i,j-1} + \mu_{i,j+1} + \mu_{i+1,j+1})}{no.\ of\ valid\ blocks\ (non\text{-}tampered / recovered)}$

Fig. 4 Adaptive neighborhood block averaging for the recovery of block 'T'

process is applied one more time to improve recovery. Finally, the recovered image is obtained.

4 Experimental Results and Discussion

Testing has been performed over 150 images of size 512 × 512 (selected from reference [9]); including medical, texture, and other standard test images. Here result of selected images (Fig. 5) is shown for succinct representation. A binary image (i.e., 32 × 32 size) is used as the robust watermark. For robust watermarking, the value of embedding parameter α is selected as $\alpha = 11$ based on the experimental evaluation in order to keep the significant trade-off between imperceptibility and robustness. The imperceptibility results are obtained by calculating PSNR (peak signal to noise ratio) [20] and SSIM (structural similarity index) [8] for different test images as shown in Table 1.

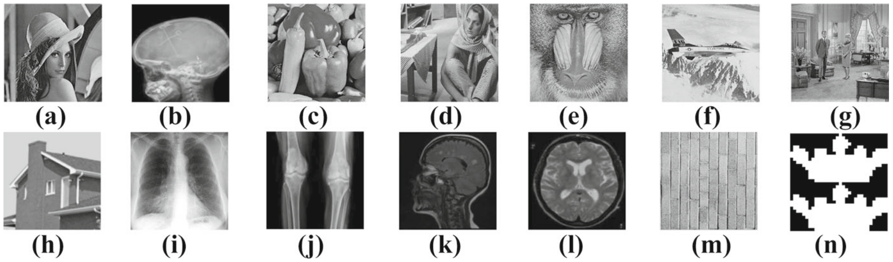


Fig. 5 Host images **a** Lena **b** M-1 **c** pepper **d** Barbara **e** Mandrill **f** F-16g Living room **h** House **i** M-2 **j** M-3kM-4lM-5 **m** Bricks **n** Robust binary watermark image

Table 1 PSNR and SSIM results for test images (after embedding)

S. No	Host image	PSNR	SSIM
1	Lena	41.1679	0.9667
2	M-1	41.7015	0.9107
3	Pepper	41.0098	0.9650
4	Barbara	41.1644	0.9734
5	Mandrill	40.1993	0.9823
6	F-16	40.6816	0.9554
7	Living room	40.3795	0.9733
8	House	41.2269	0.9490
9	M-2	41.2793	0.9480
10	M-3	41.9708	0.9091
11	M-4	41.6666	0.9501
12	M-5	41.8079	0.9475
13	Bricks	40.9271	0.9861

The average PSNR value is found to be 41.17 and the average SSIM as 0.9551. Results show that the proposed watermarking scheme is highly imperceptible to the viewers. As specified in the previous sections, the proposed scheme is a dual watermark approach and has multipurpose nature. It can be used for multiple applications such as copyright protection, ownership verification, tamper detection, tamper localization, and image self-recovery. Robust and fragile watermarking results are as follows:

4.1 Robust Watermarking Results

Different image processing attacks have been applied on the watermarked image before extracting the watermark. It gives a better insight into the robust feature of the scheme against attacks. The robustness results have been evaluated in terms of BER (bit error rate) [17]. As described in Table 2, the same watermark gets extracted (i.e., BER $=$ 0) when the watermarked image is not attacked. In the case of different noise attacks like Gaussian noise (GN), speckle noise (SN), and Salt and Pepper noise (SPN), etc., the robust mechanism of the proposed scheme gives remarkable results. Similarly, the significant robustness is achieved against filtering attacks such as Median filter (MF), Gaussian filter (GF), and Wiener filter (WF). However, the scheme needs to improve against rotation attacks. The comparison (Table 3) of the proposed robust mechanism with other existing robust schemes has been performed; which testify the dominance of the proposed scheme over the existing schemes.

4.2 Fragile Watermarking Results

In order to authenticate the image against forgery, the scheme has been checked by applying different tampering attacks. Further, the tampered region is also recovered successfully during experimentation. It is important to note that, the tamper detection process would be block-wise rather than pixel-wise. Therefore, even if one pixel of a block (i.e., 2×4 pixels) is tampered, the complete block would be considered as the tampered block. In general, the tampering/forgery is done on a portion of an image and not on a specific pixel, hence the scheme is very effective for tamper detection. For quantitative analysis, the parametric values TD_{eff}, PSNR and SSIM have been obtained for different tampering rates (TR). Here, TD_{eff} represents the efficiency of tamper detection and it is the ratio of the number of detected tampered blocks and the number of total tampered blocks. These parameters give an impression of an effective performance of the proposed scheme in terms of detection and self-recovery of the tampered part of the attacked image. The visual quality of the recovered image has been studied with respect to the watermarked (WM) image.

As presented in Table 4, the proposed scheme is able to detect and recover the tampered part of the watermarked image, even for quite high tampering rates. Different types of attacks (i.e., tampering) are applied on the watermarked images and average detection rate of 99.8% is obtained. Further, the significant results for self-recovery of the tampered images are obtained for different tampering rates. A tampered image can be recovered significantly for tampering rate up to 80%. Result of content tampering is presented in Table 5. Table 6 presents the investigational results for the recovery

Table 2 Robustness (BER) results for host images

Attacks	BER												
	Lena	M-1	Pepper	Barbara	Mandrill	F-16	Living room	House	M-2	M-3	M-4	M-5	Bricks
Attack free	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Resize (*x*-2*x*-*x*)	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Adjust Intensity[$\gamma = 0.6$]	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Adjust Intensity[$\gamma = 0.8$]	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
SN[0.01]	0.01	0.01	0.01	0.01	0.01	0.04	0.01	0.02	0.04	0.01	0.00	0.01	0.02
GN (0.001)	0.00	0.02	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.02	0.00	0.00	0.00
GN (0.005)	0.04	0.10	0.04	0.04	0.03	0.03	0.04	0.04	0.05	0.11	0.05	0.03	0.04
JPEG(40)	0.02	0.12	0.02	0.02	0.05	0.04	0.04	0.02	0.07	0.25	0.11	0.07	0.02
JPEG(50)	0.00	0.07	0.01	0.01	0.05	0.03	0.04	0.00	0.04	0.18	0.02	0.06	0.01
JPEG(60)	0.00	0.06	0.01	0.00	0.04	0.02	0.04	0.00	0.03	0.15	0.00	0.03	0.01
JPEG(70)	0.00	0.04	0.00	0.00	0.04	0.02	0.03	0.00	0.03	0.06	0.00	0.01	0.01
JPEG (80)	0.00	0.00	0.00	0.00	0.01	0.01	0.00	0.00	0.00	0.00	0.00	0.00	0.00
JPEG2000 (CR = 5)	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.01	0.00	0.00	0.07	0.01
JPEG2000 (CR = 10)	0.04	0.00	0.02	0.22	0.14	0.06	0.15	0.00	0.01	0.00	0.00	0.28	0.15
MF[3,3]	0.06	0.01	0.11	0.09	0.11	0.09	0.15	0.01	0.00	0.03	0.01	0.28	0.17
GF[3 × 3]	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
WF[3 × 3]	0.02	0.01	0.04	0.04	0.07	0.07	0.09	0.02	0.00	0.01	0.00	0.18	0.07
Sharpening [0.2]	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Crop(20 pixel on sides)	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03
Crop(5% pixel at Mid)	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00

Table 2 (continued)

Attacks	BER												
	Lena	M-1	Pepper	Barbara	Mandrill	F-16	Living room	House	M-2	M-3	M-4	M-5	Bricks
SPN (.001)	0.00	0.01	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.01	0.00	0.00	0.00
SPN (.01)	0.02	0.07	0.02	0.02	0.02	0.03	0.02	0.01	0.03	0.09	0.03	0.03	0.02
Motion blur($\theta = 7$,le$n$-10)	0.02	0.00	0.04	0.03	0.10	0.07	0.09	0.04	0.02	0.01	0.00	0.10	0.04
Rotation (2°)	0.49	0.50	0.49	0.46	0.48	0.48	0.49	0.48	0.49	0.50	0.49	0.49	0.48

Table 3 Robustness (BER) results comparison with existing schemes

Attacks	Lena				Pepper				Mandrill			
	Mehta et al. [17]	Islam and laskar [10]	Islam et al. [11]	Proposed work	Mehta et al. [17]	Islam and laskar [10]	Islam et al. [11]	Proposed work	Mehta et al. [17]	Islam and laskar [10]	Islam et al. [11]	Proposed work
SPN (0.02)	0.164	0.158	0.133	**0.060**	0.197	0.186	0.148	**0.053**	0.177	0.176	0.109	**0.056**
SPN (0.01)	0.115	0.125	0.049	**0.013**	0.123	0.122	0.068	**0.019**	0.103	0.084	0.049	**0.014**
SPN (0.005)	0.057	0.056	0.037	**0.008**	0.056	0.047	0.031	**0.002**	0.052	0.047	0.022	**0.007**
GN (0.01)	0.358	0.346	0.215	**0.100**	0.364	0.365	0.213	**0.112**	0.328	0.299	0.193	**0.100**
GN (0.005)	0.249	0.213	0.113	**0.040**	0.264	0.193	0.137	**0.043**	0.248	0.229	0.111	**0.034**
GN (0.001)	0.055	0.047	0.016	**0.000**	0.056	0.465	0.014	**0.000**	0.068	0.057	0.014	**0.000**
JPEG 70	0.000	0.000	0.000	**0.000**	0.000	0.000	0.000	**0.000**	0.005	0.000	0.004	0.040
JPEG 50	0.002	**0.002**	0.006	0.005	0.002	0.002	0.002	0.007	0.026	0.012	0.010	0.050

Table 4 Image authentication and self-recovery (with respect to the watermarked image) results for different tampering rates

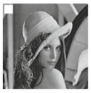
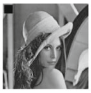
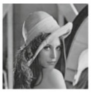
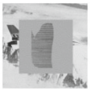
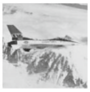
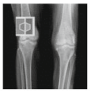
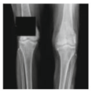
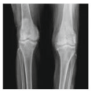
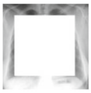
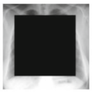
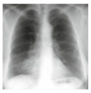
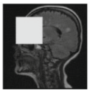
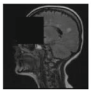
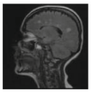
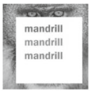
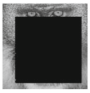
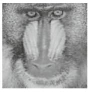
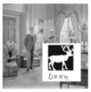
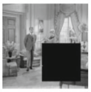
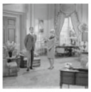
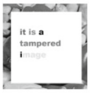
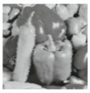
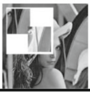
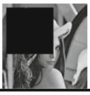
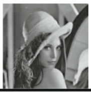
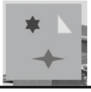
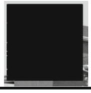
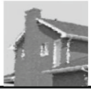
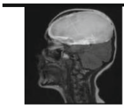
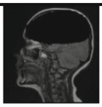
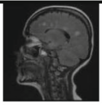
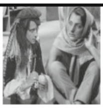
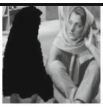
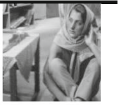
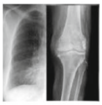
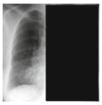
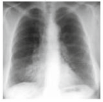
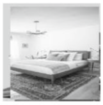
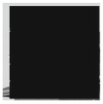
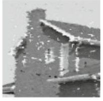
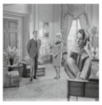
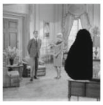
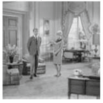
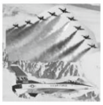
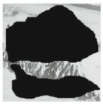
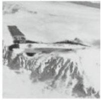
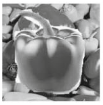
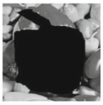
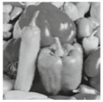
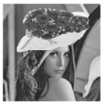
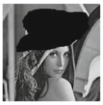
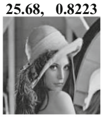
TR (%)	Tampered image	Image authentication	Image recovery	Results for tamper detection and self-recovery	*TR* (%)	Tampered image	Image authentication	Image recovery	Results for tamper detection and self-recovery
1				TD_{eff}=100% PSNR=53.89 SSIM=0.9980	40				TD_{eff}=99.95% PSNR=26.76 SSIM=0.8729
5				TD_{eff}=99.8% PSNR=41.67 SSIM=0.9891	50				TD_{eff}=100% PSNR=36.44 SSIM=0.9069
10				TD_{eff}=99.88% PSNR=40.60 SSIM=0.9785	60				TD_{eff}=99.96% PSNR=24.21 SSIM=0.6758
20				TD_{eff}=99.88% PSNR=30.85 SSIM=0.9324	70				TD_{eff}=100% PSNR=24.94 SSIM=0.7151
30				TD_{eff}=99.99% PSNR=30.20 SSIM=0.8895	80				TD_{eff}=99.94% PSNR=24.46 SSIM=0.7629

Table 5 Image authentication and self-recovery results (with respect to the watermarked image) for random tampering attacks

Tampered image	Image authentication	Image recovery (PSNR, SSIM)	Tampered image	Image authentication	Image recovery (PSNR, SSIM)
		 **38.83, 0.9697**			 **28.36, 0.8669**
		 **36.03, 0.9065**			 **20.50, 0.6636**
		 **31.48, 0.9547**			 **25.68, 0.8223**
		 **28.98, 0.8349**			 **31.05, 0.9129**

of tampered area of test images for different tampering rates in terms of PSNR and SSIM, which proves the effectiveness of the scheme. The results show that the proposed scheme is very useful to provide protection, authentication and recovery against different types of attacks.

Table 7 describes the performance of different fragile schemes, which clearly proves

Table 6 Results (PSNR, SSIM) for self-recovery of the tampered images at different tampering rates

TR (%)	PSNR, SSIM												
	Lena	M-1	Pepper	Barbara	Mandrill	F-16	Living room	House	M-2	M-3	M-4	M-5	Bricks
1	53.89, 0.9980	51.27, 0.9977	47.87, 0.9972	43.78, 0.9976	40.44, 0.9952	51.95, 0.9978	49.21, 0.9976	60.02, 0.9992	54.30, 0.9986	54.38, 0.9980	58.09, 0.9945	60.29, 0.9969	42.53, 0.9941
5	45.74, 0.9883	45.83, 0.9921	39.54, 0.9872	39.46, 0.9897	33.81, 0.9765	47.18, 0.9919	41.22, 0.9841	53.15, 0.9959	48.01, 0.9929	43.43, 0.9891	42.07, 0.9739	38.92, 0.9884	36.47, 0.9736
10	39.38, 0.9733	43.94, 0.9859	36.34, 0.9706	35.96, 0.9771	31.30, 0.9537	41.05, 0.9832	37.75, 0.9674	44.53, 0.9894	43.92, 0.9857	39.05, 0.9769	39.58, 0.9588	37.34, 0.9807	33.31, 0.9475
20	34.35, 0.9342	41.03, 0.9734	33.45, 0.9403	33.51, 0.9470	28.98, 0.9113	33.80, 0.9617	32.58, 0.9265	38.29, 0.9713	41.72, 0.9684	38.21, 0.9525	37.27, 0.9383	35.84, 0.9639	30.03, 0.8907
30	30.76, 0.8926	37.92, 0.9544	31.48, 0.9093	31.27, 0.9096	27.64, 0.8655	30.32, 0.9323	30.24, 0.8833	35.03, 0.9508	39.52, 0.9502	36.31, 0.9288	35.38, 0.9167	33.94, 0.9463	27.71, 0.8269
40	28.48, 0.8512	35.88, 0.9346	29.51, 0.8714	28.12, 0.8505	26.49, 0.8177	27.75, 0.8936	28.02, 0.8327	32.14, 0.9254	37.35, 0.9299	34.23, 0.9032	33.52, 0.8930	32.57, 0.9265	25.85, 0.7588
50	26.67, 0.8000	34.11, 0.9101	28.02, 0.8257	26.06, 0.7853	25.18, 0.7589	25.89, 0.8494	26.48, 0.7730	30.40, 0.8988	36.25, 0.9076	32.16, 0.8722	31.75, 0.8623	31.29, 0.9004	24.26, 0.6860
60	25.05, 0.7403	31.50, 0.8727	26.69, 0.7748	24.51, 0.7156	23.80, 0.6781	24.40, 0.7992	24.72, 0.7034	28.06, 0.8622	34.66, 0.8777	29.62, 0.8217	30.24, 0.8317	29.81, 0.8623	22.70, 0.5940
70	23.58, 0.6818	26.80, 0.8318	25.11, 0.7201	23.16, 0.6477	22.50, 0.5892	23.29, 0.7524	23.36, 0.6321	26.68, 0.8249	33.11, 0.8442	27.89, 0.7725	28.61, 0.7919	28.32, 0.8170	21.72, 0.5080
80	21.91, 0.6056	25.84, 0.7591	23.31, 0.6480	21.36, 0.5495	21.11, 0.4732	21.84, 0.6902	22.05, 0.5431	24.78, 0.7756	31.05, 0.7984	24.77, 0.7073	25.84, 0.7223	25.72, 0.7389	20.24, 0.4038
90	18.81, 0.4969	16.15, 0.5425	19.67, 0.5443	18.86, 0.4317	19.12, 0.3390	19.69, 0.6058	19.56, 0.4288	21.33, 0.6902	25.14, 0.7253	17.94, 0.5621	22.04, 0.5689	20.49, 0.5675	18.41, 0.2842

Table 7 Performance comparisons (fragile nature) with existing schemes

Methods	PSNR (in dB)			Condition for successful restoration
	WM (After embedding)	Recovered image		
		w.r.t. WM	w.r.t. host	
Zhu et al. [35]	36.7	22.8	22.8	Regions storing the recovery data must be intact
Zhang and Wang [32]	28.7	$+\infty$	$+\infty$	TR < 3.2%
Zhang et al. [33]-A	37.9	$+\infty$	40.7	TR < 24%
Zhang et al. [33]-B	37.9	[22, 40]	[22, 40]	TR < 66%
Zhang et al. [34]	37.9	N.A	[23, 41]	TR < 60%
Ansari et al. [1]	44	28	N.A	TR $\leq$ 50%
Singh and Singh [25]	39.0	[28.4, 40]	N.A	TR < 50%
Qin et al. [19]-A	44.2	N.A	[33, 42]	TR < 45%
Qin et al. [19]-B	44.2	N.A	[31, 40]	TR < 50%
Proposed scheme	41.17	[23.8,48.7]	[19.5,40]	TR $\leq$ 80%

the superiority of the proposed fragile watermarking mechanism. The performance of different techniques is compared in terms of PSNR of watermarked image (i.e., after embedding) and PSNR of recovered image. In addition, successful recovery condition has been compared with existing fragile watermarking methods. Most of the schemes such as [32–35], and [19]-B used an 8 × 8 block size for watermarking. Thus, if one pixel got tampered then the complete block (including 63 non-tampered pixels) is considered as a tampered region. Subsequently, preserved recovery information is used to restore the tampered region (which was almost original or non-tampered). Consequently, the performance decreases in terms of image restoration especially in case of severe tampering as can be seen in Table 7. Similarly, the schemes [1] and [19]-A used 4 × 4 size blocks for watermarking but their condition of restoration gets limited up to tampering rate of 50% and 45%, respectively. On the other side, the scheme [25] employed 2 × 2 size blocks during watermarking. The restoration capacity gets limited to a 50% tampering rate because the scheme [25] used only 5-MSB bits as the recovery data for each block. In conclusion, small block size limits the size of the recovery data and large block size limits the tamper localization capability.

Therefore, the proposed scheme opted for the block size of 2 × 4 for watermarking, which let us embed significant tamper detection data (6-bit) as well as the significant recovery data (i.e., 6 MSB bits) with decent localization ability. In addition, the ANBA approach provides remarkable improvement in recovery at high tampering rates. While maintaining the visual quality of the image, the scheme can recover the tampered area even for the 80% tampering rate. It should be noted that the proposed scheme is a multipurpose and dual watermarking scheme. Even then it provides better/significant performance as compared to the schemes dedicated to a specific purpose. Therefore, the scheme provides improved alternative for image security and monitoring. To investigate the restoration results, the average parametric values (i.e., PSNR etc.) have been calculated during the thorough experimentation. For restored images, the average range of PSNR values is [23.83, 48.78] (with respect to the watermarked image) and [19.54, 39.98] (with respect to the host image) for less than 80% tampering rate. Moreover, the average PSNR value for watermarked images turns out to be 41.17 that signify that the imperceptibility feature of the scheme is eminently admissible.

4.3 Security Analysis

The discussion about the security features of the proposed method and the advantage of dual watermark (robust and fragile) approach is presented in this section. During robust watermarking, the robust watermark has been encrypted before embedding process using Arnold transform and secret key-based random binary sequence. Therefore, even if someone illegally gets the extracted watermark, the actual/original form of the watermark information remains unintelligible. Thus, the watermark data would be utilizable only for the users with the correct secret key. Additionally, the embedding strategy is robust enough to counter general image processing attacks and provide copyright protection for images. Similarly, fragile watermarking mechanism is secured enough by using secret key-based fragile watermark data. The authentication information is completely based on secret key (seed value). During tampering detection and localization, the extracted authentication data is compared with the generated authentication data (key-based). It means that one cannot perform authentication without having secret key values. Therefore, the tamper detection and localization process is highly sensitive to the secret keys. Moreover, the recovery data of each 2×4 block is stored into another block using a specific key-based pseudo-random order. Only the knowledge of the correct key can provide the information of the block that has been used to preserve the recovery data of a block. Thus, both robust as well as fragile watermarking mechanisms are highly secured.

Many times, attackers use LSB modification tools to modify the LSB bits. In the proposed work, the fragile watermarking framework does not modify the LSB bits directly. Instead of this, the complete 2×4 size block is processed during fragile watermarking using a base-9 number system framework. Hence, attackers cannot extract the fragile watermark via LSB tools because LSB bits are not modified directly based on watermark bits. Therefore, if the attackers produce a counterfeit image using such tools then the generated image would not be able to pass the authentication process. Nonetheless, counterfeit attacks can also create issues of fake ownership claims, as discussed by authors [15]. To claim ownership, attackers can use completely different watermarking schemes or can frame up the embedding sub-bands. Even multiple users can claim over digital data by modifying or replacing the watermarking strategy. In such cases, the proposed dual watermarking approach can successfully deal with such types of attacks. The attacked image (e.g., counterfeit attacks) can be detected as a forged one during image authentication. Thus, it would be obvious that the extracted robust watermark is not correct because the image has been manipulated. When both the watermarks (robust as well as fragile) are extracted correctly and it is found that the image has not been altered, only then the user wins the ownership claim.

Hereby it is clear that the proposed multipurpose and dual watermarking mechanism is highly secured while providing image authentication, self-recovery, and copyright protection.

4.4 Relative Study with Other Existing Multipurpose Watermarking Schemes

The proposed scheme contains dual watermarking (both robust as well as fragile) mechanism. This scheme can be used effectively for copyright protection, image authentication and image restoration; thus, the scheme is having multipurpose nature. The multipurpose nature makes the watermarking methods more useful and highly desired. It can be used for different applications at the same time. Some of the multipurpose watermarking schemes from the watermarking literature have been studied and compared with the proposed watermarking method to analyze the relative features. Table 8 compares the features of the proposed watermarking method with existing multipurpose watermarking schemes. From the analysis, it is observed that the proposed scheme is more versatile and efficient than the existing schemes.

5 Conclusion

The proposed work offered a blind multipurpose image watermarking scheme that can be used for efficient copyright protection, image authentication, and self-recovery of the image. The robust mechanism worked very well against various signal processing attacks and was able to extract robust watermark efficiently. The fragile procedure was able to detect and localize the tampered portion with more than 99.8% accuracy. Additionally, a satisfactory restoration of the image is achieved for tampering rate up to 80%. The scheme was made secure against unauthorized access via four secret keys. Experimental results showed remarkable results in terms of watermarking parameters like PSNR, SSIM, BER, tamper detection accuracy, and image recovery. The limitation of the proposed work includes the poor robustness performance against the rotational attacks, which will be investigated and solved in future research work. Future research directions also includes the possibility of improving the imperceptibility feature by incorporating better embedding framework without compromising the other characteristics. Furthermore, the scheme will be extended for color images in future.

Table 8 Comparison of proposed watermarking method with existing schemes (multipurpose nature)

S No	Characteristic features	Lu and Liao [16]	Ansari et al. [1]	Liu et al. [15]	Singh and Agarwal [24]	Ansari and Pant [2]	Haghighi et al. [7]	Daneshmandpour et al. [6]	Proposed scheme
1	Nature of the scheme	Blind	Blind	Blind	Blind	Non-blind	Blind	Blind	Blind
2	Copyright /ownership	Yes	No	Yes	Yes	Yes	Yes	No	Yes
3	Image authentication	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
4	Image restoration	No	Yes	No	Yes	Yes	No	Yes	Yes
5	Embedding PSNR (dB)	~ 40	~ 44	~ 40	~ 30	~ 38	~ 38	~ 44	~ 41
6	Security	+	+ + +	+ +	+ + +	+ +	+ +	+ + + +	+ + + +
7	Robustness	+ +	-	+ + +	+ + + +	+ + +	+ + +	-	+ + + +
8	Host image (gray)	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes
9	Embedding domain	Transform + Transform	Spatial	Transform + Spatial	Transform + Spatial	Transform + Spatial	Transform + Transform	Spatial	Transform + Spatial
10	Watermarking type	Robust + Fragile	Fragile	Robust + Fragile	Robust + Fragile	Robust + fragile	Robust + Semi-fragile	Fragile	Robust + Fragile

Funding Not applicable.

Data Availability The dataset used is publicly available on the internet.

Code Availability The code will be made available on reasonable demand.

Declarations

Conflict of interest There is no conflict of interest.

References

1. I.A. Ansari, M. Pant, C.W. Ahn, SVD based fragile watermarking scheme for tamper localization and self-recovery. Int. J. Mach. Learn. Cybern. **7**(6), 1225–1239 (2016)
2. I.A. Ansari, M. Pant, Multipurpose image watermarking in the domain of DWT based on SVD and ABC. Pattern Recogn. Lett. **94**, 228–236 (2017)
3. S. Avila, M.N. Miyatake, Multipurpose image watermarking scheme based on self-embedding and data hiding into halftone image. in *2010 IEEE Electronics, Robotics and Automotive Mechanics Conference* (IEEE, Cuernavaca, Mexico, 2010), pp. 394–398
4. R. Barnett, Digital watermarking: applications, techniques and challenges. Electron. Commun. Eng. J. **11**(4), 173–183 (1999)
5. I. Cox, M. Miller, J. Bloom, J. Fridrich, T. Kalker, *Digital Watermarking and Steganography* (Morgan kaufmann, 2007)
6. N. Daneshmandpour, H. Danyali, M.S. Helfroush, Image tamper detection and multi-scale self-recovery using reference embedding with multi-rate data protection. China Commun. **16**(11), 154–166 (2019)
7. B. Haghighi, A.H. Taherinia, A. Harati, M. Rouhani, WSMN: an optimized multipurpose blind watermarking in Shearlet domain using MLP and NSGA-II. Appl. Soft Comput. **101**, 107029 (2021). https://doi.org/10.1016/j.asoc.2020.107029
8. A. Hore, D. Ziou, Image quality metrics: PSNR vs. SSIM. in *2010 20th International Conference on Pattern Recognition* (IEEE, Istanbul, Turkey, 2010), pp. 2366–2369
9. Image databases, Accessed: May 2021. [Online]. Available: http://www.imageprocessingplace.com/root_files_V3/image_databases.htm
10. M. Islam, R.H. Laskar, Geometric distortion correction based robust watermarking scheme in LWT-SVD domain with digital watermark extraction using SVM. Multimed. Tools Appl. **77**(11), 14407–14434 (2018)
11. M. Islam, A. Roy, R.H. Laskar, SVM-based robust image watermarking technique in LWT domain using different sub-bands. Neural Comput. Appl. **32**(5), 1379–1403 (2020)
12. M. Jagannatam, *Twister–A Pseudo Random Number Generator and Its Variants* (George Mason University, Department of Electrical and Computer Engineering, 2008)
13. S. Lee, C.D. Yoo, T. Kalker, Reversible image watermarking based on integer-to-integer wavelet transform. IEEE Trans. Inf. Forensics Secur. **2**(3), 321–330 (2007)
14. M. Li, Q. Liu, Steganalysis of SS steganography: hidden data identification and extraction. Circuits Syst. Signal Process. **34**(10), 3305–3324 (2015)
15. X.L. Liu, C.C. Lin, S.M. Yuan, Blind dual watermarking for color images' authentication and copyright protection. IEEE Trans. Circuits Syst. Video Technol. **28**(5), 1047–1055 (2016)
16. S. Lu, H.Y. Liao, Multipurpose watermarking for image authentication and protection. IEEE Trans. Image Process. **10**(10), 1579–1592 (2001)
17. R. Mehta, N. Rajpal, V.P. Vishwakarma, LWT-QR decomposition based robust and efficient image watermarking scheme using Lagrangian SVR. Multimed. Tools Appl. **75**(7), 4129–4150 (2016)
18. I. Podilchuk, E.J. Delp, Digital watermarking: algorithms and applications. IEEE Signal Process. Mag. **18**(4), 33–46 (2001)
19. C. Qin, P. Ji, C.C. Chang, J. Dong, X. Sun, Non-uniform watermark sharing based on optimal iterative BTC for image tampering recovery. IEEE Multimed. **25**(3), 36–48 (2018)

20. V. Rajput, I.A. Ansari, Image tamper detection and self-recovery using multiple median watermarking. Multimed. Tools Appl. **79**(47), 35519–35535 (2020)
21. M. Saito, M. Matsumoto, Variants of Mersenne twister suitable for graphic processors. ACM Trans. Math. Softw. **39**(2), 1–20 (2013)
22. M. Saito, M. Matsumoto, SIMD-oriented fast Mersenne Twister: a 128-bit pseudorandom number generator. in *Monte Carlo and Quasi-Monte Carlo Methods 2006* (Springer, Berlin, 2008), pp. 607–622. https://doi.org/10.1007/978-3-540-74496-2_36
23. J. Seitz, Digital watermarking for digital media. IGI Global (2005). https://doi.org/10.4018/978-1-59140-518-4
24. P. Singh, S. Agarwal, A self recoverable dual watermarking scheme for copyright protection and integrity verification. Multimed. Tools Appl. **76**(5), 6389–6428 (2017)
25. S.K. Singh, Block truncation coding based effective watermarking scheme for image authentication with recovery capability. Multimed. Tools Appl. **78**(4), 4197–4215 (2019)
26. R. Sinhal, I.A. Ansari, C.W. Ahn, Blind image watermarking for localization and restoration of color images. IEEE Access **8**, 200157–200169 (2020)
27. N. Tarhouni, M. Charfeddine, C.B. Amar, Novel and robust image watermarking for copyright protection and integrity control. Circuits Syst. Signal Process. **39**(10), 5059–5103 (2020)
28. X. Tong, Y. Liu, M. Zhang, Y. Chen, A novel chaos-based fragile watermarking for image tampering detection and self-recovery. Signal Process. Image Commun. **28**(3), 301–308 (2013)
29. S.H. Wang, Y.P. Lin, Wavelet tree quantization for copyright protection watermarking. IEEE Trans. Image Process. **13**(2), 154–165 (2004)
30. M. Wu, B. Liu, Watermarking for image authentication. in *Proceedings 1998 International Conference on Image Processing. ICIP98 (Cat. No. 98CB36269)* (IEEE, USA, 1998), vol. 2, pp. 437–441. https://doi.org/10.1109/ICIP.1998.723413
31. Wu, J. Zhang, W. Deng, D. He, Arnold transformation algorithm and anti-Arnold transformation algorithm. in *2009 First International Conference on Information Science and Engineering* (IEEE, Nanjing, 2009), pp. 1164–1167. https://doi.org/10.1109/ICISE.2009.347
32. X. Zhang, S. Wang, Fragile watermarking with error-free restoration capability. IEEE Trans. Multimed. **10**(8), 1490–1499 (2008)
33. X. Zhang, S. Wang, Z. Qian, G. Feng, Reference sharing mechanism for watermark self-embedding. IEEE Trans. Image Process. **20**(2), 485–495 (2010)
34. X. Zhang, Z. Qian, Y. Ren, G. Feng, Watermarking with flexible self-recovery quality based on compressive sensing and compositive reconstruction. IEEE Trans. Inf. Forensics Secur. **6**(4), 1223–1232 (2011)
35. X. Zhu, A.T. Ho, P. Marziliano, A new semi-fragile image watermarking with robust tampering restoration using irregular sampling. Signal Process. Image Commun. **22**(5), 515–528 (2007)
36. Y.Q. Zou, Z. Shi, W. Ni, Su, A semi-fragile lossless digital watermarking scheme based on integer wavelet transform. IEEE Trans. Circuits Syst. Video Technol. **16**(10), 1294–1300 (2006)