




# An efficient low bit rate image watermarking and tamper detection for image authentication

Md. Ahasan Kabir<sup>1</sup> 

Received: 3 February 2020 / Accepted: 16 February 2021 / Published online: 2 March 2021

© The Author(s) 2021 

## Abstract

This study presents the vulnerability of digital documents and its effective way to protect the ownership and detection of unauthorized modification of multimedia data. Watermarking is an effective way to protect vulnerable data in a digital environment. In this paper, a watermarking algorithm has been proposed based on a lossy compression algorithm to ensure authentication and detection of forgery. In this proposed method, the CDF9/7 biorthogonal wavelet is used to transform the watermark image and encoded the wavelet coefficients using Set Partition in Hierarchical Tree algorithm. Then, the encoded bits are encrypted by shuffling and encrypting using symmetric keys. After that the encrypted bits are inserted into the Least Significant Bit position of the cover image. In addition, two tamper detection bits are generated based on texture information and pixel location and inserted in the watermarked image. The proposed algorithm reconstructs the watermark and the tampering region more efficiently and achieved 56.5463 dB PSNR for STARE database. Experimental result shows that the proposed algorithm is effectively prevented different attacks and ensure the integrity of watermark bits within the watermarked image. Also finds the tampered region more efficiently compared with the existing state of art algorithms.

**Keywords** Wavelet transform · Tamper detection · SPIHT · Self-embedding · Encryption · Fragile-watermarking

## 1 Introduction

Due to extensive development in the internet and digital communication technologies, the data generation processes are rapidly changing in contemporary society. Presently, the online digital communication system help to easily store and spread multimedia files such as image, audio, and video. However, during multimedia transmission and storage, the data may alter for illegal use by intruders. Therefore, the copyright protection and identification of ownership, and forgery detection do not maintain data integrity and create problems with image authentication [1]. In many human-centered applications, such as medical image, military communication, remote sensing, and geographic data system implementation, this

illegal modification becomes an issue. Digital watermarking systems can be integrated to address these problems. Digital image watermarking is a technology that provides protection from an opponent by implanting an imperceptible or perceptible watermark in a digital image.

In this paper, a fragile watermarking algorithm has been proposed for image authentication, tamper identification, tamper localization, and watermark reconstruction. To prevent unlawful digital data transformation, many watermarking systems have been proposed to tackle the problem [2–4]. In this field, numerous researchers have done great work. The authors of [5, 6] proposed a Discrete Wavelet Transform (DWT) based blind image watermarking algorithm coupled with a second level Singular Value Decomposition (SVD) algorithm to improve both

✉ Md. Ahasan Kabir, kabir.ece07@gmail.com | <sup>1</sup>Department of Electronics and Telecommunication Engineering, Chittagong University of Engineering and Technology, Chittagong, Bangladesh.



imperceptibility and robustness. The authors used image blocking to find the optimum image sub-block size. Also, a two-level authentication is performed to ensure security. Liu et al. [7] proposed a chaotic-based watermarking algorithm. The watermark bits has generated by mapping the differential binary image from the original chaotic image. Then, the watermark bits have embedded into the LSB bit-plane on the original image. Rawat [8] proposed a chaotic pattern-based fragile watermarking algorithm, using an 'XoR' operation between a binary watermark image and a chaotic logistics mapping image. All these strategies are effective in some common attacks, but can't resist attacking content alone. In order to address this issue, a fragile watermarking algorithm based on [8] has been proposed by Teng et al. [9]. The Local Binary Pattern (LBP) in the watermarking area has been introduced in [10, 11]. Zhang and Shih proposed a semi-fragile aqueduct based on space-related LBP operators [10]. The host image is fitted with a binary watermark by changing the pixel values of the neighborhood in each block using its LBP pattern. Experimental results have shown that this algorithm has some degree of robustness on overall image processing operations, such as contrast and JPEG compression. The main disadvantage of these watermarking systems is that the detection process is not blind. When the detection process is applied on the receiver side, the original watermark or image required. This is not possible because it is quite difficult to provide the original watermark or image at the receiver. Therefore, the semi-blind and blind watermarking method with high detective precision becomes a subject of study. Benrhouma et al. [12] proposed a watermarking algorithm for blind manipulator detection in which a local pixel contrast is established between the pixel values of the neighborhood and the average pixel value of the respective frames. Preda [13] has proposed a semi-fragile wavelet-based watermarking scheme. The wavelet coefficients are permuted first by using a secret key and then it has been divided into various groups. The watermark is used as a binary random sequence made up of the secret key. The watermark bits are generated by quantizing the coefficients. Despite low watermark payloads, this approach achieves better image quality. Nevertheless, several noise dots are scattered in the image during tamper detection, which decreases the detection accuracy. Filtering and morphology operations are performed to purify noise points. However, for different images, it is hard to achieve and the post-processing operations should be different. The literature survey shows that any watermarking scheme requires a subset of the following property. Imperceptibility: The fundamental requirement for unseen watermarking. In other words, it is vital after the watermark is incorporated to maintain good visual quality. Robustness: The watermark should be constructed so

that all assaults do not affect the system performance. Reversibility: Watermarking is one of the finest authentications and manipulation detection methods. However, the watermark may harm the significant data in the initial cover image after the insertion phase. So, a precise cover image at the receiver is hard to obtain. However, applications include military, medical, etc., where it is important to recover initial cover media. Reversible watermarking systems are used in such applications instead of standard watermarking. Payload: The number of watermark bits is the payload. Security: security is evaluated by the assessment of the system's strength against current assaults. Existing research has shown that in practical application some safety loopholes exist in the watermarking technology. Tamper detection: Manipulation is a deliberate change of files to harm consumers. It is therefore important that during the extraction phase, the watermark and the cover image is revealed. Authentication: Authentication ensures the claimed entity.

However, there are few methods that exist to achieve tamper detection, authentication, and restoration problems in one model. Moreover, most of these study attempts focused on the gray image. Few numbers of study have been made on the enhancement of the visual appearance of the image, and many of those watermarking systems have focused on the effectiveness to detect the tamper region. So, it is essential to develop a system for watermarking which could detect manipulation and also check authenticity to fully retrieve information. Some scientists have used error recovery into account in watermarking systems through the LBP. The contributions of this paper are described as: a fragile watermarking algorithm has been proposed based on a pixel by pixel processing image authentication, tamper detection, and watermark restoration. Here the cover image has transformed into the wavelet domain using the CDF 9/7 bi-orthogonal wavelet. It has a huge success in image compression. The transform coefficient is encoded using the SPIHT algorithm. Then watermark bits have shuffled and encrypted to provide security of the watermark. The embedding process has been done pixel by pixel in the LSB layer of the cover image. Also, two tamper detection bits are embedded into the LSB of each pixel sub-blocks to detect the tampering region. Self-embedding watermarking is done to reconstruct the watermark and host image. The authentication watermark generation process is the reverse of the encoding process. The remaining paper is structured as follows. A brief literature review has presented in Sect. 2. The proposed watermarking algorithm with a suitable block diagram has been presented in Sect. 3. The experiments and performances of different methods are reported in Sect. 4 followed by the concluding remarks are given at the end of this paper.

## 2 Literature review

This section provides a brief of the development and application of the watermark authentication and recovery process. The performance of the watermarking process is generally described by the recovered watermark, recovered cover image, and the condition of the restoration process. The quality of the recovered image is compared with the original image and it is represented by Peak Signal to Noise Ratio (PSNR), Structural Similarity Index (SSIM), etc. The quality of the watermark and the restoration image is highly depending on the tampering rate. Higher the tampering rate causes more restoration data have been lost, resultant a low-quality image is recovered. A large number of algorithms exist to recover tamper content [14–16]. In image authentication techniques, generally, the watermarked image is generated by embedded the watermark bits in the LSB position of the cover image. So, any modification of the watermarked image will change the LSB bit plane and will be lost the watermark bits. The authors of [17] proposed a non-blind digital watermarking technique to preserve the ownership of the color image. In this algorithm, the original watermark is extracted from four similar watermarks. To do this, four similar watermarks are extracted from the watermarked image, which is then combined to generate sub-watermark images, among these images the appropriate watermark is selected using the correlation coefficient (CC). A lossless compression-based image watermarking scheme has been proposed in [18]. Here adaptive prediction technique is used to compress medical images to produce watermark bit and embedded in the LSB of the original image. An adaptive image watermarking algorithm has been proposed in [19] for color images by using the features of the Discrete Cosine Transform (DCT), DWT, and Arnold transformation. The DCT based watermark generation is described in [19, 20]. In these methods, the watermark and original image have divided into image sub-block and independently applied DCT on each block. The DCT coefficients of the watermark block has been partially added with the DCT coefficients of the original image and inverse DCT has been performed to generate the watermarked image.

In many watermarking algorithms, the authentication bits and recovery bits are embedded into another block of the original image. If these blocks have tampered, it is not possible to recover the watermark bits. This tampering process is called a coincidence problem. The algorithms described in [21–23] do not deal with this problem. A hierarchical watermarking algorithm has been proposed in [24]. In this algorithm, the author used four levels of tamper detection process and used

2 authentication watermark bits in each 2x2 image sub-block. Due to the block independency of the authentication, this algorithm is vulnerable against Vector Quantization (VQ) and collage attack. In the reconstruction phase, the bits are recovered by averaging the 6 MSB bit planes of the sub-block.

The authors of [14, 25] used a reference sharing mechanism to proposed a self-embedding watermarking method. By embedding the redundant information in the cover image both methods provide improved quality of the recovered cover image. Again, the described algorithm is vulnerable to the VQ attack. The accuracy of tamper localization is decreased due to the use of a large block.

In [26] authors proposed a self-embedding watermarking algorithm to avoid coincident problems. In this method, the watermark bits have been inerted to the whole image. At first, the watermark image pixels are permuted using a secret private key and a series of pixel pairs are used to divide the permuted image. The recovery bit is generated by XoR the pixel pair of the 5th MSB layer. The recovery bit is generated by XoR the pixel pair of the 5th MSB layer. The generated authentication bits and recovery bit have been embedded into the 3rd LSB bit plane of the cover image. In this method, the reference data is used to recover the 5th MSB bit plane. The percentage of the actual recover bit extraction depends on the amount of the tampering rate.

Recently the deep learning-based image watermarking became popular to achieve high capacity and robustness of the watermarking systems [27–29]. The synergetic neural networks based digital image watermarking has proposed in [27] to ensure the security and robustness of the watermarking system. The authors embedded the watermark bits into the block DCT component. In this algorithm, the cooperative neural network has been used to detect and extract the watermark. In [28], the host image is divided into equal size subblock, and each sub-block is transformed using slantlet transformation. Three copies of watermark information are embedded into the cover image. Optimal block selection logic is used coupled with a multilayer deep neural network. A robust zero watermarking algorithm has been proposed in [29] based on conventional neural networks and deep neural networks. The watermarked image has been generated using Conventional Neural Network (CNN) and XoR operation between the cover image and the watermark image.

## 3 Proposed method

The proposed watermarking algorithm is described in this section. In the proposed method, the watermark bits generation is done in the transform domain, however,

the embedding is done in the spatial domain. The overall image watermarking process is divided into five steps: bi-orthogonal CDF 9/7 wavelet transform, then encoding the wavelet coefficient using the SPIHT algorithm, after that, the watermark bits are permuted and encryption using private keys, then generated two tamper detection bits and finally the embedding process is done in the cover image. Additionally, an error correction coding is used to become the algorithm more robust against different attacks. The block diagram of the proposed watermarking algorithm is shown in Fig. 1.

### 3.1 Wavelet transformation

The wavelet transform creates a floating-point coefficient, which helps to compress the image significantly [30]. Although these coefficients are sufficient to reconstruct the original image, the quantization of the coefficient using finite arithmetic precision turns the process into lossy. In the proposed algorithm a bi-orthogonal wavelet is used to decompose the image. The bi-orthogonal wavelet has the invertible capability and supported the symmetric property. These symmetric properties of filter coefficients are required for the linear transfer function. However, the bi-orthogonal wavelet transform has two scaling functions, which efficiently generates multi-resolution coefficients. The CDF 9/7 bi-orthogonal wavelet transform produces a greater number of zero coefficients and the image energy is concentrated within fewer bits. The wavelet filter pairs have the ability to convert into a primary and dual lifting sequence to lift the application. Figure 2 shows the 2-level wavelet transform of Bird image. The 9/7 filter poly-phase matrix for effective production are as follows:

$$W(x) = \begin{bmatrix} 1 & a(1+x^{-1}) \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ d(1+x) & 1 \end{bmatrix} \begin{bmatrix} 1 & c(1+x^{-1}) \\ 0 & 1 \end{bmatrix} \begin{bmatrix} K & 0 \\ 0 & 1/K \end{bmatrix} \tag{1}$$

where a, b, c, d are the four lifting parameters and K is the scaling parameter.

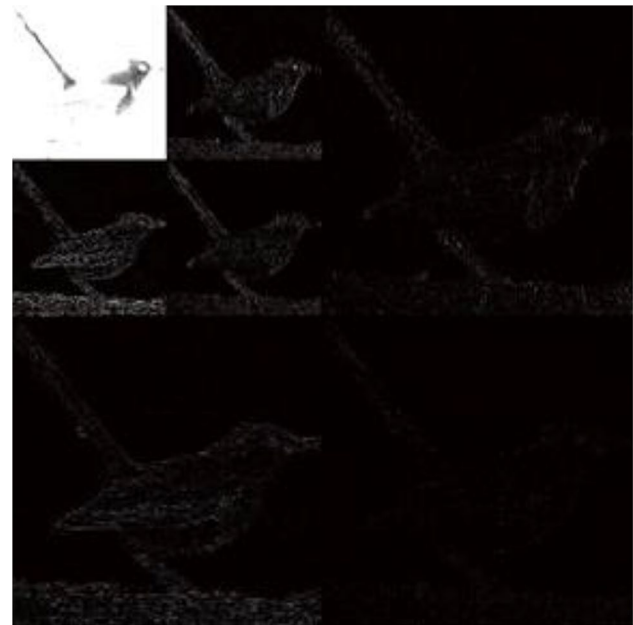


Fig. 2 The output of the two-level wavelet transform of bird image

### 3.2 Encoding with SPIHT algorithm

The set partitioning in the hierarchical tree is the most advanced image encoding technique. Its performance is quite better than the existing well-known state of art methods such as JPEG-2000, EZW. It is a progressive coding method, where the wavelet transformed coefficient is considered significant or insignificant based on a threshold [31]. If a particular coefficient of subband has the highest level of value against the threshold is considered as a significant subband otherwise insignificant. In this way, a large group of coefficients has been encoded using fewer bits. The SPIHT algorithm saves a large number of bits according to this relationship that indicates minor coefficients. SPIHT works on two steps: sorting pass and refinement pass.

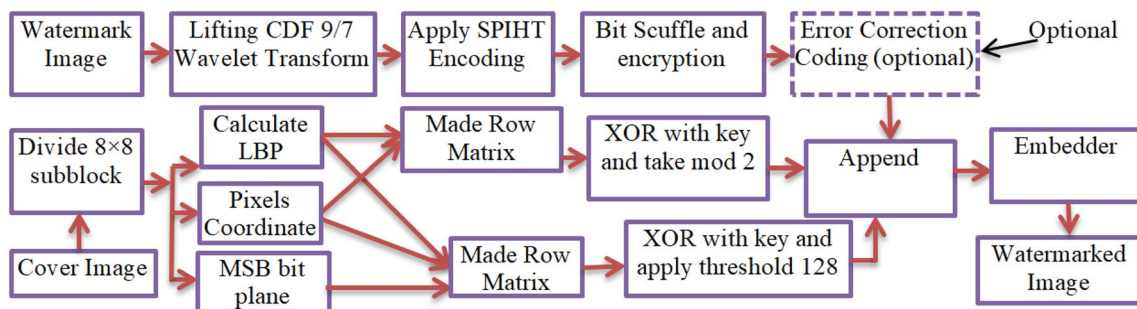


Fig. 1 Block diagram of the proposed watermarking algorithm

The block diagram of the SPIHT algorithm is presented in Fig. 3. At the beginning of the encoding process, the highest coefficient value is used to calculate the maximum iteration number. Then, the wavelet coefficient is put into the sorting pass and searching all significance coefficients. The sign of each significant coefficient has been encoded by 0 or 1 for (-) negative or (+) positive coefficient respectively. All significant coefficients are put into the refinement pass from the sorting pass for encoding each coefficient. So, two bits are required to reconstruct and approaching to the real value. The above process is repeated iteratively and the threshold  $T_n$  decreases in each step. The threshold value  $T_n = 2^n$  where  $n$  is the number of iterations starting with the highest value. The reconstruction process is just reverse and the reconstruction value is considered as  $(R_n - R_{n-1} - 1/2)$ .

### 3.3 Error correction coding

The error correction code is widely used to correct the bit error. In the proposed watermarking algorithm, the convolutional encoder has been used to correct bit error and the Viterbi decoder to decode the encoded bit sequences. The SPIHT coding is very vulnerable to reconstruct the watermark in case bit error. To reduce the bit error and to enhance the reconstructed watermark image, here used 1/2 convolutional error correction coding. At first, the SPIHT algorithm encodes the most significant coefficient and then encodes the less significant coefficient. However, the Most Significant Bit (MSB) can reconstruct the original image approximately. In this work, the first 15,000 bits have considered as a most significant bit, which is encoded by using a 1/2 convolutional encoder, and the other 5536 bits are considered as the less important bits. The less important bits kept unencoded. Finally, 35,536 bits (equivalent to 0.25 bpp) have been embedded into the cover image. Figure 4 shows the block diagram of 1/2 convolutional encoder. At the reconstruction phase, the Viterbi algorithm has been used, which is the most efficient method and used the maximum likelihood decoding algorithm. The algorithm calculates the mean distance between the received signal and the trellis path entered in each state [32]. The Viterbi algorithm drops the least likely trellis path at each stage which decreasing decoding complexity and provides efficient concentration on survival paths of the trellis.

Fig. 3 Block diagram of SPIHT algorithm

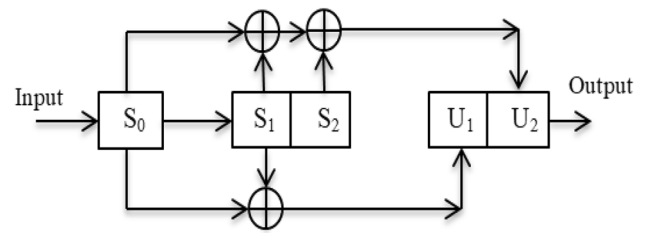
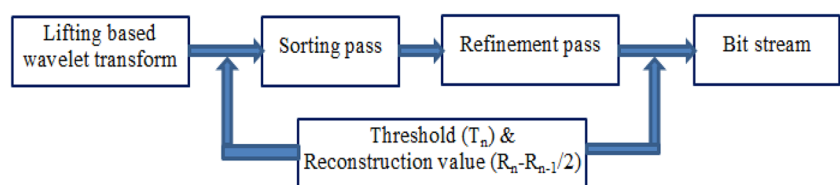


Fig. 4 Block diagram of 1/2 convolutional encoder

### 3.4 Encryption

Encryption converts the data in a form that is difficult to understand by the intruder. The encryption process in the watermarking system hides the watermark information from the intruder. Also, this system can be used in data steganography applications. Moreover, data encryption ensures that no one can reconstruct the watermark image except the owner. To keep the watermark more confidential and difficult to understand here is used data permutation and three symmetric keys. The permutation process makes the data sequence random and the keys are used to encrypt the watermark bits. Figure 5 represents the data encryption process. At first, the data stream has been converted into an  $8 \times n$  block in a zigzag manner as shown in Fig. 5. Then, XoR is performed of every odd row with the secret symmetric key and keep unchanged every even row. After that, every pixel in each row is shifted differently and the shuffling process is done as:

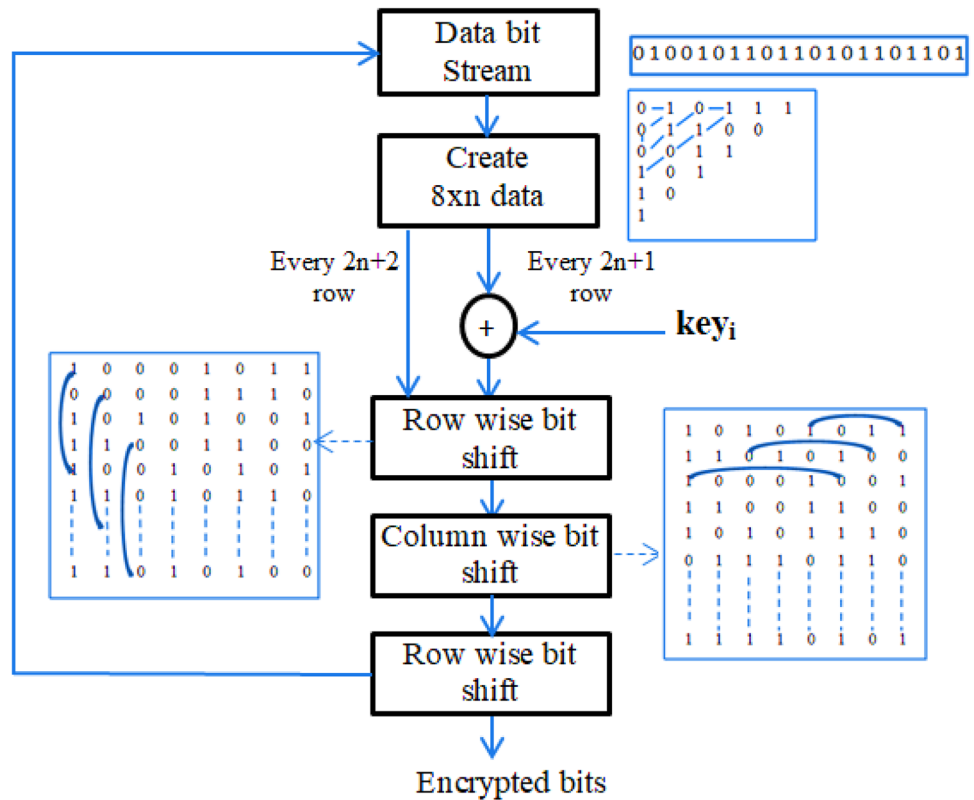
$$D_{ij} = D_{i(3m+1),j} \tag{2}$$

The initial value of 'm' is considered as 13 and decreases by one for each consecutive row. To get more random data, column-wise and row-wise shuffling is done and mixing all bits effectively. The whole process has repeated several times, in this experiment the encryption process done three times.

### 3.5 Tamper detection bits generation and embedding process

The bits have been embedded in the LSB of the cover image. The cover image has been divided into  $8 \times 8$  non-overlapping blocks. Sixteen watermark bits and 2 tamper

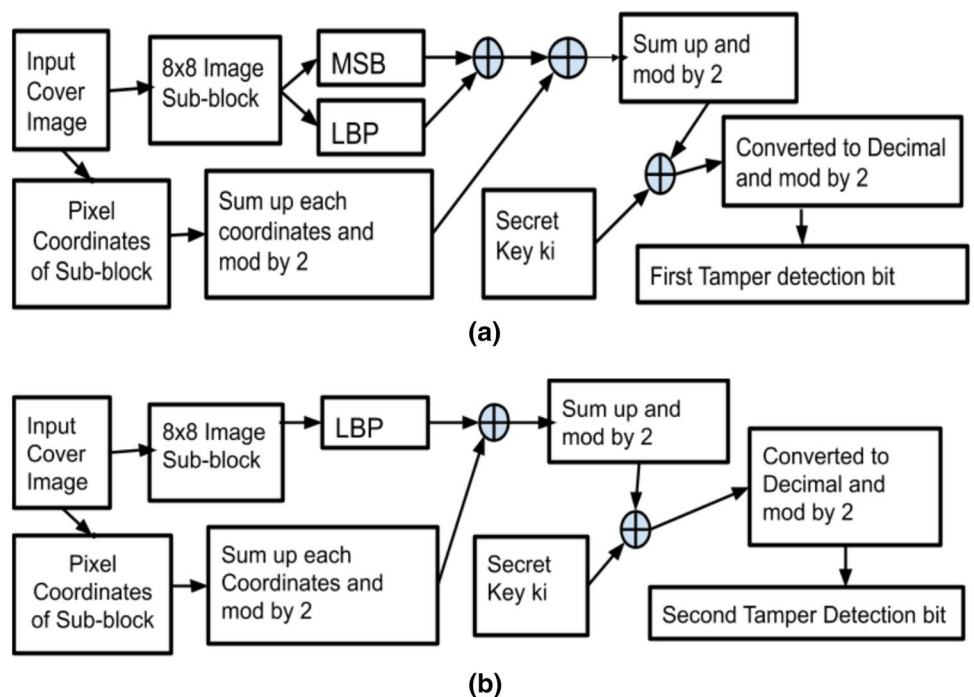
**Fig. 5** Data encryption flow chart for the proposed algorithm



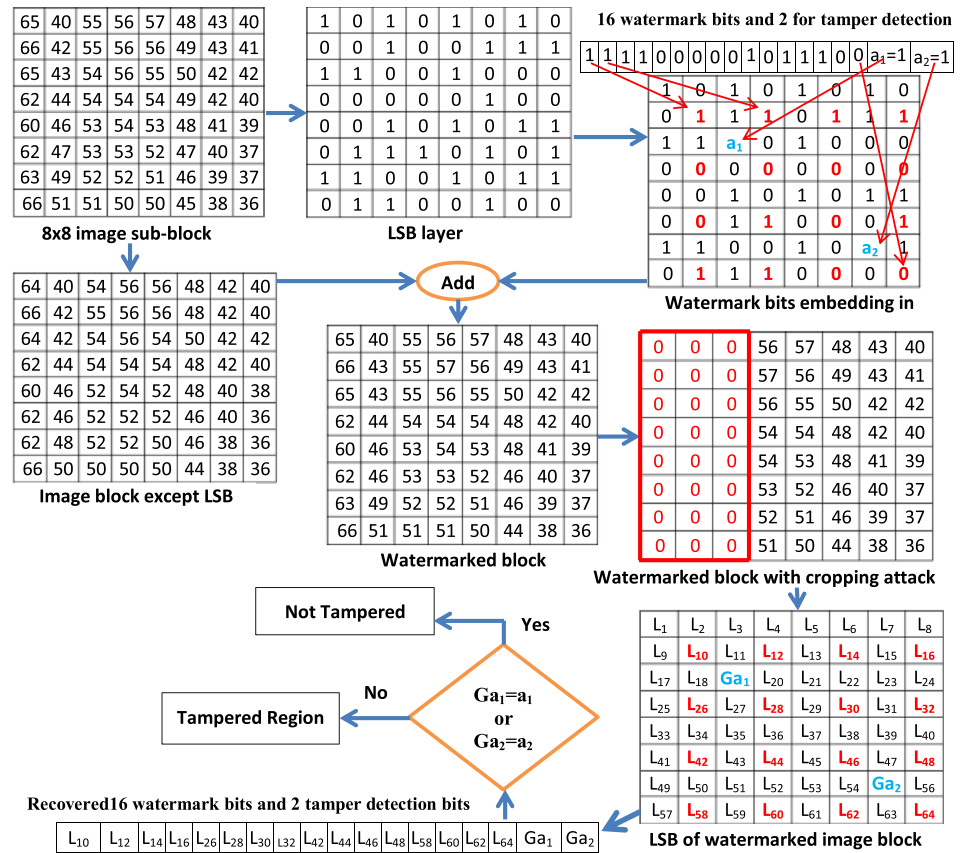
detection bits are embedded in each block and keep a specific distance between every embedded bit position. The watermark embedding process with an example is shown in Fig. 7. Two-tamper detection bits are generated

using the LBP information, pixel coordinates, MSB value, and a secret key. Figure 6 represents the key generation process for the tamper detection of the proposed watermarking algorithm. The LBP is the best technique to find

**Fig. 6** Key generation process for tamper detection of the proposed watermarking algorithm. **a** First key generation process and **b** Second key generation process



**Fig. 7** Example of the watermark embedded and extraction process of the proposed watermarking algorithm



the texture information of the cover image. The tamper detection keys generation process are described as:

1. The cover image has divided into  $8 \times 8$  non-overlapping blocks.
2. Calculated the LBP of the non-overlapping image sub-block. The LBP value is 1 when the center pixel's value is greater than its average value of the neighboring pixel, otherwise, it is 0.
3. Now, summed up each coordinate (i, j) of each block, mod it by 2, then the result is 'XoR' with LBP.
4. Summed up each column of step 3, then the result is mod by 2 to create a binary row matrix.
5. Now, the row matrix is encrypted by XoR with secret key  $k_i$ .
6. After that, the row matrix has converted into a decimal number, to get the first tamper detection bit  $a_1$ , the decimal number is modded by 2.
7. To generate the second tamper detection bit  $a_2$ , the MSB value has been 'XoR'ed with the LSB value of each pixel block.
8. Steps 5 and 6 is repeated to get the second tamper detection bit  $a_2$ .

### 3.6 Watermark extraction

The watermark extraction process is done by watermark reconstruction, tamper detection, and localization. The extraction processes are as follows:

1. The watermarked image or any suspicious image has divided into  $8 \times 8$  non-overlapping image block.
2. All bits from the specified pixel position have Extracted. These are the encrypted watermark.
3. The watermark bits are obtained by decrypting the extracted watermark.
4. The SPIHT decoding algorithm is applied to the watermark and generate the wavelet approximation coefficients.
5. After the inverse wavelet transform, the approximate watermark image is found.
6. For tamper detection and localization, the two-tamper detection bit  $Ga_1, Ga_2$  is calculated as described earlier for the taken watermarked image.
7. Tamper detection bits  $a_1, a_2$  is extracted from the watermarked image. If  $Ga_1 = a_1$  and  $Ga_2 = a_2$ , then the block is valid otherwise the block is marked as a tampered block.

### 4 Result and discussion

This section evaluates the performances of the proposed watermarking system. A set of images with size  $512 \times 512$  has been considered to test the performance of the proposed scheme. The experiment is performed in Intel core-i3, 3110M CPU, 1000 series hp laptop. Which have 4GB RAM, 64 bit windows operating system and 2.40GHz clock frequency. More specifically, here are used four different image datasets USC-SIPI [33], UCID [34], STARE [35], and HDR [36] for performance testing and also use some well-known standard images. The USC-SIPI image dataset contain digitized image with  $256 \times 256$ ,  $512 \times 512$  and  $1024 \times 1024$  pixels. The gray images are 8 bits/pixel and the color image have 24 bits/pixel. The image dataset has textures, aerials, miscellaneous, and sequences type images. UCID is an uncompressed color image dataset having 1338 images. The STARE dataset contains 20 retinal fundus images with  $700 \times 605$  pixels. The dataset has two-part, one part used for training and testing and the other part acts as baseline. The HDR image dataset has 105 images and the image is captured using a Nikon D700 digital still camera. The raw image contains 14 bits image with size  $4284 \times 2844$ . Three different types of watermark images are considered, one is a bird image; another one is a logo image and the last one is the self-embedded image. All watermark images are  $128 \times 128$  in dimension. Figure 8 shows 8 standard images along with the watermark image, the embedded watermarked images, and the corresponding recovered watermark image. Figure 7 shows that there is no visual distortion on the watermark image and the

recovered watermark approximations have perfect visual quality. To calculate the performances and effectiveness of the proposed method here are calculated Peak Signal to Noise Ratio (PSNR), Structural Similarity Index Measurement (SSIM), Mean Square Error (MSE), Quality Index (Q-index) and Normalized Correlation Coefficients (NCC). The PSNR, MSE, SSIM, NCC, and Q-index of the standard  $512 \times 512$  images are shown in Table 1. The table has shown that the average PSNR of the watermarked image is 56.21. The average MSE, SSIM, NCC and Q-index are 0.1158, 0.9988, 0.9999 and 0.9954 respectively. Also, the proposed algorithm tested on four different datasets and calculates the performance parameter which is shown in Table 2. The tested algorithm shows a better performance parameter value of the watermarked image. Also, Table 2 shows the variation of PSNR, MSE, SSIM, NCC, and Q-index value for the SIPI, UCID, STARE, and HDR image datasets. In the case of the SIPI data set used 64 texture images and 38 aerials images and achieved above 56.1374dB and 56.3774dB average PSNR. 100 images have been used for both UCID and HDR datasets and got an average of 56.5815dB and 56.615dB respectively. However, 56.5463dB average PSNR is found for 397 images in the STARE dataset. Again Table 3 represents the various evaluation results of the four individual images in four datasets. It is shown that the DHR, STARE, and UCID images have greater PSNR than 56.5dB, and SIPI images have less PSNR than 56.5dB. Table 4 shows the comparison of PSNR for Lena, Pepper, Barbara, and Soldhill images for various existing watermarking algorithms with other proposed algorithms, and the comparison of the proposed scheme is done with the

Fig. 8 Standard images along with watermark image, recovered watermark image

Image name	Cover image	Watermark image	Watermarked image	Recover watermark	Image name	Cover image	Watermark image	Watermarked image	Recover watermark
Lena					Barbara				
	512x512	128x128	56.6702dB	33.5066dB		512x512	128x128	56.0012dB	33.5066dB
Boat					Flin-stones				
	512x512	128x128	56.2712dB	33.5066dB		512x512	128x128	56.2215dB	33.5066dB
pepper					Babbon				
	512x512	128x128	56.3401dB	33.5066dB		512x512	128x128	56.429dB	33.5066dB
Im0370					Ucid 00024				
	512x512	128x128	57.1748dB	33.5066dB		512x512	128x128	56.2323dB	33.5066dB



**Table 1** Comparison of PSNR, MSE, MSSIM, NCC, Q-index and total computation time (TCT) of the standard 512 × 512 images

Image name	PSNR	MSE	SSIM	NCC	Q_index	TCT
Lena	56.6702	0.1206	0.9988	1	0.9954	14.245s
Barbara	56.0012	0.1207	0.9994	1	0.9971	14.834s
Boat	56.2712	0.1219	0.9992	1	0.9982	13.984s
Flinstones	56.2215	0.1233	0.9987	0.9999	0.9972	14.223s
Peppers	56.3401	0.1207	0.999	1	0.997	14.349s
Babbon	56.429	0.1214	0.9999	1	0.9995	14.516s
im0370	57.1748	0.075	0.9979	1	0.9882	14.401s
ucid00024	56.2323	0.123	0.9972	0.9999	0.9905	14.280s
Average	56.21	0.1158	0.9988	0.9999	0.9954	14.354s

**Table 2** Comparison of PSNR, MSE, SSIM, NCC, Q-index and total computation time (TCT) of four different dataset with standard 512 × 512 images

Database name	Image size	image number	PSNR	MSE	SSIM	NCC	Q_index	TCT
SIPI_Texture	512 × 512	64	56.1374	0.1399	0.9821	1	0.9995	14.618s
SIPI_Aerials	512 × 512	38	56.3774	0.121	0.9985	1	0.9973	14.583s
Ucid	512 × 512	100	56.5815	0.1409	0.9939	1	0.9891	14.293s
STARE	512 × 512	397	56.5463	0.1348	0.9958	1	0.9852	14.137s
HDR	512 × 512	100	56.615	0.1427	0.9638	0.9996	0.9585	14.207s

**Table 3** Comparison of PSNR, MSE, SSIM, NCC, Q-index, and total computation time (TCT) of four different dataset images

Data set	Images	PSNR	MSE	SSIM	NCC	Q_index	TCT
HDR [33]	S0010	56.6917	0.1393	0.9943	1	0.9652	14.091s
	s0020	56.2768	0.1533	0.9917	0.9998	0.9441	14.210s
	s0030	56.6899	0.1393	0.9868	0.9999	0.9507	14.235s
	s0040	56.6503	0.1406	0.9697	0.9999	0.9202	13.895s
UCID [34]	ucid00001	56.6152	0.1418	0.9981	1	0.9797	14.424s
	ucid00002	56.6624	0.1402	0.9817	1	0.9639	14.223s
	ucid00003	56.6538	0.1405	0.9997	1	0.9982	14.437s
	ucid00004	56.6645	0.1402	0.9972	1	0.9905	14.256s
STARE [35]	im001	56.2373	0.1169	0.9941	0.9999	0.978	14.167s
	im003	56.3182	0.1182	0.995	1	0.9819	14.245s
	im008	55.5621	0.119	0.9941	0.9999	0.9686	14.001s
	im009	55.7884	0.1185	0.9805	0.9999	0.9569	14.329s
	1.1.01	57.1073	0.1188	1	1	1	14.578s
SIPI [36]	1.1.02	56.2518	0.1168	1	1	0.9999	14.673s
	1.1.03	56.7757	0.116	0.9877	1	0.9997	14.762s
	1.1.04	56.4238	0.1174	0.9999	1	0.9996	14.349s

existing LBP scheme. The comparison has shown that for Lena image the proposed algorithm provides better PSNR 56.6702dB than 46.7dB-53.6dB [1, 37–42, 44–46], [47], and comparable with 57.31 [43]. The result of the proposed algorithm has shown that the scheme has better visual quality (56dB PSNR), which is very important in medical, military, and e-governance applications. Table 3 shows the performance in terms of PSNR, MSE, NCC, SSIM, and Q-index for the four different datasets images.

The robustness of the proposed algorithm is analyzed by measuring the evaluating parameters such as PSNR,

SSIM, Q-index, NCC, and BER in presence of different types of attacks as salt and pepper noise, cropping, and copy-move and forgery. The effect of the salt and pepper noise on the Lena image is shown in Figs. 9, 10, and 11 represent the effect of cropping and copy-move and forgery on the Lena and Boat image respectively. From these experiments it is shown that the reconstructed watermark image is slightly changed in quality, however, the tamper location of the watermarked image has been identified efficiently.

Figure 12 represent 3 different types of phase. The definition of each phase are:

**Table 4** Peak Signal to Noise Ratio (PSNR) comparison of various existing watermarking algorithm

	Lena	Pepper	Barbara	Goldhill	Payload (Bits)
Pabitra et al. [37]	53.57	53.57	53.59	53.56	693,600
Jana et al. [38]	52.81	52.72	52.76	52.78	74,752
Jung et al. [1]	48.18	48.18	48.15	48.19	519,180
Jafar et al. [39]	48.7	48.7	48.7	48.72	650,369
Lu et al. [40]	49.2	49.19	49.22	49.23	524,288
Qin et al. [41]	52.11	51.25	52.12	52.12	557,052
Lee and Huang [42]	49.76	49.75	49.75	49.77	1.07 bpp
Wang [43]	57.31	–	57.31	–	–
Chang et al. [44]	39.89	39.94	39.89	39.9	802,895
Cao et al. [45]	49.9898	50.0839	49.8901	–	–
Penga [46]	51.8832	51.898	–	–	–
Araghi [5]	–	46.9093	46.9161	–	–
Deng [27]	–	48.41	50.12	–	–
Sinhal [28]	39.9736	40.0318	39.0337	–	–
Proposed method	56.6702	56.3401	56.0012	55.8923	35,536 (.28125 bpp)

**Fig. 9** Effect of various strength salt and pepper noise on Lena watermark image

Cover image (512×512)	Watermark (128×128)	Watermarked image	Recovered watermarked	Data of recovered watermark images
				PSNR in dB: 24.9695 MSE: 191.1531 MSSIM: 0.7155 NCC: 0.9993 Q-index: 0.687
Lena	Logo Image	SaltPepper .005	29.5987dB	
				PSNR in dB: 22.1453 MSE: 366.2702 MSSIM: 0.5964 NCC: 0.9981 Q-index: 0.5194
Lena	Logo Image	SaltPepper .01	25.4241dB	
				PSNR in dB: 20.3589 MSE: 552.644 MSSIM: 0.5211 NCC: 0.9972 Q-index: 0.4086
Lena	Logo Image	SaltPepper .015	23.5685dB	
				PSNR in dB: 19.1208 MSE: 734.9351 MSSIM: 0.4754 NCC: 0.9968 Q-index: 0.3416
Lena	Logo Image	SaltPepper .02	21.719dB	

Phase 1: The watermark image has  $128 \times 128$  pixels and the reconstructed image have the same size ( $128 \times 128$ ).

Phase 2: The watermark image has  $128 \times 128$  pixels and the reconstructed image have  $512 \times 512$  pixels.

Phase 3: The watermark image has  $512 \times 512$  pixels and the reconstructed image have the same size ( $512 \times 512$ ).

In the proposed self-fragile watermarking algorithm, the  $128 \times 128$  image is the resized image of the cover image ( $512 \times 512$ ). After the reconstruction of the watermark image ( $128 \times 128$ ) is converted into a  $512 \times 512$  image, which is marked as phase 2 in Table 5. This reconstructed image (Phase 2) is used to reconstruct the tampered region of the watermarked image. At a low bit rate, the Phase 2 approach is well performed than when using a  $512 \times 512$  image as the watermark image (represent Phase 3). Figure 12 shows the comparison of the PSNR variation with respect to the changing of the number of bits. The experimental result has shown that at a low bit rate the Phase 2 watermark image provides better PSNR than the reconstruction done in Phase 3. However, at a higher bit rate, the reconstruction is done in Phase 3 achieve higher PSNR than the reconstruction done in Phase 2. Table 5 represents the experimental result for the reconstruct of original  $512 \times 512$  watermark images from the  $128 \times 128$  and  $512 \times 512$  watermark images. It has shown that at a lower bit rate the reconstruction from  $128 \times 128$  image (Phase 2)

provides better PSNR (23.2976, 25.8606, 27.7552 28.0593) then the process done from  $512 \times 512$  image (Phase 3) (8.9894, 11.8017, 14.184, 24.4337). Also, at a low bit rate Phase 2 provides better SSIM and MES than Phase 3. In the proposed watermarking algorithm are used 35,536 watermark bits to provide authentication of an image.

The self-embedding watermarking and reconstruction result is shown in Fig. 13. The experiment had been done on different cover images (Lena, Boat, and Barbara) and different attacks (cropping, and copy-move and forgery). It has shown that at low noise level the reconstructed watermark and the reconstructed cover image have better visual quality around 21dB and 30dB respectively. At higher cropping attack the proposed algorithm facing some vulnerability. At 40% of the cropping attack, many significant bits of the watermark image has corrupted, which destroys the reconstructed watermark image. To improve the visual quality of the watermark image, here incorporated the error correction algorithm that corrects the corrupted bits of the watermark image. The proposed algorithm used the state of art 1/2 convolutional encoder to encode the watermark bits and the Viterbi decoder is used to decode watermark bits. This approach has improved the visual quality of the watermark image and increases the visual image quality metrics such as PSNR, SSIM, Q-index, BER, and NCC. Figure 14 shows the results of the error correction approach and it is clearly shown that the analyzed result increased significantly. The proposed algorithm has tested on a different color image and provides a significant outcome. Table 6 shows the comparison of PSNR, MSE, SSIM, NCC, and Q-index for a different color image. The result has shown that the quality metrics of PSNR, MSE, SSIM, NCC, and Q-index are around 56dB, 0.14, 0.999, 1, 0.99 respectively.

**Table 5** The comparison of PSNR, MSE, and SSIM of reconstructed watermark image for the various size watermark bits

	Image size	No. of bits	PSNR	MSE	SSIM
Phase 1	$128 \times 128$	262,144	112.3527	3.2676E-07	1
Phase 2	$512 \times 512$		28.3868	84.838	0.8153
Phase 3	$512 \times 512$		38.0859	9.9484	0.8972
Phase 1	$128 \times 128$	131,072	75.3049	0.0017	1
Phase 2	$512 \times 512$		28.3768	84.8405	0.8152
Phase 3	$512 \times 512$		32.6521	32.911	0.7906
Phase 1	$128 \times 128$	65,536	51.7097	0.3785	0.9925
Phase 2	$512 \times 512$		28.0593	85.1118	0.799
Phase 3	$512 \times 512$		24.4337	273.5371	0.4322
Phase 1	$128 \times 128$	35,536	40.7459	4.7236	0.9603
Phase 2	$512 \times 512$		28.1706	89.3607	0.7399
Phase 3	$512 \times 512$		14.3217	2.44E+03	0.2014
Phase 1	$128 \times 128$	32,768	39.6951	6.0953	0.9508
Phase 2	$512 \times 512$		27.7552	91.0233	0.7234
Phase 3	$512 \times 512$		14.184	2678.8	0.1863
Phase 1	$128 \times 128$	24,576	35.9486	6.0953	0.92
Phase 2	$512 \times 512$		25.8606	91.0233	0.685
Phase 3	$512 \times 512$		11.8017	2678.8	0.108
Phase 1	$128 \times 128$	16,384	32.4234	38.748	0.8545
Phase 2	$512 \times 512$		23.2976	126.3072	0.6057
Phase 3	$512 \times 512$		8.9894	9528.8	0.0766

## 5 Conclusion

In this paper, SPIHT based fragile image watermarking scheme is presented. The CDF 9/7 wavelet transform has been used to convert the watermark image into the wavelet domain, and then the wavelet coefficients encoded using the SPIHT algorithm. This algorithm can localize the tamper region successfully and has restoration capability. The scheme also can detect copy-move falsification successfully, although a single bit is modified in an image. Due to the adaption of error correction coding, this scheme can correct the error bit which is created due to the tampering of the watermarked image and improves the quality of the reconstructed watermark image under different types of attacks. The proposed algorithm has tested on different standard benchmark images. Experimental results indicate that both watermarked images and watermarks are highly


























**Fig. 10** Effect of cropping attack on watermark Lena image

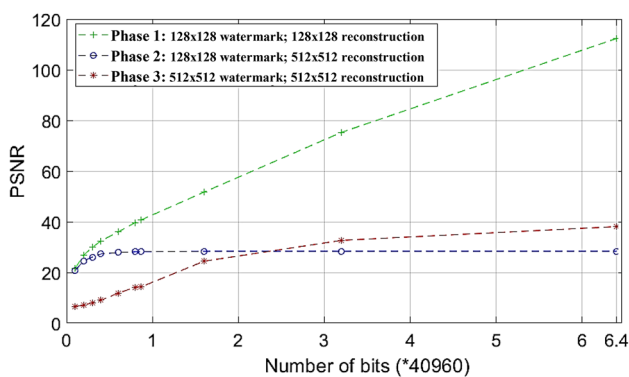
Cover Image (512×512)	Watermark (128×128)	Watermarked Image	Recovered Watermarked	Cropping Detection
				
Lena	Logo Image	Copping 51x51 pixels	PSNR= 42.2208dB NCC: 0.9935	
				
Lena	Logo Image	Copping 102x102 pixels	PSNR= 36.2008dB NCC: 0.997	
				
Lena	Logo Image	Copping 153x153 pixels	PSNR= 23.3385dB NCC: 0.9956	
				
Lena	Logo Image	Copping 204x204 pixels	PSNR= 22.2641 NCC: 0.9956	
				
Lena	Logo Image	Copping 256x256 pixels	PSNR= 21.1519 NCC: 0.9267	
				
Lena	Logo Image	Copping 307x307 pixels	PSNR= 14.2377 NCC: 0.855	

sensitive. The average PSNR of the proposed scheme is around 56dB which is higher than the existing LBP based scheme and provides better visual qualities. Also, the

security of the proposed scheme is strengthened when the block of data is encoded with the use of separate secret keys in case of a deliberate attack. It allows the proposed

**Fig. 11** Effect of copy move and forgery attack on watermark Boat image



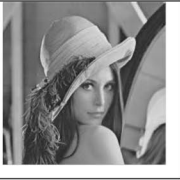




Cover image (512×512)	Watermark (128×128)	Watermarked image Copy move attack	Recovered watermarked	Copy move detection
				
Boat	Logo Image	50x50 pixels	PSNR: 39.1219 dB NCC: 0.9934	Attack 50x50 pixels
				
Boat	Logo Image	120x70 pixels	PSNR: 28.1787dB NCC: 0.9797	Attack 120x70 pixels
				
Boat	Logo Image	170x70 & 50x50 pixels	PSNR: 26.2917dB NCC: 0.9532	170x70 & 50x50 pixels
				
Boat	Logo Image	170x70 & 70x70 pixels	PSNR: 23.5359dB NCC: 0.9631	170x70 & 70x70 pixels
				
Boat	Logo Image	170x70, 70x70 & 45x45 pixels	PSNR: 19.7137 dB NCC: 0.919	Attack 170x70, 70x70 & 45x45



**Fig. 12** Comparison of the PSNR of the reconstructed watermark image

system as a better alternative for addressing authentication and copyright protection compared to similar watermarking schemes. This algorithm can be applied in many applications where image authentication and detection of tamper are essential. The proposed algorithm is a fragile watermarking scheme, so, the watermark information may be destroyed by applying basic image processing operations like blurring, contrast enhancement, JPEG compression. Therefore, in the future, the proposed scheme will be extended to a semi-fragile watermarking scheme couple with a deep learning algorithm.

**Fig. 13** Effect of different types of attacks on self-embedded watermarking approach

Cover image (512×512)	Copy move/crop attack	Attack region detection	Reconstructed watermark image	Reconstructed cover image
				
Lena	70x70 pixels	Attack 70x70 pixels	PSNR: 27.898dB NCC: 0.9931	PSNR: 39.5697 dB NCC: 1.000
				
Lena	120x70 pixels	Attack 120x70 pixels	PSNR: 27.5468dB NCC: 0.9924	PSNR: 43.4975 NCC: 1.000
				
Boat	70x70 pixels	Attack 70x70 pixels	PSNR: 24.7859dB NCC: 0.9868	PSNR: 38.2054dB NCC: 0.9997
				
Barbara	Crop attack 10%	Crop attack 10%	PSNR: 23.2836dB NCC: 0.9814	PSNR: 33.725dB NCC: 0.9999
				
Barbara	Crop attack 20%	Crop attack 20%	PSNR: 21.6853dB NCC: 0.9804	PSNR: 30.013dB NCC: 0.9993
				
Barbara	Crop attack 30%	Crop attack 30%	PSNR: 9.02dB NCC: 0.5817	PSNR: 23.7393dB NCC: 0.9819
				
Barbara	Crop attack 40%	Crop attack 40%	PSNR: 5.2976dB NCC: 0.1203	PSNR: 12.5396dB NCC: 0.5927

**Fig. 14** Effect of different types of attack on reconstructed watermark image when error correction algorithm is used

Cover image (512×512)	Watermarked image	Different attack	Reconstructed watermark image	Data of recovered watermark images
				PSNR in dB: 22.018 MSE: 534.628 MSSIM: 0.5855 NCC: 0.998 Q-index: 0.5376
Lena	Logo Image	SaltPepper .015	PSNR 22.018 dB	
				PSNR in dB: 21.2865 MSE: 623.835 MSSIM: 0.4519 NCC: 0.8935 Q-index:0.4185
Lena	Logo Image	SaltPepper .02	PSNR 21.2865 dB	
				PSNR in dB: 24.3784 MSE: 474.233 MSSIM:0.8345 NCC: .9999 Q-index:0.8536
Lena	Logo Image	Cropping 256x256 pixels	PSNR 24.3784 dB	
				PSNR in dB: 16.3675 MSE: 956.6247 MSSIM: 0.4675 NCC: 0.7752 Q-index:0.3566
Lena	Logo Image	Cropping 307x307 pixels	PSNR 16.3675 dB	
				PSNR in dB: 14.546 MSE: 957.356 MSSIM: 0.5245 NCC: 0.7153 Q-index:0.4232
Barbara	Barbara	Crop attack 30%	PSNR 14.546 dB	
				PSNR in dB: 9.8945 MSE: 1634.675 MSSIM: 0.3845 NCC: 0.6456 Q-index:0.3652
Barbara	Barbara	Crop attack 40%	PSNR 9.8945 dB	

**Table 6** Comparison of PSNR, MSE, SSIM, NCC and Q-index for Color image

Image name	PSNR	MSE	SSIM	NCC	Q-index
Lena	56.1502	0.1478	0.9989	1.000	0.9965
Peppers	56.5993	0.1481	0.9985	1.000	0.9971
Airplane	56.5207	0.1482	0.9967	1.000	0.9907
Baboon	56.212	0.1473	0.9998	1.000	0.9994
ucid00022	56.4865	0.146	0.9998	1.000	0.9995
ucid00024	56.4934	0.1458	0.9999	1.000	0.9997

**Open Access** This article is distributed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made.

**Declarations**

**Conflict of interest** The author declare that they have no conflict of interest.

**Open Access** This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing,

adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

## References

- Jung KH (2018) Authenticable reversible data hiding scheme with less distortion in dual stego-images. *Multimed Tools Appl* 77(5):62256241
- Verma VS, Jha RK, Ojha A (2015) Significant region based robust watermarking scheme in lifting wavelet transform domain. *Expert Syst Appl* 42(21):81848197
- Pal P, Chowdhuri P, Jana B (2018) Weighted matrix based reversible watermarking scheme using color image. *Multimed Tools Appl* 77(21):2307323098
- Su Q, Chen B (2018) Robust color image watermarking technique in the spatial domain. *Soft Comput* 22(1):91106
- Araghi TK, Manaf AA (2019) An enhanced hybrid image watermarking scheme for security of medical and non-medical images based on DWT and 2-D SVD. *Future Generat Comput Syst* 101:12231246
- Araghi TK, Manaf AA, Araghi SK (2018) A secure blind discrete wavelet transform based watermarking scheme using two-level singular value decomposition. *Expert Syst Appl* 112:208–228
- Liu SH, Yao HX, Gao W, Liu YL (2007) An image fragile watermark scheme based on chaotic image pattern and pixel-pairs. *Appl Math Comput* 185(2):869–882
- Rawat S, Raman B (2011) A chaotic system based fragile watermarking scheme for image tamper detection. *AEU - Int J Electron Commun* 65(10):840–847
- Teng L, Wang XY, Wang XK (2013) Cryptanalysis and improvement of a chaotic system based fragile watermarking scheme. *AEU - Int J Electron Commun* 67(6):540–547
- Zhang WY, Shih FY (2011) Semi-fragile spatial watermarking based on local binary pattern operators. *Opt Commun* 284(16–17):3904–3912
- Chang JD, Chen BH, Tsai CS (2013) LBP-based fragile watermarking scheme for image tamper detection and recovery. In: *Proceedings of the IEEE international symposium on next-generation electronics*. Taiwan, Kaohsiung, pp 173–176
- Benrhouma O, Hermassi H, El-Latif AAA, Belghith S (2016) Chaotic watermark for blind forgery detection in images. *Multimed Tools Appl* 75(14):8695–8718
- Preda RO (2013) Semi-fragile watermarking for image authentication with sensitive tamper localization in the wavelet domain. *Measurement* 46(1):367–373
- Korus P, Dziech A (2013) Efficient method for content reconstruction with self-embedding. *IEEE Trans Image Process* 22:11341147
- Korus P, Dziech A (2014) Adaptive self-embedding scheme with controlled reconstruction performance. *IEEE Trans Inf Forensics Secur* 9:169181
- Singh D, Singh SK (2015) DCT based efficient fragile watermarking scheme for image authentication and restoration. *Multimed Tools Appl* 125
- Nasir I, Weng Y, Jiang J, Ipson S (2010) Multiple spatial watermarking techniques in color images. *Signal Image Video Process* 4(2):145154
- Castiglione A, Pizzolante R, Santis AD, Carpentieri B, Castiglione A, Palmieri F (2015) Cloud-based adaptive compression and secure management services for 3D healthcare data. *Future Gener Comput Syst* 43:120134
- Kalra GS, Talwar R, Sadawarti H (2015) Adaptive digital image watermarking for color images in frequency domain. *Multimed Tools Appl* 74(17):68496869
- Das C, Panigrahi S, Sharma VK, Mahapatra KK (2014) A novel blind robust imagewatermarking in DCT domain using inter-block coefficient correlation. *AEU-Int J Electron Commun* 68(3):244253
- Li C, Wang Y, Ma B, Zhang Z (2011) A novel self-recovery fragile watermarking scheme based on dual-redundant-ring structure. *Comput Electr Eng* 37:927940
- Shivani S, Singh D, Agarwal S (2013) DCT based approach for tampered image detection and recovery using block wise fragile watermarking scheme. In: *Pattern recognition and image analysis*. Springer, pp 640647
- Singh D, Shivani S, Agarwal S (2013) Quantization-based fragile watermarking using block-wise authentication and pixel-wise recovery scheme for tampered image. *Int J Image Graph* 13
- Lin PL, Hsieh CK, Huang PW (2005) A hierarchical digital watermarking method for image tamper detection and recovery. *Pattern Recogn* 38:25192529
- Zhang X, Qian Z, Ren Y, Feng G (2011) Watermarking with flexible self-recovery quality based on compressive sensing and compressive reconstruction. *IEEE Trans Inform Forensics Secur* 6:12231232
- Zhang X, Wang S, Qian Z, Feng G (2011) Self-embedding watermark with flexible restoration quality. *Multimed Tools Appl* 54:385395
- Li D, Deng L, Gupta BB, Wang H, Choi C (2019) A novel CNN-based security guaranteed image watermarking generation scenario for smart city applications. *Inf Sci* 479:432–447
- Sinhal R, Ansari IA, Jain DK (2020) Realtime watermark reconstruction for the identification of source information based on deep neural network. *J Real-Time Image Process* 17:2077–2095
- Fierro-Radilla A, Nakano-Miyatake M, Cedillo-Hernandez M, Cleofas-Sanchez L, Perez-Meana H (2019) A robust image zero-watermarking using convolutional neural networks. In: *7th international workshop on biometrics and forensics (IWBF)*, Cancun, Mexico, pp 1–5
- Kabir MA, Khan MAM, Islam MT, Hossain ML, Mitul AF (2013) Image compression using lifting based wavelet transform coupled with SPIHT algorithm. In: *2013 international conference on informatics, electronics and vision (ICIEV)*, Dhaka, pp 1–4
- Kabir MA, Mondal MRH (2018) Edge-based and prediction-based transformations for lossless image compression. *J Imaging* 4:64
- Kulkarni A, Mantri D, Prasad NR, Prasad R (2013) Convolutional encoder and Viterbi decoder using SOPC for variable constraint length. In: *2013 3rd IEEE international advance computing conference (IACC)*, Ghaziabad, pp 1651–1655
- University of Southern California. The USC-SIPI Image Database. <http://sipi.usc.edu/database/database.php>. Accessed 30 Sept 2019
- Nottingham Trent University, UCID Image Database. <http://jasoncantarella.com/downloads/ucid.v2.tar.gz>. Accessed 30 Sept 2019
- University of California, San Diego. STARE Image Database. <https://cecas.clemson.edu/ahover/stare/>. Accessed 30 Sept 2019
- Fun B, Shi L (2019) HDR Dataset Computational Vision Lab Computing Science, Simon Fraser University, Burnaby, BC, Canada. <http://www.cs.sfu.ca/colour/data/funthdr/>. Accessed 30 Sept 2019
- Pal P, Jana B, Bhaumik J (2019) Watermarking scheme using local binary pattern for image authentication and tamper detection through dual image. *Secur Privacy* 2:e59



38. Jana B, Giri D, Mondal SK (2018) Dual image based reversible data hiding scheme using (7, 4) hamming code. *Multimed Tools Appl* 77(1):763785
39. Jafar IF, Darabkh KA, Al-Zubi RT, Saifan RR (2016) An efficient reversible data hiding algorithm using two steganographic images. *Signal Process* 128:98109
40. Lu TC, Tseng CY, Wu JH (2015) Dual imaging-based reversible hiding technique using LSB matching. *Signal Process* 108:7789
41. Qin C, Chang CC, Hsu TJ (2015) Reversible data hiding scheme based on exploiting modification direction with two steganographic images. *Multimed Tools Appl* 74(15):58615872
42. Lee CF, Huang YL (2013) Reversible data hiding scheme based on dual stegano-images using orientation combinations. *Telecommun Syst* 52(4):2237–2247
43. Wang C, Zhang H, Zhou X (2018) LBP and DWT based fragile watermarking for image authentication. *J Inf Process Syst* 14:666–679
44. Chang CC, Chou YC, Kieu TD (2009) Information hiding in dual images with reversibility. In: *Third international conference on multimedia and ubiquitous engineering*, Qingdao, China
45. Cao F, An B, Wang J, Ye D, Wang H (2017) Hierarchical recovery for tampered images based on watermark self-embedding. *Displays* 46:52–60
46. Penga Y, Niub X, Fua L, Yina Z (2018) Image authentication scheme based on reversible fragile watermarking with two images. *J Inf Secur Appl* 40:236–246

**Publisher's Note** Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.