Multimedia Tools and Applications (2019) 78:14067–14089
https://doi.org/10.1007/s11042-019-7244-x

Semi-fragile self-recovery watermarking scheme based on data representation through combination

Hanen Rhayma[1,2] · Achraf Makhloufi[2] · Habib Hamam[3] · Ahmed Ben Hamida[2]

Received: 19 December 2017 / Revised: 8 January 2019 / Accepted: 18 January 2019 /
Published online: 12 February 2019

Abstract

The widely available multimedia editing tools and their large reconstruction capabilities make digital multimedia content more sensitive to malicious tampering and manipulations. Therefore, ensuring digital image integrity has become a crucial issue. Watermarking became a popular technique for image authentication. The goal of this paper is to propose a new semi-fragile watermarking scheme for image authentication, localization, and recovery, by using two different watermarks jointly. The embedded information watermark for content recovery is computed from discrete wavelet transform (DWT) approximation coefficients of second level decomposition of the original image and compressed by using Data Representation through Combination (DRC) in order to reduce watermark payload. On another hand, authentication watermark used for both authentication and localization of image tampering is computed by using the block-based watermarking algorithm. Three pseudo-random maps are generated in order to improve the security of the proposed scheme against local attack. Both watermarks are embedded into approximation sub-band of the first wavelet decomposition. Experimental results show that our proposed approach has not only an extremely high accuracy of tampering localization but also a relatively very high recovery rate. Besides, the scheme is able to detect perfectly the difference between malicious attacks and non-malicious attacks such as JPEG compression.

Keywords Semi-fragile watermarking · Data representation through combination · DWT · Self-recovery · Localization · Authentication

1 Introduction

Data transmission of different types of information (image, video, audio...) became crucial in many applications (transfer of medical data, bank transfers, corporate communications,

✉ Hanen Rhayma
rhayma_hanen@yahoo.fr

[1] École Nationale d’Ingénieurs de Gabés (ENIG), Université de Gabés, Omar Ibn El Khattab Zrig, Gabés, 6072,Tunisia

[2] ATMS Advanced Technologies for Medecine and Signals, Enis, Université de Sfax, Sfax, Tunisia

[3] Faculty of Engineering, Université de Moncton, Moncton, NB E1A 3E9, Canada

a large amount of information through emails, etc...). In such situations, the authentication and integrity of the exchanged data remain the most important purposes. Steganography, cryptography and watermarking are three closely related fields applied to supply a secret conversation and to ensure data protection [6]. Nevertheless, these techniques are entirely different from each other. In fact, steganography conceals the existence of a message and in the best case, only the sender and the intended recipient can detect the presence of the message [3, 17], while cryptography is charged with hiding encoded information [1]. Like steganography, digital watermarking is somewhere concealing data in a way that one can see the background image without any kind of corruption in the image [4]. The particularity of watermarking comparing to the two other techniques is manifested in three important ways. Firstly, the watermark is inseparable from the work in which it is embedded, for example, a painting masterpiece. Secondly, watermark undergoes the same transformations as the work (artwork for example). Finally, a watermark has some resilience against essays to destroy it. For example, if we rotate the artwork, the hidden signature, embedded in this work as a watermark, should not be destroyed by this rotation. During the last years, miscellaneous watermarking schemes have been proposed to authenticate and verify the integrity of multimedia data especially for digital images in order to avoid false judgments. The incessantly progressing powerful digital image processing tools,_simplify the manipulating with the digital image in ways that are difficult to detect. There are some image processing manipulations which preserve image content and used in order to enhance the quality or save memory space (compression, filtering, etc. . .). Since some changes must be tolerated while others should not, authentication watermark may be classified into two big classes: Strict and selective (or also fragile and semi-fragile) authentication watermarking [13]. One of the watermarking-based authentication schemes was proposed by Chen and co-authors [8]. Four steps are performed in order to localize and recover tamper in watermarked image: watermark generation and embedding, watermark extraction, tamper detection and localizing and finally image recovery. Firstly, the host image is divided into non-overlapping blocks of size 2*2. Then, six recovery bits of recovery watermark is computed using the average intensity of each block. Two key bits are also generated and concatenated with recovery watermark to form the block feature which will be encrypted and embedded in the least significant bits of its mapping block by substituting technique. The quality of the watermarked image can achieve 44 dB while the recovery image is about 25 dB. The scheme is able to detect and localize tampering under several malicious attacks such as multi-region and multi-attack tampering. But, the lack of robustness against non-malicious attacks like compression limits the effectiveness of the method. The method is able to localize the tampered block with the capability of recovery in case of attack. The authors [20] proposed a singular value based semi-fragile watermarking scheme for tamper detection and localizing. The image is foremost divided into 4*4 blocks and one is in turn partitioned into four 2*2 sub-blocks after quantification. The singular-value decomposition (SVD) is applied separately to each sub-block and the watermark bit is generated based on the SV’ s relationships of three pairs of sub-blocks. Then, the intrinsic algebraic property PBlock is evaluated. The embedding process is performed using the adaptive quantification method in approximation sub-band of each 4*4 block to obtain the watermarked image. The scheme can identify malicious tampering, incidental modification, and localizing tampered regions under mild to severe content-preserving modifications such as JPEG compression. The average PSRN of the watermarked image is about 41 dB. Reference [30] proposed a fragile self-recovery watermarking technique with effective tamper detection capabilities. The original image is divided into blocks of size 3*3 and the 2 LSBs of each pixel are reset to zero. Then, the 6-bit parity section of the watermark is generated by applying the XOR operation on the

54 MSBs and a random crypt table. For restoration, the average intensity of pixels in an image block is used. The 6-bit parity watermark section of the image block is embedded as a payload of the same block. The two copies of the 6-bit restoration watermark section of each block are embedded based on two secret maps. The quality of the watermarked image is 44.33 dB. The work in [16] used a half-toned version of the original image to obtain the recovery watermark. First, the authors stratify the Integer Wavelet Transform (IWT) to the host image and a permuted version of the approximation sub-band level 1 is considered as recovery watermark. On the other hand, a crypto binary image is used as authentication watermark. By means of dither modulation based quantification index modulation, the recovery watermark is embedded into the high-frequency sub-bands LH2 and HL2 while the sub-bands LH1 and HL1 will be charged by the authentication watermark. The PSNR of the watermarked image of the above technique is 35 dB and the quality of the recovered image after tampering can achieve 27 dB. The scheme is able to resist JPEG compression up to a quality factor equal to 70. Chamlawi and al. [2] proposed a semi-fragile watermarking scheme using an Integer Wavelet Transform (IWT). The LL1 sub-band is correlated with a random sequence to generate the authentication watermark which embedded into the second level vertical sub-bands of the image. The recovery watermark is generated by applying the DCT to LL1 sub-band and the permuting of the coefficients in zigzag order. The Integer DCT, the Huffman coding, and the BCH error control coding are all used to decrease the length of the watermark and increase robustness. The watermark is then embedded in the same sub-band as authentication watermark. The scheme considered the lossy JPEG compression as malicious attack up to the quality factor above 70. But, the main disadvantage of this technique is that the lookup table for Huffman coding must be generated, and saved for each image. The quality of the watermarked image is 40 dB. Chunlei Li et al. [10] proposed a tamper detection and self-recovery of biometric images using salient region-based authentication watermarking scheme. Using MD5, authors compute 64 authentication bits of each 8 × 8 blocks of the original. Then encrypt result using the chaotic sequence. The authentication bits are divided into slices of 8 bits. Each slice is embedded into the Least Significant Bits (LSB) of selected pixels of 8 different blocks. The block is considered as authentic if all extracted bits are untouched otherwise it is simply marked as tampered. The sensitivity of MD5 to even minor change in a pixel value of a block reduces the effecteness of the scheme. Preda [18] proposed to embed the watermark into the wavelet domain by means of quantification. The image is transformed into the wavelet domain using the bi-dimensional Wavelet Transformation. Then, the high-frequency sub-bands of certain level $n < L$ are arranged in a mono-dimensional vector and divided into groups of a fixed element after being scrambled using a secret key. A binary sequence of size equal to the number of groups is obtained by means of a secret key and used as authentication watermark. The embedding process is performed by quantifying the weighted mean of the group according to the corresponding watermark bit which resulting in a watermarked image with 40 dB as quality. The embedded watermark is able to resist to mild to moderate JPEG compression by selecting appropriate embedding parameters. Morphological operations are also used to improve detection results by eliminating the isolated tampering that appears like noise. In this paper, we propose a semi-fragile watermarking scheme for image tampering localizing and recovery based on DRC (Data Representation through Combination) [21]. Both special and wavelet domain of the original image are used for dual watermarks generation and embedding. The authentication watermark is duplicated before embedding. By the means of three secret keys, the scheme is able to generate three maps: two maps are used for authentication watermark while the third one is reserved for recovery watermark. The embedding step is accomplished using the Quantification Index Modulation (QIM).

The DRC is practically applied to reduce the recovery watermark in order to increase the watermarked image quality. 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 showed a 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 present a brief introduction to semi-fragile watermarking, DWT and DRC technique. Section 3 explains in details_our proposed semi-fragile self-embedding watermarking scheme, including watermark generation, embedding, and extraction. Tamper detection and image recovery are also clarified in the same section. Section 4 presents the experimental results. While Section 5 concludes the proposed work.

2 Background

2.1 Fragile watermarking vs. semi fragile watermarking

The main idea of fragile watermarking algorithms [5, 7, 9, 25, 31] is to produce and embed watermark data into the host image in such way that any manipulation_that affects the image will be automatically reflected in the embedded watermark. Verifying image authenticity and eventually localizing tampered regions can be performed simply by verifying the presence of the embedded watermark. This type of watermarking does not tolerate any changes of data or distortion in the protected image. The image is qualified as authentic if only all its pixels remain untouched. Namely, even content preserving manipulations are unacceptable. Strict image authentication is suitable for many applications when a simple manipulation of few numbers of pixels in some critical type of images (medical, military) can dramatically affect the decisions and can result in costly damages. On the other hand, semi-fragile authentication techniques [11, 12, 19, 26–28] embed watermarks so robustly to survive some kinds of image processing operations. Many authentication watermarking schemes can only verify the integrity of the watermarked image and locate the modification areas to some degree, but not able to recover the damaged data. However, there are many applications that require recovering tampered content even approximately. 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. While accurate restoration means the restored image is the same as the original image exactly. 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 an 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 manipulations.

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

d. Imperceptibility: 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.

2.2 Discrete wavelet transform (DWT)

Literally, the Fourier Transform (FT) is one of the most popular transformations which have been used for signal analysis [24]. Unfortunately, this transformation gives no more than the frequency information of the signal which is suitable only for stationary signals. The Short Term Fourier Transform (STFT) extends the function of FT to be able to analyze non-stationary signals by using a window function. The width of the window imposes a real problem for those who used this kind of transformation. In fact, a window with small width offers a better time resolution but a worse frequency resolution. On the other hand, large window width gives favorable frequency resolution but also suffers from poor time resolution and may lead to the stationary condition. To overcome the quandary of resolution caused by window function choosing, the wavelet transform has come into play [14]. It is basically suitable to analyze non-stationary signals (frequency changes in time) by using a totally scalable modulated window. For a giving signal such as image, two types of filters are applied: low pass filter and high pass filter. As a result, we get two different kinds of frequency: high frequency and low-frequency. Then, we repeat the same operation, but this time with only the low-frequency portion of the signal, until a predefined level is achieved. This process leads to a set of the time-frequency representation of the signal that correspond to varies frequencies bands. The Discrete Wavelet Transform (DWT) is considered as one of the most practicable wavelet transformation especially in image processing such as image watermarking. For a giving signal, the DWT decomposes the original signal into four quadrants that present the approximation and the details information with the different interpretation: LL, LH, HL, and HH using a discrete set of scaling and wavelet functions. The decomposition is easly obtained by passing the signal into a successive high pass and low pass filters (Fig. 1).

The Fig. 2 shows the decomposition of the image Lena using discrete wavelet transform. LL: the upper left sub-band presents the approximation sub-band. It is filtered by the low pass filter $\widetilde{h}$ for both rows and columns. HL: the lower left sub-band contains the vertical edges of the signal. The rows are filtered by low pass filter $\widetilde{h}$ and the columns are filtered by high pass filter $\widetilde{g}$. LH: the upper right sub-band contains horizontal edges of the signal. It used the same filters as HL alternatively. In fact, the low pass filter $\widetilde{h}$ is used for columns and the high pass filters are employed for rows. HH: The lower right sub-band is obtained by applying a high pass filter $\widetilde{g}$ for both rows and columns. This block contains basically the edges of the original signal in the diagonal direction.

The purpose of this paper is to use the wavelet transform to embed watermark information in the most robust part of the image while maintaining the perceptual quality of image untouchable. As we can see, the decomposition of the signal into four blocks gives a global view in term of information included in each one. This decomposition may lead the process of watermark embedding. In fact, the approximation sub-band or the low-frequency sub-band, LL, which corresponds to the energy of the image increases the watermark robustness

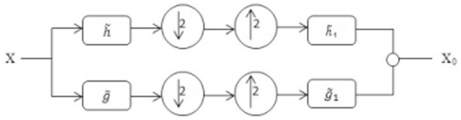


Fig. 1 The schematic diagram of the discrete wavelet transforms

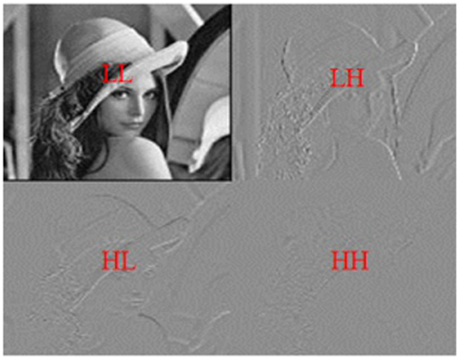


Fig. 2 **a** Host image, **b** decomposition in the first iteration

significantly but oppositely decreases the visual quality of the output image. On the other hand, the high-frequencies sub-bands, LH, HL, and HH, which correspond to the details of the image (textures and edges), provide a good output image quality since that human eye is less sensitive to changes in such sub-bands. Nonetheless, the lack of robustness makes those sub-bands inappropriate for watermark embedding. So, in order to withstand compression attacks, insertion is applied only on the frequencies that are most prominent localized in the low-frequency band since this band is weakly quantified by compression system e which always preserves the most sensitive low-frequency components of an image. However, the insertion of the mark in the area with perceptually significant components is something very visible, especially in a homogeneous area. The watermarking in this case may become visible, so it is necessary to find a compromise between robustness and invisibility of watermarking.

2.3 Data representation through combination

The proliferation of digital media makes information extremely important in our daily life. However, this powerful information needs to be now saved or transmitted. Since the bandwidth of network and storage of memory device are insufficient, the importance of data compression has become more and more significant in order to reduce the amount of information. Data compression is, in fact, a kind of application that can represent the original data with a few bits.

The basic idea of DRC image compression theory was originally proposed by [21] 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 loss-less compression and lossy compression depending on the 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 in brute form is simply computed by the following formula:

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

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 which we called nc for an image can be computing as follow:

$$nc = g^{w*h} \tag{2}$$

where: w and h are the height and the width of the image respectively and g is the number of possible values of the samples (g = 256 in case of grayscale images).

Considering a group of images of size w and h where w = 2 and h = 2 (w: width and h: height) with grayscale level b = 256. The total number of combination can be computed as flow: $G^{w*h} = 256^{2*2} = 2^{32}$. 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).

The index is practically difficult to be calculated using the current hardware. As a solution, the image is divided into slices and the index of each one is computed. The group of the index can be considered as the image index. To restore the original image, we just need the index of the image, the height, the width, and the gray scalelevel.

3 Proposed semi-fragile watermarking scheme

We designed an effective technique for image authentication that not only verifies the integrity of protected image but also localize and recover regions signed as inauthentic. For this purpose, two different kinds of watermarks are injected into original data. First, one can be considered as authentication watermark that is used to detect and localize tampered regions where the other is the information watermark for recovering aim. Our proposed watermarking scheme actually can be classified into 3 parts: watermarking generation and embedding, watermarking extraction and tampering detection and localization and finally image recovery. To improve the security of embedded watermarks and to reduce the false detection probability, 3 different maps with 3 different secret keys are generated.

3.1 Watermarking generation and embedding

3.1.1 Watermarking generation

- Authentication watermark generation

Step 1: The original image I of size $M \times M$ is divided into N nonoverlapping blocks $B_i (i = 1, 2, 3 \ldots N)$ of size 32 × 32, where $N = ((M/32) * (M/32))$.

Step 2: Each block B_i is decomposed as $B_i = B_i^M + B_i^L$ where B_i^M and B_i^L refer to the six most significant bit (MSB) planes and the two least significant bit (LSB) planes, respectively. Then, the two LSB' s of each block B_i.

Step 3: The mean of each block B_i with new pixels values is obtained as follow:

$$mean(B_i) = \frac{1}{N}\sum_{1}^{N} B_i \tag{3}$$

Step 4: Now, each block B_i is partitioned into 4 equal sub-blocks B_s of size16 × 16. The mean of each sub-block $B_s$is obtained just as step3.

Step 5: The authentication watermark for each block is generated using the following operation:

$$A_w = \begin{cases} 1 \; if \;\; meanB_s > meanB \\ 0 \qquad otherwise \end{cases} \tag{4}$$

Each block B_i will be presented by 4 authentication bits and the size of A_w is $4 * N$ (bits).

- Recovery watermark generation

In this step of the algorithm, we wish to generate the recovery watermark (information watermark) in order to reconstruct an approximated version of the regions that were damaged during undesired manipulations. In other words, a compressed version of the image is embedded within the image and extracted for recovery purpose only if the image is declared as inauthentic. Considering the tradeoff between the capacity of embedding and the perceptual quality of the watermarked image, the LL2 seems to be the optimal choice for recovery watermark generation. It represents the quarters of the original image in term of size. To optimize once more this tradeoff, the DRC previously defined is used to reduce the size of the LL2. The details are presented as follows:

Step 1: Transformation. The host image is transformed into the wavelet domain using 2D-DWT (Daubechies1) on 2-resolution level;

Step 2: Quantification. Each wavelet coefficient C_i of approximation sub-band, LL_2, of size $N_1 = ((M/4) * (M/4))$. is quantified by scalar quantification value Q as follow:

$$C_{iq} = \lfloor C_i/Q \rfloor \tag{5}$$

where $\lfloor\rfloor$refer to integer part of quotient;

Step 3: Preprocessing DRC. To reduce the size of information watermark, we apply DRC. All $C_{iq}$are divided into slice $S_j(j = 1, 2, 3, \ldots, N_2)$ of l coefficients, where $N_2 = N/l$. Then, to reduce the size of slices, we browse each slice and select the minimum and the maximum of slice coefficients $\min_j$ and $\max_j$ respectively. From each slice Sj, we subtract the minimum value $\min_j$ from every coefficient, we get $C_{iqmin} = C_{iq} - \min_j$. The minimum of each slice is recuperated into a separate secret file to be used later in the decoding process.

Step 4: Performing DRC. Compute the total number of possible combination $nC_j = \max_i^l$. To find the index of the slice S_j, we should apply (6) and (7) l times. Let $C_{iqmin}(k)$ with $(k \in \{2..l\})$ be the current coefficient.

$$C_{iqmin}(k) = C_{iqmin}(k-1)/l \tag{6}$$

$$index(k) = index(k-1) + (C_{iqmin}(i) \times nC_j) \tag{7}$$

where

$$C_{iqmin}(1) = nC_j/l$$

$$index(1) = C_{iqmin}(1) * nC_j$$

In totally, N_2 indexes are generated and the size *s-index* of each index is variable and depending principally on the value of original coefficients. Those indexes are then converted into the binary form to be embedded as recovery watermark R_w.

3.1.2 Watermark embedding

For most block-based approaches, the 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. As mentioned in Section 2.2, the lower frequency sub-bands content the most energy of the image. Therefore, it will not undergo a strong quantification in the compression process and consequently embedding watermarks in the low-frequency sub-bands may, significantly, increase robustness. Furthermore, double copies of authentication watermark are used in order to capture misclassification and ensure that the proposed method is capable to detect manipulation and localize falsifying regions while accepting incidentally attacks. The process of the embedding starts by dividing The LL_1sub-band into Nb ($Nb = 256$ for an image of size $512 * 512$) blocks $B_{lev}(B_{lev1}, B_{lev2}, \ldots, B_{levNb})$ of size $16 * 16$. Two copies of authentication watermark A_w are used A_{w1} and A_{w2}. Both the authentication watermark A_{w1} and the recovery watermark A_{w2} also $R_w$are embedded using block permutations independently to increase the security of the embedded watermarks. For authentication watermark A_{w1} and A_{w2}, every four bits representing the block B_i are embedded into two different blocks $B_j$and B_k. On the other hand, R$_w$ is divided into Nb slices S_R and each one present n bits:

$$n = (Size(R_w))/Nb(bits) \tag{8}$$

- Maps generation

Step 1: Generate three random sequences Seq_1, Seq_2 and Seq_3 of size Nb each one using three different secret keys; k_1, $K_2$and K_3respectively.

Step 2: Sort Seq_1, $Seq_2$and Seq_3 in ascending order.

Step 3: Recuperate sorting maps Mp_1, Mp_2 and Mp_3 that will be used as block mapping. $Mp_1$and Mp_2 are used for the authentication watermarks A_{w1} and A_{w2} respectively (Fig. 3), while, Mp_3 is reserved for the restoring watermark R_w.

- Recovery watermark structure

As showed in Fig. 4, for each block B_{levi} of LL_1, a vector V_{wi} representing 8 bits of the authentication watermark (4 bits for 2 different blocks B_i and B_j) and n bits of the recovery watermark are embedded.

- Applying QIM

The embedding process is accomplished using the Quantification Index Modulation (QIM) [15] approach as follow: Let $c(i, j)$ be the original coefficient value, $c'(i, j)$ be the watermarked coefficient value of such block B_{levi}, V_w is the watermark vector to embed and Δ is the quantification embedding step.

$$c'(i,j) = \begin{cases} \lfloor (\frac{c(i,j)}{\Delta}) \star \Delta \rfloor + \frac{\Delta}{4} & if\ V_w(i) = 0 \\ \lfloor (\frac{c(i,j)}{\Delta}) \star \Delta \rfloor + \frac{3\Delta}{4} & otherwise \end{cases} \tag{9}$$

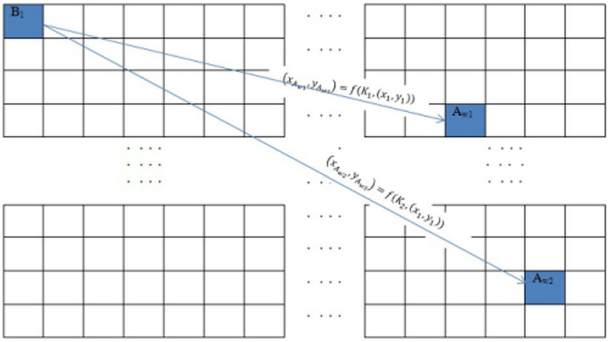

B$_1$
$(x_{A_{w1}},y_{A_{w1}}) = f(K_1,(x_1,y_1))$
A$_{w1}$
$(x_{A_{w2}},y_{A_{w2}}) = f(K_2,(x_1,y_1))$
A$_{w2}$

Fig. 3 Block mapping

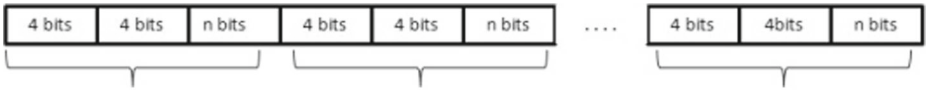


Fig. 4 Embedding payload

After the entire watermark has been embedded, the Inverse $2D - DWT$ is computed to obtain the watermarked image.

3.2 Watermark extraction and tamper detection

In this section, we present the proposed tamper detection technique. We define for each block B_i, a Boolean vector D, where $d(i) = 0$ means an authentic block, and $d(i) = 1$ means an unauthentic block. The watermark extraction and detection process imply the following steps:

Step 1: The test image $I*$ is split into N blocks B_i $(i = 1, 2 \ldots N)$ and the authentication watermark A_w^* is generated as described in the authentication watermark generation process.

Step 2: One level wavelet transform is performed for the received image. The approximation sub-band LL_1 is used to extract watermarks from watermarked coefficients ${c_w}'$ according to the following expressions:

$$y_1 = \left\lfloor \left(\frac{c'_w(i,j) + \frac{\triangle}{4}}{\triangle} \right) \right\rfloor \star \triangle \tag{10}$$

$$y_2 = \left\lfloor \left(\frac{c'_w(i,j)}{\triangle} \right) \right\rfloor \star \triangle \tag{11}$$

$$w(i) = \begin{cases} 0 \; if \quad y_1 = y_2 \\ 1 \; otherwise \end{cases} \tag{12}$$

Step 3: Every 4 bits are mapped using the two secret keys k_1 and K_2, and the 8 authentication bits that correspond to block B_i are regrouped 4 by 4 in two different vectors $A^{'}_{w1}$and $A^{'}_{w2}$. For each bit $k \in [1, 4]$, a detection indicator for the received image block is obtained by comparing the computed authentication watermark A_w^* of the block with the two corresponding retrieved authentication watermarks $A^{'}_{w1}$and $A^{'}_{w2}$ from its mapping block:

$$d_1(i) = \begin{cases} 1 \; if \quad A^{'}_{w1} \neq A_w^* \quad and \quad A^{'}_{w2} \neq A_w^* \\ 0 \; otherwise \end{cases} \tag{13}$$

Then, a tamper detection mask, $T^1 = \{d_1(i), i = 1, 2, 3, \ldots, (4 * N)\}$can be created.

Step 4: Every 4 bits of T^1 represent a block B_i of size $32 * 32$ and in the same time each bit represents one sub-block B_s of size $16 * 16$. To validate the authenticity of B_i, we fix γ as the sum of non-zero bits of the four neighborhood sub-blocks B_s:

$$d_2(i) = \begin{cases} 1 \; if \quad d_1(i) == 1 \quad and \quad \gamma > \lambda_1 \\ 0 \; otherwise \end{cases} \tag{14}$$

where λ_1 is a predefined threshold. As a result, $T^2 = \{d_2(i), i = 1, 2, 3, ..., N\}$ is generated.

Step 5: To improve the robustness of our detection process, we optimize T^2 using the recovery watermark. Performing the equations (10), (11) and (12) in step2, the embedded index is extracted. Using the inverse-DRC, the recovery watermark LL_2^* is regenerated. All coefficients are mapped back to their original positions using the inverse permutation with the secret key K_3. On the other hand, the two-level wavelet transform is performed and the approximation sub-band LL_2 is extracted. Then, the difference δ between the coefficients of the received LL_2 and the extracted one is computed. The tamper detection mask T^2 is rescaled at the same size as LL_2 sub-band. The optimization equation is written as follows:

$$d_3(i) = \begin{cases} 1 \; if \quad d_2(i) == 1 \quad and \quad \delta > \lambda_2 \\ 0 \; otherwise \end{cases} \tag{15}$$

where $\lambda_2$is a predefined threshold. Then, $T^3 = \{d_3(i), i = 1, 2, 3, \ldots, N_1\}$ is generated. The coefficients marked as maliciously attacked must be dispersed throughout the sub-bands. The real tampered blocks should have a high density of marked coefficients. The other marked coefficients should be manipulated as noise and claimed as authentic by removed isolated '1' bits in T^3 through filtering.

3.3 Tamper recover

After tamper detection, a binary authentication matrix Z of the same size as LL_2 sub-bands $(M/4 \times M/4)$ is obtained by reshaping the vector T^3. Every block of size $8 * 8$ of matrix Z is classified as authentic or unauthentic. The information watermark is already extracted in step 5 (Section 3.2) from the watermarked image blocks. For each unauthentic blocks of Z, we compare the difference between the coefficient value of LL_2 with their extracted coefficients of LL_2^*. Only the coefficients with a difference more than the predefined threshold λ_2 are replaced by extracted coefficients from LL_2^* as we mentioned in (16), while the rest of the coefficients and the authentic blocks are keeping untouched.

$$LL_2(x, y) = \begin{cases} LL_2^*(x, y) & if \; Z(x, y) == 1 \; and \; \delta > \lambda_2 \\ LL_2(x, y) & otherwise \end{cases} \tag{16}$$

Where (x, y) refers to the coefficient position; Finally, the inverse wavelet transform is performed to map back to the spatial domain and gets the recovered image.

4 Results and discussions

Watermark embedding can be generally considered as a kind of structural noise injection which may result in a degradation of visual quality. The aim of this section is to evaluate the performance of our proposed watermarking algorithm. The quality assessment between the original image and the watermarked image can be evaluated using two different ways subjective or objective techniques. In the subjective method, image quality is judged by human beings themselves. Unfortunately, this method is thought to be impractical and expensive. Wherefore, we need to exploit an automated technique that would prefigure the perceived visual quality of human being as close as possible. For this purpose, objective methods are used. They are basically based on comparisons using numerical metrics. In this paper, we used the metrics often used, including the SSIM and the PSNR for gray-level (8 bits) images. These are usually used because they are simple to calculate, have clear physical meanings, and are mathematically convenient in the context of optimization. For a given reference image X and a test image Y, both of size $H \times L$, the PSNR between X and Y is defined by:

$$PSNR(X, Y) = 10 \log_{10} \left(255^2 / MSE(X, Y)\right) \tag{17}$$

Where, the mean squared error (MSE), computed by averaging the squared intensity differences of distorted and reference image pixels as follow:

$$MSE(X, Y) = 1/HL \sum_{i=1}^{H} \sum_{j=1}^{L} \left(X_{ij} - Y_{ij}\right)^2 \tag{18}$$

The higher PSNR value means a higher image quality. In fact, a small value of the PSNR provides high numerical dissimilarity between the two images. Unlike PSNR that is essentially based on pixel different measurement, the Structural SIMilarity Index (SSIM) is known as perceptual quality metric proposed to measure the structural similarity between two images [29]. It is inspected to be correlated with the quality perception of the human visual system (HVS). Basically, the SSIM quantifies quality degradation between a reference image and a processed version of the same image based on brightness, contrast and structural similarity. The SSIM is defined as:

$$SSIM(f, g) = b(f, g)c(f, g)s(f, g) \tag{19}$$

where

$$\begin{cases} b(f, g) = \frac{2\mu_f \mu_g + C_1}{\mu_f^2 + \mu_g^2 + C_1} \\ c(f, g) = \frac{2\sigma_f \sigma_g + C_2}{\sigma_f^2 + \sigma_g^2 + C_2} \\ s(f, g) = \frac{2\sigma_{fg} + C_3}{\sigma_f + \sigma_g + C_3} \end{cases} \tag{20}$$

where μ_f, σ_f and σ_{fg} are mean of f, variance of f and co-variance of f and g respectively. C_1, $C_2$and C_3 are small constants used to avoid a null denominator. A value of 0 means no correlation between images, and 1 means that $f = g$.

To study the performance of our proposed scheme, the following parameters are also computed:

1. False positive rate (FPR) is referring to the ratio of tampered pixels detected as distorted pixels.

$$FPR = \frac{number\ of\ authentic\ pixels\ detected\ as\ tampered}{number\ of\ pixels\ in\ tampered\ region} \times 100 \tag{21}$$

2. False negative rate (FNR) is referring to the ratio of distorted pixels falsely detected as authentic pixels.

$$FNR = \frac{number\ of\ undetected\ tampered\ pixels}{number\ of\ pixels\ in\ untampered\ region} \times 100 \tag{22}$$

3. Tamper detection rate (TDR) is referring to the ratio of tampered pixels detected which are actually tampered.

$$TDR = \frac{number\ of\ tampered\ pixels\ detected}{number\ of\ tampered\ pixels} \times 100 \tag{23}$$

4.1 Analysis of algorithm performance

We perform several experiments to verify the effectiveness of our proposed method in terms of the quality of the watermarked image, the robustness of the watermark, the tamper detection and the recovery of the tampered image. The quality of the final recuperated image considerably relies on the size of tampered areas. The texture of the image content and the precision of tamper localization affect also the quality of the recovered image. The PSNR and SSIM of the recovered image with respect to the original image are commonly used to measure the quality of the recovered image. In our experiments to demonstrate the efficiency of our proposed method, a set of grayscale images which includes the popular test images such as Lena, Boat, Barbara, Peppers, Baboon, Goldhill, F-16, Sailboat, Aerial and Couple of sizes $512 * 512$ are chosen (Fig. 5).

4.1.1 Quality of the watermarked image

Image alteration is caused principally in the embedding process by modifications of wavelet coefficients. The quality of the watermarked image is affected by both quantification step Δ and watermark payload ρ. By increasing the watermark payload the imperceptibility decreases. For this purpose, we used DRC theory to reduce the payload capacity and consequently increase the quality of the watermarked image. With several gray level images, the reduction of descriptors size (recovery watermark) may exceed 50% compared to uncompressed data payload. In fact, as previously mentioned, we used the second wavelet sub-band coefficients as recovery watermark. For an image of size $512 * 512$, the size of the selected sub-band is $128 * 128$ and only the 5 most significant bits of each coefficient are tacked in our experiments which means the size of uncompressed recovery data is about 81920 bits $(128 * 128 * 5)$. The Table 1 shows the experimental results obtained by the application of our DRC method on the recovery data. The reduction rate is computed using the following expression:

$$\frac{uncompressed\ data - compressed\ data}{uncompressed\ data} \times 100 \tag{24}$$

In fact, in previous works, the information watermark is directly embedded into the host image without being compressed. For these reasons the embedded data is high and can affect the quality of the watermarked image. One more advantage of using DRC is that even if some compressed embedded recovery watermark bits are lost,_we are still able to recover

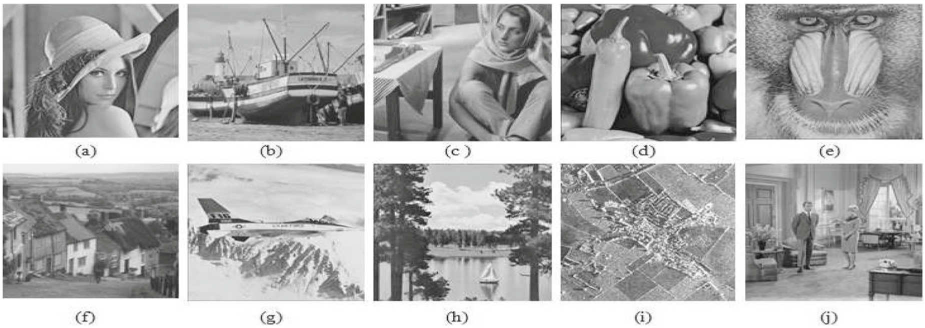


Fig. 5 **a** Lena, **b** Boat, **c** Barbara, **d** peppers, **e** Baboon, **f** Goldhill, **g** F-16, **h** Sailboat, **i** Aerial and **j** Couple

Table 1 Compression of the recovery watermark

Images	Lena	Boat	Barbara	Peppers	Baboon	Goldhill	F-16	Sailboat	Aerial	Couple
Recovery data	29084	34217	36675	34061	39955	37133	34744	37670	49888	34435
Reduction rate (%)	64	58	55	58	51	54	57	54	39	57

the image using the rest of recuperated DRC compressed embedded watermark bits. This advantage could not be realized with known loss-less compression schemes like Human or RLE [22, 23].

As the same, a higher quantification step causes more change to wavelet coefficients which leads to more degradation in the watermarked image thus the imperceptibility decreases and robustness increases. In realized experiments, we verify various scenarios in order to evaluate the performance of the proposed method. Three different quantification steps Δ_1, Δ_2 and Δ_3 (where $\triangle_1 < \triangle_2 < \triangle_3$) for the authentication watermark is executed in the embedding process while preserving the same quantification step for recovery watermark. The main goal of this process is to make the trade-off between the quality of the watermarked image and the robustness of watermark especially against non-malicious attacks JPEG compression as an example. As the watermarks are embedded in the appropriate sub-band wavelet coefficients (LL_1), the visual qualities of the watermarked images are relatively satisfying. Figure 6 shows the test images being watermarked, with $\triangle_1$, $\triangle_2$and $\triangle_3$ respectively.

Figure 7 shows the objective quality metric based on PSNR and SSIM, for different quantification steps while embedding the authentication watermark. As well, the watermark is embedded in high magnitude wavelet coefficients, which means that by increasing the quantification step; logically the PSNR and the SSIM decrease. The comparison is performed with several techniques proposed by Chunlei Li [10], Hongjie He [8], Xiaojun Qi [20], Preda [18], Phadikar [16], and Chamlawi [2] as showing in Table 2.

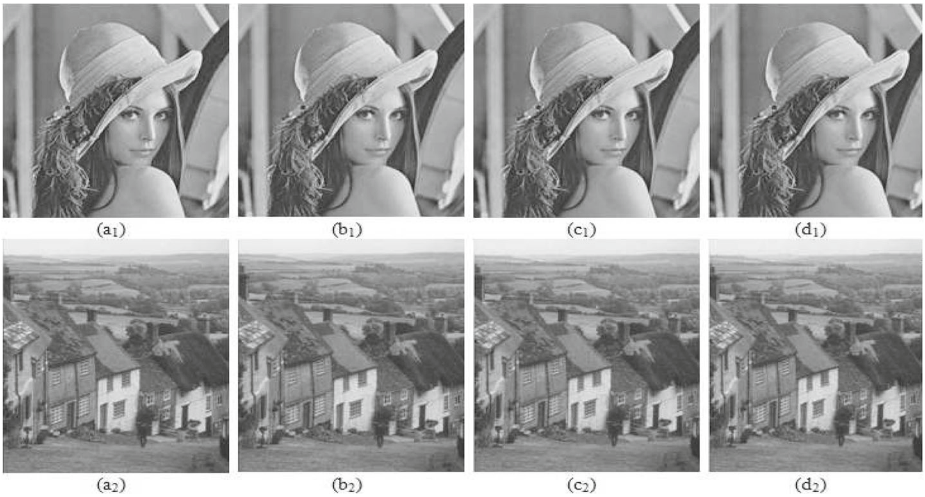


Fig. 6 (a_1) and (a_2) are the original images, (b_1) and (b_2) are the images watermarked using Δ_1, (c_1) and (c_2) are the images watermarked using Δ_2 and (d_1) and (d_2) are the images watermarked using Δ_3

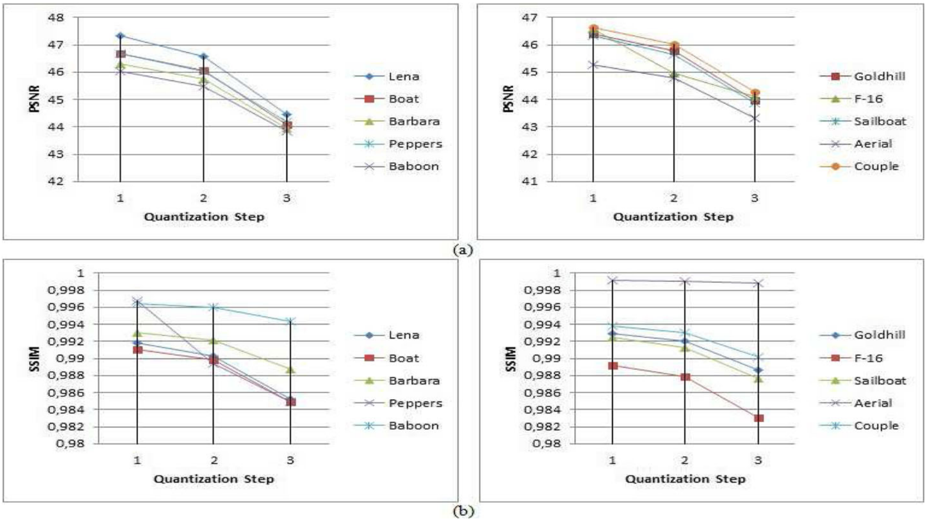


Fig. 7 PSNR and SSIM of several test images for different embedding Quantization steps (1, 2 and 3 refered to $\triangle_1$, $\triangle_2$ and $\triangle_3$ respectively)

4.1.2 Robustness of secure watermark

Since the protected image can usually undergo some image processing operations, we also test the robustness of the authentication watermarks under distortions caused by JPEG compression and ‘pepper and salt’ noise respectively. Practically, an image should be qualified as acceptably manipulated, even after applying a high compression quality factor. Figure 8 presents the recovery rate of authentication watermark under JPEG quantification factors ranging from 30 to 100 for all proposed quantification steps $\triangle_1$, $\triangle_2$ and $\triangle_3$. As it is clear from Fig. 8, the quantification step influences the robustness of the proposed technique against JPEG compression. When we raise the quantification step in embedding authentication watermarks process, the survival against JPEG compression positively increases. With the same idea, Table 3 illustrates for the two tested images Lena and Boat the PSNR and the SSIM for different quantification steps for survival level against JPEG compression. Even if the quality factor is 35, the PSNR and the SSIM are 34.93 dB and 0.9041 respectively for Lena image.

The comparison is carried out with that of Xiaojun Qi [20], Preda O [18], Phadikar [16] and Chamlawi [2] techniques which are more sensitive to JPEG compression comparing with our proposed method. For quantification factor less than 80, Phadikar [16] and Chamlawi [2] techniques considered the watermarked image as maliciously manipulated.

Furthermore, we evaluate the Bit Error Rate (BER) between the two extracted authentication watermarks and the original watermark as illustrated in Fig. 9. The robustness of the proposed scheme against ‘pepper and salt’ noise is performed and the scheme can survive with a variance up to 0.09 with PSNR equal to 15.87 dB while Phadikar method does not

Table 2 Comparison of the average PSNR of the proposed scheme with other schemes

	Proposed	Chunlei Li	Hongjie He	Xiaojun Qi	Preda O	Phadikar	Chamlawi
PSNR (dB)	45	36.5	44.5	41.39	40	35.27	40

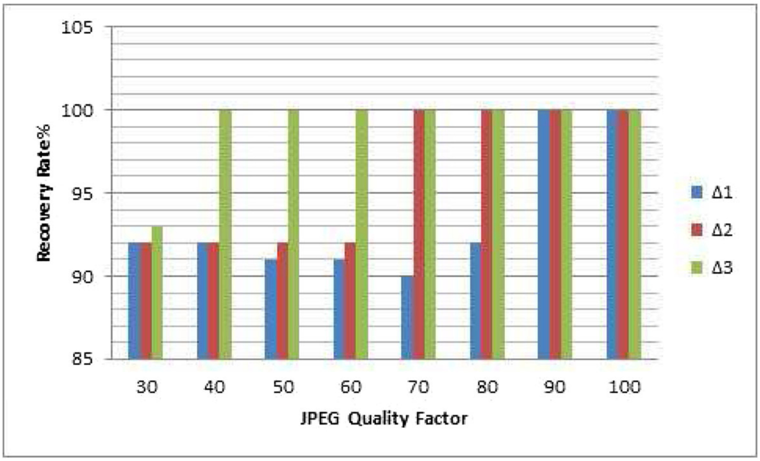


Fig. 8 Robustness of the authentication watermarks under JPEG compression

exceed 0.05. From the results already mentioned, we can assume that embedding the watermark in the approximation wavelet sub-band strengthens the change to be more robust to JPEG compression because this kind of sub-band is less modified by JPEG.

4.1.3 Tamper detection and recovery

In this section, we focus to detect and localize image tampered regions in order to demonstrate the tamper detection accuracy of the proposed technique and prove its effectiveness in localizing tampered areas. In the first experiment, we add a rectangular form of three gray-level intensities (i.e., black, gray, and white) to the watermarked image "Lena" and with different sizes. Intentionally, we choose to evaluate experiments without exposing the image to compression so that separate out its effect. Figure 10 shows tamper images followed by localization tampered regions for each one. The white regions present detected tampered regions. The non-tampered regions appear in black. Four detection levels are displayed. The fourth level shows the final result that used in the recovery step. Figure 10a, the size of the manipulated regions (white regions) 1, 2 and 3 are $(64 * 64)$, $(50 * 130)$ and $(64 * 64)$ pixels respectively. Figure 10a1, a2, a3 and a4 reveal the tampered regions from first level tampered detection to final result. The accuracy of tamper detection and localization is approximately 100%. By using the same gray-level intensities, a region of size $(130 * 115)$

Table 3 PSNR and SSIM of the Lena and Boat images under survival JPEG compression levels

Quant.step		PSNR	SSIM	Survival level against JPEG compression (%)
$\triangle_3$	Lena	34.56	0.9041	35
	Boat	33.73	0.9143	
$\triangle_2$	Lena	37.68	0.9393	70
	Boat	37.14	0.9506	
$\triangle_1$	Lena	40.68	0.9635	90
	Boat	40.84	0.9726	

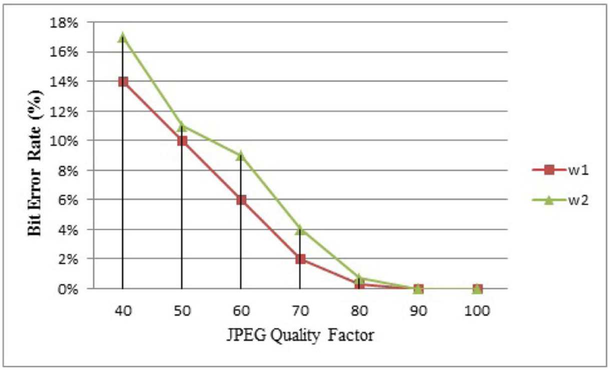


Fig. 9 Bit Error Rate evaluation of the two copies of the authentication watermark

in other location is showed in Fig. 10b. The detected results are displayed in Fig. 10b1, b2, b3 and b4. Figure 10b4, shows that the system correctly localize tampering regions with a precise final result. In the second round of experiment, we change the gray-level intensities of the attack from white to gray in the same location (Fig. 10c). The tampered region is not exactly detected. This result is due to the fact that the gray is similar to the background intensity and the detection system is treated as authentic to some degree. Black is used to evaluating the thirty round of experiments and the modified regions of size (170 ∗ 170) pixels that are accurately detected and localized as shown in the Fig. 10d4. Figure 10e each gray-level intensities (white, gray and black) is used to tampered an arbitrary region. The sizes of the modifications are (50 ∗ 130) pixels for the black, (150 ∗ 80) pixels for the white and (100 ∗ 130) pixels for the gray. Figure 10f and g present copy paste attack (from the

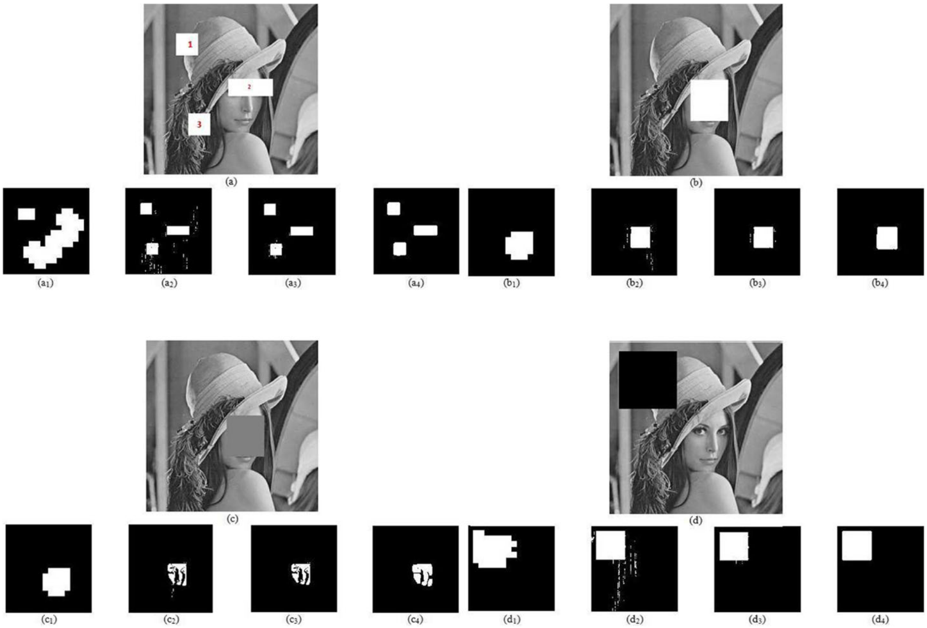


Fig. 10 Hierarchical tamper detection of the image Lena

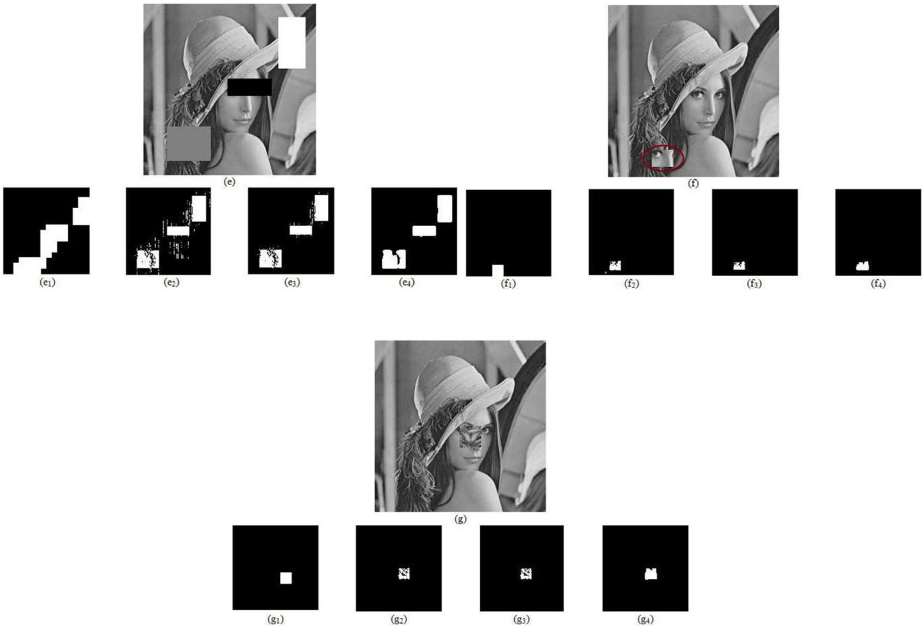


Fig. 10 (continued)

same image and from another image, respectively) with different hierarchical detection levels. From the detection and localizing results, some black spots within the tampered region are illustrated in the difference image. It can be explained by the fact that some manipulated blocks have the same intensities as the original block in the watermarked image.

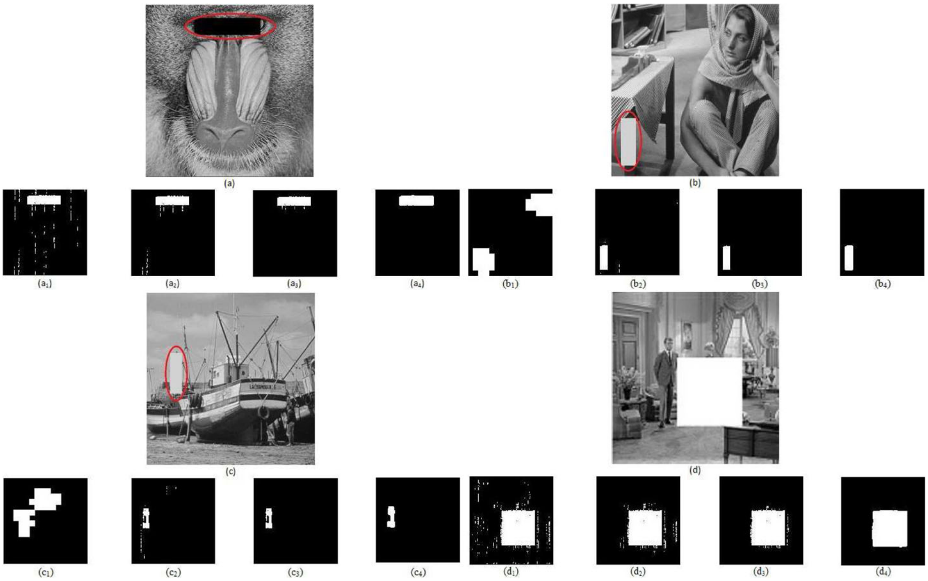
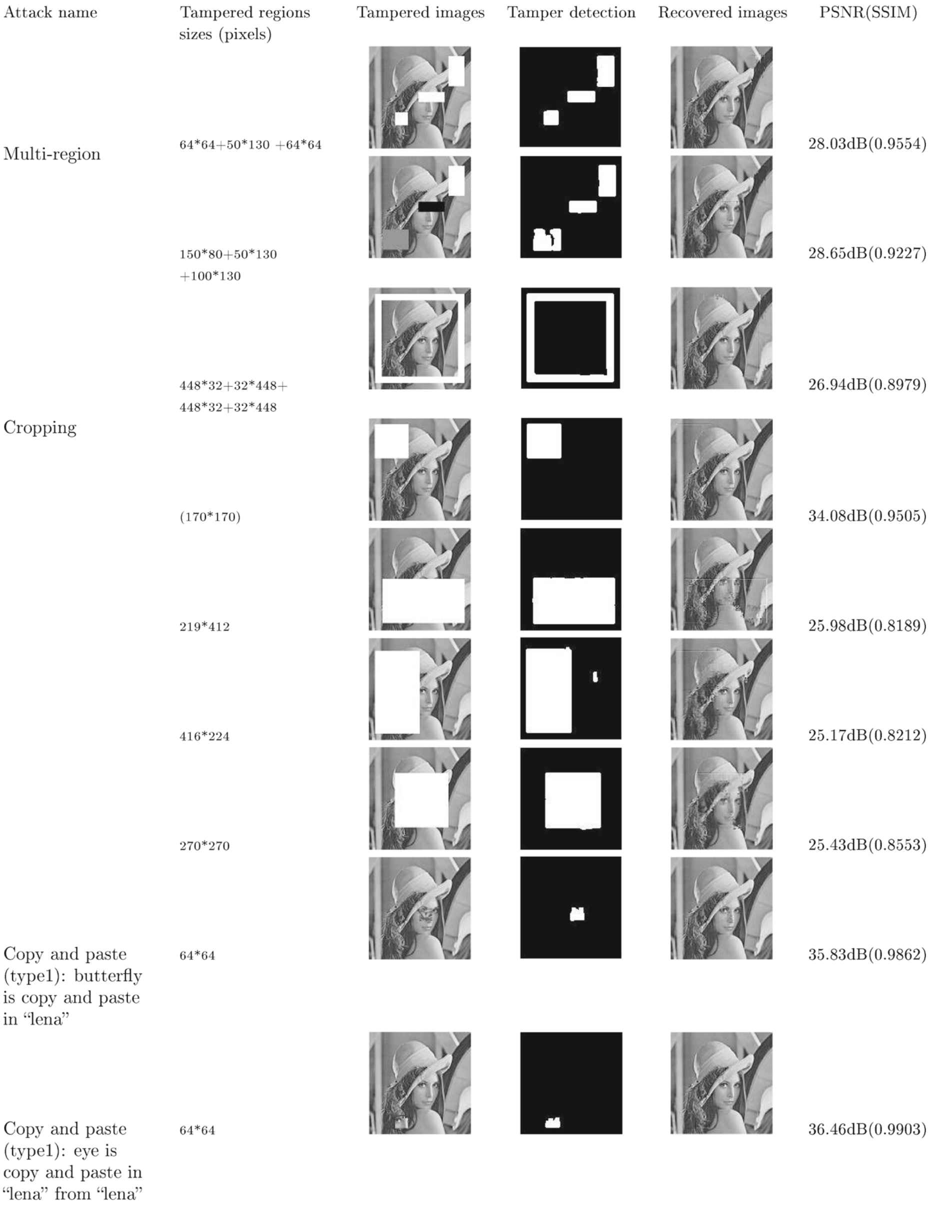


Fig. 11 Hierarchical tamper detection of Baboon, Barbara Boat and Couple

Similar to the above experiment, we tamper Baboon, Barbara Boat and Couple watermarked images in black or gray colors at different locations without applying any other attack such as compression. The tampered regions are indicated by red ellipse. It can be clearly noticed in Fig. 11 that the system is able to detect successfully most modifications and proves high accuracy localization regardless of the location of manipulations.

Figure 12 shows some examples of the tamper detection and tamper recovery of the proposed scheme. According to the results in Fig. 12, we can note that the proposed algorithm



Attack name	Tampered regions sizes (pixels)	Tampered images	Tamper detection	Recovered images	PSNR(SSIM)
Multi-region	64*64+50*130 +64*64				28.03dB(0.9554)
	150*80+50*130 +100*130				28.65dB(0.9227)
Cropping	448*32+32*448+ 448*32+32*448				26.94dB(0.8979)
	(170*170)				34.08dB(0.9505)
	219*412				25.98dB(0.8189)
	416*224				25.17dB(0.8212)
	270*270				25.43dB(0.8553)
Copy and paste (type1): butterfly is copy and paste in “lena”	64*64				35.83dB(0.9862)
Copy and paste (type1): eye is copy and paste in “lena” from “lena”	64*64				36.46dB(0.9903)

Fig. 12 Tampered images Lena and their corresponding tamper localization and self-recovery

Table 4 The PSNR and SSIM of the tampered image and the recovered image

Tampering rate (%)	Tampered image		Recovered image	
	PSNR (dB)	SSIM	PSNR (dB)	SSIM
5	17.98	0.9644	33.28	0.9678
10	14.72	0.9197	32.69	0.9470
15	12.78	0.8845	29.08	0.9275
20	12.98	0.8500	28.94	0.8979
25	11.37	0.8312	27.46	0.8857
30	10.58	0.7926	25.15	0.8389
35	9.27	0.7613	25.98	0.8346
40	8.67	0.6987	25.96	0.8153
average	10.92	0.7447	28.56	0.8893

is able to detect correctly_the tampered regions with different sizes and provide clearly a good quality of the recovered images. In fact, The PSNR and the SSIM mentioned in the same figure respect to their original versions are up to 25 dB and 0.8 respectively in the worst cases where the tampering is greater than or equal to 40%.

Table 4 shows the variation of PSNR and SSIM of various recovered images depending on the percentage of tampering of the watermarked images (Lena). The average is about 28.56 dB and 0.8893 for both the PSNR and SSIM respectively. Even with a high tampering, the scheme is still able to recover the tampering images with satisfactory qualities. The variations of FPR, FNR, and TDR are also computed for different tampering rate under cropping attacks as shown in Table 5. Concerning Table 5, it turned out that it is quite obvious that PNR of the proposed algorithm is zero where the TDR is 100% for different test images and for different tampering rate which confirms the performance of the algorithm to detect attacks. The FPR is less or equal to 10%.

4.1.4 Comparison with other approaches

We construe the performance of our proposed scheme by means of experimental results and compare with previous approaches. We summarize the comparative analysis of the proposed

Table 5 Variation of FPR, FNR, and TDR of the different tampered host with respect to tampering percentage

	FPR				FNR				TDR			
Tampering Rate(%)	10	20	30	40	10	20	30	40	10	20	30	40
Lena	8%	7%	8%	7%	0%	0%	0%	0%	100%	100%	100%	100%
Couple	10%	9%	8%	9%	0%	0%	0%	0%	100%	100%	100%	100%
Peppers	9%	8%	9%	8%	0%	0%	0%	0%	100%	100%	100%	100%
Goldhill	10%	8%	7%	8%	0%	0%	0%	0%	100%	100%	100%	100%
Saillboat	9%	10%	10%	10%	0%	0%	0%	0%	100%	100%	100%	100%
Barbara	10%	9%	7%	9%	0%	0%	0%	0%	100%	100%	100%	100%
Boat	9%	8%	10%	8%	0%	0%	0%	0%	100%	100%	100%	100%
Baboon	10%	9%	9%	9%	0%	0%	0%	0%	100%	100%	100%	100%
Airplane (F-16)	10%	8%	8%	7%	0%	0%	0%	0%	100%	100%	100%	100%

Table 6 Summary of the methods ensuring an authentication service

Features	Proposed	[2]	[16]	[18]	[20]	[8]	[10]	[30]
class	Semi-fragile	Semi-fragile	Semi-fragile	Semi-fragile	Semi-fragile	Fragile	Fragile	Fragile
localization	YES	YES	YES	NO	YES	YES	YES	YES
Quality of watermarked image	45	40	35	40	41	44	36	44
Survival against compression (JPEG QF)	40	80	70	adaptive	75	NO	NO	NO
recovery	YES	YES	YES	NO	YES	NO	YES	YES
cover	Wavelet	Wavelet	Wavelet	Wavelet	Wavelet	LSB	LSB	LSB

technique carried out with different reference methods presented in this article in Table 6 below. Fragile and semi-fragile indicate the class to which each method belongs as well as the perceptual quality of the watermarked image, the capability of the system to resist to compression attacks (JPEG) and if the scheme proposes an adequate localization and/or recovering of the areas tampered with. The comparison is performed according to two principal features: the quality of the watermarked image and the resistance of the watermark against non-malicious attacks such as JPEG compression. According to the above summary table, there is a deep dependency between the robustness of the watermarking scheme (especially JPEG compression) and the watermark cover (spatial domain: LSB or transform domain). In fact, all schemes are able to detect malicious attacks to some degree but the robustness against non-malicious attacks is not guaranteed by some categories since the watermark is hidden into the LSB bits. Our proposed method is characterized by high survival level against JPEG compression compared to other methods using the same transform domain. In fact, our method outperforms semi-fragile watermarking scheme such as Chamlawi et al. [2], Phadikar et al. [16], Qi et al. [20], Wang et al. [28], and Lin et al. [12] under JPEG compression with a quality factor 80, 70, 75, 65 and 50 respectively. Moreover, the algorithms performances are very similar but our proposed algorithm offers a high watermarked image quality compared to [2, 18, 20]. Besides, we may find some techniques offering high PSNR values, exceeding 45 dB. These techniques generally use the least significant bits (LSB) to embed the watermark. The alteration of the LSB is imperceptible by the human eye, therefore the PSNR is high. However, those technique lack robustness to special filtering operations, such a frequency based compression (JPEG,. . .).

5 Conclusion

In this work, we proposed a semi-fragile watermarking scheme based on Data Representation through Combination (DRC) for image tampering detection, localizing and recovery. Two watermarks are designed and hidden into blocks of size $16*16$ of DWT approximation sub-band on first level decomposition. In fact, Four bits from each block of size $32 * 32$ of the original gray-scale image represent the authentication watermark used for tamper detection and localization. The generated authentication watermark is duplicated and embedded in two different blocks to increase the security of watermark by means of two secret maps. While the recovery watermark, generated from the DWT approximation sub-band of the second level decomposition, is compressed using the DRC technique in order to reduce the payload which enhances further the perceptual quality of the watermarked image. The recovery watermark is embedded using the third map. Experimental results exhibit an ability to detect malicious attack with a high capability of localization. Besides, in the case of tampering, it produces a good estimation of the original content with an average of 28 dB of the recovered tampered image quality. The quality of the watermarked image is extremely high compared with other approaches in the literature ($> 45\ dB$). The embedded watermark is also robust to JPEG compression. The use of two copies of authentication watermark decreases the misclassification of the detection system which makes the method less sensitive to error pixels and introduces much less false alarms.

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

References

1. Boneh D, Shoup V (2015) A graduate course in applied cryptography, version 0.2
2. Chamlawi R, Khan A, Usman I (2010) Authentication and recovery of images using multiple watermarks. Comput Electr Eng 36(3):578–584
3. Cheddad A, Condell J, Curran K, Kevitt PM (2010) Digital image steganography: Survey and analysis of current methods. Signal Process 90(3):727–752
4. Cox IJIJ (2008) Digital watermarking and steganography. Morgan Kaufmann, San Mateo
5. Di Martino F, Sessa S (2012) Fragile watermarking tamper detection with images compressed by fuzzy transform. Inform Sci 195:62–90
6. Haouzia A, Noumeir R (2008) Methods for image authentication: a survey. Multimed Tools Appl 39(1):1–46
7. He HJ, Zhang JS, Tai HM (2009) Self-recovery fragile watermarking using block-neighborhood tampering characterization. Lecture notes in computer science (including subseries lecture notes in artificial intelligence and lecture notes in bioinformatics) 5806 LNCS:132-145
8. He H, Chen F, Tai H, Member S, Kalker T, Zhang J (2012) Performance analysis of a block-neighborhood- based self-recovery fragile watermarking scheme. IEEE Trans Inf Forensics Secur 7(1):185–196
9. Li C, Wang Y, Ma B, Zhang Z (2011) A novel self-recovery fragile watermarking scheme based on dual-redundant-ring structure q. Comput Electr Eng 37:927–940. [Online]. Available: http://or.nsfc.gov.cn/bitstream/00001903-5/88341/1/1000002175455.pdf
10. Li C, Wang Y, Ma B, Zhang Z (2012) Tamper detection and self-recovery of biometric images using salient region-based authentication watermarking scheme. Computer Standards and Interfaces 34(4):367–379
11. Li C, Zhang A, Liu Z, Liao L, Huang D (2015) Semi-fragile self-recoverable watermarking algorithm based on wavelet group quantization and double authentication. Multimed Tools Appl 74(23):10581–10604
12. Lin C-Y, Chang S-F (2000) Semi-fragile watermarking for authenticating JPEG visual content. In: Proceedings of the SPIE security and watermarking of multimedia contents II, San Jose, pp 140–151
13. Ling C, Ur-rehman O (2015) Robust image authentication in the presence of noise. Springer, Cham, pp 43–53
14. Liu C-L (2010) A tutorial of the wavelet transform Chapter 1 Overview 1.1 Introduction
15. Ouled Zaid A, Makhloufi A, Bouallegue A, Olivier C (2009) Improved QIM-based watermarking integrated to JPEG2000 coding scheme. SIViP 3(3):197–207
16. Phadikar A, Maity SP, Mandal M (2012) Novel wavelet-based QIM data hiding technique for tamper detection and correction of digital images. J Vis Commun Image Represent 23(3):454–466
17. Poornima R, Iswarya R (2013) And overview of digital image steganography. International Journal of Computer Science & Engineering Survey 4(1):23–31
18. Preda RO (2013) Semi-fragile watermarking for image authentication with sensitive tamper localization in the wavelet domain. Measurement 46(1):367–373

19. Qi X, Xin X (2011) A quantization-based semi-fragile watermarking scheme for image content authentication. J Vis Commun Image Represent 22:187–200
20. Qi X, Xin X (2015) A singular-value-based semi-fragile watermarking scheme for image content authentication with tamper localization. J Vis Commun Image Represent 30:312–327
21. Said J, Souissi R, Hamam H (2013) A new representation of image through numbering pixel combinations. Journal of Information Security Research 4:1
22. Salomon D (2007) Data compression: the complete reference. Springer, Berlin
23. Salomon D (2008) A concise introduction to data compression, ser. Undergraduate topics in computer science. Springer, London
24. Sayood K (2006) Introduction to data compression, Third edition (Morgan Kaufmann Series in multimedia information and systems)
25. Tong X, Liu Y, Zhang M, Chen Y (2013) A novel chaos-based fragile watermarking for image tampering detection and self-recovery. Signal Process Image Commun 28(3):301–308
26. Tsai T, Wu C, Fang C (2014) Design and Implementation of a joint data compression and digital watermarking system in an MPEG-2 video encoder. J Sign Process Syst 74:203
27. Ullah R, Khan A, Malik AS (2013) Dual-purpose semi-fragile watermark: Authentication and recovery of digital images. Comput Electr Eng 39(7):2019–2030. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0045790613001213
28. Wang H, Ho AT, Zhao X (2012) A novel fast self-restoration semi-fragile watermarking algorithm for image content authentication resistant to JPEG compression. Lecture notes in computer science (including subseries lecture notes in artificial intelligence and lecture notes in bioinformatics) 7128 LNCS:72–85
29. Wang Z, Bovik AC, Sheikh HR, Member S, Simoncelli EP, Member S (2004) Image quality assessment : from error visibility to structural similarity. IEEE Trans Image Process 13(4):1–14
30. Wu C-M, Shih Y-S (2013) A simple image tamper detection and recovery based on fragile watermark with one parity section and two restoration sections. Optics and Photonics Journal 03(02):103–107
31. Xiao D, Shih FY (2012) An improved hierarchical fragile watermarking scheme using chaotic sequence sorting and subblock post-processing. Opt Commun 285(10–11):2596–2606. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S0030401812001368

Hanen Rhayma received the license degree in computer science and multimedia in 2009 from the Higher Institute of Computer Science and Multimedia of Gabs (I.S.M.G) University of Gabs and the master degree in 2011. She is now a PhD student at National School of Engineers of Gabs (E.N.I.G) and member of Advanced Technologies for Medicine and Signals (A.T.M.S). Her current interests are in the areas of image watermarking.