ISSN: 0976-9102 (ONLINE)
DOI: 10.21917/ijivp.2025.0509

SELF RECOVERABLE ADAPTIVE FRAGILE WATERMARKING SCHEME WITH TAMPER DETECTION AND RECOVERY

Nandhini. S[1] and Durgesh Singh[2]

[1] *Department of Electronics and Communication Engineering, College of Engineering, Guindy, Anna University, Chennai, India*
[2]*Department of Computer Science and Engineering, PDPM Indian Institute of Information Technology Design and Manufacturing, India*

Abstract

A self recoverable adaptive fragile watermarking scheme to detect and recover attacked parts with improved tamper detection ability is proposed in this paper. The Cover image is divided into 2x2 blocks and an adaptive watermark is generated from the quantized version of the 2x2 block. Instead of choosing the best possible values, the proposed watermark generation scheme divides the 2x2 quantized block into two 1x2 blocks to form the watermark. In order to aid in tamper detection, authentication bits are generated from the mapped block of the 2x2 block. The watermark bits (authentication bits and recovery bits) are embedded into the mapped block to form the watermarked image. The proposed watermark embedding scheme provides a quality PSNR of the watermarked image well above 35 dB. The watermarked image was tampered using different attacks like object deletion, object addition, change of content attack and addition of noises. The tampered blocks were detected using the proposed multi-level tamper detection scheme. The attacked parts of the watermarked image were reconstructed using the proposed tamper recovery scheme. The proposed tamper recovery scheme provides a quality PSNR well above 30 dB for various types of attacks. The performance of the proposed fragile watermarking scheme was also evaluated in terms of PSNR (peak signal to noise ratio), SSIM (Structural Similarity Index Measure), Probability of False Rejection (PFR) and Probability of False Acceptance (PFA) of the reconstructed image for various tampering ratios. The PFR and PFA Values of the proposed scheme are close to zero indicating that the tampered pixels are detected correctly.

Keywords:

Authentication, Self Recoverable, Tamper Detection, Tamper Recovery, Fragile Watermarking

1. INTRODUCTION

In the last decade, the digital world of internet has grown exponentially and has become irreplaceable. Most of our day-to-day activities like transportation, banking, grocery shopping, etc. depend wholly on the Internet. As more and more applications are available online, it does not show any signs of slowing down. The amount of data shared per second via the internet comes to billions of bytes. With its abundance and availability, the Internet has its own share of advantages and disadvantages. As the globe becomes more interconnected and reliant on digital technologies, cybercrime is surging. The year 2023 saw a notable increase in cyberattacks, resulting in more than 343 million victims. Between 2021 and 2023, data breaches rose by 72%, surpassing the previous record. A data breach costs $4.45 million on average. In 2022, compromised business emails accounted for $2.7 billion in losses [1,2]. As the number of malicious attacks is on the rise, it is important for any organization to secure their information in the safest way possible. Security has moved from being an optional feature to becoming the essential part of any data transmitting mechanism.

One statistic note that in the next five years, cybercrime might become the greatest threat to every person, place and thing in the world [3]. By taking this reality into account, it is imperative to protect sensitive assets of any country like its intellectual property, Military records, healthcare records etc. from hackers and confidential transmission of these assets is imminent. Though the research in information security has been going for a long time, its need has never been more important until today.

In this digital age, with the abundance and availability of different types of malicious parties it is important to develop security measures that help in preventing image manipulation [4-6]. Watermarking is primarily used to detect tampering and to identify and recover the portions in the received image which are tampered. Digital Watermarking schemes can be broadly divided into robust, fragile and semi-fragile watermarking schemes [4] [7-11]. Fragile Watermarking scheme are vulnerable slightly to both the content preserving Manipulations and to the Malicious Manipulations [12] [13] [22]. Semi Fragile Watermarking scheme are tolerant to content preserving Manipulations [14] [15] but not to Malicious Manipulations. Robust Watermarking Scheme are neither tolerant to the content preserving Manipulations nor to the Malicious Manipulations [10] [16].

Many researchers have proposed fragile watermarking techniques. Primarily, most self-recoverable fragile watermarking schemes use a block-based authentication procedure. Lee et al. [17] used a self-recoverable watermarking technique for detecting the tampered blocks and the tampered pixels while transmitting data through wireless sensor networks. Though the scheme had the least operation count, the watermark size was not adaptive and it is the same for all images and also the integrity of the watermarked image was not discussed.

In order to reduce the problems arising out of integrity and Confidentiality issues, Li et al. [12] had proposed a fragile watermarking scheme using scrambled images in order to embed the watermark. Though this scheme achieved high quality restoration of the tampered areas, the scheme was lacking in terms of efficiency of the algorithm and the time complexity. In the scheme proposed by swain et al. [18], a watermarking technique based on block truncation coding (BTC) and singular value decomposition (SVD) is proposed. The cover image is divided into 4x4 non overlapping blocks to generate the authentication watermark using XOR and SVD. Using BTC, the recovery watermark is generated, and it is embedded using the mapped block of the original block. The proposed scheme was found to have worked against various kinds of attacks. As the block size of the proposed scheme was 4x4, the avenue for improvement in the tampered block restoration at the receiver side can be improved by decreasing the block size.

In the scheme proposed by Ramos et al. [19], discrete wavelet transform is used to embed the watermark bits. The watermark

bits generated are independent of the image and are obtained from the chaotic sequences. A part of the chaotic sequence is also available at the receiver which helps to increase the security aspect of the scheme. Here, if the chaotic sequence is accessed by a malicious third party, the received image can be compromised. Lin et al. [20] had proposed a fragile watermarking scheme using AMBTC compressed codes as authentication bits and recovery bits are obtained from VQ Compressed code. The merit of the proposed scheme is to reduce the blocking effect obtained from calculating the average value of the intensity of the pixels. The scheme also produced a high-quality watermarked image.

Singh et al. [21] had proposed a fragile watermarking scheme based on Integer Wavelet transform (IWT). In this scheme, the authentication bits are obtained from the location of the pixels and the secret keys, The restoration bits are obtained from the 2x2 non overlapping blocks of the cover image using IWT. Though this scheme was found to yield a high PSNR, typical image processing operations may destroy the watermark bits resulting in the inefficiency of the restored image at the receiver end. So, in order to address the issues in the existing papers, the following improvements have been made in the proposed scheme.

Contributions of the proposed scheme:

- The proposed scheme tries to overcome the disadvantages of the existing spatial domain schemes by developing an adaptive watermarking technique whose size varies from image to image.
- As the proposed technique divides the cover image into 2x2 blocks to generate the watermark and also as the entire quantized version of the DCT matrix is embedded as a watermark, the proposed scheme had improved tamper detection ability.
- The proposed Multilevel Tamper detection scheme combined with neighborhood approximation was tested for object deletion, object addition, change of content attack and addition of Noises.
- The performance of the proposed tamper recovery scheme was also evaluated in terms of PSNR (peak signal to noise ratio), Probability of False Rejection (PFR) and Probability of False Acceptance (PFA) of the reconstructed image for various tampering ratios.

2. PROPOSED SCHEME

The main components of the proposed scheme are watermark bits generation and embedding, multi-level tamper detection and tamper recovery which shown as block diagram in Fig.1 - Fig.4 respectively.

2.1 BLOCK MAPPING

In order to provide better tamper recovery at the receiver side, the proposed scheme divides the original image (I) of size $M\times M$ into 2×2 blocks and numbers them raster scan order. This numbering comes in handy during block mapping. Block mapping is a 1-D transformation of mapping an original image block to a mapped block calculated using the below equation:

$$MB = ((K*B) \bmod N)+1 \quad (1)$$

where MB is the mapped block number, K is the key, B is the block number of the original image, N is the total number of 2×2 blocks in I given by $\frac{M \times M}{4}$.

2.2 WATERMARK GENERATION AND EMBEDDING

The step-by-step process of generating the watermark from the original image and the subsequent embedding to form the watermarked image is explained below:

1. Divide the original cover image I of size $M\times M$ into 2×2 blocks $B_i(\ )$. The number of 2×2 blocks is given by $N = (M*M)/4$.
2. Each 2×2 block B_i is quantized using the *Quantmatrix* = [16 11;12 12]. Each quantized 2×2 block $Q_i()$is divided into two 1×2 blocks in order to generate the Recovery bits, R. The elements of Q_i are represented by $[E_1\ E_2\ ;\ E_3\ E_4]$.
3. In order to store the generated recovery bits each 2×2 block B_i of the original image is mapped to a 2×2 block $MB_i(\ )$ in the original image. The mapped blocks are formed according to the Eq.(1).

$X_{(i-1,j-1)}$	$X_{(i-1,j)}$	$X_{(i-1,j+1)}$
$X_{(i,j-1)}$	$X_{(i\ j)}$	$X_{(i,j+1)}$
$X_{(i+1,j-1)}$	$X_{(i+1,j)}$	$X_{(i+1,j+1)}$

Fig.3. Eight block neighbourhood of the highlighted block X

4. Each 2×2 Mapped block MB_i is divided into two 1×2 blocks and Each 1×2 block of MB_i is used to generate an authentication bit (auth) using Eq.(2). The elements of MB_i are represented using $\begin{bmatrix} h_1 & h_2 \\ h_3 & h_4 \end{bmatrix}$.
5. The generated recovery bits(r) from B_i are combined with the authentication bits(auth) from MB_i to form the watermark(w) of B_i.
6. Each quantized 1×2 block will generate a watermark of size 5 or 7 Bits.
7. Depending on the values present in Q_i, the length of the generated watermark varies. So, the proposed watermark generation scheme is an adaptive scheme. In order to obtain better tamper reconstruction at the receiver side, it is necessary to carry forward as much information as possible from the original image. So, the proposed watermark generation scheme embeds both the sign and the value of all the elements in Q_i into the generated watermark, W. Since the proposed scheme is adaptive, there are indicator bits (v) formed to find the number of watermark bits generated from each 1×2 block of Q_i.
8. Finally, Using LSB substitution the generated watermark is stored in the Mapped block MB.
9. Repeating the steps 2-9 for the entire image results in the watermarked image, FW which is sent to the receiver along with the indicator bits.

10. The entire procedure of generating the watermark, forming the recovery bits and embedding the watermark is shown in Pseudo code 1.

Pseudo code 1: Pseudo code for Watermark generation and Embedding

Input: 2×2 block B_i ($1 \le i \le N$) of the original image.

Output: Watermarked image blocks $FW_i(1 \le i \le N)$ and indicator bits V.

2DDCT – Two-dimensional Discrete Cosine Transform

for i=1:1:N

$C_i = 2 \cdot DCT\left(\frac{B_i}{8} - 16\right)$

$Q_i = \text{round}\left(\frac{C_i}{\text{Quantmatrix}}\right)$; //Quantized original block using

$\text{Quantmatrix} = \begin{bmatrix} 16 & 11 \\ 12 & 12 \end{bmatrix}$

y=1; j=1;

$Q_i = \begin{bmatrix} E_1 & E_2 \\ E_3 & E_4 \end{bmatrix}$

if $E_1 = E_2$

$v(j) = 1$

$r(y) = \begin{cases} 0 & \text{if sign}(E_1) = \text{Positive} \\ 1 & \text{if sign}(E_1) = \text{Negative} \end{cases}$ // Forming the recovery bits

$r(y+1) = \begin{cases} 0 & \text{if sign}(E_2) = \text{Positive} \\ 1 & \text{if sign}(E_2) = \text{Negative} \end{cases}$ // Forming the recovery bits

If ($abs(E_1)$>3) then E_1=3

$r(y+2 : y+3) = \text{decimaltobinary}(E_1)$ //Forming the recovery bit

else $E_1 \neq E_2$

$v(j) = 0$

$r(y) = \begin{cases} 0 & \text{if sign}(E_1) = \text{Positive} \\ 1 & \text{if sign}(E_1) = \text{Negative} \end{cases}$ // Forming the recovery bits

$r(y+1) = \begin{cases} 0 & \text{if sign}(E_2) = \text{Positive} \\ 1 & \text{if sign}(E_2) = \text{Negative} \end{cases}$ // Forming the recovery bits

If ($abs(E_1)$>3) then E_1=3

$r(y+2 : y+3) = \text{decimaltobinary}(E_1)$ // Forming the recovery bits

If ($abs(E_2)$>3) then E_2=3

$r(y+4 : y+5) = \text{decimaltobinary}(E_2)$ // Forming the recovery bits

end

$MB_i = \begin{bmatrix} h_1 & h_2 \\ h_3 & h_4 \end{bmatrix}$; //Finding the Mapped Block of the original block

$\text{auth} = \text{XOR}(\text{decimaltobinary}((h_1 + h_2)/2))$;//Forming the Authentication Bits (2)

W = [r *auth*] //Forming the Watermark Bits

L=Length (W);

if L==5

$h_1 = \text{decimaltobinary}(h_1)$

$h_2 = \text{decimaltobinary}(h_2)$

$h_1(6:8) = W(1:3)$ // Embedding the Watermarks

$h_2(7:8) = W(4:5)$ // Embedding the Watermarks

$WM_1 = \text{binarytodecimal}(h_1)$ //Forming the watermarked pixels

$WM_2 = \text{binarytodecimal}(h_2)$ //Forming the watermarked pixels

elseif L==7

$h_1 = \text{decimaltobinary}(h_1)$

$h_2 = \text{decimaltobinary}(h_2)$

$h_1(5:8) = W(1:4)$ // Embedding the Watermarks

$h_2(6:8) = W(5:7)$ // Embedding the Watermarks

$WM_1 = \text{binarytodecimal}(h_1)$ //Forming the watermarked pixels

$WM_2 = \text{binarytodecimal}(h_2)$ //Forming the watermarked pixels

end

Repeat the same steps for h3 and h4 and form WM_3, and WM_4

$FW_i = \begin{bmatrix} WM_1 & WM_2 \\ WM_3 & WM_4 \end{bmatrix}$; //Watermarked Pixels of the mapped Block

j=j+1;

end

Pseudocode 2: Pseudo code for recovery for the tampered block.

Input: Tampered blocks $TA_i(1 \le i \le T)$ of the received image, where T is the number of tampered blocks

Output: Recovered blocks $RC_i(1 \le i \le T)$ of the tampered blocks TA_i

2DIDCT-Two dimensional Inverse Discrete Cosine transform

for i=1:1:N

j=1;

if BR_i == TA_j

MTA_i =*Mapped block* (TA_i) //Find the Mapped block of the tampered block

$MTA_i = \begin{bmatrix} S_1 & S_2 \\ S_3 & S_4 \end{bmatrix}$;

if $v(i) = 1$

$Length(EW) = 5$ && | S_1| ==| S_2|

$S_1 = decimaltobinary(S_1)$

$S_2 = decimaltobinary(S_2)$

$EW(1:3) = S_1(6:8)$ // Extracting the watermark Bits

$EW(4:5) = S_2(7:8)$ // Extracting the watermark Bits

$sign(Y_1) = \begin{cases} Positive & \text{if } EW(1) = 0 \\ Negative & \text{if } EW(1) = 1 \end{cases}$

$sign(Y_2) = \begin{cases} Positive & \text{if } EW(2) = 0 \\ Negative & \text{if } EW(2) = 1 \end{cases}$

$Y_1 = binarytodecimal\left(EW(3:4)\right)$

$Y_2 = binarytodecimal\left(EW(5:6)\right)$

$Y_1 = \text{sign}(Y_1) * Y_1$

$Y_2 = \text{sign}(Y_2) * Y_2$

elseif $v(i)$==0

$Length(EW) = 7$ && $|S_1| \neq |S_2|$;

S_1=decimaltobinary(S_1)

S_2=decimaltobinary(S_2)

$EW(1:4)=S_1(5:8)$ // Extracting the watermark Bits

$EW(5:7)=S_2(6:8)$ // Extracting the watermark Bits

$$sign(Y_1) = \begin{cases} Positive & \text{if } EW(1) = 0 \\ Negative & \text{if } EW(1) = 1 \end{cases}$$

$$sign(Y_2) = \begin{cases} Positive & \text{if } EW(2) = 0 \\ Negative & \text{if } EW(2) = 1 \end{cases}$$

$Y_1 = binarytodecimal\left(EW(3:4)\right)$

$Y_2 = binarytodecimal\left(EW(5:6)\right)$

$Y_1 = \text{sign}(Y_1) * Y_1$

$Y_2 = \text{sign}(Y_2) * Y_2$

end

Repeat the steps to find Y3 and Y4 using S3 and S4

$$ReC_i = \begin{bmatrix} Y_1 & Y_2 \\ Y_3 & Y_4 \end{bmatrix};$$

$ReC_i = 2 \cdot IDCT(ReC_i \cdot \text{Quantmatrix}) + 16$

for x=1:2, y=1:2

$$RC_i(x,y) = \begin{cases} 0 & \text{if } ReC_i(x,y) < 0 \\ 31 & \text{if } ReC_i(x,y) > 31 \text{ //Restored Pixels for the tampered block} \\ ReC_i(x,y) & \text{otherwise} \end{cases}$$

end

$j=j+1$;

else

$RC_i=BR_i$;

end

2.3 MULTI LEVEL TAMPER DETECTION AND TAMPER RECOVERY

The step-by-step process of the proposed multilevel tamper detection scheme followed by tamper recovery is explained below:

- Divide the received image *RI* of size $M \times M$ into 2×2 blocks $BR_i(\,)$. The number of 2×2 blocks is given by $N = (M * M)/4$.
- At the receiver side, a multilevel tamper detection scheme is proposed in order to accurately identify the tampered region in the original image. The proposed multilevel tamper detection scheme has three levels and each of the levels are explained below:
  a) **Level 1:** In this level, the tampered image is divided into 1×2 blocks and authentication bits are calculated for each 1×2 block according to Eq.(2). This is compared with the embedded authentication bit. The corresponding 1×2 block is identified as authenticated if the authentication bits match else the block is identified as tampered.
  b) **Level 2:** In this level, the tampered image is divided into 2×2 blocks. If one of the 1×2 blocks in a 2×2 block is identified as tampered, the entire 2×2 block is marked as tampered, else it is an authenticated block
  c) **Level 3:** This level takes into consideration the eight neighbourhood blocks of a 2×2 block to finally identify it as tampered or authenticated. For each authenticated block of size 2×2, count the number of tampered 2×2 blocks in its eight-block neighbourhood as shown in Fig.3. If the number of tampered blocks is greater than or equal to three, then mark the corresponding authenticated 2×2 block as tampered. At the end of the multilevel tamper detection every 2×2 block in a tampered image will be marked authenticated or tampered.
- After identification of the tampered blocks, the next step is tamper recovery. In order to ease the process of tamper recovery, four different cases of tamper recovery are considered. The different cases depend on the whether the corresponding mapped block of the tampered block is identified as tampered or authenticated.

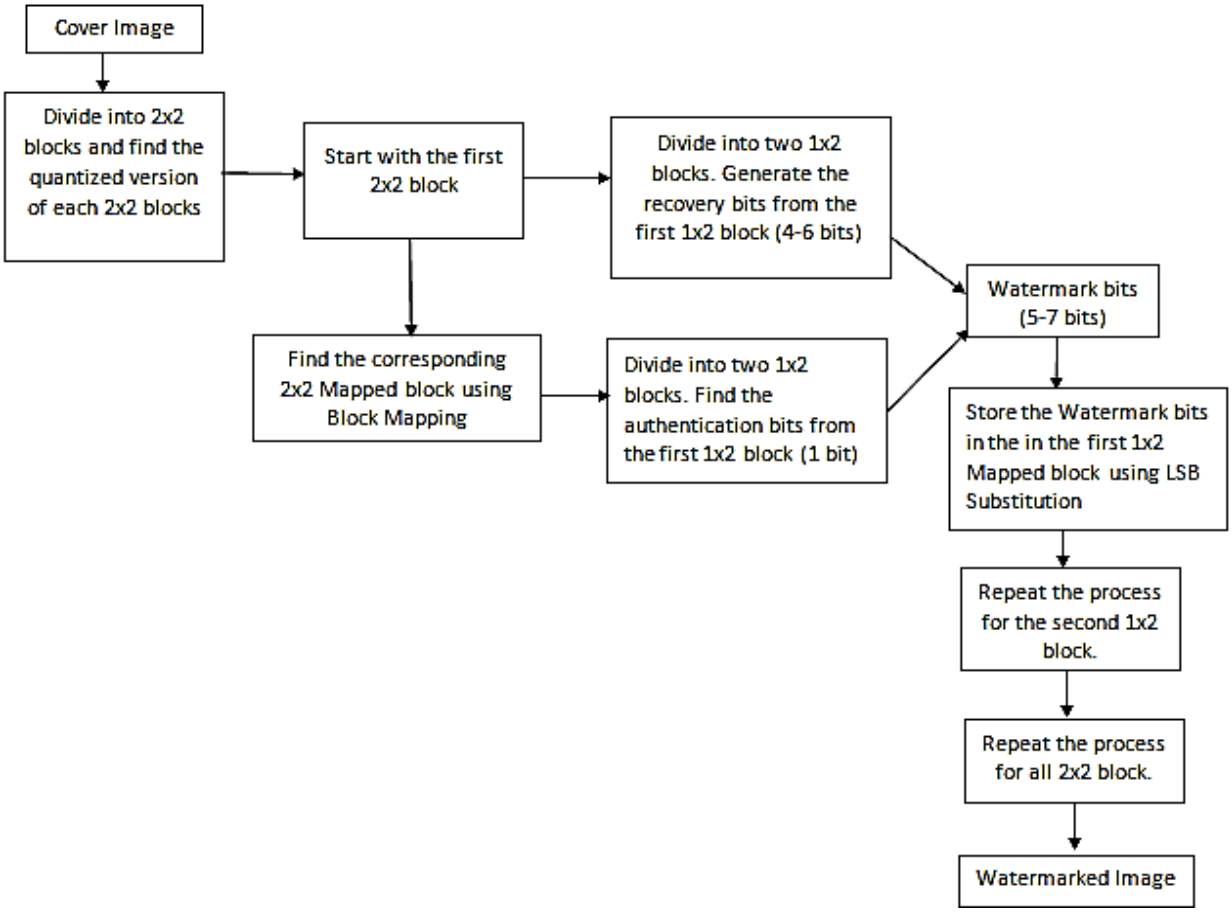


Fig.1. Block diagram showing the generation and embedding of the recovery bits

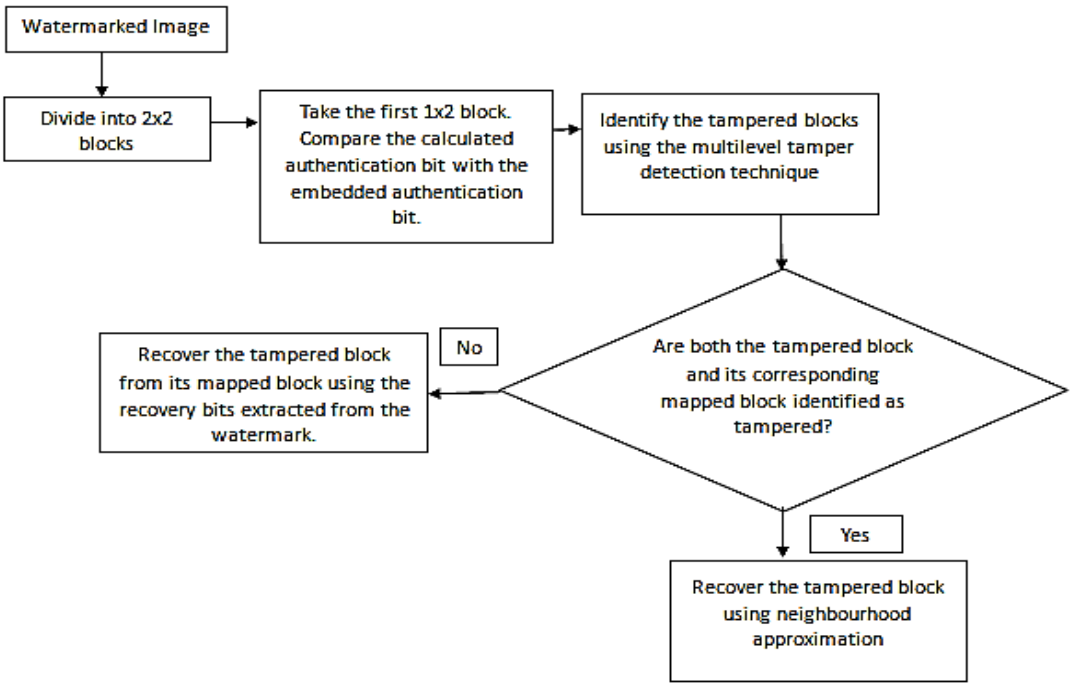


Fig.2. Block diagram showing the identification of the tampered blocks using multilevel tamper detection related work

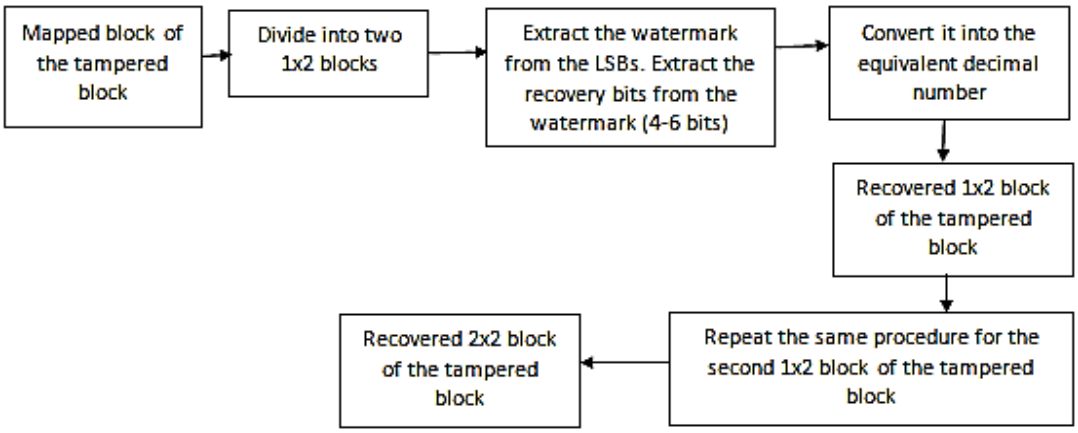


Fig.4. Block diagram showing the reconstruction of the tampered blocks using the recovery bits

- If the corresponding mapped block of the tampered block is identified as authenticated, then the watermark bits are extracted from the corresponding mapped block and the extracted recovery bits from the watermark are used for the reconstruction of the tampered block. The reconstructed 2×2 blocks from the tampered blocks are represented by $RC_i(1 \le i \le T)$ and each RC_i is a 2×2 block represented by $[Y_1\ Y_2;\ Y_3\ Y_4]$. The entire procedure of recovering a tampered block from its corresponding mapped block is shown in algorithm 2.
- If the corresponding mapped block of the tampered block is identified as tampered, then the eight block neighbourhood of the tampered block are used for recovery. The detailed steps are explained below:
  - (a) Find the eight 2×2 block neighbourhood of the tampered block as shown in Fig.3.
  - (b) Calculate the average of each authenticated 2×2 neighbourhood block.
  - (c) Finally calculate the total average of all the authenticated 2×2 neighbours.
  - (d) The average value represents the reconstructed values of the tampered block.

3. RESULTS AND DISCUSSION

The proposed watermark generation scheme and its subsequent multi-level detection and tamper recovery were tested on a variety of cover images of size 512×512 using MATLAB R2014a.

3.1 EVALUATION OF THE PROPOSED WATERMARK GENERATION SCHEME

In order to find the visual quality of the watermarked images of the proposed watermark embedding scheme, Peak signal to noise ratio (PSNR) and Structural similarity index measure (SSIM) is used, which are shown in Eq.(3) and Eq.(4), respectively. Let X and Y represent two $M \times M$ images, then PSNR is defined as:

$$PSNR = 10 \times \log_{10}\left(\frac{255 \times 255}{MSE}\right);\ MSE = \frac{\sum_{i=1}^{M}\sum_{j=1}^{M}\left(X_{i,j} - Y_{i,j}\right)^2}{M \times M} \quad (3)$$

where SSIM is calculated between the cover image and the watermarked image. The Structural Similarity quality assessment index is based on the computation of three terms, namely the luminance, contrast and the structural terms. The overall index is a multiplicative combination of the three terms and is given by,

$$SSIM = [l(x,y)]^{\alpha} \cdot [c(x,y)]^{\beta} \cdot [s(x,y)]^{\gamma} \quad (4)$$

where $\alpha = 1,\ \beta = 1,\ \gamma = 1$

The proposed scheme was tested for various test cover images obtained from the image database (USC-SIPI 1977) and the obtained PSNR and SSIM is shown in Table.1. Some of the watermarked images are shown in Fig.5. The proposed watermark embedding scheme provides a quality PSNR of the watermarked image well above 35 dB and an average SSIM of 0.80 which proves that the watermarked image and the original image are Structurally Similar.

Table.1. PSNR Value (in dB) and SSIM values of watermarked images

Cover Image	PSNR (in dB) of watermarked Image	SSIM
Cameraman	36.962	0.5350
Baboon	37.328	0.9569
House	38.379	0.5707
Sail Boat	37.006	0.8547
Fishing Boat	37.6923	0.8787
Barbara	37.2483	0.8258
Elaine	37.2483	0.8798
Peppers	37.4708	0.8117
Goldhill	37.5245	0.8782
Rice	37.9280	0.7150
Baby	37.2178	0.5212

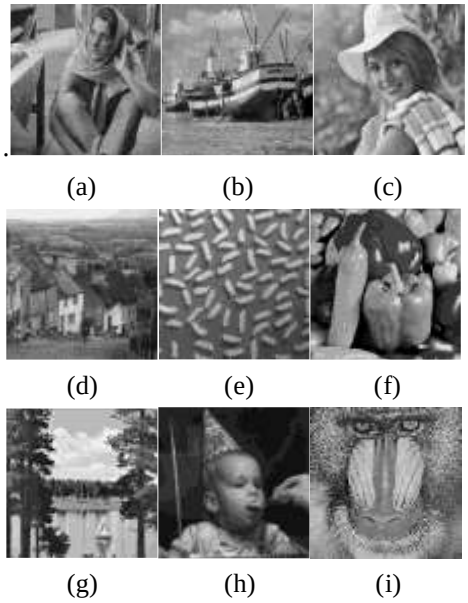


Fig.5. Watermarked Images of (a) Barbara (b) Fishing Boat (c) Elaine (d) Goldhill (e) Rice (f) Peppers (g) Sailboat (h) Baby (i) Baboon

3.2 EVALUATION OF THE PROPOSED TAMPER DETECTION AND TAMPER RECOVERY SCHEME

In order to evaluate the efficiency of the proposed tamper detection scheme, the watermarked image was tested in the following ways: The watermarked image was tampered with a variety of attacks and subsequently PSNR of the recovered image was calculated. The attacks on the cover image included one object addition, two object addition, one object deletion, two object deletion and change of content attack. In the one object addition attack, A part of Flintstones image is rice image. In the two-object addition attack, different objects like a dollar bill and a boat were added to the marked objects like a dollar bill and a boat were added to the watermarked image of car_house image. In the one object deletion attack the camera in the cameraman image was deleted. In the two-object deletion attack, the two eyes in the baboon image were deleted. In the change of content attack, the position of boat and the trees were interchanged.

Table.2. Different attacks and the Subsequent tamper detection and Recovery using the Proposed Scheme

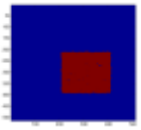
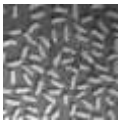
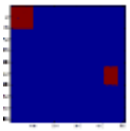
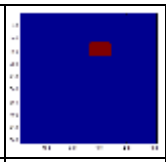
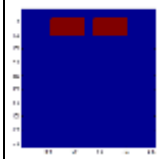
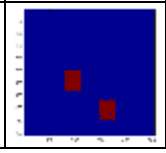
Attacks	Attacked Image	Detected Tampered Region	Tamper recovery	PSNR of the reconstructed image (in dB)
One object addition				27.867
Two object addition				32.396
One object Deletion				33.45
Two object Deletion				29.02
Change of content				32.005

Table.3. Different tests and subsequent tamper detection and recovery using the proposed scheme

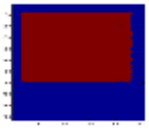
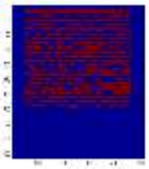
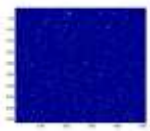
Test 1	Test 2	Test 3
Tampering, Tamper Detection and Tamper Recovery		
		
		
		
PSNR of the recovered Image		
21.37 dB	22.41 dB	27.867 dB

Table.4. PFA and PFR values for various tampering ratios using the proposed scheme

Tampering Ratio	PFR	PFA
5	0.4	0
10	0.496	0
15	0.708	0
20	1.04	0
25	1.444	0
30	1.565	0
35	1.579	0
40	2.097	0
45	2.083	0
50	2.794	0

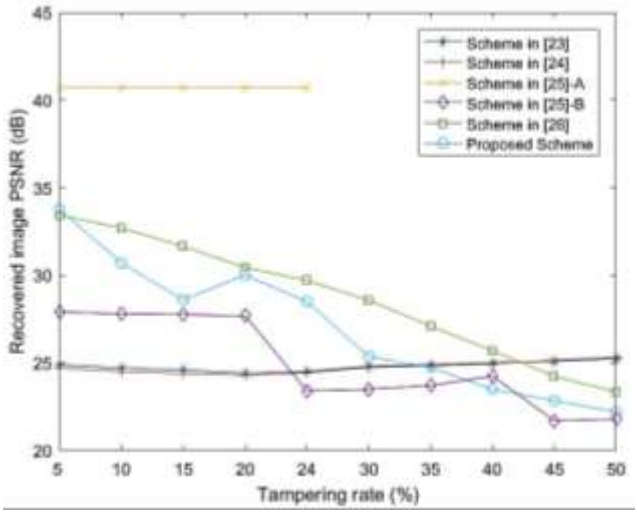
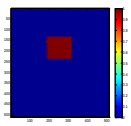
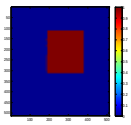
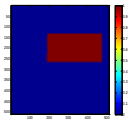
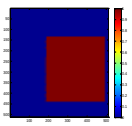
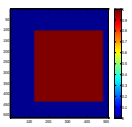


Fig.6. PSNR (dB) of recovered image under different tampering rate

Table.5. PSNR of recovered images using the proposed tamper recovery scheme for various tampering rates

Host Image	Tampering Rate				
	5%	15%	25%	35%	45%
Cameraman	25.850	21.927	22.641	19.818	17.559
Baboon	33.766	28.607	28.497	24.733	22.849
Sail-Boat	29.008	24.895	23.887	22.175	20.238
House	33.246	28.274	26.663	24.721	23.705
Fishing Boat	32.380	26.495	26.856	21.336	20.400
Barbara	31.331	25.915	26.847	22.128	21.419
Elaine	30.840	26.829	27.353	23.328	21.923
Peppers	31.909	27.290	26.377	21.761	20.672
Goldhill	33.228	28.256	28.314	23.132	22.258
Rice	33.965	27.811	28.071	23.761	22.187
Baby	32.562	25.983	24.376	20.742	19.797

Table.6. Performance of the proposed tamper recovery scheme for various tampering rates

Tampering Rate	Tampered Image	Detected Tampered Region	Tamper Recovery
5%			
15%			
25%			
35%			
45%			

The Table.2 shows the different attacks and the resultant tamper detection and tamper recovery using the proposed scheme. The Table.2 also shows the PSNR of the reconstructed images after tamper recovery. The PSNR values exceed the acceptable value. To illustrate that the proposed scheme provides better performance in identifying different types of noises, three different tests were performed. The tests are:

- A rectangular Portion (300×420) is tampered in the watermarked *baboon* image,
- 20 rectangles of varying gray values between [200,223] were used to blur the watermarked Flinstones image
- Salt and Pepper Noise was added to the Elaine image

The tampered images of Baboon, Flintstones and Rice are shown in Table.3. The tamper detection and recovery performance of the proposed scheme for the three different tests are also shown in Table.3. Due to the reproduction of the maximum information from the original image into the embedded watermark, the proposed scheme was able to detect the attacks and recover the tampered portion. The performance of the proposed tamper detection and recovery performance for various tampering ratios ranging from 5% to 45% was tested on various image and the calculated PSNR (in dB) is shown in Table.5. The Table.6 shows the performance of the proposed tamper detection and tamper recovery scheme on the watermarked image of Barbara for various tampering rates. The Table.5 and Table.6 clearly shows that the boundary of the tampered part is identified by the proposed tamper detection scheme and the PSNR Values of the recovered image using the proposed tamper recovery scheme progressively decrease for increased tampering rates. Though images with various variations were tested by the proposed scheme, the average PSNR for a tampering rate of 45% was maintained around 21 dB.

3.3 EVALUATION IN TERMS OF PFA AND PFR

To find the efficiency of the proposed tamper detection and recovery scheme, Probability of False Rejection (PFR) and Probability of False Acceptance (PFA) for various tampering ratio (TR) were calculated. These are defined by Eq.(3) - Eq.(5).

$$TR = \left(\frac{100 \cdot N_t}{N} \right)\% \tag{3}$$

$$PFR = \left(\frac{100 \cdot N_{vd}}{N - N_t} \right)\% \tag{4}$$

$$PFA = \left(\frac{100 \cdot (N_t - N_{td})}{N_t} \right)\% \tag{5}$$

where N_t is the number of tampered pixels, N is the total number of pixels, N_{vd} is the number of valid pixels that are wrongly

detected as tampered and N_{td} is the number of tampered pixels that are correctly detected as tampered. Finally, the obtained PFA and PFR Values using the proposed tamper detection and tamper recovery scheme for various tampering ratios is shown in Table.4. The PFR values are closer to zero and the PFA value of the proposed scheme is zero for various tampering ratios proving that the tampered pixels are detected accurately. Fig.5 shows the PSNR values of the restored image with varying tampering from 5% to 50%. At lower PSNR values, (i.e,) when the number of tampered pixels are high, the proposed scheme outperforms the existing schemes.

3.4 FEATURES OF THE PROPOSED SCHEME

The features of the proposed scheme were analysed in terms of imperceptibility, robustness, security and capacity. The imperceptibility of the proposed Scheme was analysed in terms of PSNR and SSIM as shown in Table.1. The robustness of the proposed scheme was analysed in terms of different attacks and different tampering rates. It is shown in Table.2, Table.3 and Table.6. The security of the proposed scheme lies in the creation of the mapped block using Eq.(1) and in the creation of authentication bits using Eq.(2). As the proposed watermark generation scheme is adaptive, the capacity depends on the number of watermark bits generated which varies from image to image. The step-by-step process of watermark generation is explained in Section 2.2.

4. CONCLUSION

A self-recoverable watermarking scheme with adaptive watermarking, where the watermark size varies from image to image is proposed. As, the proposed watermark generation scheme utilizes the maximum information from the original image, the proposed scheme performs better in terms of better tamper detection and tamper recovery. The proposed tamper detection scheme was tested for different attacks like object deletion, object addition, change of content and addition of noises. Due to the better performance of the proposed tamper detection scheme, the tampered regions were properly identified and was efficiently restored. The proposed tamper recovery scheme was tested for different tampering ratios and the recovered region was analysed in terms of PFA and PFR.As the proposed scheme PFR and PFA values were close to zero, the performance of the proposed scheme was much better. Future work will focus on improving the quality of the tamper recovered part of the received image.

REFERENCES

[1] M. St. John, B. Swanston and C. Ayona, "Cybersecurity Stats: Facts and Figures You Should Know", Available at https://www.forbes.com/advisor/education/it-and-tech/cybersecurity-statistics/, Accessed in 2024.

[2] "130 Cyber Security Statistics: 2024 Trends and Data", Available at https://www.terranovasecurity.com/blog/cyber-security-statistics, Accessed in 2024.

[3] "Cyber Security Facts Stats", Available at https://www.cybintsolutions.com/cyber-security-facts-stats/, Accessed in 2025.

[4] D. Singh and S.K. Singh, "DCT based Efficient Fragile Watermarking Scheme for Image Authentication and Restoration", *Multimedia Tools and Applications*, Vol. 76, pp. 953-977, 2017.

[5] S. Jain and D. Singh, "VGG16Unet: Effective Passive Model for Image Splicing Forgery Localization", *Journal of Electronic Imaging*, Vol. 32, No. 4, pp. 1-7, 2023.

[6] M. Verma and D. Singh, "Survey on Image Copy-Move Forgery Detection", *Multimedia Tools and Applications*, Vol. 83, No. 8, pp. 23761-23797, 2024.

[7] A. Maurya and D. Singh, "Rotation, Scaling and Translation Invariant an Optimized and Effective Robust Watermarking Scheme", *Multimedia Tools and Applications*, Vol. 83, No. 7, pp. 20033-20053, 2024.

[8] D. Singh, S.K. Singh and S.S. Udmale, "An Efficient Self-Embedding Fragile Watermarking Scheme for Image Authentication with Two Chances for Recovery Capability", *Multimedia Tools and Applications*, Vol. 82, No. 1, pp. 1045-1066, 2023.

[9] 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, 2016.

[10] D. Singh and S.K. Singh, "DWT-SVD and DCT based Robust and Blind Watermarking Scheme for Copyright Protection", *Multimedia Tools and Applications*, Vol. 76, No. 11, pp. 13001-13024, 2017.

[11] 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, 2019.

[12] L. Huang, D. Kuang, C.L. Li, Y.J. Zhuang, S.H. Duan and X.Y. Zhou, "A Self-Embedding Secure Fragile Watermarking Scheme with High Quality Recovery", *Journal of Visual Communication and Image Representation*, Vol. 83, pp. 1-10, 2022.

[13] D. Singh, S. Shivani and S. Agarwal, "Quantization-based Fragile Watermarking using Block-Wise Authentication and Pixel-Wise Recovery Scheme for Tampered Image", *International Journal of Image and Graphics*, Vol. 13, No. 2, pp. 1-7, 2013.

[14] Nandhini Sivasubramanian and Gunaseelan Konganathan, "A Novel Semi Fragile Watermarking Technique for Tamper Detection and Recovery using IWT and DCT", *Computing*, Vol. 102, pp. 1365-1384, 2020.

[15] H. Rhayma, A. Makhloufi, H. Hamam and A.B. Hamida, "Semi-Fragile Watermarking Scheme based on Perceptual Hash Function (PHF) for Image Tampering Detection", *Multimedia Tools and Applications*, Vol. 80, No. 17, pp. 26813-26832, 2021.

[16] O. Evsutin and K. Dzhanashia, "Watermarking Schemes for Digital Images: Robustness Overview", *Signal Processing: Image Communication*, Vol. 100, pp. 1-11, 2022.

[17] C.F. Lee, J.J. Shen, Z.R. Chen and S. Agrawal, "Self-Embedding Authentication Watermarking with Effective

Tampered Location Detection and High-Quality Image Recovery", *Sensors*, Vol. 19, No. 10, pp. 1-7, 2019.

[18] Li Huang, Da Kuang, Cheng-long Li, Yu-jian Zhuang, Shao-hua Duan and Xiao-Yi Zhou, "A Self-Embedding Secure Fragile Watermarking Scheme with High Quality Recovery", *Journal of Visual Communication and Image Representation*, Vol. 83, pp. 1-9, 2022.

[19] Monalisa Swain and Debabala Swain, "An Effective Watermarking Technique using BTC and SVD for Image Authentication and Quality Recovery", *Integration*, Vol. 83, pp. 12-23, 2022.

[20] M. Andy Ramos, A.P. Jose Artiles, P.B. Daniel Chaves and Cecilio Pimentel, "A Fragile Image Watermarking Scheme in DWT Domain using Chaotic Sequences and Error-Correcting Codes", *Entropy*, Vol. 25, No. 3, pp. 1-23, 2023.

[21] Chia-Chen Lin, Ting-Lin Lee, Ya-Fen Chang, Pei-Feng Shiu and Bohan Zhang, "Fragile Watermarking for Tamper Localization and Self-Recovery based on AMBTC and VQ", *Electronics*, Vol. 12, pp. 1-9, 2023.

[22] D. Singh, S.S. Udmale and S.K. Singh, "Integer Wavelet Transform based an Effective Fragile Watermarking Scheme for Exact Authentication and Restoration", *Journal of Ambient Intelligence and Humanized Computing*, Vol. 14, pp. 4841-4852, 2023.

[23] T.Y. Lee and S.D. Lin, "Dual Watermark for Image Tamper Detection and Recovery", *Pattern Recognition*, Vol. 41, No. 11, pp. 3497-3506, 2008.

[24] 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, 2011.

[25] 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, 2011.

[26] 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, 2011.