A Secure Self-Embedding Watermarking Scheme for Ensuring Digital Image Integrity

Monalisa Swain, Debabala Swain*
Rama Devi Women's University, Bhubaneswar, India
Corresponding author: debabala.swain@gmail.com

Article Info
Page Number: 1134 – 1149
Publication Issue:
Vol. 71 No. 3 (2022)

Article History
Article Received: *12 January 2022*
Revised: *25 February 2022*
Accepted: *20 April 2022*
Publication: *09 June 2022*

Abstract
With the rise of digital communication and multimedia information exchange, unauthorized access and manipulation of multimedia content are on the rise. Tamper detection and recovery mechanisms are necessary for maintaining the authenticity and protection of the transmitted images. There is a need for novel self-embedding fragile watermarking techniques with improved tamper recovery capabilities. In this work, we present a new method for watermarking in which the cover image gets divided into 2x2 sized non-overlapping blocks. The watermark information is generated by using six MSBs of each pixel in the block. A key value for each block is used to generate a mapping block number for its respective block. The mapping block is used to embed recovery data for each block. The presented method is validated with the number of altered photos and varying tampering rates. The PSNR and SSIM results show that the proposed technique provides better performance.

Keywords: - Block mapping; Fragile watermarking; Least significant bit; Self-embedding; Spatial domain; Tampered image recovery.

1. Introduction

Due to the network's rapid advancement, people are increasingly exchanging information over the Internet. The depth and breadth of digital media information transmission have reached unparalleled heights. People's lives are increasingly being influenced by image, music, and video. Digital image content is vulnerable to fraudulent changes and modifications due to advanced image processing technology and the widespread accessibility of editing software. The identification and localization of altered images, as well as their restoration, have become crucial challenges [1]. In critical situations, such as a patient's medical report, a little change occurs in the principal content of the medical image, and then it may cause a wrong diagnosis and hence wrong treatment for the patient. Identifying modifications in the images, localizing modified areas, and restoring the digital images have become critical issues [2-3].

In order to protect the integrity of digital images, there are various ways available. Digital Steganography, cryptography, and watermarking are considered effective approaches for ensuring data security and integrity. Steganography conceals a hidden message such as an image, video, or audio file within another signal. One of the primary uses of Steganography is the concealment and distribution of sensitive information [4]. When hidden information is embedded in images, this is referred to as "Digital Image Steganography" [5]. Another method of protecting data is cryptography. Digital image watermarking is a widely used technique for protecting the integrity of digital images with restoring capability. Watermark-based image authentication approaches are classified into three groups based on their authentication aims.

The first technique is known as "robust watermarking," and it can recover watermarks even after they have been assaulted by typical photo editing tools [6]. So, the robust watermark approach is widely employed in copyright verification and intellectual property. The second technique is known as fragile watermarking [7]. The watermark in this approach is extremely sensitive to manipulation, even if the image is just slightly altered. [8]. This approach can also identify and retrieve the tampered region. The third technique is known as semi-fragile watermarking [9]. Semi-fragile watermarking approaches are designed to withstand acceptable content-preserving modifications while still detecting modifications of content. This technology provides the best of the previous two technologies and is resistant to image processing.

Secret data is inserted in a cover image to prove the image's authenticity. Later it is extracted to show the identity of the content owner [10-12]. The secret information is embedded into original images to result in the watermarked image. A watermark may be derived from the cover image or it may be some other meaningful image. It may also be a random image or a random pattern of bits. For verifying the authenticity of a particular cover image, fragility is required. Out of the different watermarking techniques available, fragile watermarking is highly sensitive to a single bit of modification. A fragile watermark is embedded into the cover image in such a way that if the watermarked image tampers then the associated fragile watermark with that content is also tampered or destroyed. Self-embedding is the most suitable fragile watermark generation approach because it is completely based on user-defined algorithms and it is more accurate because of its tight coupling between the cover and watermark bits. A fragile watermark is simply a mark which will be destroyed as soon as any modification is made to the watermarked image. [13-15].

In this paper, a self-embedding fragile watermarking scheme is proposed, where the original image is divided into blocks of 2×2 pixels. The self-embedding technique is used to generate the watermark blocks. The Least Significant Bit (LSB) of each pixel is used to embed watermark information. As LSBs are the most suitable place for fragile watermark embedding. The paper contributes a novel fragile watermarking on sensitive images where the original image is used for watermarking using self-embedding. It signifies that the image can independently generate its watermark. The fragile watermark has its robustness than other watermark techniques. Because it can easily detect very minor changes (even a single bit) in the watermarked image, during transmission. This kind of detection is not possible in the robust watermark technique. Another implication of fragile watermarking is the property of imperceptibility, where the watermark image cannot be visually differentiated from the original image. The proposed work in the spatial domain represents the pixel-to-pixel transformation in the watermark image, which in reverse retrieves the accurate pixel value during the image recovery. When compared to existing procedures, the projected technique is better in terms of image recovery, as evidenced by the PSNR and SSIM values of the recovered images.

The remaining part of this work is stated as follows: Section II presents relevant work. The proposed scheme is described in Section III. Section IV presents the results of the experiments, and Section V presents the conclusions.

2. Related work

In the last few years, many fragile watermarking methods with blind recovery have been proposed for image security and authentication.

In [16], researchers presented a watermarking approach based on the Multiple Transform Technique for Image Contents. First, a JPEG image is created from the original image, and a 2D barcode and scrambling are used to create the watermark. Secondly, 2D DWT is used to decompose the JPEG image into 3 sub-bands: H, V, and D. Third, the DFRNT is applied to the sub-band coefficients (discrete fractional random transform). The quantized watermark image is then placed into the sub-band coefficient value. Finally, the inverse DFRNT and inverse DWT are applied, followed by the creation of a watermarked JPEG image. The suggested approach is robust and has high invisibility and retrieval efficiency.

In [17], researchers proposed a watermarking scheme for authentication and recovery of the digital image. Using a self-embedding method, the watermark data is generated by capturing 5MSBs of each pixel. The cover image is divided into 2 × 2 non-overlapping blocks. Watermarks are generated in blocks of 12 bits, with 10 bits acting as recovery data and 2 bits acting as authentication data. The entire watermark data is inserted into the mapping block of the respective block. The techniques of quantization and BTC are used while generating recovery data. The authentication data was obtained from the host image's MSBs. The experimental results of this scheme are satisfactory even for 50% of the tampering rate.

In [18], researchers proposed a watermarking scheme with superior localization of both natural and text images. This scheme is fragile and has restoring capacity. The host image was split into two separate block sizes, i.e., 4 × 4 and 2 × 2. Here, the watermark information contains data for both authenticity and restoration of the image. The block of size 4 × 4 was taken for authentication watermark generation using a hash function. The block of size 2 × 2 was taken for recovery watermark generation by using a binary pseudo-random sequence and key. The size of the recovery watermark varies depending on the nature of the block, whether it was a smooth or textured block. The authentication information was embedded in the same 4 × 4 block, and the recovery watermark was embedded in the mapping 2 × 2 blocks. The multi-stage neighbor detection approach was created to precisely discover the altered image blocks.

In [19], researchers proposed a self-recovery fragile watermarking approach for authentication and recovery of medical images. Here, images are divided into 4×4 blocks and singular value decomposition is applied to each block. Traces of SVD are embedded into the LSBs of the pixel value. As self-recovery information, an average value of the five most significant bits (MSB) is used, and authentication information is generated from the singular matrix in each block. Arnold transformation is used for bit recovery, embedding, and extraction. This scheme may withstand a vector quantization attack. This scheme effectively recovers different attacks with tamper localization accuracy and good PSNR value.

In [20], researchers proposed a watermarking system in which images are separated into Regions of Interests (ROI) and Regions of Non-Interests (RNI). This scheme has used Recursive

Dither Modulation (RDM), Slantlet transform and SVD. The Hash function was used for tamper detection and Cyclic Redundancy Check (CRC) calculation in each block of ROI was used for localization of the tampered area. Further, integer wavelet transform was used to generate recovery data and Block Truncation Coding (BTC) was used to reduce the size of recovery information. Watermarked data was embedded in the whole image. This scheme provides reliable authentication, tamper detection, and recovery.

In [21], researchers proposed a fragile watermarking approach for image authentication. This scheme has used 5 MSBs for computing authentication code and used 3 LSBs for embedding authentication code. A secret sequence obtained from a logistic map embeds the watermark bit into the LSB position of each pixel. The experimental results of the proposed scheme showed altered or modified regions are identified accurately.

Table 1: Comparison of related works

Scheme	Basic domain	Tamper detection & Recovery	Watermarked PSNR (dB)	Recovery PSNR (dB)
[10]	Spatial	✓	39.0	[28.42,40]
[11]	Spatial	✓	[40,45]	[30,37]
[12]	Spatial	✓	-	[30.25,38.96]
[13]	Spatial	✓	-	41.30
[14]	Spatial	No recovery	42.79	-
[15]	Spatial	✓	[44,46]	[25,45]

In [29], researchers proposed a watermarking scheme with a large-scale tamper detection ability. Two different watermarking strategies using spatial domain and transform domain were offered in their method. This algorithm is meant to provide high-quality restorations with less than 50% of the tampered region. The advantage of this strategy is that the watermark from the untampered region can be used to reconstruct the three tampered regions even if three of the four regions have tampered. Table 1 represents the comparison of experimental results of related works.

3. Proposed Method

The proposed watermarking scheme is divided into three main sections: watermark embedding, tampered block identification, and tampered block recovery.

A. Watermark embedding

The embedding watermark procedure includes embedding generated watermark data to the pixel intensity value of the block. The watermark data is the combination of the authentication bit and recovery bit. Authentication bits are used to check the integrity of the image and identify any changes made to the block. Recovery bits are used to recover the blocks that are marked as modified during integrity checking. Authentication data is generated pixel-wise by applying

XOR operation between bits of the pixel value and also key is used for more security. The average pixel value of the associated block is used to generate recovery data. To generate sequential mapping blocks for cover image blocks, a secret key is used. The mapping block is used to embed recovery data for each block. Phases of the proposed watermark embedding technique are demonstrated in Figure 1.

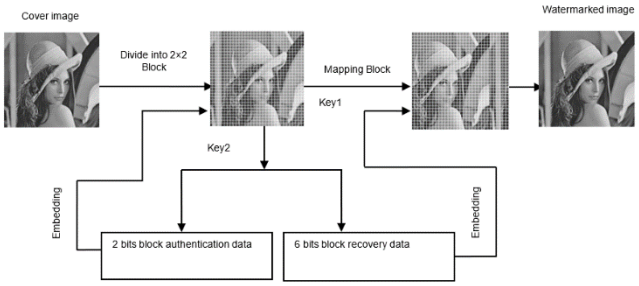

Figure 1. Phases of Watermark Embedding

The following are the steps for embedding the watermark:

Step 1: The cover image C is divided into 2 x 2 size blocks Each block is assigned a sequential integer number B, B∈{1,2,3.....Z} with Z = (M/2) × (N/2) is the total no of block in the image. Where M x N is the size of the cover image.

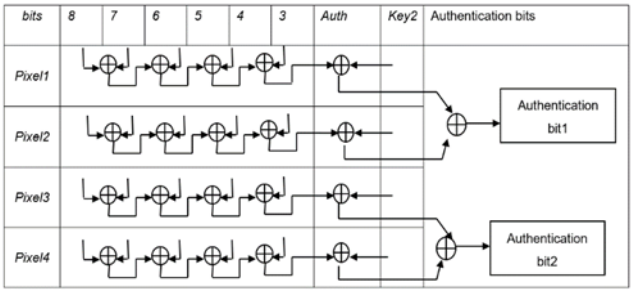

Figure 2. Process of Authentication bit generation

Step 2: Each block is mapped to another block by the block number generated by equation 1.

$$B' = (key1 + B) mod\ Z \qquad (1)$$

where key1 denotes a private key, a number, and key1 ∈ [1, Z]

Step 3: Taking 6 MSBs of each pixel intensity value, the authentication bits (Abs) for each block are generated. Phases of the Ab generation procedure are shown in Figure 2. For each block, two Abs are calculated. X-OR operations are applied between 6 MSBs of each pixel resulting in 4 bits (Auth). X-OR operations are again applied between these 4 bits and a secret key (key2). Which was again converted into two authentication bits using X-OR operation. The key1 and key2 are two random numbers, preferably prime numbers, which can be chosen by the embedder.

Step 4: Taking 6 MSBs of each pixel intensity value, the recovery bits for each block are generated. The recovery generation procedure is shown in Figure 3. Here, after setting 2LSBs to zero, the block's average intensity is calculated as follows:

$$Avg = (\sum_{i=1}^{m} Pixel\_Value_i)/4 \qquad (2)$$

Where m=4, Avg∈ [0,255]

The block's average intensity is quantized from [0, 255] to [0, 64] as below to reduce the number of recovery bits:

$$Avg = round(Avg/4) \quad (3)$$

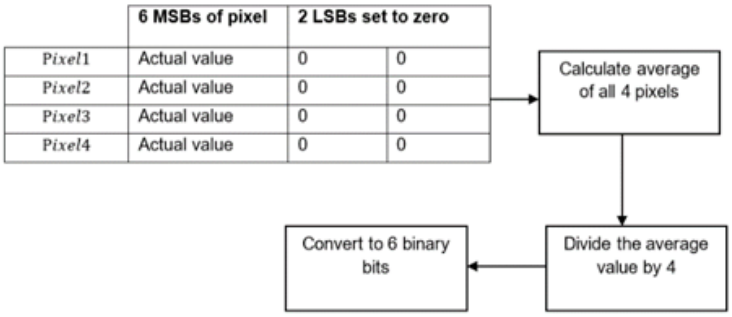

Figure 3. Recovery bit generation

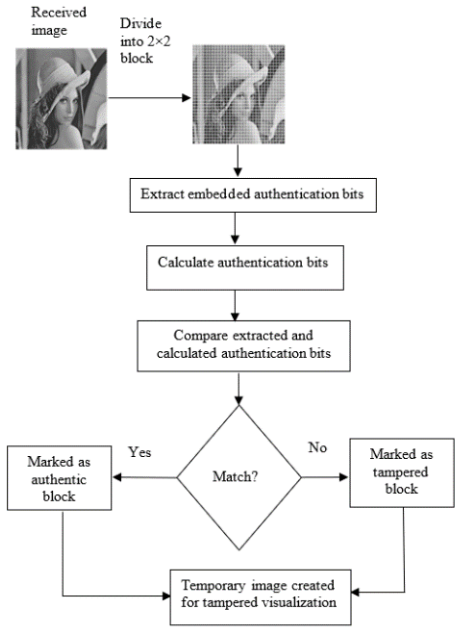

Figure 4. Tamper Detection Phases

Step 5: Watermark embedding process:

For each block, the embedding procedure is achieved by embedding the two authentication bits into the LSB1 of two pixels in the first column of block B. Two recovery bits are encoded in the first LSB of two pixels in the second column of block B', out of a total of six recovery bits. In block B', the remaining four recovery bits are stored in the second LSB of each pixel.

B. Tampered block identification

After the image is received by the receiver, first the authenticity of the image needs to be checked. The received image is divided into 2 x 2 size blocks. Then the tampered blocks are detected by the following steps. Figure 4 shows the phases of the proposed tamper detection process.

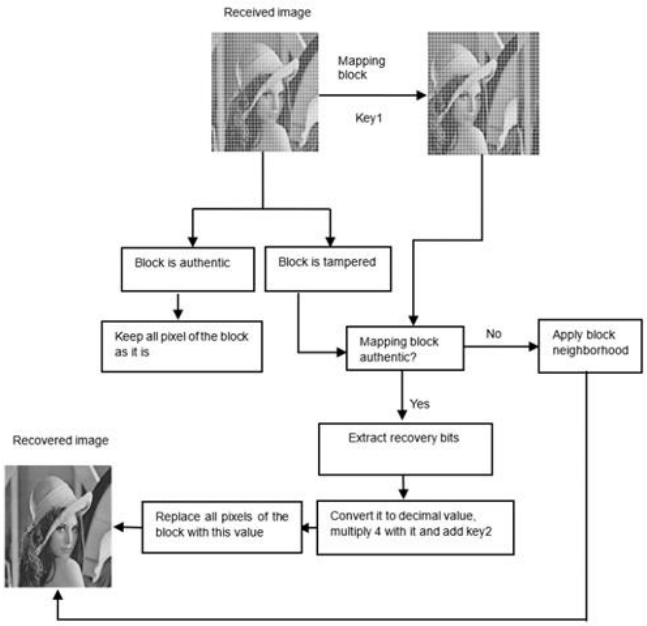

Figure 5. Tamper Recovery Phases

For each block, the embedded authentication bits are extracted. Also, the authentication bits are generated using the authentication bits generation process. The generated authentication bits are compared to the extracted bits from the block. Mark the block as authentic if a match is found; otherwise, mark it as tampered. For tamper visualization, a temporary image is presented in Figure 4 by setting tampered block pixels to white value and authentic block pixels to black value.

C. Tampered block recovery

During tampered block detection procedures, all blocks are labeled as authentic or tampered. These marked tampered blocks need to be reconstructed and this is achieved by the following steps. Figure 5 shows the phases of the proposed tamper recovery process. For every block, the mapping block number is generated as per equation (1).

If the mapping block is not tampered with, then extract the embedded recovery bits from LSB1 and LSB2 of the mapping block with the same sequence as it was embedded (watermark embedding phase). These recovery bits are converted to their decimal value multiply 4 and add Key2 to compensate for the value loss during quantization at the embedding step to get the final pixel recovery value. Replace all the pixels of the block in which any one of the pixels is tampered with this value by taking into the probability that other pixels may be altered.

If the mappings block B’ is tampered with, then all 8-neighborhood blocks of block B which are marked as authentic are taken, and the mean values of those blocks are calculated and taken as recovery values.

4. Experimental Results

The proposed watermarking scheme is verified on grayscale images of size 512×512 to analyze its performance against tampering. The experimentation was performed on Matlab 2018a installed on a computer having an Intel i7 10th generation processor (2.6GHz) with 32GB of RAM. To measure the imperceptibility and integrity of the image we use two evaluation parameters Peak signal-to-noise ratio (PSNR) and Structural Similarity Index (SSIM).

PSNR [22] is a basic statistic for calculating the amount of distortion between original and watermarked images. The PSNR approaches infinity as the MSE approaches zero, implying that a higher PSNR value indicates less distortion and better picture quality [23]. The PSNR is computed as follows [23]:

$$\boldsymbol{PSNR(X,Y) = 10log10\left(\frac{255^2}{\frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}(X_{ij}-Y_{ij})^2}\right)dB} \qquad (4)$$

where M ×N is the size of the image. The pixel at location (i , j) in the original image X is referred to as Xij, while the pixel at position (i , j) in the watermarked image Y is referred to as Yij.

The SSIM can be computed as follows [23]:

$$\boldsymbol{SSIM(I,R) = \frac{(2\mu_X\mu_Y+C_1)(2\sigma_{XY}+C_2)}{(\mu_X^2+\mu_Y^2+C_1)(\sigma_X^2+\sigma_Y^2+C_2)}} \qquad (5)$$

where μ_X is the average of original image X,$\mu_Y$is the average of watermarked image Y,$\sigma_{XY}$is the covariance of X and Y,σ_X^2 is the variance of X, σ_Y^2 is the variance of Y,$C_1 = (K_1L)^2, C_2 = (K_2L)^2$are two variables to stabilize the division with weak denominator, L is the dynamic range of the pixel-values, K1=0.01 and K2=0.03 by default.

The PSNR and SSIM measurements of watermarked images and cover images are shown in Table 2. In this scenario, the PSNR and SSIM values are both high, indicating that the watermarked image is identical to the original and achieves imperceptibility.

This presented approach is tested with four standard images: Lena, Cameraman, Baboon, and Number plate. Different watermarked images of Lena and its recovered images are shown in Figure 6. Figure 6(a) depicts the original image, whereas Figure 6(b) depicts the watermarked image, which has a PSNR of 57.15 dB and an SSIM of 0.9981. Visually both of these images are very similar. Figures 6(c) – 6(f) show images with tampering rates of 5%, 10%,20% and object inserted tampered on the principal content of images.

Table 2: Performance Measure of Watermarked Image

Cover Image (512×512)	PSNR	SSIM
Lena	57.15 dB	0.9981
Cameraman	57.11 dB	0.9976
Baboon	57.13 dB	0.9992
Number plate	57.15 dB	0.9977

Figure 6(g) – 6(j) represents images with visual authentication, where the areas in white color are tampered or modified and the areas in black color are unmodified. Figure 6(k)-6(n) shows

recovered images with PSNR values 50.91dB, 48.41dB, 45.30 dB, 51.55 dB and average SSIM value is 0.9848 with reference to the watermarked image. As an outcome, the retrieved image's PSNR and SSIM are satisfactory.

Watermarked and recovered Cameraman images are shown in Figure7. Figure7 (a) shows the original image. Figure7 (b) is the watermarked image with PSNR 57.11 dB and SSIM 0.9976. Visually these two images are very similar. Figures 7(c) – 7(f) show images with tampering rates of 5%, 10%, 20%, and objects inserted tampered on the principal content of images. Figures 7(g) –7(j) represent images with visual authentication, where the areas in white color are tampered or modified and the areas in black color are unmodified. Figures 7(k) – 7(n) show recovered images with PSNR values 50.59 dB, 48.91 dB, 46.30 dB, 54.45 dB and average SSIM value of 0.9873 with reference to the watermarked image. As an outcome, the retrieved image's SSIM and PSNR are satisfactory.

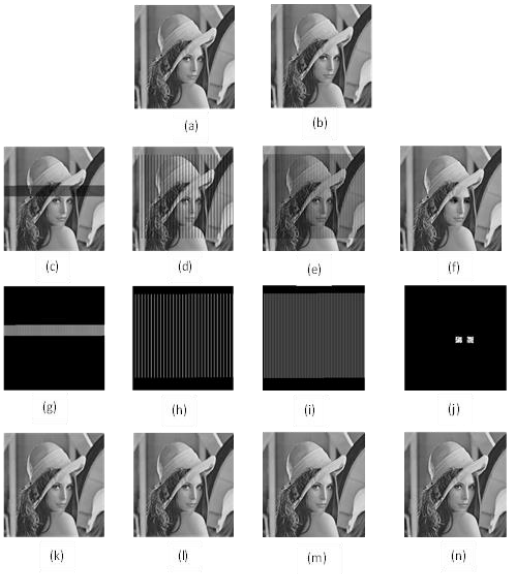

Figure 6. (a) Original Lena Image, (b) Watermarked Image, (c) - (f) Different Tampered Image (g) - (j) Visually Tampered Detected images, (k) – (n) Recovered Images

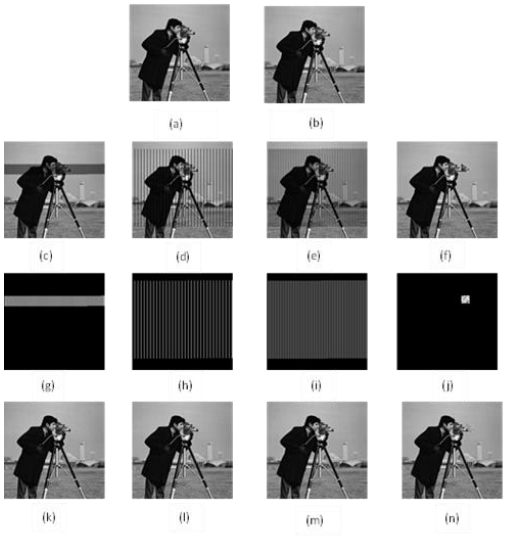

Figure 7. (a) Original Cameraman Image, (b) Watermarked Image, (c) - (f) Different Tampered Image (g) - (j) Visually Tampered Detected images, (k) -(n) Recovered Images

Table 3 represents the PSNR and average SSIM of restored images under various tampering scenarios for all test images. Table 4 presents a comparison of the proposed scheme's watermarked image with the scheme proposed by [17]. The suggested technique's embedding PSNR is greater than the approach employed by [17].

Table 3. Quality Measurement of Recovered Image

Original Image (512×512)	PSNR (dB) of Recovered Image				SSIM(Avg.)
	<5%	5%	10%	20%	
Lena	51.55	50.91	48.41	45.30	0.9848
Cameraman	54.45	50.59	48.91	46.08	0.9873
Baboon	48.34	44.53	44.04	41.08	0.9728
Number plate	48.97	47.26	48.40	45.16	0.9880

Watermarked and recovered images of the Baboon are shown in Figure8. The original image is shown in Figure 8(a). The watermarked image in Figure 8(b) has a PSNR of 57.13 dB and an SSIM of 0.9992. Visually both these two images are very similar. Figures 8(c) – 8(f) show images with tampering rates 5%, 10%, 20% and objects inserted tampered on the principal content of images. Figures 8(g) – 8(j) represent images with visual authentication, where the areas in white color are tampered or modified and the areas in black color are unmodified. Figures 8(k) – 8(n) show recovered images with PSNR values 44.53 dB, 44.04 dB, 41.08 dB, 48.34 dB and average SSIM value is 0.9728 with reference to the watermarked image. As an outcome, the retrieved image's SSIM and PSNR are satisfactory.

Table 4. Comparison of Embedded image PSNR

Cover Image (512×512)	Embedding PSNR	
	Proposed Scheme	[17]
Lena	57.15 dB	39.86 dB
Cameraman	57.11 dB	39.00 dB
Baboon	57.13 dB	40.96 dB
Number Plate	57.15 dB	39.08 dB

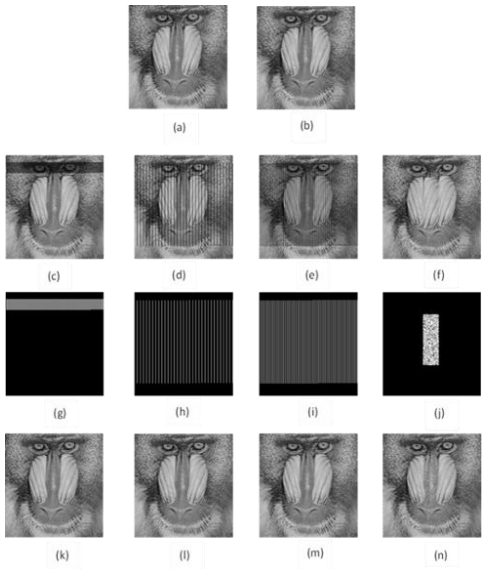

Figure 8. (a) Original Baboon, (b) Watermarked Image, (c) - (f) Different Tampered Image (g) - (j) Visually Tampered Detected images, (k) – (n) Recovered Images

Watermarked and recovered images of Number Plates are shown in Figure9. The original image is shown in Figure 9(a). The watermarked image in Figure 9(b) has a PSNR of 57.15 dB and an SSIM of 0.9977. Visually both these two images are very similar. Figures 9(c) – 9(f) show images with tampering rates of 5%, 10%, 20%, and objects inserted tampered on the principal content of images. Figures 9(g) – 9(j) represent images with visual authentication, where the areas in white color are tampered or modified and the areas in black color are unmodified. Figures 9(k) – 9(n) show recovered images with PSNR values of 47.26 dB, 48.40 dB, 45.16 dB, 48.97 dB, and the average SSIM value is 0.9880 with reference to the watermarked image. To ensure the reliability of the proposed technique the images with 50% tampering were also tested. The test outputs of the recovered image are also mentioned in Figure 10 and Table 5. The above discussion concludes that the quality of the retrieved images is quite satisfactory.

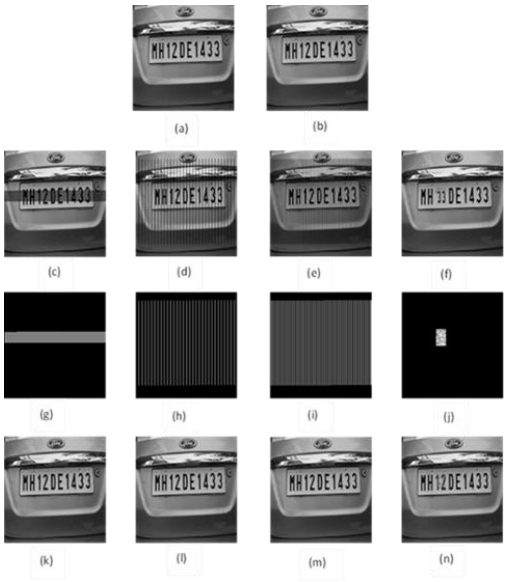

Figure 9. (a) Original Number Plate image, (b) Watermarked Image, (c) - (f) Different Tampered Image, (g) - (j) Visually Tampered Detected images, (k) – (n) Recovered Images

Figure 10. (a) 50% Tampered Images (b) Visually Tampered Detected images, (c) Recovered Images

Table 5 compares the quality of the recovered image of the proposed approach to that of [17]. Similarly, the suggested scheme's recovered image PSNR is greater than that of [17]. As a result, the suggested technique is more appropriate and adaptable for recovering manipulated images.

Table 5. Comparison of recovered Image PSNR

Tamper Rate		Cover Image		
		Lena	Cameraman	Baboon
5%	Proposed	50.91	50.59	44.53
	[17]	39.14	37.91	38.07
10%	Proposed	48.41	48.91	44.04
	[17]	36.04	35.35	35.35
20%	Proposed	45.30	46.08	41.08
	[17]	32.67	32.43	32.31
50%	Proposed	30.48	31.40	30.71
	[17]	28.77	29.01	28.42

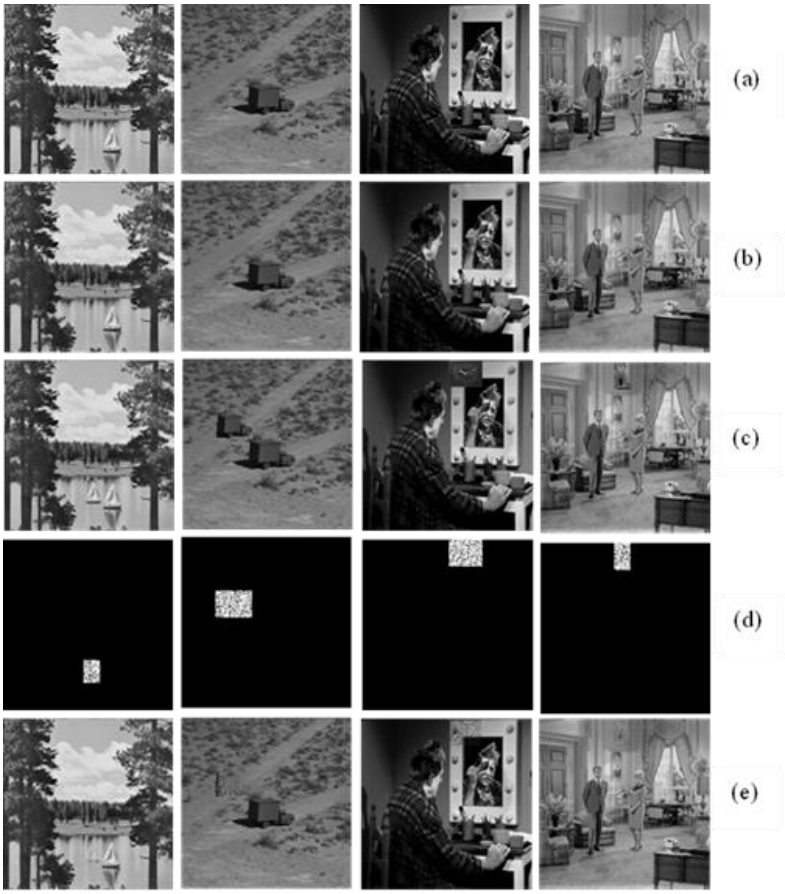

Figure 11. (a) Original images, (b) Watermarked Images, (c) Tampered Images, (d) Visually Tampered Detected images, (e) Recovered Images.

Watermarked and recovered images of four other test images are shown in Figure11. The original images are shown in Figure 11(a). The watermarked images are shown in Figure 11. (b), which indicates higher imperceptibility. Figure 11(c) shows watermarked images that have been modified by adding content. The identification of the tampered area is shown in Figure 11(d). The recovered images are shown in Figure 11(e).

Table 6. PSNR and SSIM of watermarked and recovered images under object addition attack

Cover Image (512×512)	Watermarked Image		Recovered Image	
	PSNR	SSIM	PSNR	SSIM
Boat	57.14 dB	0.9986	52.51dB	0.9919
Truck	56.69 dB	0.9986	45.06 dB	0.9751
Clown	58.30 dB	0.9978	46.22 dB	0.9758
Couple	57.17 dB	0.9988	50.44 dB	0.9880

Table 6 represents the performance of the proposed scheme under object addition attack. The high PSNR value of watermarked images represents higher imperceptibility. The PSNR and SSIM of recovered images indicate quality recovery of tamper images.

Table 7 represents the performance of the embedded and recovered images of the proposed method in comparison to other existing methods. It can be easily noticed that the proposed

method performs better in terms of watermarked image quality. The PSNR value obtained from the recovered image also depicts that the proposed technique recovers higher quality images as compared to existing techniques [17, 20,24-29]. Due to the use of a small non-overlapping block of size 2×2, we get good results for tamper localization and image recovery with high accuracy value.

Table 7. Comparison of Recovered image PSNR with multiple schemes

Scheme	Embedding PSNR (dB)	Restoration PSNR (dB)	Condition of restoration
[24]	37.90	35.0	Tampering rate < 35%
[25]	37.90	[24,41]	Tampering rate < 60%
[26]	37.90	37.90	Tampering rate < 6.6%
[27]	37.90	40.7	Tampering rate < 24%
[28]	37.90	[22, 38]	Tampering rate < 54%
[17]	39.0	[28.42, 40]	Tampering rate ≤ 50%
[20]	41.30	[45,47]	Tampering rate < NA
[29]	44.50	[34,41]	Tampering rate ≤ 50%
Proposed	57.13	[41,50]	Tampering rate ≤ 50%

5. Conclusions

This work presented a self-recovery fragile watermarking scheme in spatial domain using a self-embedding approach. We used XOR operation due to its reversibility property and the tendency to give maximum variations in its truth table, which is not present in other logical operations. With an average PSNR, the imperceptibility of a watermarked image is high. Due to the use of a small non-overlapping block of size 2×2, tamper localization and image recovery are performed efficiently with a high accuracy value. The simulation findings reveal that the suggested technique delivers improved recovery quality and invisibility due to the embedded recovery information. Moreover, compared to the previous techniques, the proposed technique is less computationally intensive. In the future, we will apply sophisticated image watermarking approaches to improve tamper detection accuracy and quality recovery. We also intend to update the mapping block generation approach to increase the quality of the recovered image and to incorporate color images for watermarking and tampering analysis.

References

[1] H. Shi, X. Wang, M. Li, J. Bai, and B. Feng, “Secure variable-capacity self-recovery watermarking scheme,” Multimedia Tools and Applications, vol. 76, no. 5, pp. 6941–6972, Feb. 2016.

[2] O. Benrhouma, H. Hermassi, and S. Belghith, “Tamper detection and self-recovery scheme by DWT watermarking,” Nonlinear Dynamics, vol. 79, no. 3, pp. 1817–1833, Nov. 2014.

[3] Z. Liu, F. Zhang, J. Wang, H. Wang, and J. Huang, “Authentication and recovery algorithm for speech signal based on digital watermarking,” Signal Processing, vol. 123, pp. 157–166, Jun. 2016.

[4] Gutub, Adnan & Aljuaid, Nouf, "Multi-bits stego-system for hiding text in multimedia images based on user security priority,". 2018.

[5] A. A.-A. Gutub, "Pixel Indicator Technique for RGB Image Steganography," Journal of Emerging Technologies in Web Intelligence, vol. 2, no. 1, Feb. 2010

[6] A. K. Singh, B. Kumar, M. Dave, and A. Mohan, "Robust and Imperceptible Dual Watermarking for Telemedicine Applications," Wireless Personal Communications, vol. 80, no. 4, pp. 1415–1433, Sep. 2014.

[7] Nouby M. Ghazaly, M. M. A. . (2022). A Review on Engine Fault Diagnosis through Vibration Analysis . International Journal on Recent Technologies in Mechanical and Electrical Engineering, 9(2), 01–06. https://doi.org/10.17762/ijrmee.v9i2.364

[8] S. Bravo-Solorio and A. K. Nandi, "Secure fragile watermarking method for image authentication with improved tampering localisation and self-recovery capabilities," Signal Processing, vol. 91, no. 4, pp. 728–739, Apr. 2011.

[9] X. Qi and X. Xin, "A singular-value-based semi-fragile watermarking scheme for image content authentication with tamper localization," Journal of Visual Communication and Image Representation, vol. 30, pp. 312–327, Jul. 2015.

[10] C. Li, A. Zhang, Z. Liu, L. Liao, and D. Huang, "Semi-fragile self-recoverable watermarking algorithm based on wavelet group quantization and double authentication," Multimedia Tools and Applications, vol. 74, no. 23, pp. 10581–10604, Aug. 2014

[11] I. J. Cox, M. L. Miller, and J. A. Bloom, "Digital watermarking and steganography," Amsterdam; London: Elsevier, 2008.

[12] F. Hartung and M. Kutter, "Multimedia watermarking techniques," Proceedings of the IEEE, vol. 87, no. 7, pp. 1079–1107, Jul. 1999.

[13] I. Nasir, Y. Weng, J. Jiang, and S. Ipson, "Multiple spatial watermarking technique in color images," Signal, Image and Video Processing, vol. 4, no. 2, pp. 145–154, Feb. 2009.

[14] D. Singh and S. K. Singh, "Effective self-embedding watermarking scheme for image tampered detection and localization with recovery capability," Journal of Visual Communication and Image Representation, vol. 38, pp. 775–789, Jul. 2016.

[15] C. Song, S. Sudirman, and M. Merabti, "A robust region-adaptive dual image watermarking technique," Journal of Visual Communication and Image Representation, vol. 23, no. 3, pp. 549–568, Apr. 2012.

[16] Alaria, S. K., A. . Raj, V. Sharma, and V. Kumar. "Simulation and Analysis of Hand Gesture Recognition for Indian Sign Language Using CNN". International Journal on Recent and Innovation Trends in Computing and Communication, vol. 10, no. 4, Apr. 2022, pp. 10-14, doi:10.17762/ijritcc.v10i4.5556.

[17] X. Zhang and S. Wang, "Fragile watermarking scheme using a hierarchical mechanism," Signal Processing, vol. 89, no. 4, pp. 675–679, Apr. 2009.

[18] Kim, M. & Li, D. & Hong, S, "A Robust and Invisible Digital Watermarking Algorithm based on Multiple Transform Method for Image Contents," Lecture Notes in Engineering and Computer Science. 1. 449-452,2013.

[19] Gupta, D. J. . (2022). A Study on Various Cloud Computing Technologies, Implementation Process, Categories and Application Use in Organisation. International Journal on Future Revolution in Computer Science &Amp; Communication Engineering, 8(1), 09–12. https://doi.org/10.17762/ijfrcsce.v8i1.2064

[20] D. Singh and S. K. Singh, "Block Truncation Coding based effective watermarking scheme for image authentication with recovery capability," Multimedia Tools and Applications, vol. 78, no. 4, pp. 4197–4215, Dec. 2017.

[21] O. Hemida, Y. Huo, H. He, and F. Chen, "A restorable fragile watermarking scheme with superior localization for both natural and text images," Multimedia Tools and Applications, vol. 78, no. 9, pp. 12373–12403, Oct. 2018.

[22] A. Shehab et al., "Secure and Robust Fragile Watermarking Scheme for Medical Images," IEEE Access, vol. 6, pp. 10269–10278, 2018.

[23] X. Liu et al., "A Novel Robust Reversible Watermarking Scheme for Protecting Authenticity and Integrity of Medical Images," IEEE Access, vol. 7, pp. 76580–76598, 2019.

[24] S. Prasad and A. K. Pal, "A Secure Fragile Watermarking Scheme for Protecting Integrity of Digital Images," Iranian Journal of Science and Technology, Transactions of Electrical Engineering, vol. 44, no. 2, pp. 703–727, Oct. 2019.

[25] M. Dursun and N. Goker, "Evaluation of Project Management Methodologies Success Factors Using Fuzzy Cognitive Map Method: Waterfall, Agile, And Lean Six Sigma Cases", Int J Intell Syst Appl Eng, vol. 10, no. 1, pp. 35–43, Mar. 2022.

[26] S. Bhalerao, I. A. Ansari, and A. Kumar, "A secure image watermarking for tamper detection and localization," Journal of Ambient Intelligence and Humanized Computing, vol. 12, no. 1, pp. 1057–1068, May 2020.

[27] Laouamer L. A New Image Watermarking Technique in Spatial Domain Using DC Coefficients and Graph Representation. AMLTA 2019. Advances in Intelligent Systems and Computing, vol 921. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-14118-9_63.

[28] Z. Qian, G. Feng, X. Zhang, and S. Wang, "Image self-embedding with high-quality restoration capability," Digital Signal Processing, vol. 21, no. 2, pp. 278–286, Mar. 2011.

[29] X. Zhang, Z. Qian, Y. Ren, and G. Feng, "Watermarking with Flexible Self-Recovery Quality Based on Compressive Sensing and Compositive Reconstruction," IEEE Transactions on Information Forensics and Security, vol. 6, no. 4, pp. 1223–1232, Dec. 2011.

[30] X. Zhang and S. Wang, "Fragile watermarking scheme using a hierarchical mechanism," Signal Processing, vol. 89, no. 4, pp. 675–679, Apr. 2009.

[31] X. Zhang, S. Wang, Z. Qian, and G. Feng, "Reference Sharing Mechanism for Watermark Self-Embedding," IEEE Transactions on Image Processing, vol. 20, no. 2, pp. 485–495, Feb. 2011.

[32] X. Zhang, S. Wang, Z. Qian, and G. Feng, "Self-embedding watermark with flexible restoration quality," Multimedia Tools and Applications, vol. 54, no. 2, pp. 385–395, May 2010.

[33] D. Sarkar, S. Palit, S. Som, and K. N. Dey, "Large scale image tamper detection and restoration," Multimedia Tools and Applications, vol. 79, no. 25–26, pp. 17761–17791, Feb. 2020.