Multimedia Tools and Applications (2023) 82:42739–42761
https://doi.org/10.1007/s11042-023-14974-1

A secure DWT-based dual watermarking scheme for image authentication and copyright protection

A. Hernández-Joaquín[1] · G. Melendez-Melendez[1] · R. Cumplido[1]

Received: 20 January 2022 / Revised: 28 June 2022 / Accepted: 22 February 2023 /
Published online: 21 April 2023

Abstract

Digital watermarking mechanisms have become an essential tool for guaranteeing copyright protection and content authentication. However, most state-of-the-art works focus on providing only one of these services. In this paper, a dual watermarking scheme for image authentication and copyright protection is introduced. The proposed scheme simultaneously embeds two watermarks in the host image by exploiting the discrete wavelet transform (DWT). A fragile watermark and a robust watermark are embedded into frequency domain by modifying DWT coefficients of high-frequency sub-bands. To improve the scheme security, host image undergoes a chaotic transformation while robust watermark is obtained by using a particular visual cryptography technique. The proposed scheme provides satisfactory watermark imperceptibility levels, achieving PSNR values above 49dB when a small watermark is used and above 40dB when a larger watermark is embedded. Several image processing attacks are applied to evaluate the watermark robustness, obtaining normal correlation coefficient values near to 1 against most attacks. Finally, an authentication accuracy near to 1 is achieved when marked images undergo tampering attacks. The obtained results show that proposed scheme achieves competitive results in terms of imperceptibility and outperforms similar state-of-the-art dual watermarking methods in terms of watermark robustness and authentication accuracy.

Keywords Dual watermarking · Image authentication · Copyright protection · Visual cryptography · Discrete wavelet transform

✉ R. Cumplido
rcumplido@inaoep.mx

A. Hernández-Joaquín
ahernandezj@inaoep.mx

G. Melendez-Melendez
melendez@inaoep.mx

[1] National Institute of Astrophysics, Optics and Electronics,
Luis Enrique Erro 1, Santa Maria Tonantzintla, 72840, Puebla, Mexico

1 Introduction

As a result of technological development and the Internet, it is a fact that the digital media industry has been going through a prosperous up-growth in recent decades. Originators rights and publishers reputation are troubled due to various infringement practices; particularly, media manipulations have occurred. Accordingly, verifying the authenticity of digital media has become a significant challenge. Digital watermarking is a technology that can be used to provide security in a wide variety of scenarios where digital content protection is required. Digital watermarking has been used in content authentication, owner identification, transaction tracking, copy control, among other applications [10]. Therefore, researchers focus on developing digital watermarking systems as a complement to cryptography [9] for the protection of digital content including images, audio, video, etc [24].

Image watermarking is a suitable alternative for copyright protection and authentication of images in famous communication environments such as the Internet, which is sensitive to illicit practices. Image watermarking is the process of imperceptibly embedding a piece of digital information known as watermark into a host image, also known as cover image. A watermark is a binary code that contains useful information about the image in which it is being embedded. After the embedding process, a watermarked image is produced, which can be stored or transmitted. Then, when it is required, the watermark is extracted and used in the specific application.

There are three essential features to be considered when new watermarking schemes are designed: imperceptibility, embedding capacity, and robustness.

- **Imperceptibility** refers to the invisibility of a watermark. As the host image is modified to embed a watermark, the produced watermarked image will contain distortion. Therefore, host and watermarked images must be very similar in such a way that human eyes can perceive no visible changes. In other words, the watermarked image should not attract the attention of malicious people.
- **Embedding capacity** is the maximum amount of information bits that can be embedded into the host image.
- **Robustness** is the resistance level to attacks, i.e., the capacity of the method to extract the embedded watermark even if watermarked image went through attacks.

The primary constraint involved in digital watermarking is maintaining a trade-off among watermark robustness and embedding capacity while keeping the visual perception of the original image intact. However, watermarking scheme quality largely depends upon the choice of the watermark structure and insertion strategy.

Digital watermarking is usually classified according to robustness feature as fragile, semi-fragile, and robust [42]. In fragile schemes, watermarks are designed to be distorted even if watermarked image undergoes a minimum modification, i.e., fragile watermarks are vulnerable to any kind of manipulation. Therefore, fragile watermarks are primarily used to verify the integrity or authenticity of images. Semi-fragile watermarks tolerate a certain set of manipulations and are distorted with non-allowable attacks. Semi-fragile watermarks can be detected in scenarios where content preserving operations or incidental attacks occur; meanwhile, they are distorted with malicious attacks. Finally, robust watermarks are very difficult to remove from their corresponding watermarked images. Therefore, they are designed to survive against aggressive intentional attacks, making them suitable for copyright protection.

Watermarks can be embedded into the host image using two well-defined domains: spatial domain and frequency domain [37]. In spatial domain methods, watermarks are embedded by directly altering the pixel values of the host image, typically with least significant bit (LSB) replacements. This is much simple, straightforward, and less complex; however, it is not robust against attacks. In order to provide robustness, frequency domain watermarking techniques are used. In frequency domain methods, a transformed image is obtained by using Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), Integer Wavelet Transform (IWT), Singular Value Decomposition (SVD), etc. Therefore, watermarks are embedded by modulating the coefficients of the corresponding transform. As a result, the watermarks are irregularly distributed over the whole image; therefore, it is difficult for the attackers to read or decode them.

Multiple watermarking methods, in which more than one watermark is embedded into the host image, arose to improve the performance of traditional watermarking methods. The improvement is obtained because watermarks can be designed to face different security problems simultaneously. In this paper, a dual watermarking scheme for multipurpose applications is introduced. The proposed scheme can provide image authentication and copyright protection at the same time. A robust watermark is embedded into the highest frequency subband of second-level DWT transform to provide copyright protection. Additionally, a fragile watermark is embedded into the high-frequency sub-bands to provide image authentication. Visual cryptography is applied over a secret image to generate a share, which is encoded as a robust watermark. The scheme security is improved by performing a host image mapping using a chaotic transformation. The proposed scheme effectively inserts information and takes advantage of frequency domain characteristics to obtain optimal performance. Experimental results show that the proposed dual watermarking scheme provides a watermark robustness and authentication accuracy improvement compared to other relevant schemes while obtaining competitive results regarding watermark imperceptibility.

The rest of this paper is organized as follows. Section 2 presents a review of relevant state-of-the-art watermarking methods. Section 3 provides a brief explanation of two techniques which are used in the proposed scheme: visual cryptography and Arnold transformation. Section 4 details the proposed scheme, including embedding and extraction processes. Obtained results and a comparison with relevant watermarking schemes are reported and discussed in Section 5. Finally, conclusions are drawn in Section 6.

2 Related work

Several image watermarking methods have been proposed in the literature, including robust and fragile approaches [1, 51].

Fragile image watermarking is an optimal solution to deal with image authentication as well as tampering localization issues. In fragile watermarking approaches, watermarks must be sensitive to any modification; then, watermarks are designed to be distorted when watermarked images undergo even slight modifications. Fragile watermarking schemes often embed authentication codes into the spatial domain [28, 45] or the high-frequency coefficients of some transformation [43, 44].

Conversely, robust watermarking schemes are typically employed to provide copyright protection since embedded watermarks are able to survive even if watermarked images undergo aggressive malicious attacks. Usually, robust watermarks are created using an

image, logo, or copyright information related to the host image owner. The extracted watermark information can be employed in case of a dispute.

Some robust schemes incorporate the watermarks into the spatial domain [5, 40, 53, 59]; however, a limitation of watermarking methods based on spatial domain is that these methods do not provide enough robustness since watermarks are commonly embedded by directly altering the least significant bits of image pixels. Then, most robust watermarking methods operate in the frequency domain, where watermarks are embedded by manipulating coefficients obtained with some transformation such as DCT [12, 21, 22], DWT [29, 47, 60], etc. Another schemes modify some singular values provided by the SVD transformation [8, 52]. Recently, geometrically invariant methods have been proposed using Legendre-Fourier moments [17, 19, 20] to provide robustness against geometric attacks such as rotation, scaling and translation, offering superior performance when compared with previous methods. Frequency domain is preferred to provide robustness because watermarks are irregularly spread over the whole image when the corresponding inverse transformation is applied, making them difficult to remove. In order to improve watermark imperceptibility while maintaining robustness, some hybrid domain watermarking methods were proposed [3, 7, 14, 23, 25, 32, 34, 36, 46, 49]. Hybrid methods arose as an extension of frequency domain methods, then, two or more transformations are used. Commonly, a wavelet transform is first applied to the host image, then a frequency sub-band is selected and transformed using DCT. Finally, SVD transformation is applied to the DCT coefficients and some singular values are modified to embed the watermark bits [14, 49].

Recent state-of-the-art works [2, 11, 15, 16, 18, 27, 30, 31, 33, 38, 50, 56] indicate that watermarking methods' performance can be improved by embedding multiple watermarks. As each embedded watermark may be designed to address a different problem, these schemes are called dual, multiple or multipurpose watermarking schemes. The first multipurpose watermarking scheme was introduced in [31]. The authors proposed a dual watermarking scheme in which robust and fragile watermarks are simultaneously embedded by quantizing some DWT coefficients. The scheme can perform copyright protection and basic image authentication at the same time. In [27], authors introduced a hybrid dual watermarking scheme that operates in the spatial and DCT domains. This scheme incorporates a visible watermark into the spatial domain and an invisible watermark into the frequency domain for copyright protection. A multiple robust watermarking method for color images is proposed in [33]. The authors embed robust watermarks by exploiting RGB and YCbCr color spaces, which improve robustness in the spatial domain. In [18] a multiple zero-watermarking method for color medical images is proposed. Gegenbauer moments of fractional orders are used to extract geometrically invariant features of medical images, enhancing watermark robustness against standard and geometric attacks. A zero-watermarking based method for copyright protection of color images is proposed in [56]. Three watermarks are created by an accurate selection of coefficients of decimal-order polar harmonic transforms, improving watermark robustness. The scheme security is enhanced by scrambling the watermarks using a chaotic system. In order to improve imperceptibility, a hybrid scheme based on DWT-DCT-SVD transformations was proposed in [50]. This scheme embeds two robust watermarks created with an image and textual information to provide copyright protection. In [11], two robust watermarks are embedded into the hybrid domain DWT-SVD. A genetic algorithm is used to select embedding locations, which benefits the scheme security for copyright protection. The schemes proposed in [16, 38] provide image authentication with tampering localization as well as reconstruction of tampered regions by incorporating authentication codes and recovery information as watermarks.

In [15], two fragile watermarks, i.e., diffusion watermark and authentication watermark, are employed to provide high sensitivity against tampering manipulations and enhance the scheme security. Recently, a blind dual watermarking scheme for color image authentication and copyright protection was proposed in [30]. Two color spaces are employed to embed the watermarks. A robust watermark is embedded into the DWT transformation of YCbCr color space and a fragile watermark is embedded by replacing the LSBs of RGB color space.

Frequency domain offers versatility to incorporate whatever the type of watermark is. In this paper, the DWT frequency domain is exploited to achieve two applications: authentication (to detect and localize tampering on watermarked images) and copyright protection (to determine image owner). The proposed scheme merges and takes advantage of two state-of-the-art methods. A robust watermark is embedded into the quantized low-frequency coefficients and replaced into the highest sub-band of the DWT transform at the second resolution level, as it is exposed in [30]. Simultaneously, a fragile watermark is embedded into high-frequency DWT coefficients at the second resolution level using the strategy proposed in [43]. The security of the proposed scheme is enhanced by pre-processing the watermark and the host image, as explained in next section.

3 Preliminaries

The security of the proposed scheme relies on the use of secret keys and two techniques, i.e., visual cryptography and Arnold's cat map transformation. Visual cryptography is used to obtain a share, which is embedded as a robust watermark; meanwhile, Arnold's cat map is applied to the cover image to improve the security of the watermark embedding phase. These techniques are briefly explained next.

3.1 Visual cryptography

Visual cryptography theory was first introduced in [39]. The authors proposed a visual version of secret sharing in which an image is broken into n structured images known as shares. The obtained shares do not show any visual information about the input image. The image content can only be revealed by stacking k or more than k shares, where $(k \leq n)$. Any $k-1$ shares combination will not provide information about the target image. The (k, n) visual secret sharing (VSS) scheme can be adapted and implemented to be used in a wide variety of application domains where security is required [57].

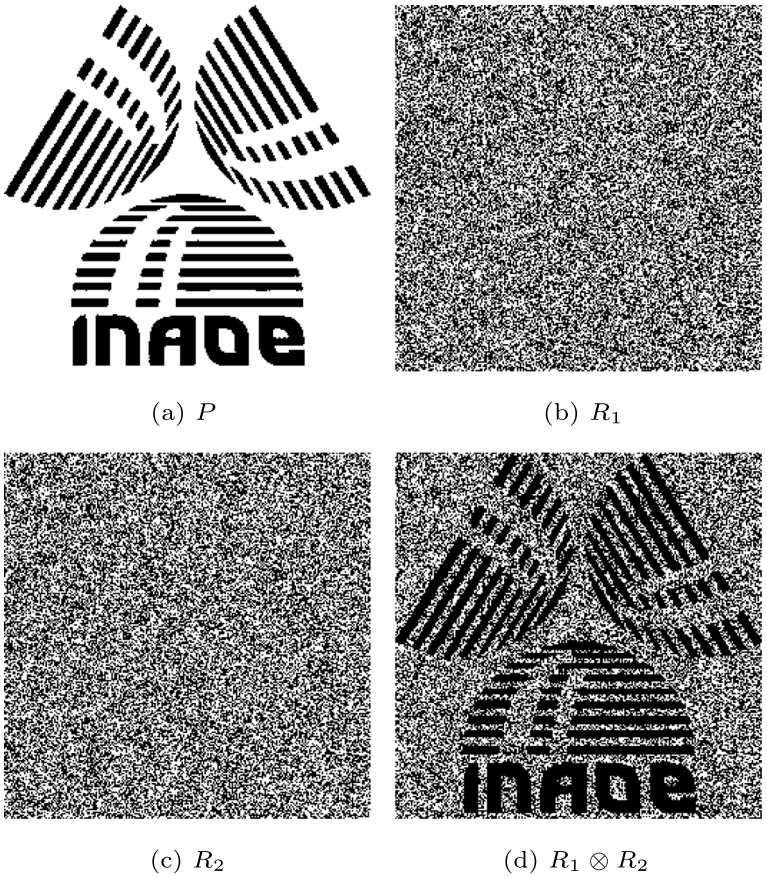
Some digital right management issues can be addressed by combining digital watermarking with visual cryptography techniques since a secret image can be used to get two shares using VSS. One of the obtained shares can be embedded as a watermark in the host image. Finally, when required, the share can be extracted and used to recover the secret image.

In this work, a $(k = 2, n = 2)$ VSS scheme is used to generate two shares. Traditional (2,2) VSS scheme takes a binary image of size $M \times N$ and splits it into two shares, each one of size $(2M \times 2N)$. To perform this, image pixels are transformed into (2×2) sized blocks, i.e., each block contains four binary values. Thus, every pixel in the original image is encoded to produce two blocks. After all image pixels are encoded, the first set of blocks is used to create one share, and the remaining blocks are used to create an additional share. Original secret pixels can be recovered by overlapping the two corresponding blocks. If the compared blocks are similar, the decoded secret pixel is white; if the blocks are complementary, the decoded secret pixel is black.

Table 1 Encoding / decoding operations of (2, 2)-VCRG scheme

p	Probability	r_1	r_2	$r = r_1 \otimes r_2$
1	0.5	1	1	1
	0.5	0	0	0
0	0.5	1	0	0
	0.5	0	1	0

To maintain a balance among watermarking properties, a special (2,2) VSS is used. The (2,2)-VCRG (visual cryptograms of random grids) proposed in [48] is employed to generate two shares. This technique is used because the obtained shares are of the same size as the input image, in contrast with traditional VSS, where the shares duplicate the input image size. The encoding process is performed with the help of Table 1. Every input pixel p is randomly encoded into two pixels r_1 and r_2. First, a binary value for r_1 is randomly obtained. The probability of $r_1 = 0$ is $\frac{1}{2}$. Next, a binary value is set to r_2 according to the input pixel p. If p is a white pixel (1), then $r_2 = r_1$. Nevertheless, if p is a black pixel (0), then



(a) P (b) R_1

(c) R_2 (d) $R_1 \otimes R_2$

Fig. 1 Visual cryptography example using (2,2)-VCRG scheme

$r_2 = \tilde{r}_1$, where $\tilde{r}_1$ is the complement of r_1. After all image pixels are encoded, two shares are obtained. The image content can be revealed by applying the decoding operation $r_1 \otimes r_2$ from Table 1. An example of (2,2)-VCRG scheme is shown in Fig. 1, where Fig. 1a shows the input secret image, Fig. 1b and 1c are the obtained shares and Fig. 1d shows the decoded image, which reveals secret image content.

3.2 Arnold's cat map

To enhance the scheme security, the host image pixels are scramble using a chaotic transformation. Chaos theory was first introduced to the watermarking field in [54]. The authors proposed a watermarking scheme in which a chaotic system *Toral Automorphis* is used.

Arnold's cat map theory is a practical image transformation technique that reorders image pixels based on a chaotic system. It was introduced in [4]. Arnold's cat map theory shows that image pixels can be apparently randomly organized, and after a number of enough iterations original image is returned, see Fig. 2.

The chaotic function is iteratively applied over the input image to relocate its pixels. Let T be the period of the function, where T depends on the image size [26]. When the chaotic function is applied to the image by T iterations, the original image is obtained, i.e., pixels recover their original positions.

From the above, if an image pixel has initial coordinates (x, y) into an image of size $M \times M$ [6], the next coordinates (x', y') are computed by the chaotic function using (1).

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \cdot \begin{bmatrix} x \\ y \end{bmatrix} \bmod M \tag{1}$$

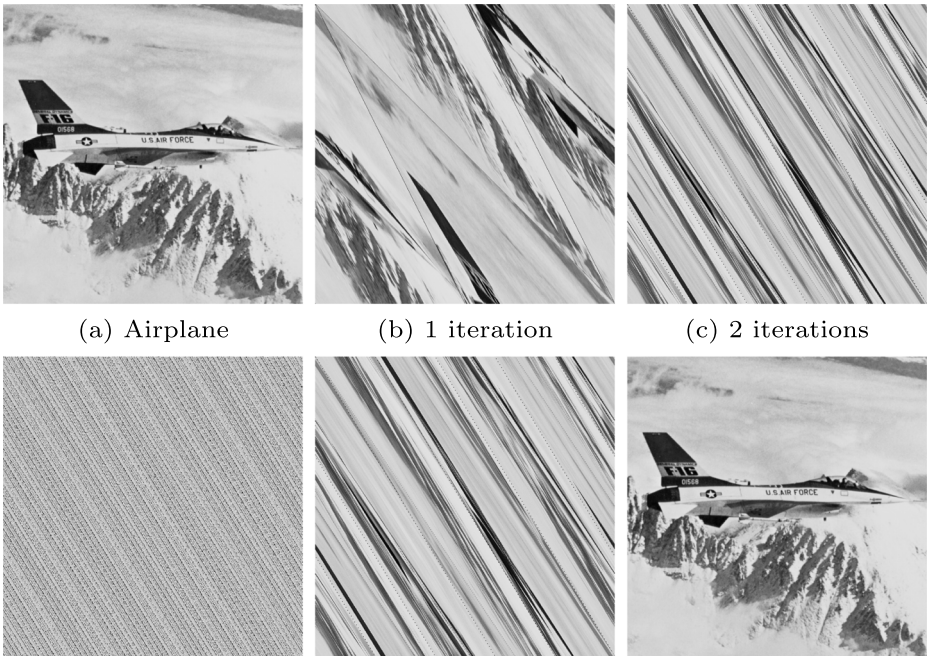


Fig. 2 Arnold transformation example over the *Airplane* image

Chaotic transformations can be used to break local spatial similarity of images and obtain a larger number of significant coefficients when moving to the frequency domain (e.g., DCT, DWT coefficients), in contrast with those obtained when original images are transformed.

4 Proposed scheme

This section explains the proposed watermarking scheme in detail. The steps for dual watermark embedding, extraction and authentication phases are explained in Sections 4.1, 4.2 and 4.3, respectively.

4.1 Embedding process

Figure 3 summarizes the principal stages of our watermark embedding process, where two main phases are well identified. On the one hand, robust watermark embedding uses the low-frequency DWT sub-band as a reference to embed the watermark into the highest frequency sub-band. On the other hand, a fragile watermark is incorporated into high-frequency DWT sub-bands. Watermarks are embedded based on two state-of-the-art works [30, 43] to take advantage of the frequency domain. A detailed explanation of this process is presented next.

1. Initially, the original host RGB image is used. Then, the blue component is selected to perform Arnold transformation several times. The blue component is used because modifications on this component are difficult to perceive by human eyes.
2. The secret image is processed using (2,2)-VCRG technique to generate two shares. Share 1 is selected to be embedded into the host image as a robust watermark.
3. DWT transform is applied at the 2nd resolution level over the obtained chaotic image channel to get LL_2, LH_2, HL_2 and HH_2 sub-bands [13, 35]. LL_2 sub-band is used as reference to embed robust watermark into HH_2 sub-band while LH_2, HL_2 and HH_2^w sub-bands are used to embed fragile watermark.

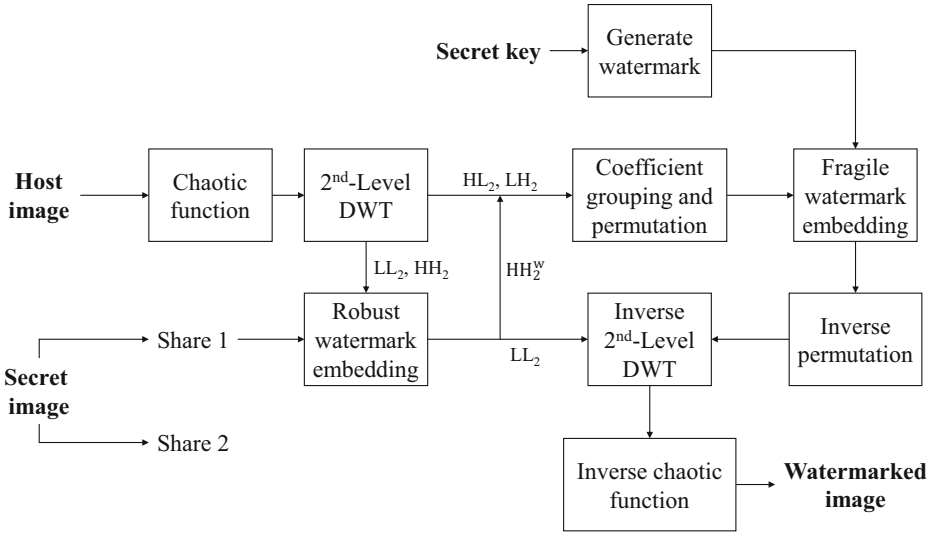


Fig. 3 Proposed dual watermark embedding process

Table 2 Luminance quantization table

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

4. LL_2 sub-band is divided into several non-overlapping blocks of size 8×8. Then, every block value is quantized with the help of the luminance quantization table commonly used in JPEG compression [55], which is shown in Table 2. Here each coefficient is divided by its corresponding value in the table.
5. Robust watermark is embedded into quantized QLL_2 sub-band as next:

$$QLL_{2_i}^{w} = QLL_{2_i} + \alpha I_{w_i} \tag{2}$$

where:

I_{w_i} is the i-th robust watermark bit.
α is a constant watermark scale factor. A high value improves watermark robustness, however, imperceptibility is decreased.
$QLL_{2_i}^{w}$ is the i-th watermarked coefficient corresponding to QLL_{2_i}.

6. Finally, HH_2 sub-band is replaced with the resultant QLL_2^w to obtain the watermarked sub-band HH_2^w.

4.1.1 Fragile watermark embedding

1. Wavelet coefficients corresponding to sub-bands HL_2, LH_2, HH_2^w are concatenated into a one-dimensional vector C. Next, C is randomly permuted using a secret key to obtain vector C'. Previous permutations guarantee that coefficients corresponding to the same spatial location will be separated in C'.
2. C' is split into sets of size d. Fragile watermark w is created by generating a random binary sequence with a secret key K_w. The created watermark is used as an authentication code and has the same dimension as the number of coefficients sets d.
3. Weighted mean m_i corresponding to the ith coefficients set c_i is computed using (3).

$$m_i = \sum_{j=1}^{d} (-1)^j |c_i(j)| \tag{3}$$

where:

$c_i(j)$ is the jth coefficient into set i.
$(-1)^j$ is an operation used to improve scheme robustness against frequent image processing operations.

4. Next, weighted mean m_i is modified to embed a watermark bit using (4). Here m_i value is quantized to the immediate odd or even value according to the corresponding watermark bit w_i.

$$m_i^w = \begin{cases} \lfloor m_i/Q \rfloor \cdot Q & \text{if } mod2(\lfloor m_i/Q \rfloor) = w_i \\ \lfloor m_i/Q \rfloor \cdot Q + Q & \text{if } mod2(\lfloor m_i/Q \rfloor) \neq w_i \end{cases} \tag{4}$$

where:

Q represents sensitivity of the tampering detection for different group sizes. It can be adapted, a higher value increases the sensitivity but decreases quality of watermarked image.

5. Weighted mean m_i of the ith coefficients set c_i is replaced with the corresponding watermarked mean m_i^w by altering the wavelet coefficient with the maximum absolute value: $c_{i,\max}(j)$. As random permutation was previously applied, every set of coefficients should have at least one coefficient with highest absolute value. Then, $c_{i,\max}(j)$ is updated using (5).

$$c'_{i,\max}(j) = c_{i,\max}(j) + (-1)^j \cdot sign(c_{i,\max}(j)) \cdot (m_i^w - m_i) \tag{5}$$

where:

$c'_{i,\max}(j)$ is the watermarked coefficient and

$$sign(\mathrm{c}) = \begin{cases} -1 & \text{if c} \leq 0 \\ 1 & \text{if c} > 0 \end{cases} \tag{6}$$

6. After all coefficients with the highest absolute values in each set are updated, coefficients are reordered to their original positions by performing the inverse permutation using the same secret key.
7. Finally, the watermarked image channel is obtained by applying the inverse 2D-DWT transform over modified coefficients and performing the chaotic transformation to reallocate image pixels to their original positions.

4.2 Extraction process

The corresponding watermark extraction process is shown in Fig. 4. Two principal phases can be identified, i.e., the fragile watermark is extracted from high-frequency sub-bands of the second resolution level DWT transform to perform image authentication; meanwhile, low-frequency sub-band is used as a reference to extract the robust watermark from the highest frequency sub-band for copyright protection. A step-by-step detail of this process is presented next.

1. Initially, a watermarked (possibly manipulated) image is received. Then, the blue component is selected to perform Arnold transformation the same number of times as in the embedding process. Finally, the chaotic image channel is transformed into the frequency domain by applying DWT transform on two resolution levels.
2. LL_2 sub-band is used as reference to extract robust watermark from HH_2 sub-band and LH_2, HL_2 and HH_2 sub-bands are used to extract fragile watermark.
3. LL_2 sub-band is divided into 8×8 sized blocks for robust watermark extraction. Then, every block is quantized by dividing each coefficient by its corresponding value in the luminance quantization table, see Table 2.

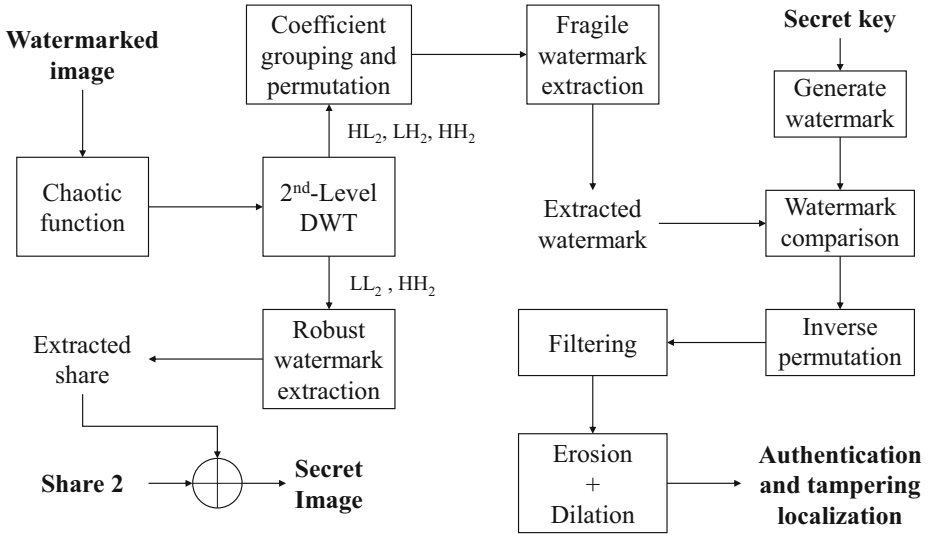


Fig. 4 Proposed dual watermark extraction process

4. Once all blocks are quantized, a quantized QLL_2 sub-band is generated.
5. Robust watermark bits are extracted from HH_2 sub-band using (7).

$$RW_i = (HH_{2_i} - QLL_{2_i})/\alpha \tag{7}$$

Where:

QLL_{2_i} is the ith coefficient in QLL_2 sub-band.
HH_{2_i} is the ith coefficient value in HH_2 sub-band.
α is the same constant used in the watermark embedding process.
RW_i is the ith extracted robust watermark bit.

6. After all robust watermark bits are extracted, Share 1 should be obtained. Then, the extracted share is used with the additional share to reveal the secret image, which can be identified by the host image owner.
7. Fragile watermark is extracted from the coefficients of high-frequency sub-bands. Then, the selected coefficients are concatenated, and a random permutation is performed using the same key as in the embedding process.
8. The sequence of permuted coefficients is divided into sets of d coefficients.
9. The weighted mean m_i' of every coefficient set is computed.
10. A watermark bit w_i' is extracted from the weighted mean of every set using (8).

$$w_i' = mod2(\lfloor m_i'/Q \rfloor) \tag{8}$$

4.3 Authentication process

Image is authenticated as in [43] by following the next steps.

1. Original watermark sequence w is first generated using the same secret key as in the embedding process. Now, w and w' are compared. If w' matches with w, the image is considered authentic. Otherwise, tampering detection is performed with the next steps.

2. All extracted watermark bits in w' that do not match their original ones w are identified. If the extracted watermark bit w'_i, corresponding to the ith set of coefficients, mismatches the original watermark bit w_i, all coefficients of the corresponding ith set are labeled as tampered.
3. Permuted coefficients are relocated to their original positions by applying the corresponding inverse permutation. Now coefficients labeled as tampered are spread over the three high-frequency sub-bands. Then, tampered regions should have a high density of coefficients labeled as tampered. The remaining coefficients labeled as tampered should be distributed like random noise. However, some false positives can occur, and these coefficients can be stated as authentic.
4. Next, a binary authentication matrix M_a with the same dimensions as the sub-bands is created. Every coefficient in the position (i, j) of the three sub-bands LH_2, HL_2 and HH_2 is scanned. If there is at least one coefficient labeled as tampered in any sub-band, then $M_a(i, j) = 1$.
5. The isolated bits 1 are removed from M_a with filtering. Then, to further eliminate incorrectly labeled coefficients from M_a, successive erosion and dilation are applied with a radius of R pixels and a square of size $S \times S$. Now the tampered locations should be correctly identified.
6. Finally, matrix M_a is mapped to the spatial domain to highlight the tampered areas.

Parameter Q is the quantization step size and can be adapted for the sensitivity of the tampering detection; it defines the size of the structural elements used for erosion and dilation in step 5. A larger Q value must be used to increase the sensitivity, and it will also decrease the probability of false alarms. A solution must be found for specific applications.

5 Experimental results

This section presents several experiments that show the effectiveness of the proposed scheme. According to the used techniques, it is expected that results on the images will be highly effective against attacks such as compression, noise, filtering, as well as detection and location of tampered image regions.

Imperceptibility, fragile watermark, and robust watermark results of the proposed scheme are presented in Sections 5.1, 5.3, and 5.2, respectively. Finally, Section 5.4 presents a comparison with relevant related works to show the advantages of the proposed scheme over similar schemes in terms of imperceptibility, watermark robustness and authentication accuracy.

Experiments were carried out using benchmark color images, most of which were taken from the USC-SIPI dataset [41]. Figure 5 shows test images. All images are of size 512×512. Although all images were tested in all experiments, this section presents most results using the well-known *Lena* image to have a concise presentation. A binary image logo of different sizes, i.e., 32×32, 64×64 and 128×128 is used in robust watermark embedding experiments. On the other hand, fragile watermarks are created by generating a pseudo-random binary sequence with a predefined secret key.

5.1 Imperceptibility results

Imperceptibility performance of the proposed dual watermarking scheme was evaluated using two well-known metrics: Peak Signal-to-Noise Ratio (PSNR) and Structural

Fig. 5 Test images

Similarity Index (SSIM). These metrics were selected since they are two common image quality assessment (IQA) metrics, which measure image similarity by directly comparing image pixels and image statistics [58].

Parameter α plays an important role in the proposed dual watermarking scheme. Watermark robustness is improved as parameter α increases; however, watermark imperceptibility is affected. For this reason, imperceptibility evaluation was performed by setting different α values, i.e., the watermarks were embedded by setting α from 1 to 1/16. Figures 6 and 7 show the imperceptibility results in terms of PSNR and SSIM metrics over different α values, respectively. It can be observed that as α value decreases, watermark imperceptibility is improved, obtaining PSNR values over 30dB. Best imperceptibility results are obtained when α value is set to 1/16, where the proposed scheme achieves more than 45dB over the six watermarked images. However, PSNR values decrease when α value is set to 1, obtaining $\sim$ 30dB in average. For this reason, to maintain a trade-off between watermark imperceptibility and robustness, α value was established to 1/8, obtaining a PSNR average of $\sim$ 45dB. Finally, it can be observed that results on the six images experience a small shift. Image characteristics are different, e.g., Lena image results are better than those obtained in Baboon image in terms of PSNR. This is because the Baboon image is considered a more complex image as it has high-contrast and textured regions compared with the Lena image.

5.2 Robust watermark results

Watermark robustness is essential to provide copyright protection in watermarking schemes. This section presents the experiments and obtained results related to robust watermarks.

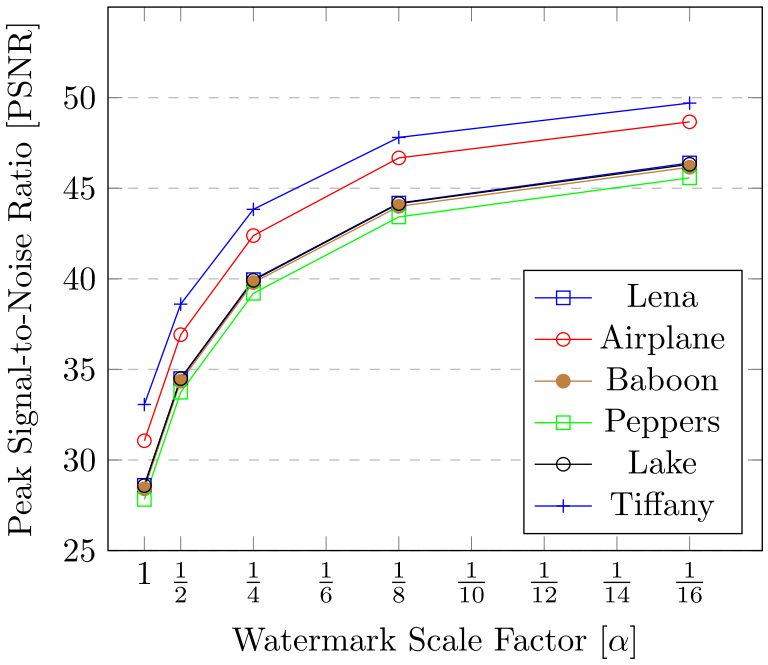


Fig. 6 Results of dual watermarked images in terms of PSNR using different α values

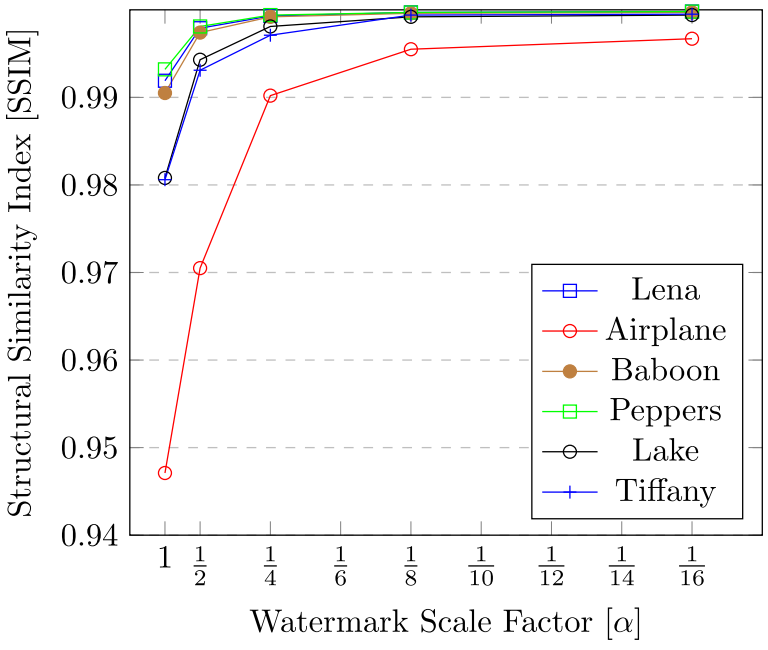


Fig. 7 Results of dual watermarked images in terms of SSIM using different α values

Several image processing attacks such as salt and pepper noise, JPEG compression, blurring, Gaussian noise, brighten, darken, torsion, scaling, collage and tone mapping attacks were applied into all watermarked images using different robust watermark sizes, i.e., 32×32, 64×64 and 128×128. After attacks took place, the robust watermark is extracted from the attacked image. Extracted watermark is used to reveal secret image using visual cryptography and compared with the corresponding embedded image using normalized correlation coefficient (NCC). It is expected that after attacks, extracted watermarks are visually perceptible, i.e., recovered watermarks must be very similar to original ones.

Some attacked images, as well as corresponding visual inspection of extracted watermarks after applying (2,2)-VCRG, are shown in Fig. 8. It can be observed that extracted watermarks are visually perceptible in most attacked images. The proposed robust watermark embedding is highly associated to the DWT HH sub-band at the second resolution level; thus, an extreme distortion on this sub-band will cause a watermark robustness loss. Despite different attacks were applied, most extracted watermarks were successfully extracted, i.e., the scheme provides enough watermark robustness since recovered watermarks can be recognizable by the human eye. This experimental assessment proves that the proposed watermarking scheme can be used to protect digital images strongly against most common image processing attacks, which is favorable to maintaining susceptible images' value.

An objective comparison of robust watermarking results is provided in Table 3. PSNR and NCC metrics are used to evaluate watermarks imperceptibility and extracted watermarks similarity with original watermarks. Several attacks were applied over all marked images using different robust watermarks sizes. It can be observed from Table 3 that as watermark size is increased, marked images quality decreases. It comes about because more information is embedded into the host image, however a larger watermark provides better robustness compared with a smaller watermark. It can also be observed that in most attacks a NCC value near to 1 is achieved, suggesting a strong relationship between embedded and extracted watermarks. However, a decreased performance is noted for torsion, scaling and tone mapping attacks. When images were attacked with geometric transformations such as torsion and scaling, the obtained watermarks achieved NCC values near to 0.8. This is because DWT is not geometrically invariant and although watermarks are still recognizable, better results can be obtained with geometrically invariant methods [17, 20]. On the other hand, when images were attacked with tone mapping attack, NCC values near to 0.3 were obtained. This is because the tone mapping attack maps one set of colors to another

Fig. 8 Robust watermark results. Each column of the figure lists an attacked image and the obtained secret image using the extracted robust watermark (share) after different attacks were applied, i.e, JPEG compression 50% (a), blurring (b), Gaussian noise (c), salt & pepper noise (d), brighten (e), visible watermark adding (f) and tone mapping (g)

Table 3 Imperceptibility and robust watermark results in terms of PSNR and NCC for different robust watermark sizes

		Lena			Airplane			Babbon			Peppers			Lake			Tiffany		
	Watermark size	32x32	64x64	128x128	32x32	64x64	128x128	32x32	64x64	128x128	32x32	64x64	128x128	32x32	64x64	128x128	32x32	64x64	128x128
	PSNR (dB)	49.08	44.21	40.21	51.56	42.23	39.23	48.65	44.15	42.15	49.41	45.26	40.26	50.12	43.15	38.15	48.12	43.12	39.12
Attack	Parameter																		
Salt & pepper	0.01	1	1	0.9999	1	1	0.9999	1	1	0.9999	1	1	0.9999	1	1	0.9999	1	1	0.9999
	0.02	1	1	0.9999	1	1	0.9999	1	1	0.9999	1	1	0.9999	1	1	0.9999	1	1	0.9999
	0.04	0.9999	0.9999	0.9999	0.9999	0.9999	0.9999	1	1	0.9999	1	1	0.9999	1	1	0.9999	0.9999	0.9999	0.9999
	0.08	0.9998	0.9998	0.9998	0.9998	0.9998	0.9998	0.9999	0.9999	0.9998	0.9999	0.9999	0.9998	0.9999	0.9999	0.9998	0.9998	0.9998	0.9998
JPEG	90	1	0.9999	0.9999	0.9999	0.9999	0.9998	0.9999	0.9998	0.9999	1	0.9998	0.9990	1	0.9999	0.9999	1	0.9999	0.9999
	80	0.9988	0.9988	0.9988	0.9990	0.9993	0.9963	0.9933	0.9672	0.9843	1	0.9925	0.9987	0.9976	0.9869	0.9956	0.9999	0.9934	0.9979
	70	0.9921	0.9891	0.9891	0.9906	0.9958	0.9946	0.9841	0.9521	0.9838	0.9847	0.9871	0.9821	0.9817	0.9675	0.9803	0.9705	0.9729	0.9964
	60	0.9784	0.9565	0.9565	0.9560	0.9343	0.9432	0.9745	0.9546	0.9607	0.9819	0.9663	0.9227	0.9803	0.9787	0.9494	0.9697	0.9558	0.9823
Blurring	0.1	0.9987	0.9980	0.9980	0.9771	0.9903	0.9986	0.9889	0.9857	0.9890	0.9810	0.9918	0.9887	0.9834	0.9717	0.9811	0.9903	0.9927	0.9797
	0.2	0.9832	0.9832	0.9832	0.9657	0.9844	0.9920	0.9889	0.9787	0.9654	0.9722	0.9893	0.9745	0.9824	0.9576	0.9734	0.9795	0.9800	0.9479
	0.3	0.9767	0.9775	0.9567	0.9802	0.9515	0.9832	0.9696	0.9604	0.9300	0.9889	0.9845	0.9791	0.9727	0.9603	0.9469	0.9653	0.9590	0.9369
Gaussian noise	0.1	0.9965	0.9981	0.9823	0.9947	0.9998	0.9928	0.9801	0.9803	0.9616	0.9835	0.9876	0.9897	0.9926	0.9962	0.9809	0.9855	0.9863	0.9975
	0.3	0.9774	0.9864	0.9612	0.9589	0.9930	0.9510	0.9769	0.9761	0.9429	0.9795	0.9783	0.9779	0.9760	0.9803	0.9361	0.9728	0.9734	0.9451
	0.5	0.9448	0.9261	0.9148	0.9498	0.9414	0.9300	0.9529	0.9425	0.9314	0.9554	0.9212	0.8763	0.9486	0.9122	0.9129	0.9544	0.9407	0.8955
Brighten	50	0.9721	0.9721	0.9474	0.9681	0.9786	0.9433	0.9700	0.9650	0.9432	0.9814	0.9775	0.9420	0.9535	0.9764	0.9526	0.9621	0.9697	0.9816
	80	0.9512	0.9233	0.9233	0.9338	0.9094	0.9326	0.9652	0.9384	0.9138	0.9463	0.9252	0.9168	0.9323	0.9317	0.9328	0.9392	0.9002	0.8999

Table 3 (continued)

	Watermark size PSNR (dB)	Lena			Airplane			Babbon			Peppers			Lake			Tiffany		
		32x32	64x64	128x128	32x32	64x64	128x128	32x32	64x64	128x128	32x32	64x64	128x128	32x32	64x64	128x128	32x32	64x64	128x128
		49.08	44.21	40.21	51.56	42.23	39.23	48.65	44.15	42.15	49.41	45.26	40.26	50.12	43.15	38.15	48.12	43.12	39.12
Darken	50	0.9713	0.9589	0.9589	0.9614	0.9661	0.9547	0.9765	0.9943	0.9177	0.9766	0.9435	0.9566	0.9424	0.9540	0.9428	0.9684	0.9691	0.9557
	80	0.8967	0.8659	0.8659	0.8983	0.8797	0.8515	0.9268	0.8881	0.8780	0.8893	0.8704	0.8474	0.8772	0.8508	0.8312	0.8731	0.8445	0.8530
Torsion	50	0.7991	0.7799	0.7799	0.7924	0.7491	0.7545	0.7701	0.7701	0.7889	0.8076	0.7814	0.7714	0.8016	0.7722	0.7623	0.7934	0.7544	0.7840
	− 50	0.7929	0.7729	0.7729	0.8159	0.7593	0.7730	0.7853	0.7562	0.7801	0.7714	0.7574	0.7352	0.8123	0.7988	0.7701	0.7883	0.7367	0.7345
Scaling	200%	0.7804	0.6869	0.6869	0.7837	0.6971	0.6746	0.7754	0.6685	0.6677	0.7725	0.6869	0.6548	0.7595	0.7126	0.7046	0.7806	0.6925	0.7001
	50%	0.6034	0.5009	0.5009	0.5994	0.4749	0.4977	0.6143	0.5386	0.5274	0.6301	0.4991	0.4681	0.5961	0.4696	0.5069	0.5908	0.4944	0.5234
Contrast	50	0.9234	0.8721	0.8721	0.9270	0.8855	0.8888	0.9307	0.8768	0.8510	0.9329	0.8744	0.8784	0.9492	0.8688	0.8246	0.9246	0.8521	0.8511
	− 50	0.8737	0.8281	0.8281	0.8825	0.8173	0.8259	0.8840	0.8060	0.8377	0.8669	0.8185	0.8260	0.8754	0.8016	0.8534	0.8831	0.8330	0.8385
Collage	10%	0.9512	0.9213	0.9213	0.9371	0.8918	0.9145	0.9578	0.9241	0.9283	0.9644	0.9353	0.9284	0.9619	0.9485	0.9335	0.9490	0.8897	0.9382
	30%	0.9353	0.9145	0.9145	0.9385	0.8934	0.9239	0.9427	0.9203	0.9435	0.9512	0.9345	0.9178	0.9489	0.9318	0.9084	0.9427	0.923	0.925
Cropping	10%	0.9791	0.9508	0.9508	0.9819	0.9548	0.9259	0.9763	0.9752	0.9440	0.9931	0.9730	0.9917	0.9764	0.9677	0.9593	0.9895	0.9298	0.9429
	30%	0.9694	0.9213	0.9213	0.9660	0.9094	0.8998	0.9549	0.9590	0.9074	0.9812	0.9300	0.9252	0.9475	0.9407	0.8915	0.9493	0.9180	0.8997
Tone mapping	Auto	0.3559	0.3287	0.3039	0.3591	0.3324	0.3175	0.3459	0.3431	0.3178	0.3693	0.3148	0.2812	0.3680	0.3197	0.3102	0.3527	0.3285	0.3085

in order to approximate a high dynamic range (HDR) image, altering not only RGB color representation, but also high frequency detail, in which our watermarks are embedded.

5.3 Fragile watermark results

Authentication codes that were embedded as fragile watermarks are extracted from the high-frequency DWT coefficients. As a result, DWT provides high tampering detection rates while maintaining optimal images quality using smaller watermarks.

Authentication results are shown in Fig. 9. Figure 9(a), shows tampered images when applying three different malicious attacks, i.e., copy-move, blurring and visible watermark adding attacks. Authenticated images are shown in Fig. 9(b), where tampered regions are localized. Finally, authenticated images obtained after filtering are shown in Fig. 9(c). Authenticated images undergo a filtering stage as well as morphological operations to

Fig. 9 Fragile watermark results. Attacked images with copy-move, blurring and collage attacks are shown in column (a) respectively. Authenticated images before filtering are listed in column (b). After filtering, authenticated images of column (c) are obtained

highlight tampered areas. Parameters used in filtering stage are the same used in [43], $n = 2, d = 8$ and $Q = 8$. From the above, a detection resolution of $2n \times 2n = 4 \times 4$ pixels is achieved. This configuration allows the proposed scheme to detect tampered regions with an accuracy of ~ 0.99.

It can be seen that regardless of the applied attack, the scheme can detect and localize tampered regions in watermarked images accurately (nearly 100%). Experiments suggest that the proposed scheme provides enough watermark fragility, which is crucial to detect and localize tampered regions on watermarked images.

5.4 Dual watermarking schemes comparison

In order to show the advantages of the proposed scheme, this subsection presents a comparison among different dual watermarking methods previously proposed in the literature, including [2, 27, 30, 31, 33]. Table 4 shows a functionalities comparison among the six dual watermarking methods.

Principal differences among the six schemes are detailed next. Initially, the proposed scheme, together with [2, 30, 31] provide image authentication and copyright protection, in contrast with [27, 33], where schemes are focused on watermark robustness for copyright protection, and authentication is not favored. This fact provides an advantage of the proposed scheme and [2, 30, 31] because if a watermarked image is tampered, schemes in [27, 33] will not be able to detect manipulations neither localize them. The six watermarking schemes provide copyright protection, however, [31, 33] require information about the host image to extract watermarks, then schemes are not blind. Another variation is that the proposed scheme, together with [2, 30, 31, 33], work with color images, then schemes can be used in a wide variety of scenarios. It can be observed that when a larger watermark is embedded, the proposed scheme achieves an optimal PSNR value of $\sim$40dB in average, which is similar to [30]. However, when a smaller watermark is embedded the proposed scheme provides a PSNR average value of $\sim$49dB, indicating that the proposed scheme is competitive with the state-of-the-art works. Finally, the proposed scheme together with [30] outperforms [2] in terms of authentication accuracy obtaining an accuracy value of 0.99, indicating that tampering image regions are well localized. Therefore, the proposed scheme can be used to effectively protect color images by incorporating fragile and robust watermarks without attracting the attention of malicious people.

6 Conclusions

In this paper, we presented a secure dual watermarking scheme for color images, providing image authentication and copyright protection. Two watermarks are embedded into the frequency domain using the DWT transform at the second resolution level of the blue component in RGB color space. A fragile watermark is embedded in high-frequency sub-bands, whereas a robust watermark is incorporated using the quantized low-frequency sub-band to replace the highest sub-band. The scheme's robustness is tested by performing several image processing attacks such as salt & pepper noise, JPEG compression, blurring, Gaussian noise, tone mapping, etc. The recovered watermarks are visually recognizable after all attacks took place in most experiments. PSNR and NCC results proved the robustness of the scheme. On the other hand, authentication results show that image manipulations can be localized accurately.

Table 4 Functionalities comparison among relevant dual watermarking schemes

Functionality	[31]	[27]	[33]	[30]	[2]	Proposed Scheme
Dual watermarks	Fragile + Robust	Robust + Robust	Robust + Robust	Fragile + Robust	Fragile + Robust	Fragile + Robust
Embedding domain	DWT + DWT	Spatial + DCT	Spatial + Spatial	Spatial + DWT	Spatial + DWT & SVD	DWT + DWT
Visibility	Invisible + Invisible	Visible + Invisible	Invisible + Invisible	Invisible + Invisible	Invisible + Invisible	Invisible + Invisible
Blind extraction	Yes + No	Yes + Yes	Yes + No	Yes + Yes	Yes + Yes	Yes + Yes
Target image	Color	Gray–scale	Color	Color	Color	Color
Maximum watermark size	16 × 16	64 × 64	50 × 50	64 × 64	32 × 32	128 × 128
Marked image PSNR	∼40 dB	∼30 dB	∼39 dB	∼ 40 dB	∼52 dB	32 × 32: ∼49 dB 64 × 64: ∼44 dB 128 × 128: ∼40 dB
Copyright protection	Yes	Yes	Yes	Yes	Yes	Yes
Image authentication	Yes	No	No	Yes	Yes	Yes
Authentication accuracy	–	NA	NA	∼ 0.99	∼ 0.94	∼ 0.99

The principal contribution of this research is that the proposed scheme allows the detection and localization of tampered regions when an image is manipulated while copyright protection is allowed. The scheme achieves competitive performance against relevant state-of-the-art works since results are competitive in terms of imperceptibility, watermark robustness and authentication accuracy. Furthermore, the scheme security is enhanced by using visual cryptography and chaotic transformation. Finally, host image information is not required to extract the embedded watermarks as it occurs in other schemes, so blind watermark extraction is also included.

Acknowledgements This work was supported by the National Council of Science and Technology of Mexico - CONACyT [grant numbers 702608 and 731618].

Data Availability All data generated or analyzed during this study are included in this published article (and its supplementary information files).

Declarations

Conflict of Interests The authors declare that they have no conflict of interest.

References

1. Agarwal N, Singh AK, Singh PK (2019) Survey of robust and imperceptible watermarking. Multimed Tools Appl 78(7):8603–8633. https://doi.org/10.1007/s11042-018-7128-5
2. Ahmadi SBB, Zhang G, Rabbani M et al (2021) An intelligent and blind dual color image watermarking for authentication and copyright protection. Appl Intell 51(3):1701–1732. https://doi.org/10.1007/s10489-020-01903-0
3. Ali M, Ahn CW, Pant M (2014) A robust image watermarking technique using svd and differential evolution in dct domain. Optik 125(1):428–434. https://doi.org/10.1016/j.ijleo.2013.06.082
4. Arnold VI, Avez A (1968) Ergodic problems of classical mechanics, vol 9. Benjamin
5. Behnia S, Ahadpour S, Ayubi P (2014) Design and implementation of coupled chaotic maps in watermarking. Appl Soft Comput 21:481–490. https://doi.org/10.1016/j.asoc.2014.03.022
6. Chen W, Quan C, Tay C (2009) Optical color image encryption based on arnold transform and interference method. Opt Commun 282(18):3680–3685. https://doi.org/10.1016/j.optcom.2009.06.014
7. Chrysochos E, Fotopoulos V, Xenos M et al (2014) Hybrid watermarking based on chaos and histogram modification. Signal Image Video Process 8(5):843–857. https://doi.org/10.1007/s11760-012-0307-3
8. Chung KL, Yang WN, Huang YH et al (2007) On svd-based watermarking algorithm. Appl Math Comput 188(1):54–57. https://doi.org/10.1016/j.amc.2006.09.117
9. Cox IJ, Doërr G, Furon T (2006) Watermarking is not cryptography. In: Digital watermarking. Springer, Berlin, pp 1–15. https://doi.org/10.1007/11922841_1
10. Cox I, Miller M, Bloom J et al (2008) Digital Watermarking and Steganography, 2nd edn. The Morgan Kaufmann Series in Multimedia Information and Systems, Morgan Kaufmann Publishers Inc., San Francisco. https://doi.org/10.1016/B978-012372585-1.50005-X
11. Darwish SM, Al-Khafaji LDS (2020) Dual watermarking for color images: a new image copyright protection model based on the fusion of successive and segmented watermarking. Multimed Tools Appl 79(9):6503–6530. https://doi.org/10.1007/s11042-019-08290-w
12. Das C, Panigrahi S, Sharma VK et al (2014) A novel blind robust image watermarking in dct domain using inter-block coefficient correlation. AEU - Int J Electron Commun 68(3):244–253. https://doi.org/10.1016/j.aeue.2013.08.018
13. Daubechies I (1992) Ten lectures on wavelets. SIAM
14. Fazli S, Moeini M (2016) A robust image watermarking method based on dwt, dct, and svd using a new technique for correction of main geometric attacks. Optik 127(2):964–972. https://doi.org/10.1016/j.ijleo.2015.09.205
15. Gong X, Chen L, Yu F et al (2020) A secure image authentication scheme based on dual fragile watermark. Multimed Tools Appl 79(25):18,071–18,088. https://doi.org/10.1007/s11042-019-08594-x

16. Haghighi BB, Taherinia AH, Harati A (2018) Trlh: fragile and blind dual watermarking for image tamper detection and self-recovery based on lifting wavelet transform and halftoning technique. J Vis Commun Image Represent 50:49–64. https://doi.org/10.1016/j.jvcir.2017.09.017
17. Hosny KM, Darwish MM (2018) Robust color image watermarking using invariant quaternion legendre-fourier moments. Multimed Tools Appl 77(19):24,727–24,750. https://doi.org/10.1007/s11042-018-5670-9
18. Hosny KM, Darwish MM (2021) New geometrically invariant multiple zero-watermarking algorithm for color medical images. Biomed Signal Process Control 70:103,007. https://doi.org/10.1016/j.bspc.2021.103007
19. Hosny KM, Darwish MM, Fouda MM (2021a) New color image zero-watermarking using orthogonal multi-channel fractional-order legendre-fourier moments. IEEE Access 9:91,209–91,219. https://doi.org/10.1109/ACCESS.2021.3091614
20. Hosny KM, Darwish MM, Fouda MM (2021b) Robust color images watermarking using new fractional-order exponent moments. IEEE Access 9:47,425–47,435. https://doi.org/10.1109/ACCESS.2021.3068211
21. Hu HT, Chang JR, Hsu LY (2016) Robust blind image watermarking by modulating the mean of partly sign-altered dct coefficients guided by human visual perception. AEU - Int J Electron Commun 70(10):1374–1381. https://doi.org/10.1016/j.aeue.2016.07.011
22. Khalili M (2015) Dct-arnold chaotic based watermarking using jpeg-ycbcr. Optik 126(23):4367–4371. https://doi.org/10.1016/j.ijleo.2015.08.042
23. Kumar A, Agarwal P, Choudhary A (2016) A digital image watermarking technique using cascading of dct and biorthogonal wavelet transform. In: Proceedings of the international conference on recent cognizance in wireless communication & image processing. Springer, New Delhi, pp 21–29, https://doi.org/10.1007/978-81-322-2638-3_3
24. Kumar S, Singh BK, Yadav M (2020) A recent survey on multimedia and database watermarking. Multimed Tools Appl 79(27):20,149–20,197. https://doi.org/10.1007/s11042-020-08881-y
25. Lei B, Tan EL, Chen S et al (2014) Reversible watermarking scheme for medical image based on differential evolution. Expert Syst Appl 41(7):3178–3188. https://doi.org/10.1016/j.eswa.2013.11.019
26. Li B, Xu JW (2005) Period of arnold transformation and its application in image scrambling. J Cent South Univ Technol 12(1):278–282. https://doi.org/10.1007/s11771-005-0414-1
27. Lin PY, Lee JS, Chang CC (2009) Dual digital watermarking for internet media based on hybrid strategies. IEEE Trans Circuits Syst Video Technol 19(8):1169–1177. https://doi.org/10.1109/TCSVT.2009.2020263
28. Liu SH, Yao HX, Gao W et al (2007) An image fragile watermark scheme based on chaotic image pattern and pixel-pairs. Appl Math Comput 185(2):869–882. https://doi.org/10.1016/j.amc.2006.07.036
29. Liu H, Xiao D, Zhang R et al (2016a) Robust and hierarchical watermarking of encrypted images based on compressive sensing. Signal Process Image Commun 45:41–51. https://doi.org/10.1016/j.image.2016.04.002
30. Liu XL, Lin CC, Yuan SM (2016b) Blind dual watermarking for color images' authentication and copyright protection. IEEE Trans Circ Syst Video Technol 28(5):1047–1055. https://doi.org/10.1109/TCSVT.2016.2633878
31. Lu CS, Liao HY (2001) Multipurpose watermarking for image authentication and protection. IEEE Trans Image Process 10(10):1579–1592. https://doi.org/10.1109/83.951542
32. Luo T, Jiang G, Yu M et al (2019) Robust high dynamic range color image watermarking method based on feature map extraction. Signal Process 155:83–95. https://doi.org/10.1016/j.sigpro.2018.09.024
33. Lusson F, Bailey K, Leeney M et al (2013) A novel approach to digital watermarking, exploiting colour spaces. Signal Process 93(5):1268–1294. https://doi.org/10.1016/j.sigpro.2012.10.018
34. Makbol NM, Khoo BE, Rassem TH (2016) Block-based discrete wavelet transform-singular value decomposition image watermarking scheme using human visual system characteristics. IET Image Process 10(1):34–52. https://doi.org/10.1049/iet-ipr.2014.0965
35. Mallat SG (1989) A theory for multiresolution signal decomposition: the wavelet representation. IEEE Trans Pattern Anal Mach Intell 11(7):674–693. https://doi.org/10.1109/34.192463
36. Mishra A, Agarwal C, Sharma A et al (2014) Optimized gray-scale image watermarking using dwt–svd and firefly algorithm. Expert Syst Appl 41(17):7858–7867. https://doi.org/10.1016/j.eswa.2014.06.011
37. Mohanarathinam A, Kamalraj S, Venkatesan GP et al (2019) Digital watermarking techniques for image security: a review. J Ambient Intell Humaniz Comput:1–9. https://doi.org/10.1007/s12652-019-01500-1
38. Molina-Garcia J, Garcia-Salgado BP, Ponomaryov V et al (2020) An effective fragile watermarking scheme for color image tampering detection and self-recovery. Signal Process Image Commun 81:115,725. https://doi.org/10.1016/j.image.2019.115725

39. Naor M, Shamir A (1994) Visual cryptography. In: Workshop on the theory and application of of cryptographic techniques. Springer, Berlin, pp 1–12. https://doi.org/10.1007/BFb0053419
40. Nikolaidis N, Pitas I (1998) Robust image watermarking in the spatial domain. Signal Process 66(3):385–403. https://doi.org/10.1016/S0165-1684(98)00017-6
41. of Southern California U (1977) Sipi data base. http://sipi.usc.edu/database/
42. Podilchuk CI, Delp EJ (2001) Digital watermarking: algorithms and applications. IEEE Signal Process Mag 18(4):33–46. https://doi.org/10.1109/79.939835
43. Preda RO (2013) Semi-fragile watermarking for image authentication with sensitive tamper localization in the wavelet domain. Measurement 46(1):367–373. https://doi.org/10.1016/j.measurement.2012.07.010
44. Preda R, Vizireanu D (2015) Watermarking-based image authentication robust to jpeg compression. Electron Lett 51(23):1873–1875
45. Qin C, Ji P, Zhang X et al (2017) Fragile image watermarking with pixel-wise recovery based on overlapping embedding strategy. Signal Process 138:280–293. https://doi.org/10.1016/j.sigpro.2017.03.033
46. Rawat S, Raman B (2012) A blind watermarking algorithm based on fractional fourier transform and visual cryptography. Signal Process 92(6):1480–1491. https://doi.org/10.1016/j.sigpro.2011.12.006
47. Reyes R, Cruz C, Nakano-Miyatake M et al (2010) Digital video watermarking in dwt domain using chaotic mixtures. IEEE Lat Am Trans 8(3):304–310. https://doi.org/10.1109/TLA.2010.5538406
48. Shyu SJ (2015) Visual cryptograms of random grids for threshold access structures. Theor Comput Sci 565:30–49. https://doi.org/10.1016/j.tcs.2014.10.048
49. Singh AK, Dave M, Mohan A (2014) Hybrid technique for robust and imperceptible image watermarking in dwt–dct–svd domain. Natl Acad Sci Lett 37(4):351–358. https://doi.org/10.1007/s40009-014-0241-8
50. Singh AK, Dave M, Mohan A (2015) Hybrid technique for robust and imperceptible multiple watermarking using medical images. Multimed Tools Appl:1–21. https://doi.org/10.1007/s11042-015-2754-7
51. Sreenivas K, Prasad VK (2018) Fragile watermarking schemes for image authentication: a survey. Int J Mach Learn Cybern 9(7):1193–1218. https://doi.org/10.1007/s13042-017-0641-4
52. Su Q, Niu Y, Zou H et al (2013) A blind dual color images watermarking based on singular value decomposition. Appl Math Comput 219(16):8455–8466. https://doi.org/10.1016/j.amc.2013.03.013
53. Su Q, Chen B (2018) Robust color image watermarking technique in the spatial domain. Soft Comput 22(1):91–106. https://doi.org/10.1007/s00500-017-2489-7
54. Voyatzis G, Pitas I (1996) Applications of toral automorphisms in image watermarking. In: Image processing 1996. Proceedings international conference on. IEEE, pp 237–240. https://doi.org/10.1109/ICIP.1996.560753
55. Wallace GK (1992) The jpeg still picture compression standard. IEEE Trans Consum Electron 38(1):xviii–xxxiv. https://doi.org/10.1109/30.125072
56. Xia Z, Wang X, Han B et al (2021) Color image triple zero-watermarking using decimal-order polar harmonic transforms and chaotic system. Signal Process 180:107,864. https://doi.org/10.1016/j.sigpro.2020.107864
57. Yan B, Xiang Y, Hua G (2020) Basic Visual Cryptography Algorithms. Springer, Singapore, pp 15–33. https://doi.org/10.1007/978-981-13-8289-5_2
58. Zhang L, Zhang L, Mou X et al (2011) Fsim: a feature similarity index for image quality assessment. IEEE Trans Image Process 20(8):2378–2386. https://doi.org/10.1109/TIP.2011.2109730
59. Zhu P, Jia F, Zhang J (2013) A copyright protection watermarking algorithm for remote sensing image based on binary image watermark. Optik 124(20):4177–4181. https://doi.org/10.1016/j.ijleo.2012.12.049
60. Zope-Chaudhari S, Venkatachalam P, Buddhiraju KM (2015) Secure dissemination and protection of multispectral images using crypto-watermarking. IEEE J Sel Top Appl Earth Obs Remote Sens 8(11):5388–5394. https://doi.org/10.1109/JSTARS.2015.2475169