International Journal of Advanced Science and Technology
Vol.98 (2017), pp.45-56
http://dx.doi.org/10.14257/ijast.2017.98.04

Invisible Image Watermarking on Selected Regions using DWT

Jobin Abraham[1*] and Varghese Paul[2]

[1,2]*Mahatma Gandhi University, Kottayam, India*
[1]*jnabpc@gmail.com*

Abstract

This paper proposes a novel grayscale image watermarking scheme using discrete wavelet transform. The objective of the scheme is to improve the existing digital watermarking techniques in terms of imperceptibility and robustness. The proposed watermarking process performs watermark embedding without introducing any significant content degradation. A block based region selective algorithm is proposed to identify least perceptible areas to human eyes for integrating the watermark instead of applying the watermark over the entire image area thereby impairing the visual quality of host image. After avoiding all sensitive regions in the image from the process of watermark embedding, a two-level DWT operation is used for integrating the watermark bits. The experimental results obtained for PSNR, SSIM and NCC measurements stands for the superior image quality and higher resilience to attacks on watermarked images.

Keywords*: digital watermarking, grayscale image, watermark embedding, extraction, frequency domain, DWT*

1. Introduction

Digital watermarking mechanism is widely used for authentication and copyright protection of digital resources. Recently, digital watermarking is viewed as an area of high relevance due to wide use of digital data formats and increasing use of Internet as the most preferred choice for data communication. The earlier analog data formats are almost completely replaced with digital formats that allows for easier data storage and efficient error free transfer. The biggest risk associated is that digital data formats can be easily downloaded from the Internet and illegally modified or redistributed. In this context digital watermarking emerged as a mechanism predominantly for content ownership protection.

Digital watermarking mechanisms can be used to embed a unique mark within the digital contents that needs to be safeguarded. In image watermarking the digital image will be embedded with an identification code or a logo image that corresponds to its owner before distribution or storage for protection of ownership rights of the original image [1]. The hidden mark is known as the watermark. This can be detected and extracted whenever suspicions over the image ownership surfaces in future. In addition to digital image, the technique of content marking for ownership declaration can be implemented over any digital resource such as audio, video or on any digital data file including data base. In each of these cases the hidden mark serves to authenticate the contents by way of successful extraction.

Digital watermarking mechanisms can be broadly classified into two: spatial domain mechanisms and frequency domain mechanisms. Spatial domain mechanisms operate at pixel level. An image can be treated as a two-dimensional array of pixels with finite values represented using 8 or 24 bits. The spatial domain mechanisms usually alter least significant bits (LSB) of the image pixels to hide the watermark information [2, 3]. On the other hand, frequency domain watermarking mechanism transforms the image to another domain and embeds watermark information on resulting transformed coefficients. The

ISSN: 2005-4238 IJAST

commonly used transforms are Discrete Cosine Transform (DCT) [4], Discrete Sine Transforms (DST)[5], Fast Fourier Transform (FFT) [6] and Discrete Wavelet Transforms (DWT)[7, 8]. Some schemes employees a combination of two or more transforms so as to enhance the overall robustness [9,10,11]. The choice of the transform used depends upon the technique employed to achieve imperceptibility or robustness whilst embedding the watermark. Literature survey reveals that majority of papers published are based on discrete cosine transform or discrete wavelet transform techniques.

The image watermarking method proposed in [12] embeds two different watermarks meant for content authentication and recovery. First is a binary watermark, which serves to authenticate the contents and also to detect alterations whenever host image is subjected to tampering. Second watermark is a highly compressed version of the base image itself. The purpose of this piece of information is to regenerate an approximate of the original image if the image is found altered anytime later. The results show that algorithm works fairly with higher quanta. However, the payload of the two watermarks adds up to a significant value that can in turn degrade the image leading to low watermarked image quality.

The algorithm presented in [13] uses DWT to decompose the image and embed the watermark. Watermark bits are embedded in LH and HL frequency band. Pseudorandom sequences are used to spread the watermark bits. Hence, though proposed as blind method, the key is essential for the regeneration of PN sequence at the time of watermark extraction. Fallibility with the method is that, random regions are selected by PN sequence ignoring the sensitivity and construct of the region. Thus there exists the possibility of embedding in sensitive regions which can contribute to visual distortions.

Amol et al [14] presents a method using two-level DWT. The first level LL_1 band is further decomposed to generate next level frequency coefficients. Next, to hide the watermark information, LL_2 values and watermark values are halved and added together. Hence the maximum payload that could be stored is limited by the size of the LL_2 band of the base image. Moreover the coefficients in LL_2, which is a significant band, are reduced to half to make way for watermark information. Thus many regions get affected due to this process as almost half of the values in the host image get curtailed. Watermarking scheme discussed in [15] is employed for image tamper detection and recovery of tampered portions. Two authentication bits and ten recovery bits are embedded in the three LSB bits of selected pixel block to facilitate tamper detection and recovery operations. The recovery information is constructed using two significant DCT coefficients taken from all non-overlapping 2x2 sub-blocks in the image. A mapping function is used to figure out the block B_j where the recovery information for block B_i is to be embedded.

An image authentication scheme is presented in [16]. The semi-fragile watermarking scheme detects and locates image tampering. The image is decomposed using DWT and the three bands other than the low-level band are used for watermark embedding. All the coefficients in the chosen bands are concatenated to from a one dimensional vector and are permuted. These are then grouped depending on the number of watermark bits to be embedded. The authentication is done by the watermark used, which is a binary sequence generated using a secret key.

A color image watermarking scheme is presented in [17] by Thein Huynh-The et al. RGB channels are decomposed using level-four DWT and selected optimal HL_4 and LH_4 coefficients are employed for embedding binary watermark bits. The information associated with coefficient shuffling and channel selected are stored as a key and are required at the time of extraction. The method seems to be weak to jpg compression and fails to effectively resist compressions over 50%.

The rest of the paper is organized as follows. The proposed watermarking scheme is presented in section 2. Section 3 describes the experimental analysis and the results obtained. Finally, section 4 concludes the work.

2. The Proposed Watermarking Algorithm

Watermarking algorithms essentially consists of two major processes: watermark embedding and watermark extraction. The watermark embedding phase embeds the identification code or watermark in the host digital media. And the watermark extraction process retrieves the embedded watermark whenever need arises to prove the ownership of the digital media. Though the watermarking process can serve several purposes with regard to image protection, the process of watermarking embeds an external signal which in fact introduces modifications in the original contents. Hence to minimize the level of such image degradation it is important that safer regions in image must be identified prior to random embedding of the watermark information. A scheme known as WRS is presented to search for regions that are insensitive to human visual system (HVS).

2.1 Image region identification using WRS

The selection of appropriate region for hiding the watermark imperceptibly is addressed using Watermarkable Region Selector (WRS). All pixel blocks in the host image are tested using dual criteria laid by WRS. This approach identifies the blocks that can accommodate the watermark information imperceptibly without easily getting detected. Thus the two level tests involved in WRS are tuned to discover regions that do not arouse suspicion over any possible presence of the watermark to the eyes of intentional attackers. The two levels of testing by WRS are described below.

Level 1 Test:

The first step is to generate the difference matrix of host image I for estimating possibly potential sub-blocks for integrating the watermark. The difference matrix D is determined using equation (1). Using this formula for a host image of size NxN a similar sized two-dimensional array is generated. To compute D we have assumed that I is temporarily padded with a N+1 row populated with elements copied from N^{th} row. This assumption will not make much difference in the result because in the border regions the image pixels are more or less similar.

$$D(x,y) = (|f(x, y) – f(x+1, y)|); x,y =1, 2…N \quad (1)$$

Next the average value (D_{avg}) and threshold value (Th_{avg}) are determined using equation (2) and equation (3).

$$D_{avg} = \frac{\sum D(x, y)}{NxN} ; x,y =1, 2…N \quad (2)$$

$$Th_{avg} = \alpha D_{avg} , \text{where } \alpha \geq 1. \quad (3)$$

It can be seen that Th_{avg} is derived from D_{avg} and is used to make the block selection count flexible. The Th_{avg} value is normally set to be equal to or slightly greater than the D_{avg} and this has a say on the number of sub-blocks selected in the subsequent phase of WRS. In the next step, the host image is decomposed into non-overlapping blocks of size nxn. Let B_{ij} be the host image block and D_{ij} be its corresponding block from D. The example in figure 1 shows the block D_{ij} at pixel position (65:72, 65:72) in the difference matrix of Lena image. Compute the sum of terms in difference block using equation (4). If the sum of terms is above the threshold level Th_{avg}, the block B_{ij} is marked as potential block and test 2 is performed for further confirmation otherwise discard the block and proceed with the test considering the next image block.

$$SD = \sum_{x,y=1}^{n} D_{ij}(x, y); \text{ where } x,y = 1, 2 \ldots n \quad (4)$$

5	2	7	3	1	2	10	7
3	0	0	1	3	3	4	6
4	3	3	0	1	1	6	2
4	3	3	2	1	2	11	3
3	2	9	1	1	5	8	3
2	2	10	4	2	6	0	4
0	4	10	4	6	1	3	7
1	5	9	1	3	2	1	5

Figure 1. Difference block $D_{ij}(x,y)$

Level 2 Test:

The next level of test is performed over the N_4 neighboring blocks for all blocks that were flagged in level 1. The figure 2 shows the neighboring blocks of block B_{ij}. The N_4 block neighbors are $B_{i,j-1}$, $B_{i-1,j}$, $B_{i,j+1}$ and $B_{i+1,j}$. The sum of difference terms of neighboring blocks is computed and the sum is compared against the selected threshold Th_{avg}. If the block difference sum for the neighbor is greater than the adopted Th_{avg}, set the block selection counter to score one. Inspect all the remaining blocks in the neighborhood and each time increment the score when the sum of difference for any sub-block is found to exceed the threshold Th_{avg}. At the end of this inspection on N_4 neighbors if the counter score reads greater than a predefined value (v), set based on the desired imperceptibly requirement, the block can be finalized to be eligible for hiding the watermark or not. Since we are using N_4 neighboring blocks the value v can be set to 1/2/3/4 depending on the desired quality of watermarked image and the watermark payload. For instance, if watermark payload is larger the v value may be set to a lower value so that more blocks are picked to accommodate the additional watermark information.

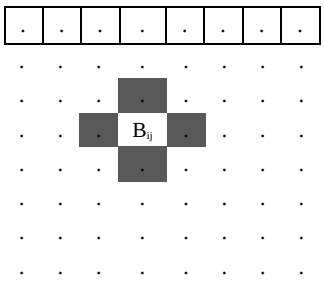

Figure 2. N_4 Neighboring Blocks of B_{ij}

All the blocks (B_{ij}) that yielded positive result at the end of two-layered WRS tests are termed to be eligible to embed the external watermark. The identified blocks are turned in to the following watermark embedding phase for integrating the watermark.

2.2 Watermark Embedding

The watermarking algorithm discussed in this section adopts a block based approach. The method accepts NxN sized grayscale image as the base image and a binary image with size PxQ as the watermark meant for resource identification. In the pre-watermark embedding phase WRS identifies the blocks that can hide watermark information safely. These blocks (B_{ij}) are then transformed into frequency domain using DWT. DWT decomposes the array intensity values into four frequency sub-bands, LL, HL, LH and HH. The lower frequency band LL_1 is further decomposed using two-level DWT. The

resulting HL_2 and LH_2 band are used for watermark embedding. Use of multiple bands for watermark embedding is adopted here to enhance redundancy thereby ensuring a greater level of accuracy at the time of watermark extraction. The block diagram for watermark embedding and extraction is shown in figure 3.

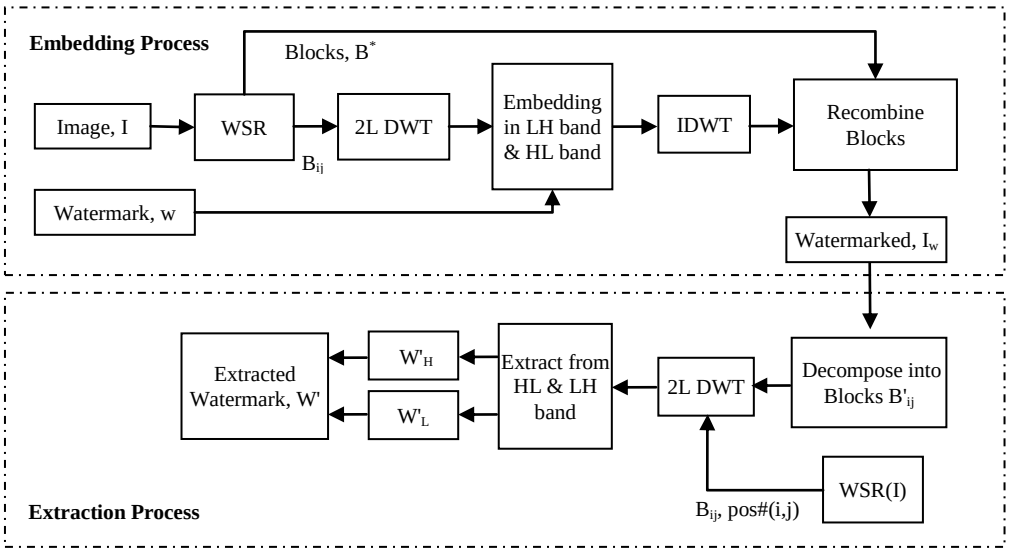

Figure 3. Watermark Embedding and Extraction Process

The details of the steps involved in watermark embedding are outlined below:

1. Input a host image, I of size NxN and the watermark image, W of size PxQ.
2. Reshape the watermark to one dimensional array of values, W_t where i=1,2…P*Q.
3. Divide the original image I into non-overlapping sub-blocks (B) of size 8x8. The total number blocks are M= M_1xM_2 = (N/8*N/8)
4. Apply WRS all blocks B_{ij}, where i,j=1,2.. M
5. Compute two-level DWT on selected blocks B_{ij}.
6. Enforce the watermark information using the embedding algorithm, Algorithm1.
   In the embedding algorithm the watermark bit W_t is embedded in two mid-frequency bands, X_1 =HL_2 and X_2= LH_2 in the same manner.
7. Find inverse DWT of all modified block.
8. Repeat the procedure from step 5 to embed all the watermark bits till i,j==M.
9. Output the watermarked image I_w.

Algorithm 1: Watermark Embedding

***INPUT**: two-level DWT of B_{ij}: X_s = {HL_2, LH_2}, Watermark Vector: W_t*

```
1: procedure Watermark Embedding
2: for s ← 1 to 2 do
3:     for m ←1 do
4:         for n ← 1 to 2 do
5:             if (Wt ==1) then
6:                 Xs(m,n)= β1 * Xs(m,n)
7:             else
8:                 Xs(m,n)= (1/ β1) * Xs(m,n)
9:             end if
10:                if ( Wt ==0) then
11:                    Xs(m,n)= β2* Xs(m,n)
12:                else
```

13: $X_s(m,n)= (1/\beta_2) * X_s(m,n)$
14: *end if*
15: *if* $(X_s(m,n)< Th)$ && $(X_s(m,n) >Th)$ *then*
16: *if(* $X_s >0$ *)&&(*$W_t ==1$*)*
17: $X_s = sf * X_s$
18: *else*
19: $X_s = (1/sf) * X_s$
20: *end if*
21: *end if*
22: *t=t+1*
23: *end for n*
24: *end for m*
25: end for s
26: end procedure
***OUTPUT**: Watermark embedded* HL_2, LH_2

2.3 Watermark Extraction

Watermark extraction algorithm retrieves the hidden mark. The original image is used for comparison to aid the extraction process for decoding the embedded information.

The steps for watermark extraction are as follows.

1. Input the host image I and watermarked image I_w.
2. Decompose the image I into non-overlapping sub-blocks of size 8x8.
3. Apply WRS on I to identify the positions of marked blocks used whilst embedding.
4. Compute two-level DWT on the corresponding block B'_{ij} taken from I_w.
5. Extract the set of two watermark bits from HL_2 and LH_2 sub-bands using Algorithm2.
6. Repeat from steps 3 for finding and extracting the remaining watermark bits from subsequent marked blocks.
7. Reshape the extracted bits to form the two dimensional watermark image, W'.

The above steps result in two set of watermarks; one from HL_2 band and the other from LH_2 band. Using the two sets, a final copy of the extracted watermark is formed. The two signals are compared and whenever an erratic or inconsistent bit is spotted they are replaced using the immediate previous non-erratic bit state.

Algorithm 2: Watermark Extraction
***INPUT**:* $X_s = \{HL_2, LH_2\}$, $X'_s = \{HL'_2, LH'_2\}$,
1: procedure Watermark Extraction
2: for s ← 1to 2
3: *for m ←1 do*
4: *for n ← 1 to 2 do*
5: *if (*$|X'_s(m,n)>X_s(m,n)|$*) then*
6: $W'_s(t) = 1$
7: *else*
8: $W'_s(t) = 0$
9: *end if*
10: *t=t+1*
11: *end for n*
12: *end for m*
13: end for s
14: end procedure
OUTPUT: W'_1, W'_2

3. Experimental Analysis

The watermarking algorithm presented in section 2 is tested on various images. The results obtained after watermark embedding on four popular test images, Lena, Boat, Pirate and Mandrill are shown in the figure 4.

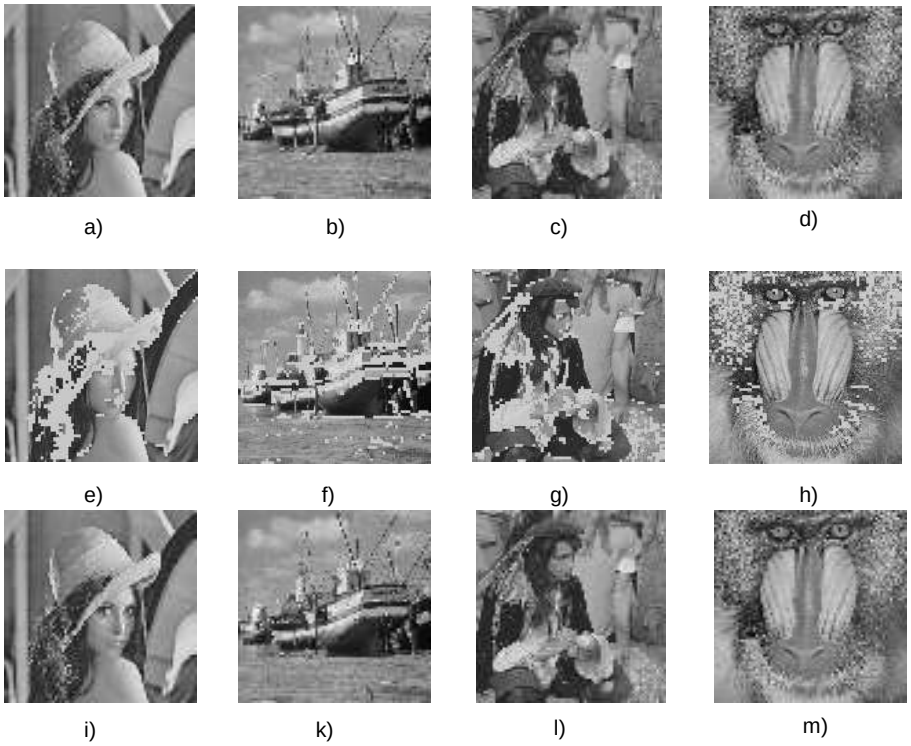

Figure 4. Base images (a-d), block selected (e-h), watermarked image (j-m)

All images are initially subjected to twin tests laid by WRS for finding the regions or blocks that can accommodate watermark with minimal visual damages. The second rows in figure 4 shows the regions identified as suitable for watermarking. For each case shown, equation 3 is used to determine an appropriate threshold value specific to the image. These values may be so set to ensure sufficient numbers of blocks are selected for integrating the watermark stream. For instance, the threshold value set for Lena image is 500 and for Boat it is 750. A binary 32x32 logo image is used as the watermark signal. The last row of figure 4 shows the resultant watermarked images.

The watermark signal embedded in the host images are later extracted from the watermarked copies. Extraction process commence with identifying the blocks where the watermark bits were hidden with the aid of original image. Once the blocks employed for hiding the watermark are found, DWT transform is applied on those regions. The coefficients obtained are then compared against the originals to detect the hidden information. The status of alteration in watermarked image coefficients is decoded as the output watermark bits. Two set of watermarks are generated as the band HL_2 and LH_2 were simultaneously used at the time of embedding process. The two separate copies are compared against one another to form the final extracted watermark image W'. This in turn improves the quality of the results.

Next, the watermarked image is analyzed using various quality measurement tests. Peak Signal to Noise Ratio (PSNR) indicates the impact of watermarking algorithm on the image quality. PSNR ratio indicates how far the base carrier has been distorted by the watermark added during the process of watermarking. Greater the noise induced lesser the PSNR ratio. PSNR value is computed using equation (5). Mean squared error (MSE) is

given by the equation (6) for any two images I and I′ of size MxN. PSNR readings for various watermarked test images are listed in the table 1.

$$\mathrm{PSNR} = 10\log_{10}\frac{\mathrm{R}^2}{\mathrm{MSE}} \tag{5}$$

$$\text{Here, } \mathrm{MSE} = \sum_{i=1}^{M}\sum_{j=1}^{N}\frac{[\mathrm{I}(i,j) - \mathrm{I}'(i,j)]^2}{\mathrm{M} * \mathrm{N}} \tag{6}$$

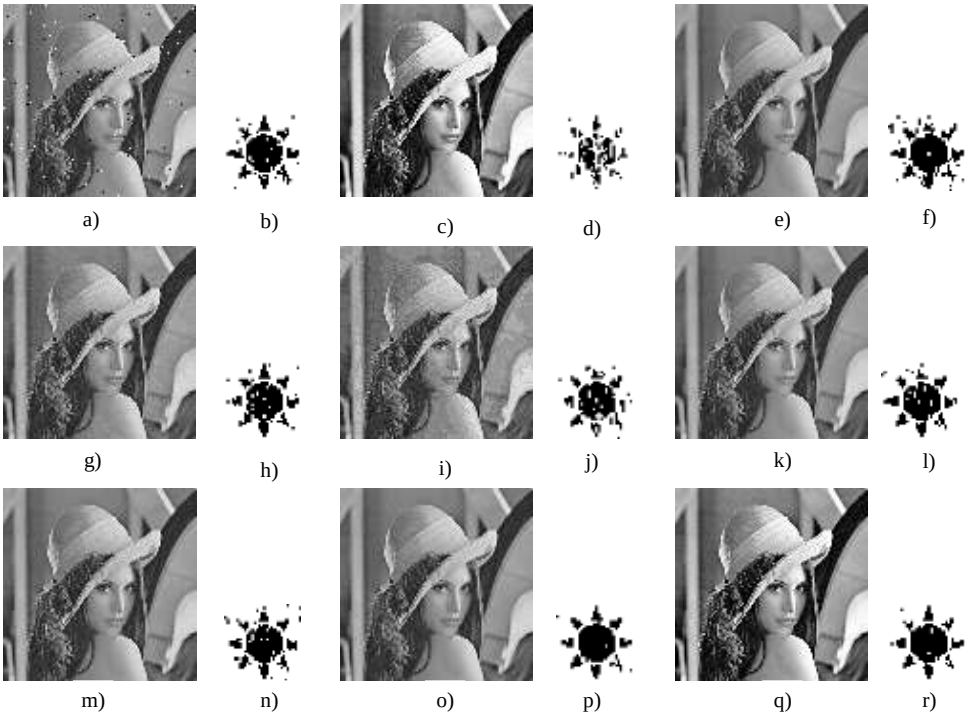

Figure 5. Attacked watermarked image and extracted watermark a) Salt & Pepper b) extracted watermark c) Histogram equalized image d) extracted watermark e) Weiner filtering f) extracted watermark g) 3LSB reset h) extracted watermark i) 4LSB reset j) extracted watermark k) JPG compressed (QF:60) l) extracted watermark m) JPG compressed (QF:50) n) extracted watermark o) Gaussian LPF p) extracted watermark q) Contrast adjusted r) extracted watermark

The metric Global Embedding Impact (GEI) estimates the spread of watermark over each host image pixel. GEI is computed using equation (7). This value varies in the range [0 to R] and for grayscale images, R=255. A GEI value close to zero means that the overall pixel intensity variation after the watermark embedding process is negligible and hence the net impact is minimal.

$$\mathrm{GEI} = \sum_{i=1}^{M}\sum_{j=1}^{N}\left|(\mathrm{I}(i,j) - \mathrm{I}'(i,j))\right| / (\mathrm{MxN}) \tag{7}$$

A third metric used here for imperceptibility evaluation is Structural Similarity Index (SSIM) [18]. A value close to 1 indicates that the compared images are identical. And when the original image and its watermarked version are different, the SSIM value drops from 1 reflecting the depth of variation.

Table 1. Peak Signal to Noise Ratio

Image	One level DWT			Two level DWT		
	PSNR	GEI	SSIM	PSNR	GEI	SSIM
Lena	50.12	0.07	0.9991	41.28	0.42	0.9923
Boat	49.13	0.08	0.9992	40.20	0.48	0.9926
Peppers	46.19	0.09	0.9993	40.96	0.42	0.9925
Mandrill	48.16	0.10	0.9925	40.49	0.48	0.9951
Pirates	49.41	0.08	0.9989	41.73	0.39	0.9932

Another metric used here for analysis is Normalized Correlation Coefficient (NCC) computed using (8). Here W and W' are the original and the extracted watermarks respectively. NC is commonly used for testing the robustness of watermarking algorithm to attacks. Figure 5 shows few attacked watermarked images along with the extracted watermark signal. Table 2 is the statistics for NC after subjecting the watermarked image to an array of attacks. As shown in equation (8), NC is measured by comparing the extracted output against the original watermark. This measure reflects how close the extracted content is similar to the original. The NC varies in the range of 0 to 1. A zero means signals compared shares no similarity and the upper limit value 1 indicates that the both signals are same bit-to-bit.

$$NCC = \frac{\sum_{i=1}^{P}\sum_{j=1}^{Q} W(i,j).W'(i,j)}{\sqrt{\sum_{i=1}^{P}\sum_{j=1}^{Q} W(i,j)}\sqrt{\sum_{i=1}^{P}\sum_{j=1}^{Q} W'(i,j)}} \quad (8)$$

Another metric used to evaluate the correctness of watermark is BER. The bit error ratio (BER) measures the error generated by the extracted watermark. BER thus reflects the robustness of the watermarking algorithm to attacks. BER is calculated as follows:

$$BER = \frac{e_b}{pxq} \quad (9)$$

Here e_b is the count of erratic bits and pxq is the size of the watermark image. The value of BER converges to zero when the recovered watermark closely resembles the original. Figure 6 shows the BER comparison of one-level DWT with the proposed two-level DWT scheme for watermark embedding operation. The x axis of the plot follows the order of attacks as listed in table 2.

The readings in table 1 and table 2 illustrate that imperceptibility and robustness are interdependent. These parameters are inversely proportional to one other and when one requirement is satisfied the other has to be compromised. However as the prime objective of watermarking is content protection against malicious abuses robustness of embedded watermark signal may be given prominence. And at the same time a fair and reasonable image quality should also be ensured. To this end the second method using two-level DWT outperforms the other. Moreover, figure 6 illustrates that the proposed method using two-level DWT exhibits a low error ratio and yield steady results at the time of attacks on watermarked images.

Table 2. Correlation Coefficient for Lena image undergone different attacks

Attack type	One level DWT		Two level DWT	
	NC	BER	NC	BER
Salt & Pepper	0.9812	0.0264	0.9705	0.0410
Histogram Equalization	0.8957	0.1602	0.9168	0.1299
Weiner Filtering	0.7595	0.2959	0.9516	0.0664
Gaussian LPF	0.9058	0.1260	0.9838	0.0225
Contrast Adjustment	0.9679	0.0449	0.9793	0.0293
Median Filtering	0.5210	0.5059	0.8520	0.1904
JPG Compression(QF: 60)	0.7831	0.2881	0.9940	0.0430
JPG Compression(QF: 50)	0.7604	0.3184	0.9587	0.0576
JPG Compression(QF: 40)	0.7327	0.3486	0.9478	0.0732
JPG Compression(QF: 30)	0.6806	0.4023	0.9303	0.0986
JPG Compression(QF: 20)	0.6219	0.4580	0.9139	0.1221
JPG Compression(QF: 10)	0.5265	0.5420	0.8472	0.2158
LSB Reset (b_0)	0.9766	0.0322	0.9979	0.0029
LSB Reset (b_1b_0)	0.9585	0.0576	0.9909	0.0127
LSB Reset (b_2 b_1b_0)	0.9372	0.0889	0.9692	0.0430
LSB Reset ($b_3b_2b_1b_0$)	0.9225	0.1094	0.9478	0.0742
LSB Reset ($b_4b_3b_2b_1b_0$)	0.9108	0.1299	0.9086	0.1328

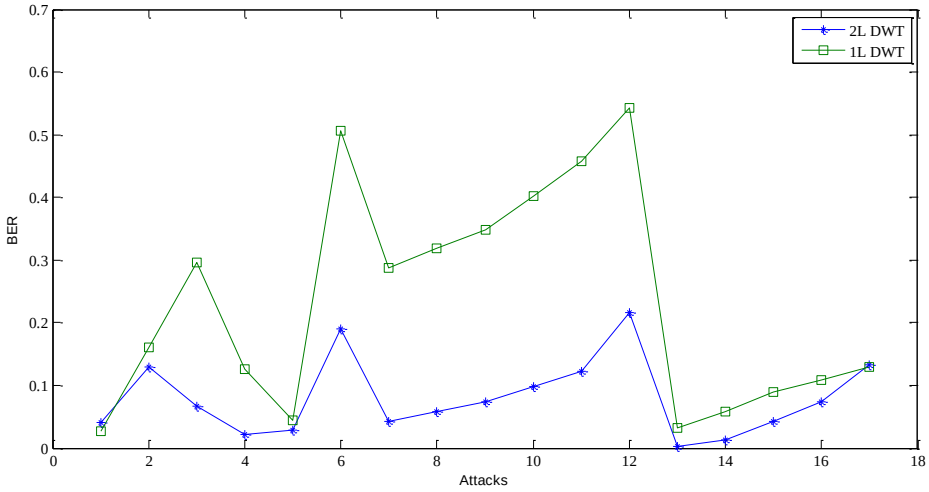

Figure 6. Bit Error Ratio (BER) Comparison

The proposed method delivers watermarked images with high PSNR value indicating that the base image is least affected during the process of embedding. A high PSNR also ensures that the extent of degradation incurred by the watermarked copy is minimal. The metric NC is used as a measure of similarity check on the extracted watermark signal. A high correlation factor indicates that the output is good enough to declare the authenticity without any room for doubt. Also the results obtained after subjecting the watermarked image to compression, noise attack and contrast adjustment are sound. Comparison of the proposed method with another image watermarking scheme presented in [19] is shown in table 3. The outcomes reveal the performance of the scheme is superior in terms of quality and robustness to attacks including jpg compression.

Table 3. Comparison of proposed method with Qingtang Su [19]

	Qingtang Su [19]	Proposed
Host image size	3x512x512	512x512
Watermark type	Binary	Binary
Watermark size	64x64	2x(32x32)
Operating domain	Spatial domain	2L DWT
JPG Compression	Stronger at higher QF	NC > 0.85 for QF ≥ 10
SSIM (Lena)	0.9869	0.9923

4. Conclusion

Digital watermarking is intended to protect the digital image from illegal abuses and solve issues related to the ownership and copyrights of digital images. The proposed Watermarking algorithm adopts a block based approach for selection of optimum regions for hiding the watermark imperceptibly. In order to improve the robustness and imperceptibility of watermarked images appropriate regions in the image are determined prior to embedding using selection policies set by watermarkable region selector (WRS). Watermarking algorithm uses two-level DWT transform to convert the intensity values from spatial domain to frequency domain whilst watermark embedding and for watermark extraction employs a non-blind strategy. The use of redundant watermarking that embeds two copies of watermark enhances the accuracy of watermark detection. Though redundant information may contribute to the image degradation it is offset by the use of safer regions in the image identified by WRS. Thus there is an increase in successful watermark bit detection without significant degradation in image quality. The use of transformed domain adds to the robustness of the method. Experimental analysis shows the structural similarity index measurement (SSIM) values are fairly high for the proposed algorithm. Also comparisons in the line of normalized correlation and bit error ratio shows that the proposed scheme employing two-level DWT operation is robust to wider set of malicious attacks compared to several other embedding schemes.

References

[1] Shiguo Lian, Dimitris Kanellopoulos, Giancario Ruffo, "Recent Advances in Multimedia Information Security", Informatica **(2009)**, pp3-24.
[2] Phen Lan Lin, Chung-Kai Hsieh, Po-Whei huang, "A hierarchical digital watermarking method for image tamper detection and recovery", Pattern Recognition, **(2005)**, pp2519-2529.
[3] Zhicheng Ni, Yun-Qing Shi, Nirwan Ansari, Wei Su, "Reversible Data Hiding", IEEE Transactions on circuits and systems for video technology, **(2006)**, 16(3), pp354-362.
[4] Qingtang Su, Yugang Niu, Xianxi Liu, Tao Yao, "A novel blind digital watermarking algorithm for embedding color image into color image", International Journal of Light and Electron Optics (Optik), 124 **(2013)** 3254-3259
[5] Himeur Yassine, Boudraa Bachir, Khelalef Aziz, "A Secure and High Robust Audio Watermarking System for Copyright Protection", International Journal of Computer Applications, **(2012)**, 53(17), pp33-36.
[6] Chih-Wei Tang, Hsueh-Ming Hang, "A Feature based Robust Digital Image Watermarking Scheme", IEEE Transactions on Image Processing, 51(4), **(2003)**
[7] Hanna A. Abdullah, Mohily M. Hadhoud, "Blind Wavelet-Based Image Watermarking", International Journal of Signal Processing, Image Processing and Pattern Recognition, **(2011)**, 15-27.
[8] Qing Liu, Jun Ying, "Grayscale Image Digital Watermarking Technology Based on Wavelet Analysis", IEEE Symbosium on Electrical and Electronics Engineering, **(2012)**.
[9] S. Manikandan Prabu, Dr.S Ayyasamy, "An Efficient Watermarking Algorithm Based on DWT and FFT Approach", International Journal on Computer Science and Engineering, **(2014)**, 6(6), pp211-216.
[10] Chunlin Song, Peng Xiao, Sud Sudirman, Madjid Merabti, "Region adaptive digital image watermarking sytem using DWT-SVD algorithm", NASA/ESA Conference on Adaptive Hardware and Sytems, **(2014)**, pp196-201

[11] Ali Al-Haj, "Combined DWT-DCT Digital Image Watermarking", Journal of Computer Science, **(2007)**, 3(9), pp740-746.
[12] Rafiullah Chamlawi, Asifullah Khan, Imran Usman, "Authentication and recovery of images using multiple watermarks", Computers and Electrical Engineering, **(2010)**, pp 578-584.
[13] P.Ramana Reddy, Dr. Munaga V Nk Prasad, Dr. D Sreenivasa Rao, "Robust Digital Watermarking of Images using Wavelets", International Journal of Computer and Electrical Engineering, **(2009)**, pp 111-116.
[14] Amol R Madane, K.T Talele, M.M Shah, "Watermark Logo in Digital Image using DWT", Proceedings of SPIT-IEEE colloquium and International Conference, **(2007)**, pp121-126.
[15] Durgesh Singh, Sanjay K.Singh, "Effective self-embedding watermarking scheme for image tampered detection and localization with recovery capability", Journal of Visual Communication and Image representation, 38 **(2016)** pp775-789
[16] Radu O. Preda, "Semi-fragile watermarking for image authentication with sensitive tamper localization in the wavelet domain", Measurement, 46 **(2013)**, pp 367-373
[17] Thein Huynh-The, Oresti Banos, Sungyoung Lee, Yongik Yoon, Thuong Le-Tien, "Improving digital image watermarking by means of optimal channel selection", Expert Systems With Applications, 62 **(2016)**, pp177-189
[18] Z.Wang, A.C Bovik, H.R Sheik, E.P Simoncelli, "Image Quality Assessment from error visibility to structural similarity", IEEE Transactions on Image Processing, 13(4), **(2004)**, pp600-612.
[19] Qingtang Su, Yugang Niu, Qingjun Wang, Guorui Sheng, "A blind color image watermarking based on DC component in the spatial domain", International Journal of Light and Electron Optics (Optik) 124, **(2013)**, pp 6255-6260

