The International Journal of Engineering and Science (IJES)
|| Volume || 7 || Issue || 7 Ver. I|| Pages || PP 08-18 || 2018 ||
ISSN (e): 2319 – 1813 ISSN (p): 23-19 – 1805

Self-Embedding Watermarking Scheme Based On Discrete Wavelet Domain

Hanen Rhayma[1,2], Achraf Makhloufi[2], Habib Hamam[3],Ahmed Ben Hamid A[2]

1École nationale d'ingénieurs de Gabès (ENIG), Université de Gabès, Tunisia
2 Advanced Technologies for Medecine and Signals, Enis,Université de Sfax, Tunisia (ATMS)
3Faculté d'Ingénierie, Université de Moncton, Canada
Corresponding Author:Hanen Rhayma

--***ABSTRACT***--

Image authentication watermarking scheme can substantially solve the security of digital images transmitted through insecure channel. In this paper we propose a semi-fragile watermarking scheme for image authentication, localizing and recovering. The approximation sub-band of the second Discrete Wavelet Transformation (DWT), LL_2 is used as recovery watermark while the fifth approximation sub-band LL_5 is used as authentication and localizing watermark. The two watermarks are embedded into the first approximation sub-band LL_1 using the Quantization Index Modulation (QIM). To reduce the size of the recovery watermark, Data Representation through Combination (DRC) is practically used. The experimental results show that our proposed algorithm can resist JPEG compression and give an acceptable estimation of the watermarked image even after the watermarked image has been tampered.

KEYWORDS:*semi-fragile watermarking, DRC, authentication, localizing, recovering.*

Date of Submission: 22-06-2018 Date of acceptance: 07-07-2018

I. INTRODUCTION

Digital images are usually shared and transmitted through non secure channels like internet. Wherefore, it should be protected against any attempt of manipulations. Image authentication techniques present a reliable solution to the problems associated with image content manipulations. The main goal of image authentication is to verify the authenticity of the image content, with the possibility to localize and recover the original content of altered image, independent of its format. Image authentication schemes can be classified under two main categories: fragile scheme and semi-fragile scheme. The fragile watermarking schemes are characterized by their high sensitivity to the minor change that makes them advantageous for some applications where strict authentication is required. Fragile watermarking [1], [2],[3],[4],[5][6]is designed to be easily destroyed after any kind of manipulations of the protected image. While, the concept of semi-fragile watermarking scheme[7][8][9] impose that watermark should be embedded in such kind that only malicious attacks are detected. Recently, the authentication watermarking schemes look not only to detect image manipulations but also localize and approximately recover tampered regions. Altered region recovery is achieved by replacing the altered pixels with their corresponding embedded as watermark data. Generally, Tamper restoration is divided into two types: accurate restoration and vague restoration. Accurate restoration means the restored image is the same as the original image exactly. However, vague restoration means restore damage area approximately. The principal advantage of this method is its restoration capabilities of the corrupted image regions. For both fragile and semi-fragile authentication schemes, there are some specific requirements that are extremely important for any authentication scheme.

a. Robustness: In such authentication system, watermark must tolerate image processing operations. This property is just appropriate for schemes that provide a semi –fragile authentication algorithm.

b. Security: The authentication system must have the capacity to protect a digital watermark even after undergoing some serious manipulation.

c. Capacity: also called payload. It is maximum amount of data, which can be embedded into an image without noticeably reducing image quality.

d. Perceptibility: the original cover image and the watermarked image should be indistinguishable.

e. Localization: is used to identify the specific positions where the tamper has occurred.

f. Recovery: The authentication system must be capable to partially or completely recuperate the image regions considered inauthentic.

In[10], author proposed self-recovery in wavelet domain method. The coefficients of the approximation sub-band LL_2 of the second wavelet decomposition are used as a recovery watermark. These coefficients are embedded in the first wavelet decomposition sub-band coefficients using QIM approach. To reduce the payload only the n most significant bits of every wavelet coefficient from LL_2. The scheme can resist cropping attack but it presents a weakness against quantization and compression attacks. The scheme proposed in[11]is based on two watermarks. The first one is the digest which is evaluated for each 4×4 sub-block by multiplying each pixel in it by one of the 16 pseudorandom numbers generated from a secret key embedded for authentication purpose. The second one is used for recovery purpose. It consists of a number of descriptors. It is evaluated through series of transformation. DWT transformation of entire image is followed by block based DCT transformation of the LL part of the DWT transformed image and its quantization. The scheme can effectively thwart collage attack but it can't resist compression attack. Authors in [12]present a fragile image watermarking algorithm. Block numbers and image unique index are used to extract watermarks and locate tampered position. The watermark is embedded into all the 2-bit LSBs of original image. The scheme can detect any changes to the pixels or any destruction to the image integrity and effectively implements the authentication of image integrity and restoresthe tampered regions. In [13], authors proposed a statistical fragile watermarking scheme, in which a set of tailor-made authentication data for each pixel together with some additional test data are embedded into the host image. On the authentication side, examining the pixels and their corresponding authentication data will reveal the exact pattern of the content modification. Experimental results show that the method has high tampering location accuracy. In [14]authors proposed a fragile watermarking scheme for image tamper localization and recovery. The Singular Value Decomposition (SVD) of each block of size 4*4 of the original image is performed and used to compute the tamper localization watermark. Where, the recovery watermark is computed from the four 2*2 sub-blocks of each 4*4 block. The two watermarks are embedding in the first and second Least Significant Bits (LSB). Rosales-Roldan and al. [15]proposed a two watermarking approaches for image authentication, localization and recovery of the tampered areas. The halftone version of original image is used as watermark and embedded into two different domains (the Discrete Cosine Transform (DCT) and Integer Wavelet Transform (IWT)). The Structural Similarity index (SSIM) criterion is using for tampered regions detection. Where, the inverse halftoning process is used to recover the tampered regions. In previous work [16]we proposed self-authentication mechanism for JEPG2000 image authentication based on secure semi fragile watermarking Perceptual Hash Function (PHF). The hash was performed using the fifth approximation sub-band (LL_5) coefficients of discrete wavelet transformation generated by jpeg2000 encoder and embedded into the same sub-band using QIM approach. To increase the robustness of watermark only n Most Significant Bit (MSB) of The LL_5 sub-band coefficients are used to generate the hash value. Sha256 function is used to increase the security of the generated hash value. The scheme can robustly survive compression attacks generated by the JPEG2000 encoder themselves with a high perceptual watermarked image quality while still able to detect malicious attacks. In[17], we proposed a fragile watermarking scheme for not only image authentication but also for tampered regions localizing and recovering. Two watermarks are generated. The first one is the authentication watermark which is generated from the Singular Value Decomposition (SVD) for each block of approximation sub-band of second level wavelet decomposition (DWT) to detect and localize tampered regions. The second one is the information watermark which generated from the same approximation sub-band and compressed using Data Representation through Combination (DRC). Both of them are embedded into approximation sub-band coefficients of first wavelet decomposition using Quantization Index Modulation (QIM). The scheme can detect malicious attack and precisely localize tampering regions while preserving a high watermarked image quality. As limitation, the scheme is not able to survive compression attacks. For this reason, in this present work we propose a semi-fragile watermarking scheme for image tampering localizing and recovery based on DRC (Data Representation through Combination) [18]. The proposed scheme can effectively detect malicious attacks and distinguish it from no malicious attacks such as JPEG compression. Sustained by the experiments, our method has been showed good estimate of the original image, even if the watermarked image has severely been tampered with. The rest of this paper is organized as follows. In Section 2, we briefly describe some related works such as Discrete Wavelet Transform (DWT) and Data Representation through Combination technique. In Section 3, the proposed image recovery scheme is presented with detailing the steps of the algorithm. Section5 shows the experimental results. Section 6 concludes the proposed scheme.

II. RELATED WORKS

2.1 Discrete Wavelet Transform (DWT)

Discrete Wavelet transform (DWT) is known as a mathematical tool. It is used to decompose an image in a hierarchical manner. In this transformation process, the temporal information is maintained, unlike conventional Fourier transform .Wavelets are produced by translations and dilations of a fixed function called mother wavelet. Both frequency and spatial description are provided by wavelet transform. For a one dimensional signal, the main idea in the Discrete Wavelet transform is as flow. A signal is split into two parts of high frequencies and low frequencies. The part with the high frequencies is basically the edge components of the signal. The part with the low frequencies is split again into two parts of high and low frequencies. This process is continued an arbitrary number of times. For 2-D images, applying DWT corresponds to processing the image by 2-D filters in each dimension. The filters divide the input image into four non-overlapping multi-resolution sub-bands LL_1, LH_1, HL_1 and HH_1 Figure 1 The sub-band LL_1 (called approximation sub-band) represents the coarse-scale DWT coefficients while the sub-bands LH_1, HL_1 and HH_1 represent the fine-scale of DWT coefficients.

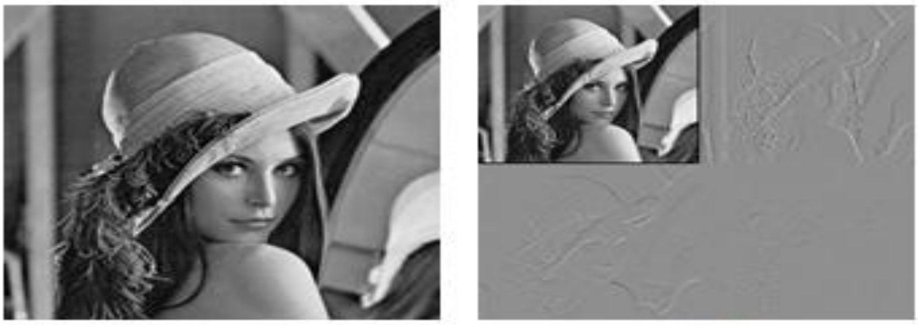

(a) (b)

Figure 1: (a) Host Image, (b) Decomposition in the first iteration

To obtain the next coarser scale of wavelet coefficients, the sub-band LL1 is further processed until some final scale N is reached Figure 2. When N is reached we will have 3N+1 sub-bands consisting of the multi-resolution sub-bands LL_N and LH_x, HL_x and HH_x where x ranges from 1 until N.

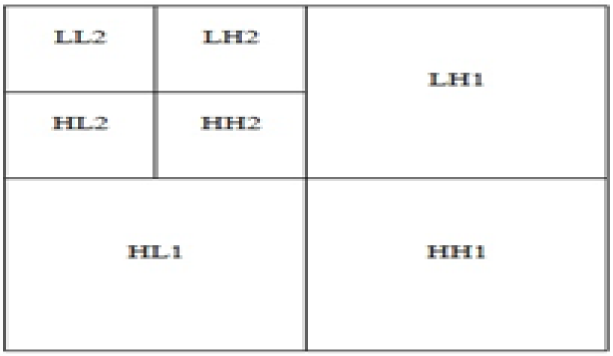


Figure 2:Sketch Map of Image DWT Decomposed

Furthermore, from these DWT coefficients, the original signal can be reconstructed. This reconstruction process is called the inverse DWT (IDWT). Due to its excellent spatio-frequency localization properties, the DWT is very suitable to identify the areas in the host image where a watermark can be embedded effectively. In general most of the image energy is concentrated at the lower frequency sub-bands LL_x and therefore embedding watermarks in these sub-bands may degrade the image significantly. Embedding watermark in the low frequency sub-bands, however, could increase robustness significantly. On the other hand, the high frequency sub-bands HH_x include the edges and textures of the image and the human eye is not generally sensitive to changes in such sub-bands. This allows the watermark to be embedded without being perceived by the human eye. The main strength offered by transform domain techniques is that they can take advantage of special properties of alternate domains to address the limitations of spatial domain or to support additional features. The purpose of this paper is to use the wavelet transform to embed watermark information in most robust and imperceptible part of image. The wavelet transform has a number of advantages over the other transforms, namely the DCT: The DWT is a multi-resolution description of an image: the decoding can be processed sequentially from low resolution to higher resolutions. The DWT is closer to human visual system than DCT. Hence, the artifacts introduced by wavelet domain coding with high compression ratio are less annoying than those introduced at the same bit rate by DCT. In the propose method, we take these benefit of DWT to choose the most proper sub-bands in case of robustness and imperceptibility.

2.2 Data Representation through Combination

The basic idea of DRC image compression theory was originally proposed by [18]as a new way to represent an image. It is a theory which precise a unique representation for each image. DRC can be used in both lossless compression and lossy compression depending on application's needs. Usually, an image is represented by a matrix of pixels where each pixel can be written in binary form. Thus For an image of size w × h and bit depth b, the original image size S is simply computed by the following formula.

$S = w \times h \times b(\text{ bits })$ (1)

Using DRC, an image can be represented in memory by a unique reference number called "index" which represents the number of the pixel combinations. This identifier will be stored in memory instead of the image with the number of columns and lines. The number of combination witch we called nc for an image can be computing as follow:

$nc = g^{w \times h}$(2)

Where: w and h are the height and the weight of the image respectively and g is the number of possible values of the samples (g=256 in case of gray scale images).Considering a group of images of size w and h where w=2 and h= 2 (w: width and h: height) with gray scale level b=256. The total number of combination can be computed as flow:

$G^{w \times h} = 256^{2\times 2} = 256^{32}$ (3)

Each image with same features may have an index between 0 and 2^{32-1} . To memorize this index in a file, between 0 to 32 bits are required (where 32 bits is the worst case).

To explain our proposed method inspired from DRC theory: Let I be an image with h=n, w=m and gray level g= l;

- First, we will compute the total number of possible combination: $nc = l^{n \times m}$;
- Then for each group of pixels, we will compute the number of possible combination: $nc_g = nc/l$;
- Now, to find the index of the image, we should apply (4) and (5). Let p(i) be the current pixel.

$$nc_g(i) = nc_g(i - 1)/l \quad (4)$$

$$index(i) = index(i - 1) + nc_g(i) \times p(i) \quad (5)$$

III. PROPOSED SEMI-FRAGILE WATERMARKING SCHEME

In this section, we will describe our proposed watermarking scheme illustrate in Figure 3. The proposed method can be classified into 4 parts: watermarking generation and embedding, watermarking extraction, tampering detection and localization and finally image recovery.

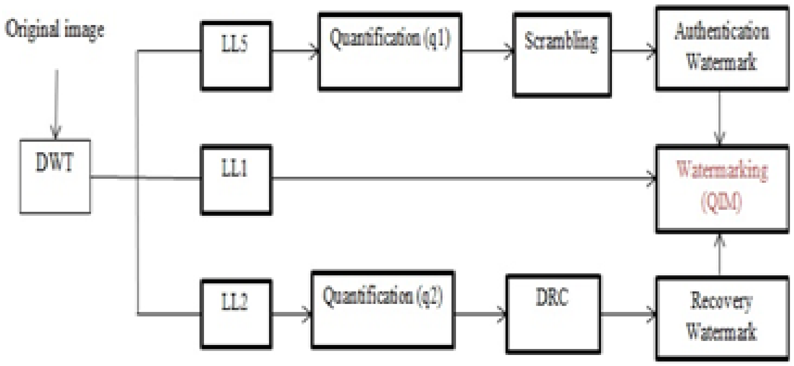


Figure 3 : General Embedding Process

3.1 Watermarking Generation and Embedding

3.1.1 Authentication watermark generation

Step1: Transformation. The host image *Img* of size *N*N* is transformed into the wavelet domain by performing the bi-dimensional Discrete Wavelet Transform 2D-DWT (Daubechies 1) on 5 resolution level.

Step2: Quantification. All coefficients AC_{5i} of the approximation sub-band, LL_5, of size $S_5 = ((N/32)*(N/32))$ are quantified by scalar quantification value *Sq* as follow:

$AC_{5iq} = \lfloor AC_{5i}/S_q \rfloor$(6)

Step3: Decomposition. Each quantified coefficient AC_{5iq} (256 coefficients for an image of size 512*512) is decomposed as AC_{5iq}=$AC_{5iq}^{M} + AC_{5iq}^{L}$. Where *M* and *L* correspond to the most significant bit (MSB) planes and the least significant bit (LSB) planes, respectively;

Step3: Each *5* MSB bits are concatenated in one vector W_A and scrambled using a secret key k_1;

3.1.2 Recovery Watermark Generation

Step1: Transformation. The host image is transformed into wavelet domain using 2D-DWT (Debauchies 1) on 2 resolution level.

Step2: Decomposition. Each wavelet coefficients $AC_{2i}$of approximation sub-band LL_2, of size S2 = ((N/4)*(N/4)) is decomposed as AC_{2i}=$AC_{2i}^{M}+AC_{2i}^{L}$. Where M and L correspond to the most significant bit (MSB) planes and the least significant bit (LSB) planes, respectively;

Step3: Data Representation through combination (DRC). To reduce the size of the information watermark, we apply the DRC. The LL_2 sub-band is firstly reshaped to one dimensional vector V_2. Then, V_2 is divided into *P* blocks B_j of *nb* coefficients where *nb*= S_2/*P*. The DRC is applied to each block and *P* index presenting the information watermark I_w are finally generated.

Step 4: Watermark scrambling. Using a second secret key k_2, the information watermark values are randomly permuted.

3.1.3 Watermark Embedding

For most block based approaches, watermark is embedded into image block with at least one bit in each block. In fact, these methods provide a high embedding capacity while there are fragile against many attacks such as lossy compression, noise addition and resetting LSB. In our case, the watermark is embedded into each group of wavelet coefficients of the first approximation sub-band LL_1. In fact, as mentioned in section 2.1, the lower frequency sub-bands content the most energy of the image. Therefore, it will not undergoes a strong quantization in the compression process and consequently embedding watermarks in the low frequency sub-bands may ,significantly, increase robustness. The process of the embedding start by dividing The LL_1 sub-band into p (p=256 for an image of size 256*256) blocks b (b_1, b_2 … b_p) of size 16*16. The two generated watermarks $v_a$and $v_r$are concatenated in one watermark vector v_wFigure 4.

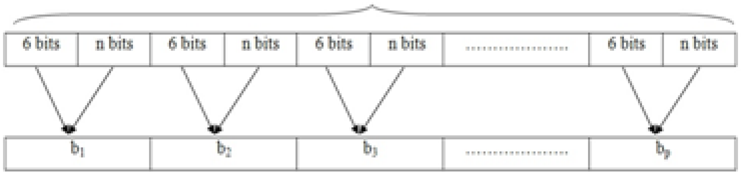


Figure 4 : Watermark capacity

In fact, six authentication bits and n recovery bits are embedded into each block, where:

$$n = \sum_{1}^{l} index - size/p \qquad (8)$$

Each watermark bit from watermark vector V_w is embedded into the original wavelet coefficients, using a Quantization Index Modulation (QIM) [19] approach as follow:

Let $AC_1(x,y)$ be the original coefficient value, $AC_1'(x,y)$ be the watermarked coefficient value and Q is the quantification embedding step:

$$\mathrm{AC}_1'(\mathrm{i},\mathrm{j}) = \left\lfloor \frac{AC_1(i,j)}{Q} \right\rfloor + \frac{\mathrm{Q}}{4}(if V_w(i) \quad (9)$$

$$\mathrm{AC}_1'(\mathrm{i},\mathrm{j}) = \left\lfloor \frac{AC_1(i,j)}{Q} \right\rfloor * \mathrm{Q} + \frac{3\mathrm{Q}}{4}(otherwise)(10)$$

After the entire watermark has been embedded, the Inverse 2D−DWT is calculated to obtain the watermarked image.

3.2 Watermark extraction

The watermark extraction process implies the following steps:

- Step1: The received image is transformed into wavelet domain using bi-dimensional discrete wavelet transforms decomposition “db1” level 1, 2 and 5.
- Step2: From LL_1 approximation sub-band, we extract the watermark bit w from each watermarked coefficients AC_1^* according to the following expressions:

$$z_1 = \lfloor AC_1^*(i,j) + Q/4)/Q \rfloor * Q \qquad (11)$$

$$z_2 = \left\lfloor \frac{AC_1^*(i,j)}{Q} \right\rfloor * Q \qquad (12)$$

$$w^*(i) = \begin{cases} 0 \; if \; z_1 = z_2 \\ 1 \; otherwise \end{cases} \qquad (13)$$

- Step3: The six authentication bits are collecting in one vectorW_a^*.
- Step4: The authentication watermark $W_a^*$of the received image is computed as described in the watermark generation process.
- Step5: By comparing the two authentication watermark, a detection indicator for each test sub-band LL_2 block B_k is computed as follows:

$$d(i) = \begin{cases} 1 \; if w^{'}(i) \neq w^*(i) \\ 0 \qquad otherwise \end{cases} \qquad (14)$$

- Step6: A tamper detection masks, M can then be generated based on the detection indicator d.

3.3 Recovery

After tamper detection, all blocks are classified as authentic or unauthentic. The information watermarks $w_r^{'}$are extracted from LL_1 sub-band and are rearranged using random position sequence generated by using secret key k_3. If any block of LL_2 sub-band is qualified unauthentic:

- The inverse DRC is performed using the extracted information watermark $w_r^{'}$to get the original coefficients.
- The unauthentic block coefficients are replaced by their correspondent extracted coefficients from $w_r^{'}$.
- Finally, the inverse wavelet transform is performed to get the recovered image.

IV. EXPERIMENTAL RESULTS

Different types of gray images, of size 512 x 512 with different formats were used to evaluate the feasibility and the performance of the proposed scheme. We show the impact of watermarks, tamper detection and localization, image recovery, and incidental manipulation (such as JPEG compression) as follows.

4.1 Reduce capacity: DRC

We used DRC theory to reduce the payload capacity and consequently increase the quality of watermarked image. With several gray level images, the reduction of descriptors size (recovery watermark) may exceed 50% compared to uncompressed data payload. In fact, in previous works[10], the information watermark is directly embedded into the host image without being compressed for these reasons the embedded data is so big and can affect the quality of watermarked image. Besides, the DRC can preserve the image quality. One more goal of this theory is that even if some DRC compressed watermark bits are losted, we still able to recover the image using the rest of recuperated DRC compressed watermark bits. This advantage could not be realized with known lossless compression schemes like Huffman or RLE [20].

4.2 Watermark Analysis:

Table 1 gives the quality measurement in terms of PSNR and SSIM of the watermarked images for different host images ‘Lena”, ‘Baboon’, ‘Boat’, ‘Goldhill’, ‘Barbara’ and ‘Peppers’ using different quantization values in the embedding process. As we can see in Table 1 for different given images, the average PSNR and SSIM for Q=8 are respectively up to 46 and 0.99. It is evident that the higher quantization step value causes image quality degradation. In this paper, we set the quantization step to 8.

	Quantization Step			
	8		16	
	PSNR	SSIM	PSNR	SSIM
Lena	47.64	0.9920	41.68	0.9713
Boat	46.75	0.9913	40.36	0.9717
Baboon	46.13	0.9965	40.36	0.9871
Goldhill	46.38	0.9929	40.58	0.9744
Barbara	46.46	0.9932	40.71	0.9763
Peppers	46.75	0.9909	41.01	0.9979

Table1 : Image QualityMeasurements

The proposed scheme gives a high PSNR values compared to reference schemes as shown in Table 2 even if we choose 16 as quantization step (>40 db). Thus the watermarked images retain better visual quality and the distortion is imperceptible (Figure.5).

Images	Proposed	[6]	[5]	[8]	[9]
PSNR (db)	46	40	44.15	40	43

Table 2 : The PSNR Values Comparison

4.3 Tamper detection:

In this section, we focus to detect and localize image tampered using cropping or copy-move attacks. The experiments show that the proposed scheme can successfully detect and localize tampers (Figure 5). In case of 512 × 512 image sizes, the detection resolution of the algorithm is (32 × 32). In fact, each wavelet coefficient used as authentication watermark represents a block of size ($2^5 \times 2^5$) pixels in the watermarked image (section 3.1.1).

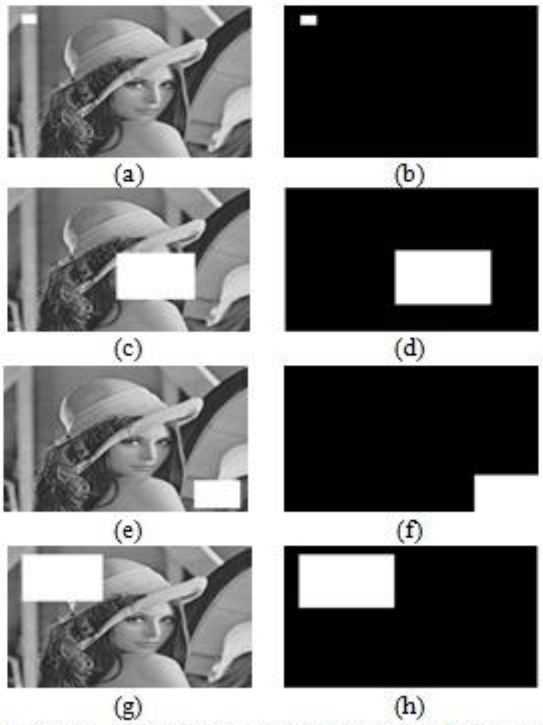


Figure 6 :(a), (c), (e) and (g) tampered images and (b), (d), (f) and (h) tampered detection with blocks resolution of size 32*32

4.4 Image Recovery:

Figure7(b) presents the recovered image when the watermarked image was not attacked. The approximation sub-band on 2 resolution levels, LL_2, is replaced by information watermark. Compared to the original image, the PSNR and the SSIM of the recovered image are 34.95 dB and 0.9738, respectively. As we can see the selected information watermark can gives an acceptable estimation of the original image.

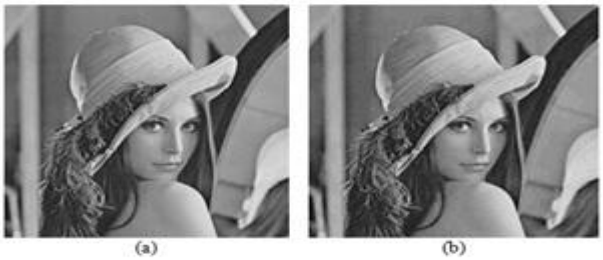


Figure 7: (a) original image, (b) recovered image (no attack)

Now after tamper detection test, all blocks in the watermarked image are marked as either authentic or unauthentic. The information watermark that is embedded in the image will be used to recover the unauthentic blocks. In the proposed scheme, the image recovery process is accomplished just by replacing the intensity of each coefficient within the invalid block with the corresponding embedded information watermark. Figure 8. a,c,e and g shows the watermarked image with an unauthentic region of different size. The tampered blocks are represented by the extreme white. Figure8 b, d, f and h present the recovered images versions. In all cases, PSNR value in the restored areas is up towhite. Figure8 b, d, f and h present the recovered images versions. In all cases, PSNR value in the restored areas is up to 30dB compared to the original images as reference as presented in Table 3.

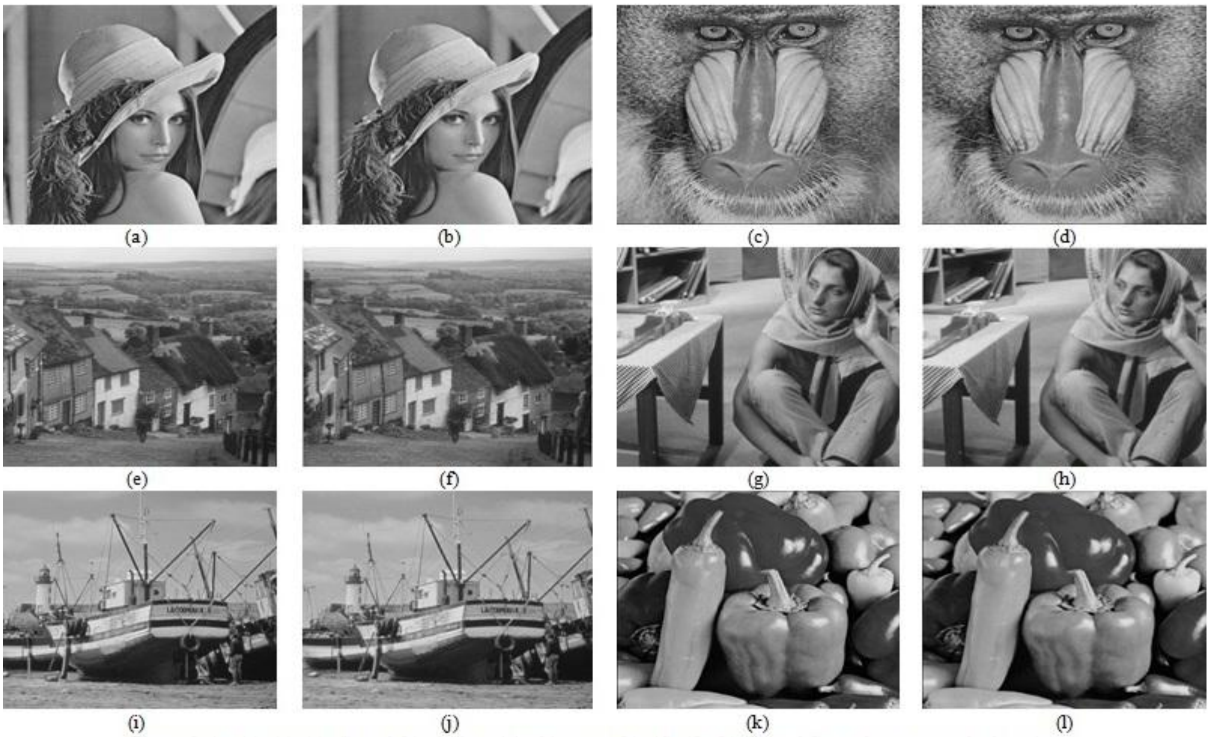
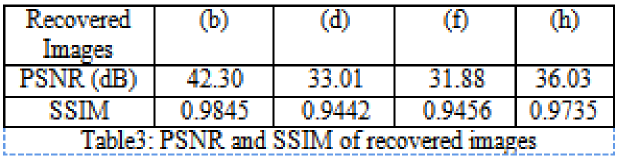


Figure 5: (a ,(c), (e), (g), (i) and (k) are the original images, (b), (d), (f), (h), (j) and (l) are the watermarked versions

We have proved the performance of our proposed approach in several tampering schemes with the above tests. The PSNR and the SSIM prove that our approach has not only an extremely high accuracy of tampering localization but also a relatively an acceptable recovery rate.



Recovered Images	(b)	(d)	(f)	(h)
PSNR (dB)	42.30	33.01	31.88	36.03
SSIM	0.9845	0.9442	0.9456	0.9735

Table3: PSNR and SSIM of recovered images

4.5 Tamper detection under incidental manipulation

We also evaluate the robustness of our proposed approach against non-malicious tamper produced by JPEG compression. In fact, lossy compression, such as JPEG, is frequently used in common image operation, thus the authentication algorithm should resist to image compression and distinguish it from malicious attack. For this purpose, we perform some test to precisely determine the quantization step for authentication mark embedding in order to survive JPEG compression attack.

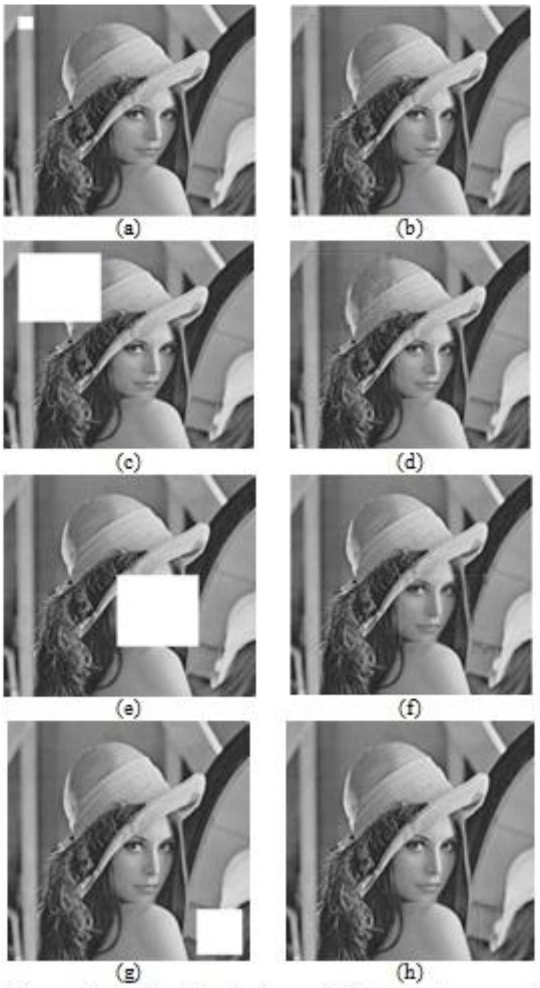
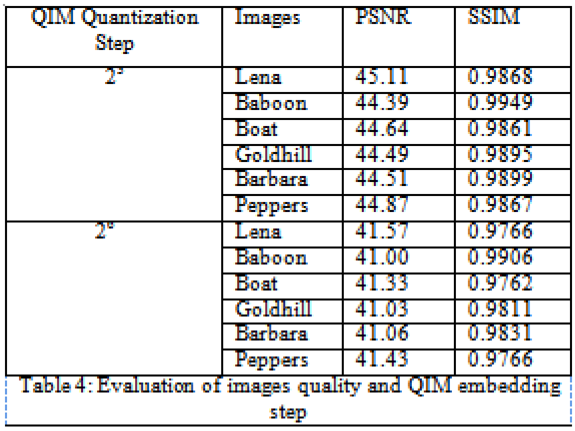


Figure 8: (a), (c), (e), and (g) are tempered images, (b), (d), (f) and (h) are recovered versions

Table 4 shows the measurement quality of different images with Q=8 for information watermark embedding and Q=2^5 and Q=2^6 for authentication watermark embedding, respectively.

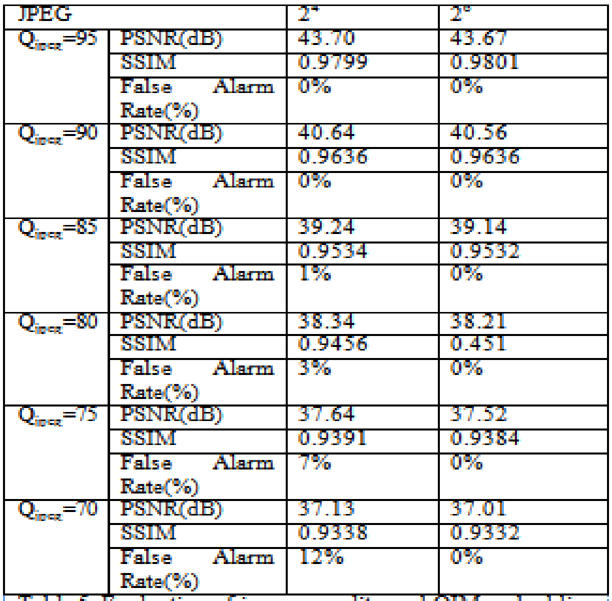
Image quality still acceptable even with high quantization step (≥41dB). Increasing Q will increase the robustness of thealgorithm to JPEG compression operation as we can inTable 5, but also decrease the image quality.

A compromise between these parameters has to be found for specific needs. Figure 9 (a) present the watermarked image maliciously tampered and also compressed by JPEG (Q_{jpeg}=70) with PSNR=15.21. Figure 9 (b) tampered block is located correctly and recovered with extracted information watermark. In this case, PSNR value of the restored image is 30.25dB when regarding original image as reference (Figure 9 (c)).



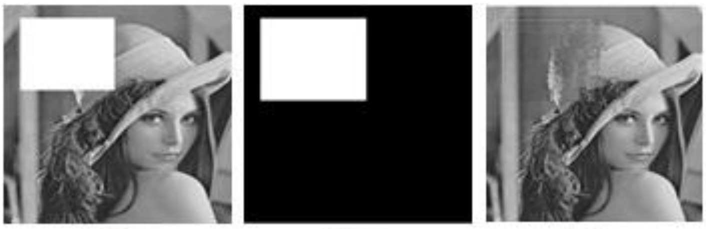
QIM Quantization Step	Images	PSNR	SSIM
2^5	Lena	45.11	0.9868
	Baboon	44.39	0.9949
	Boat	44.64	0.9861
	Goldhill	44.49	0.9895
	Barbara	44.51	0.9899
	Peppers	44.87	0.9867
2^6	Lena	41.57	0.9766
	Baboon	41.00	0.9906
	Boat	41.33	0.9762
	Goldhill	41.03	0.9811
	Barbara	41.06	0.9831
	Peppers	41.43	0.9766

Table 4: Evaluation of images quality and QIM embedding step



JPEG		2^4	2^6
Q_{jpeg}=95	PSNR(dB)	43.70	43.67
	SSIM	0.9799	0.9801
	False Alarm Rate(%)	0%	0%
Q_{jpeg}=90	PSNR(dB)	40.64	40.56
	SSIM	0.9636	0.9636
	False Alarm Rate(%)	0%	0%
Q_{jpeg}=85	PSNR(dB)	39.24	39.14
	SSIM	0.9534	0.9532
	False Alarm Rate(%)	1%	0%
Q_{jpeg}=80	PSNR(dB)	38.34	38.21
	SSIM	0.9456	0.451
	False Alarm Rate(%)	3%	0%
Q_{jpeg}=75	PSNR(dB)	37.64	37.52
	SSIM	0.9391	0.9384
	False Alarm Rate(%)	7%	0%
Q_{jpeg}=70	PSNR(dB)	37.13	37.01
	SSIM	0.9338	0.9332
	False Alarm Rate(%)	12%	0%

Table 5: Evaluation of images quality and QIM embedding step



(a) (b) (c)

Figure 9: (a) tampered watermarked image (Q_{jpeg}=70), (b) tamper detection, (c) recovered image (PSNR=30.25, SSIM=0.8711)

4.6 Comparison with Previous Approaches

We construe the performance of our proposed scheme by means of experimental results and compare with previous approaches. We summarize the different salient features in Table 7 below. Fragile, semi-fragile indicated the class to which each method belongs, as well as the type of data used as watermark, the data cover, the objectives regarding integrity (i.e., strict or content indicating sensitivity to JPEG compression), and whether the method offers a possible localization and/or reconstruction of the tampered areas. By analyzing this table, we can notice that the fragile watermarking schemes [9][5][4][11] allow only a strict authentication. However, the semi-fragile watermarking methods such as our proposed method allow a selective authentication which is more interesting for image that enables manipulations in such way that the semantic interpretation still unchanged. The performance of our performance method is also compared with [8] and [9]in term of PSNR. Our proposed method offers a high watermarked image quality up to46dB compared to reference approaches [8] and [9].

V. CONCLUSION

In this work, we propose a semi-fragile watermarking scheme based on Data Representation through Combination for image tampering detection, localizing and recovery. Two watermarks are used and hidden into DWT approximation sub-band. Experimental results exhibit an ability to detect malicious attack with a high capability of localization. Besides, in case of tampering, it produces a good estimation of the original content and preserves the watermarked image quality. The quality of watermarked image is extremely high compared with other approaches in literature. The embedded watermark is also robust to JPEG compression.

REFERENCES

[1]. H. He, F. Chen, H. Tai, S. Member, T. Kalker, and J. Zhang, “Performance Analysis of a Block-Neighborhood- Based Self-Recovery Fragile Watermarking Scheme,” *Ieee Trans. Inf. Forensics Secur.*, vol. 7, no. 1, pp. 185–196, 2012.

[2]. F. Di Martino and S. Sessa, “Fragile watermarking tamper detection with images compressed by fuzzy transform,” *Inf. Sci. (Ny).*,

vol. 195, pp. 62–90, Jul. 2012.

[3]. 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.

[4]. C.-M. Wu and Y.-S. Shih, “A Simple Image Tamper Detection and Recovery Based on Fragile Watermark with One Parity Section and Two Restoration Sections,” *Opt. Photonics J.*, vol. 03, no. 02, pp. 103–107, 2013.

[5]. H. J. He, J. S. Zhang, and H. M. Tai, “Self-recovery fragile watermarking using block-neighborhood tampering characterization,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 5806 LNCS, pp. 132–145, 2009.

[6]. X. Tong, Y. Liu, M. Zhang, and Y. Chen, “A novel chaos-based fragile watermarking for image tampering detection and self-recovery,” *Signal Process. Image Commun.*, vol. 28, no. 3, pp. 301–308, 2013.

[7]. C. Li, R. Yang, Z. Liu, J. Li, and Z. Guo, “Semi-fragile self-recoverable watermarking scheme for face image protection,” *Comput. Electr. Eng.*, no. February, 2015.

[8]. R. O. Preda, “Semi-fragile watermarking for image authentication with sensitive tamper localization in the wavelet domain,” *Measurement*, vol. 46, no. 1, pp. 367–373, 2013.

[9]. Y. Li and L. Du, “Semi-fragile watermarking for image tamper localization and self-recovery,” in *Proceedings 2014 IEEE International Conference on Security, Pattern Analysis, and Cybernetics, SPAC 2014*, 2014, pp. 328–333.

[10]. R. O. Preda, “Self-recovery of unauthentic images using a new digital watermarking approach in the wavelet domain,” pp. 0–3, 2014.

[11]. P. P. Augustus and D. S. George, “Watermarking Technique for Self Authentication and Recovery,” pp. 157–165, 2013.

[12]. Y. Ke-xin, Z. Jian-qi, L. Bing, and Z. Guan-qun, “Pixel-Based Fragile Image Watermarking Algorithm,” in *2010 Second International Workshop on Education Technology and Computer Science*, 2010, pp. 134–137.

[13]. X. Zhang and S. Wang, “Statistical Fragile Watermarking Capable of Locating Individual Tampered Pixels,” *IEEE Signal Process. Lett.*, vol. 14, no. 10, 2007.

[14]. I. Ahmad, A. Millie, P. Chang, and W. Ahn, “SVD based fragile watermarking scheme for tamper localization and self-recovery,” *Int. J. Mach. Learn. Cybern.*, 2015.

[15]. L. Rosales-Roldan, M. Cedillo-Hernandez, M. Nakano-Miyatake, H. Perez-Meana, and B. Kurkoski, “Watermarking-based image authentication with recovery capability using halftoning technique,” *Signal Process. Image Commun.*, vol. 28, no. 1, pp. 69–83, 2013.

[16]. H. Rhayma, A. Makhloufi, and A. Ben Hmida, “Self-Authentication Scheme Based on Semi-Fragile Watermarking and Perceptual Hash Function,” pp. 1–6, 2014.

[17]. H. Rhayma, A. Makhloufi, A. Ben Hamida, and H. Hamam, “Self-Embedding Authentication Scheme based on Data Representation through Combination with Recover Capability,” *13th ACS/IEEE Int. Conf. Comput. Syst. Appl. AICCSA*, pp. 1–5, 2016.

[18]. J. Said, R. Souissi, and H. Hamam, “A New Representation of Image Through Numbering Pixel Combinations,” *J. Inf. Secur. Res.*, vol. 4, no. 1, 2013.

[19]. O.-Z. Azza, A. Makhloufi, A. Bouallègue, C. Olivier, and A. Naït-Ali, “Blind watermarking integrated to wavelet image coding scheme,” *Int. Rev. Comput. Softw.*, vol. 3, no. 1, pp. 53–61, 2008.

[20]. D. Salomon, *A Concise Introduction to Data Compression*. London: Springer London, 2008.

Features ***Methods***	***Class***	***Cover***	***Mark***	***Integrity***	***Localization***	***Recovery***	***Quality***
Proposed	Semi-fragile	Wavelet coef.	Wavelet coef.	Content: Survives Jpeg compression	YES	Recover the estimated image	46
[6]	Fragile	LSB	Block-based	Strict: Cannot survive JPEG compression	YES	Recover the estimated image	40
[5]	Fragile	LSB	Block-based	Strict: Cannot survive JPEG compression	YES	Recover the estimated image	44
[8]	Semi-fragile	Wavelet coef.	Wavelet coef.	Content: Survives Jpeg compression	YES	Cannot recover the estimated image	40
[9]	Semi-fragile	Wavelet coef.	SVD	Content: Survives Jpeg compression	YES	Recover the estimated image	43
[4]	Fragile	LSB	Block-based	Strict: Cannot survive JPEG compression	YES	Recover the estimated image	44
[11]	Fragile	LSB	DCT coef and checksum	Strict: Cannot survive JPEG compression	Yes	Recover the estimated image	48

Table 6 : Salient Features Of Our Proposed Method

Hanen Rhayma "Self-Embedding Watermarking Scheme Based On Discrete Wavelet Domain." The International Journal of Engineering and Science (IJES) 7.7 (2018): 08-18