

Novel dynamic color image watermarking based on DWT-SVD and the human visual system

Youssra Lakrissi¹  · Abderrahim Saaidi^{1,2} ·
Abdelouahed Essahlaoui¹

Received: 17 November 2016 / Revised: 3 May 2017 / Accepted: 21 June 2017 /
Published online: 6 July 2017
© Springer Science+Business Media, LLC 2017

Abstract In this paper, a novel dynamic color image watermarking based on discrete wavelet transform (DWT) and singular value decomposition (SVD) is proposed. The watermark is embedded in different random block in every execution. This random movement minimizes more the risk of detecting the watermark and makes it difficult to find and to destroy. The encrypted binary watermark is embedded by modifying the singular values of a dynamic block generated randomly using a pseudo random generator from the sub-band LL after applying the DWT on the original image. This method respects the Human visual system (HVS) since the scaling factor used is adaptive to the image features in order to achieve the tradeoff between robustness and visual quality of the watermarked image. It is a semi-blind scheme because some of the original data are used for extraction. The experimental results show a good visual quality for the watermarked images and high robustness against several attacks avoiding at the same time the false positive error known by most of the SVD schemes and ensuring more security the authors.

Keywords Dynamic watermarking · Dwt · SVD · JND · Robustness · Imperceptibility · False positive error

✉ Youssra Lakrissi
lakrissi.youssra@gmail.com; youssra.lakrissi@usmba.ac.ma

Abderrahim Saaidi
abderrahim.saaidi@usmba.ac.ma

Abdelouahed Essahlaoui
abdelouahed.essahlaoui@usmba.ac.ma

¹ LSI, Engineering Sciences Laboratory, Polydisciplinary Faculty, Sidi Mohamed Ben Abdellah University, B.P 1223 Taza, Morocco

² LIAN, Department of Mathematics and Computer Sciences, Faculty of Sciences Dhar Mhraz, B.P 1796 Atlas-Fez, Morocco

1 Introduction

During the last decade, the rapid development of internet and computer networks have made the distribution of digital media (e.g. audio, image, video) much easier, but sometimes without the agreement or the consciousness of the property, so raising a lack in the copyright protection methods. Thus, how to protect and secure the multimedia data from illegal usage has been receiving more and urgent attention [33, 67]. Digital image watermarking techniques are considered as a powerful solution to provide digital content protection [30, 35, 46]. The main idea is to embed visible or invisible watermark information that represents the identity of the property [11] in the host image without any perceptual changes or loss of information and cannot be removed easily [12].

Watermarking can be used in different applications such as authentication [9], integrity [27], author copyright [10]. This is why, digital watermarking techniques are classified according to various criteria. The first classification (robust, fragile, semi fragile) is based on the resilience of the method against intentional or unintentional attacks [43]. The robust watermarking as in [10, 41] is often used to protect copyright and property verification since it resists to image processing operations. Fragile watermarking techniques as in [27, 43] are used for authentication and identity integration, they are designed to detect any unauthorized alterations, so that slight modification in the watermarked image will destroy or change the watermark. While the semi fragile methods allow non malicious changes such as compression. However, they are weak against malicious attacks [34] that change the image content meaning.

The second classification of watermarking techniques is based on the information needed when extracting the watermark [27]. We talk about blind watermarking [15] when the original image and original watermark are not needed for extraction. Unlike the non-blind watermarking algorithms where the original host image is required to extract the watermark, which means it can only be extracted by the person who has a copy of the original image and the secret key used for extraction. The last type in this classification is the semi blind watermarking [6] where some embedding process information are used for extraction.

The third category is classified depending on watermark embedding domain [26]: spatial domain and frequency domain. In the spatial domain [48], the watermark is inserted directly by modifying the original image pixel values [36, 66]. Techniques in this domain have the advantage of easy implementation and low cost of operation. Nevertheless, they are not robust against many attacks [4]. While in frequency domain methods, the image representation in the spatial domain is transformed into the frequency domain to insert the watermark, presenting better performance compared with spatial domain. There are many transforms in the frequency domain, the most familiar are Discrete Cosine Transform (DCT) [3, 15, 23, 26, 47, 52, 54], Discrete Fourier Transform (DFT) [31, 59], Discrete Wavelet Transform (DWT) [4, 23, 40, 45, 47, 60–64], Singular Values Decomposition (SVD) [3–6, 19, 20, 25, 45, 47] and other decompositions [42, 51, 53].

For all the classifications listed above, we add a new classification based on static or dynamic watermarking. In this paper, we focus on dynamic image watermarking which provides movement to the embedded watermark ensuring an additional difficulty when detecting and extraction the watermark for unauthorized people. As shown in Fig. 1, the watermark is embedded in a random block selected from the original image and changes the position in every execution without any visual alterations on the watermarked image. In the extraction process, a secret key is used to find the embedding block, and the watermark is detected by performing a correlation criterion in order to extract the final watermark. The diagram of the presented method is illustrated in Fig. 1.

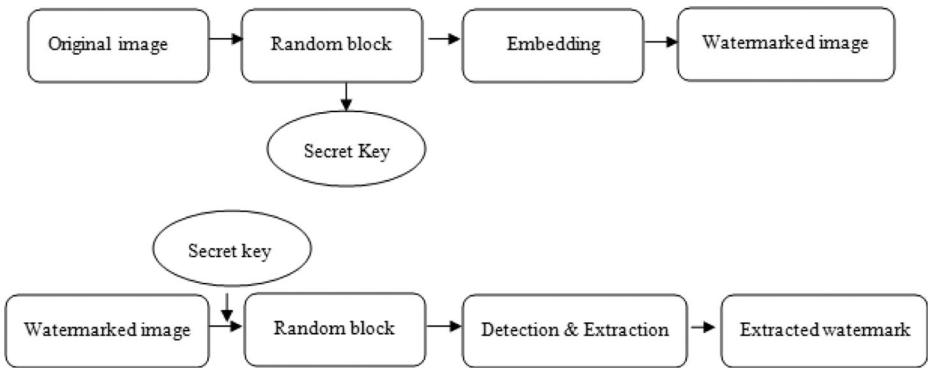


Fig. 1 Outline of the presented watermarking scheme

The rest of the paper is organized as follow: Section 2 presents an overview of some watermarking techniques. The proposed approach is explained in section 3. The experimental results are discussed in section 4. Finally, conclusions are made in section 5.

2 Previous work

The term of “Digital watermark” was employed for the first time by Andrew Trikel and Charles Osburne in 1992 [57]. Later, Ingimer Cox [13] popularized the spread spectrum techniques for digital watermarking. Progressively, with the development of multimedia information i.e. audio, video, image, digital watermarking has become the best solution to prevent the illegal use of information and more research is conducted in this area.

In [15], Das et al. proposed a blind watermarking in DCT domain using the correlation between two DCT coefficients of adjacent blocks in the same position to insert the binary watermark. To change the DCT coefficient value, they subtracted DC and median of few low frequency AC coefficients. Then the result is normalized by DC coefficient. In [23], Hu and Hsu combined DWT and DCT for watermarking. Firstly, the image is decomposed by DWT, then the DCT is applied to every blocks divided from of the approximate coefficients. The targeted coefficients are chosen according to human visual characteristic using the quantization index modulation (QIM) to improve the performance in robustness and imperceptibility and minimize the binary error rate (BER) in watermark extraction. In [64], Yadav proposed a spread spectrum watermarking based on standard deviation technique for an adaptive strength factor proportional to the image local characteristics. In this scheme, the selective embedding of the binary watermark has been done in 8*8 building blocks of low-frequency wavelet coefficient the original image, depending on the respective entropies of the blocks. M.Ali suggested in [3] a watermarking algorithm based on DCT and SVD for gray scale images which are portioned into blocks and the blocks are transformed into DCT. The DC of each block is selected to construct a low-resolution image and apply SVD on it. Then the watermark is embedded by modifying the low-resolution approximation image singular values by the singular values of the watermark using multiple scaling factors designed by the Differential Evolution algorithm (DE) in order to achieve a good performance of robustness without compromising with the quality of the image. However the scheme is non-blind and the PSNR of the watermarked image does not exceed 37db.

Recently, The Singular Value Decomposition (SVD) is very used as watermarking technique since the singular values have a good stability, when a small perturbation is added to an image, its singular values do not change significantly and provide good visual quality. Nevertheless, the false positive detection comes when the attacker can extract a new watermark (which is not the embedded one) by changing the value of U and V matrices with their desired to pretend the false ownership. In order to solve the false positive error, Loukhaoukha et al. [37] proposed to apply one way hash function on U and V matrices and stored privately so they can be used for authentication during extraction. To avoid the same problem, Gobta et al. [22] proposed to embed the principal component of the watermark into the singular value of the original image and used Practical Swarm Optimization (PSO) to get optimal scaling factors. However, one or more singular values must be modified to keep the order of singular values, which might degrade the quality of the watermarked images. In [4], Ali presented a hybrid watermarking scheme based on DWT-SVD. In the embedding process, the gray scale watermark is inserted by modifying the singular values of low pass (LL) and high pass (HH) of the third level DWT decomposition of the original image. In order to avoid the false positive error, the LL band is shuffled by Arnold transform and applied the Otsu's method to get a binary image and then performed the XOR operation on this binary image and the binary watermark to generate a secret key. Then the binary watermark is hidden in the secret key instead of the host image. For extraction process, the secret key is used to calculate the estimated binary watermark, and a correlation function is performed between the original and extracted watermarks. If the correlation value is greater than a predefined threshold then the grayscale watermark is extracted, otherwise an authentication message is displayed. In [6], Ansari et al. almost proposed the same principle by modifying the singular values of the original image except that they used the Integer Wavelet Transform (IWT) instead of DWT and the scaling factor is optimized by performing the artificial Bee Colony (ABC) in order to further improve the quality of watermarking. In this scheme, the false positive problem is also solved by generating a signature from U and V matrices obtained by applying SVD on the modified image. The signature is then embedded in the horizontal coefficients (HH) of the original image. In the extracting process, the signature generated is compared with the extracted one from the watermarked image using a threshold based on hamming distance. This leads to authenticate the right and the wrong owner.

In the field of image watermarking, studies have been mostly dedicated to gray scale techniques, but color image watermarking is a crucial challenge in modern digital watermarking. In [2], a color watermarking algorithm based on DWT using the HSV color space where the watermark is inserted in the V channel. Moreover, the effects of using different color spaces on the visibility and robustness of watermark schemes has been studied [28, 38, 52].

Although, all the techniques mentioned above and others insure good imperceptibility and robustness against different attacks, the embedding process still static. It means that every time the watermarked image is sent to many people, the position of the embedded watermark still the same for each one of them. This kind of watermarking will sometimes cause a problem if the attacker can determine the position of the embedded watermark. Consequently, the images will be copied, modified and diffused with the wrong ownership.

In this paper, we propose a randomly dynamic color image watermarking based on DWT and SVD. The concept of dynamic watermarking is featured by the fact that the embedding position changes with every execution. First of all, the original image is decomposed by third level DWT and the embedding block is selected by applying a pseudo random generator on the low frequency coefficients ($LL3$). The position of the selected block changes in each execution

even if the same image is used for watermarking. After that, SVD transform is applied on the random selected block and its singular values are modified by the binary watermark, already encrypted by AES algorithm to enhance its security. Thus, the watermark is embedded every time in different position without visual alteration on the watermarked image. The strength factor has been always a topic of discussion in several researches and many of the existing watermarking schemes have been taking strength factor as a single constant value. In this work, we are working with Just Noticeable Distortion technique (JND) [8] based on the image local characteristics to respect the tradeoff between invisibility and robustness against attacks. This is a semi-blind scheme since the secret key of the pseudo random generator and the encrypted eigenvectors U and V values are used for extraction process. The experimental results showed that the proposed method has achieved a high level of robustness not only against image processing attacks but also against geometric attacks using images of different sizes.

3 Proposed method

Most of watermarking methods use a static embedding [20, 21, 36]. In this work, we propose a dynamic watermarking where the watermark is embedded in different random block in every execution (see Fig. 3). This random movement minimizes more the risk of detecting the watermark and makes it difficult to find and to destroy in order to guarantee more security for the watermarked images and save the authors copyrights. The embedding block is selected by a pseudo random generator with a secret key shared only between the concerned users. Otherwise the embedding block will be different than the extracting block and then the extracted watermark will not look like the original one.

The proposed method is a hybrid method based on Discrete Wavelet Transform (DWT) and Singular Values Decomposition (SVD). The DWT is known by its *space frequency localization* which makes the watermark most robust to the geometric attacks. *Multi-resolution representation* allows detecting the hierarchical process which is very important for watermark detection. As for SVD, it is invariant against geometrical attacks and when a small alteration is added to an image, its singular values do not change significantly. The original image is first converted from the RGB color space to the YCbCr color space and decomposed into third-level of DWT. Then select a block from the $LL3$ sub-band using a pseudo random generator in order to embed the encrypted binary watermark. After that, SVD is applied on the selected block where embedding is done by modifying the block singular values using an adaptive scaling factor assuring the invisibility of watermarking and robustness against different attacks.

In order to enhance the binary watermark security as well as other requisite information for extraction (Fig. 4), the symmetric encryption algorithm AES is used to cipher these information and the asymmetric encryption algorithm RSA is used to cipher the AES private key and the pseudo random generator secret key. After embedding the watermark, inverse SVD is applied to the modified block used to reconstruct the new sub-band $LL3^*$ which is used for inverse DWT to generate a new image that is converted back to RGB color space to get the final watermarked image.

The extraction process is important when a conflict occurs between persons claiming ownership of the original image. In this method, to extract the watermark, the first steps of embedding are the same in here starting by conversion to the YCbCr color space and applying

DWT on the luminance component Y . Then, using the decrypted secret keys by RSA, we can know the block position where the watermark was embedded.

Before extracting the watermark, a verification test is performed using a correlation function between the saved data while embedding and the ones used for extraction. If the correlation value is equal or greater than a predefined threshold then the extraction is processed, otherwise the verification test is failed and the program stops (Fig. 4).

3.1 Embedding process

3.1.1 Conversion to YCbCr color space

Most scientific researches use the RGB color space for image watermarking methods [46, 56] using each component R, G or B or combine them for embedding the watermark. However, the RGB color space is not very efficient as regards to “real images” [26], because the image colors and intensity are separated causing a loss of the hue upon a modification as compression or filtering attacks where every component energy will be reduced. Also, the information redundancy between the three components is relatively close. Thus, the original image is first converted from RGB color space to YCbCr color [18] space using the Eq. (1):

$$\begin{cases} Y = 0.299R + 0.587G + 0.114B \\ C_b = -0.169R - 0.331G + 0.500B \\ C_r = 0.500R - 0.419G - 0.081B \end{cases} \quad (1)$$

3.1.2 Application of the discrete wavelet transform DWT:

The basic idea of discrete wavelet transform is to separate frequency detail [39]. It decomposes an image into four sub-bands called respectively LL (approximation coefficient), LH (vertical details), HL (horizontal details) and HH (diagonal details). The LL coefficients belong to low frequencies while HL , LH and HH belong to the high frequencies. The most of the information contained in the original image is concentrated into the LL image, whereas texture and edge information are focused in the detail coefficients HL , LH , and HH .

To calculate the DWT of an image of size $M \times N$, it must identify the wavelet function W_ψ^i responsible of horizontal, vertical and diagonal coefficients $\{H, V, D\}$ and the scale function W_φ to define the approximation coefficients [21] following the equations below:

$$W_\varphi(j_0, m, n) = \frac{1}{\sqrt{MN}} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} I(x, y) \varphi_{j_0, m, n}(x, y) \quad (2)$$

$$W_\psi^i(j_0, m, n) = \frac{1}{\sqrt{MN}} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} I(x, y) \psi_{j_0, m, n}^i(x, y) \quad (3)$$

with:

$$1 \leq i \leq 3, \psi_{j_0, m, n}^i(x, y) = \frac{1}{2^j} \psi^i\left(\frac{x-2^j n}{2^j}, \frac{y-2^j m}{2^j}\right) \quad i = \{H, V, D\} \quad (4)$$

$$\varphi_{j,m,n}(x,y) = \frac{1}{2^j} \varphi\left(\frac{x-2n}{2^j}, \frac{y-2m}{2^j}\right) \tag{5}$$

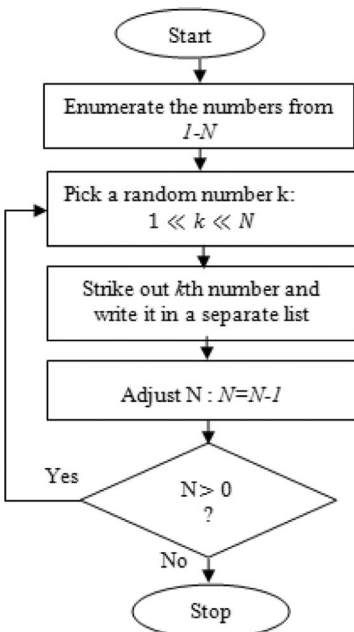
j_0 is the start resolution and the scale parameter j is always greater or equal to j_0 . In general, we choose $j_0 = 0$ and $N = M = 2^j$ in order that $j = 0, 1, \dots, j-1$ and $m, n = 0, 1, \dots, 2^j-1$.

Therefore, once the original image is converted to the YCbCr color space, the third level of DWT is applied on the luminance image Y which represents its gray scale using Eqs. (2) and (3) in order to get respectively approximation, vertical, horizontal and diagonal coefficients ($LL3, LH3, HL3, HH3$) with 3 is the level number of the decomposition.

3.1.3 The random embedding block selection

For a dynamic move of the watermark, a pseudo random generator (PRG) is performed using a private key Key_bloc on the sub-band $LL3$ in order to define random coordinates of the embedding block (which has the same size of the watermark). The generator (PRG) is based on ‘Fisher Yates’ permutation algorithm [17] as described in algorithm 1 and illustrated in Fig. 2. The main idea of using Key_bloc is to make the embedding location more specific in order o use it for extraction. Then Key_bloc is saved and ciphered by RSA [68] in order to enhance its security.

The RSA algorithm is based on the difficulty of factoring large numbers into product of two large prime factors to generate public and private key. But it takes more computational time for big size information, so the RSA algorithm will be used only to encrypt all secret keys because they are not very large. Thus, this ensures quick and secure secret keys distribution.



Algorithm 1: Fisher-Swap
Input: List L of size N
 Integer i, j
Start
 For i in N-1 to 1 Loop
 j ← random number between 0 and i
 Swap L[i] and L[j]
 End
End

Algorithm 2: Rand-position
Input: LL image of size M*N
 Integer mpart, npart // Define the size
 of the selected random position
Output: Integer x, y // the random position
 coordinates
Start
 x= Fisher-Swap (M-mpart+1)
 y= Fisher-Swap (N-npart+1)
End

Fig. 2 « Fisher-Yates » algorithm principle

3.1.4 SVD application on the random selected block

The singular Value Decomposition (SVD) is a symmetric matrix decomposition tool based on a theorem of linear algebra to diagonalize the rectangular matrix. In order to expose the various relationships among the original data, SVD transforms correlated variables into a set of uncorrelated ones [7].

In our method, the SVD is applied on the random selected block B to separate its singular values S_1 from eigenvectors U_1 and V_1 using the Eq. (6):

$$B = U_1 S_1 V_1^T \quad (6)$$

With: V_1^T is the transpose of V_1 .

3.1.5 Binary watermark encryption

In order to improve its security, the binary watermark is firstly encrypted using the symmetric encryption AES [14] (Advanced Encryption Standard) with a private key of size 128bit (see Eq. 7). However, Acharya et al. recommended in [1] to use AES with private key of size 256 to ensure a good compromise between confidentiality level and the computation time.

The AES algorithm is recommended by NIST (National Institute of Standards and Technology) and it is very known by fast implementation in both software and hardware since it is based on block encryption in several rounds, which is very efficient for images encryption.

$$W_{encrypt} = AES_Encrypt(W_{orig}) \quad (7)$$

With: W_{orig} is the original watermark and $W_{encrypt}$ is the encrypted watermark via AES.

The objective of employing a symmetric encryption using a private key is to keep the concept of having a single shared key that can be changed by the concerned users at any time as well as the secret key used for generating a random embedding position. The AES private key is encrypted later by the asymmetric algorithm RSA.

3.1.6 Embedding the watermark

To embed to watermark, the diagonal singular values of the block B are modified by the encrypted watermark values, and then transformed again by SVD (Eq. 9) to get the modified block as in Eq. (10).

$$Temp = S_1 + \alpha W_{encrypt} \quad (8)$$

$$SVD(Temp) = U_{IW} S_{IW} V_{IW}^T \quad (9)$$

$$B_{IW} = U_1 S_{IW} V_1^T \quad (10)$$

The value of S_1 , U_{IW} , V_{IW} are encrypted using AES and saved as secret keys so as to be used in extraction process. Besides, the AES private key will be also encrypted using RSA algorithm.

The variable α is the adaptive scaling factor designed according to the human visual model system that take into account many factors such as brightness, frequency and style of texture.

Motivated by these facts, Barni et al. [8] computed the quantization of each coefficient in the DWT domain as a product of three terms: frequency sensitivity (f_q), luminance sensitivity (l_c) and texture masking (tx).

$$quantization(n, c, i, j) = f_q(n, c) \cdot l_c(n, i, j) \cdot tx(n, i, j)^{0.2} \tag{11}$$

Where: n is DWT decomposition level. $n \in \{0, 1, 2, 3\}$.
 c is wavelet coefficient orientation $c \in \{LL, LH, HL, HH\}$
 $A^{n \cdot c}(i, j)$ Wavelet coefficient at position (i, j)

The first expression in Eq. (11) is the frequency sensitivity (f_q) which deals with sensitivity to the noise change according to the decomposition level and orientation as shown in Eq. (12).

$$f_q(n, c) = \left\{ \begin{array}{l} \sqrt{2} \text{ Si } c \\ 1 \text{ sinon} \end{array} \right\} \cdot \left(\begin{array}{l} 1 \text{ si } n = 0 \\ 0.032 \text{ Si } n = 1 \\ 0.16 \text{ Si } n = 2 \\ 0.10 \text{ Si } n = 3 \end{array} \right) \tag{12}$$

While the luminance sensitivity (l_c) is based on the local brightness of the gray level values of the low pass images. Barni et al. [8] are based on the fact that the human eye is less sensitive to changes in regions with high brightness but also in the darkest regions and proposed to calculate the luminance sensitivity for color images using Eq. (13), (14) and (15).

$$l_c(n, i, j) = 1 + L'(n, i, j) \tag{13}$$

$$L'(n, i, j) = \left(\frac{1 - L(n, i, j)}{L(n, i, j)} \cdot \frac{\text{Si } L(n, i, j) < 0.5}{\text{Sinon}} \right) \tag{14}$$

$$L(n, i, j) = \frac{1}{256} A^{3,LL} \left(1 + \left\lfloor \frac{i}{2^{3-n}} \right\rfloor, 1 + \left\lfloor \frac{j}{2^{3-n}} \right\rfloor \right) \tag{15}$$

The last term in the Eq. (11) is the texture masking which measures the texture activity in the neighborhood of the pixel and it is composed as the product of two contributions as shown in Eq. (16).

$$tx(n, i, j) = \sum_{k=0}^{3-n} 16^{-k} \sum_C^{LH,HL,HH} \sum_{x=1}^2 \sum_{y=1}^2 \left[I_{k+r}^c \left(y + \frac{i}{2^k}, x + \frac{j}{2^k} \right) \right]^2 \tag{16}$$

$$* \text{Var} \left\{ I_3^{LL} \left(1 + y + \frac{i}{2^{3-r}}, 1 + x + \frac{j}{2^{3-r}} \right) \right\}_{\substack{x=1,2 \\ y=1,2}}$$

The first term in Eq. (16) is the local mean square value of the DWT coefficient in all detail sub-bands of a small 2×2 neighborhood corresponding to the location (i, j) and the second term calculates the local variance of the low pass sub-band.

Since $quantization(n, c, i, j)$ is chosen as the quantization step for a DWT coefficient at location (i, j) , it implies that distortions having value lower than $quantization(n, c, i, j)/2$ are supposed to be invisible. Hence, the JND (Just Noticeable Distortion) value is defined as:

$$JND(n, c, i, j) = 0.5^* quantization(n, c, i, j) \quad (17)$$

In order to define the scaling factor of singular values modification, Li et al. [32] have proposed to determine a relation between s_i which represents the singular values and $JND(n, c, i, j)$. For every matrix A of size $M \times N$, let δs_i be the change of its i -th singular value s_i . Thus, the modification is invisible on if:

$$|\delta s_i| \leq \frac{JND(x, y)}{|U_i V_i^T(x, y)|} \quad (0 \leq x \leq M, 0 \leq y \leq N) \quad (18)$$

Where: $JND(x, y)$ is Just Noticeable Distortion, U_i and V_i are the eigenvectors of matrix A .

Thus, the scaling factor is calculated by scaling down the change of the first and the largest singular value of the random block as shown in Eq. (19):

$$\alpha = \frac{\min(|\delta s_i|)}{S_1(1, 1)} = \frac{\min\left(\frac{JND(x, y)}{|U_i V_i^T(x, y)|}\right)}{S_1(1, 1)} \quad (19)$$

With: $S_1(1, 1)$ is the first singular value of the block B , and U_i, V_i are the eigenvectors of the block B .

After that, the sub-band $LL3$ is modified by the new values of the watermarked block B_{TW} , and it is used to reconstruct the watermarked image by applying the inverse DWT. Finally, the watermarked image is converted back to the RGB space color using Eq. (20) to get the final watermarked image.

$$\begin{cases} R = 1.00Y - 0.001C_b + 1.402C_r \\ G = 1.00Y - 0.344C_b - 0.714C_r \\ B = 1.00Y + 1.722C_b + 0.001C_r \end{cases} \quad (20)$$

The above description of the embedding process is illustrated in Fig. 3:

We propose a dynamic watermarking where robustness and security are the most important criteria as illustrated in Fig. 3. However, the computation time will be higher comparing with other static watermarking methods since we are using some encryption algorithm beside the random selection of the embedding block.

3.2 Extraction process

Firstly, the watermarked image is converted from the RGB color space to the YCbCr color space using Eq. (1) and decomposed by DWT 3level into frequency coefficients using Eqs. (2) and (3). The block B^* where the watermark was embedded is selected from the sub-band $LL3^*$ using the pseudo random generator and the secret key key_bloc . And then, using the Eq. (6), SVD is applied on the selected block to get its singular values.

Before proceeding to the next step, a verification test based on correlation between the encrypted values of U_{TW} and V_{TW} to be provided by the user and those saved with the program.

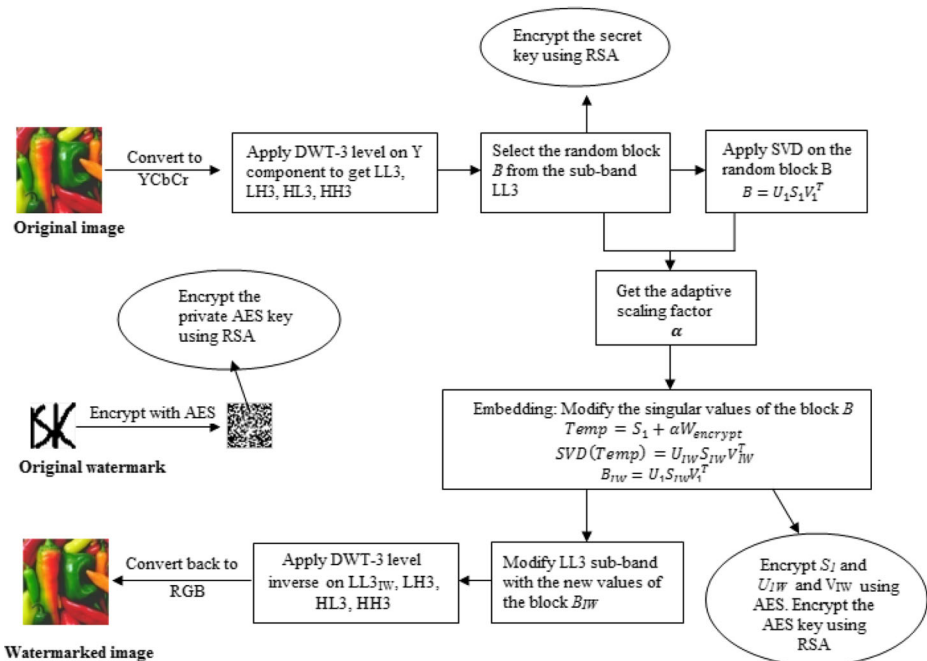


Fig. 3 The proposed embedding scheme

If the correlation value is greater than a predefined threshold $T = 0.9$ then continue the extraction process otherwise, the program will stop. In general, the threshold value should equal to $T = 1$, but taking into account the small changes than can undergo the encrypted values of U_{1W} and V_{1W} we have decided to work with $T = 0.9$.

After the successful verification of the authentication test, the private key of RSA is used to decrypt the AES key which will be used subsequently to decrypt S_1 , U_{1W} and V_{1W} . The extraction is then produced by Eqs. (21) and (22).

$$S_{ext} = U_{1W}S_2 + V_{1W}^T \tag{21}$$

$$W_{ext} = (S_{ext} - S_1) / \alpha \tag{22}$$

Where: S_{ext} are the extracted singular values from the block B^* and W_{ext} is the encrypted extracted watermark.

Once the encrypted watermark is extracted, we decrypted it using AES decryption to recover the final extracted watermark as illustrated in Fig. 4.

In this case, secret keys are very important to extract the watermark since the secret key used to find the embedding block need to be decrypted. Hence, it must be a correct sharing of the RSA encryption and decryption keys. So, one mistake can cause the loss of information and select a false position. Consequently, the extracted watermark will not be the same as the original. Remains to mention that computation time will be higher too due to decryption algorithms and the correlation test that ensures the user authentication.

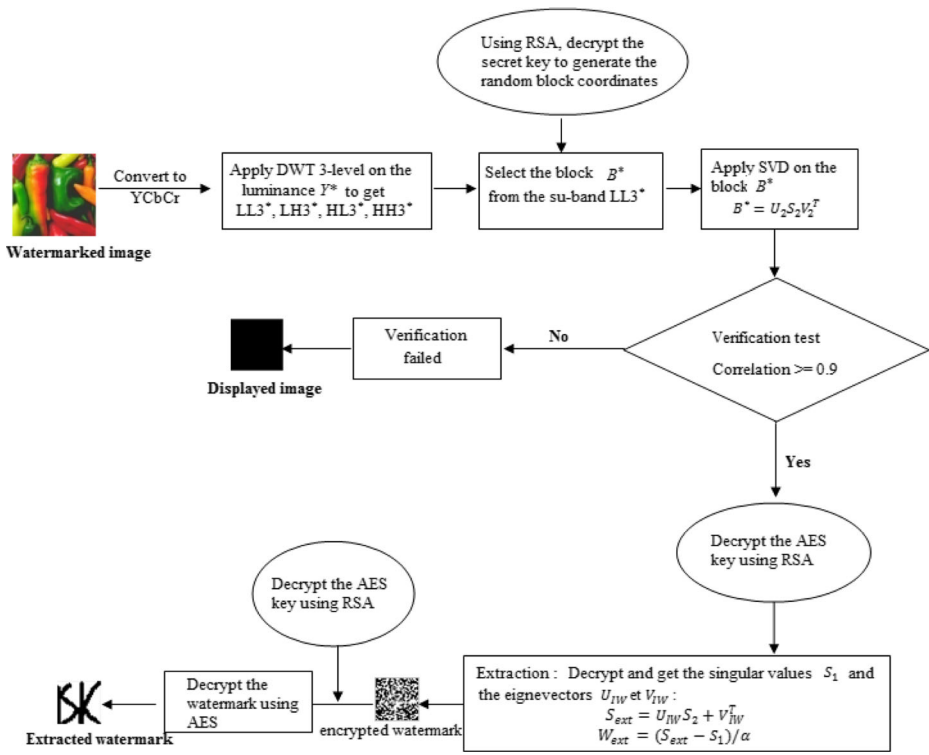


Fig. 4 The proposed extraction scheme

4 Experimental results and discussion

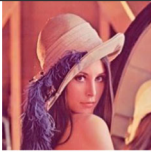


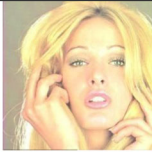




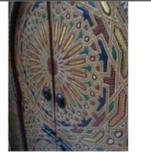
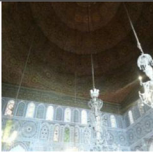



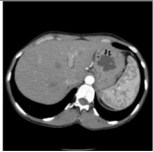
In this paper, the performance of the proposed method is measured by the watermark invisibility and robustness against different attacks. We have used color images from different data bases such as USC-SIPI [49], KODAK [29], medical images from DICOM [16] and some personal images. The main features of the images used are listed in Table 2 and represented in Table 1. Those images are chosen with different size, extension, texture style, edges and luminance brightness in order to study the proposed method performance under different criteria that can influence on the image quality. The method is implemented on a PC with 4GB RAM and 2.20 GHz Intel Core i3.

The binary watermark of 32×32 as original size is illustrated in Fig. 5. There is kind of relationship between the original image and watermark size when using DWT for watermarking. The watermark size should not exceed the embedding sub-band size depending of the decomposition level in order not to have overlapping pixels. In our proposed method, the watermark size must satisfy the following condition:

$$W_{orig}(i, j) = \left\{ p(i, j) \ / \ i = \frac{M}{2^{l+1}}, j = \frac{N}{2^{l+1}} \right\} \tag{23}$$

Where: W_{orig} is the original watermark, $p(i, j)$ is the original watermark pixels where i and j are their coordinates. M and N are respectively the height and width of the original image.

Table 1 Visual representation of the test images

USC-SIPI					
	(a)	(b)	(c)	(d)	
	Kodak				
		(e)	(f)	(g)	(h)
Personal					
		(m)	(n)	(o)	(p)
	DICOM				
		(q)	(r)		

$l \in \{0, 1, 2, 3, \dots\}$ is the DWT level. If the binary watermark size does not satisfy the condition (23), it should be resized before proceeding to the embedding process.

The PSNR (Peak Signal to Noise Ratio) metric (24) is used in order to measure the quality of the watermarked image. The watermarked image is estimated to have a good visual quality and similarity with original image when PSNR is higher than 30db [24]. The higher the PSNR values of the watermarked image the closer the resemblance with the original one [65].

Table 2 Images features

Image_Id	Image Name	Size	Extension	Feature
(a)	Lenna	512 × 512	JPEG	Higher contrast and sharp feature points
(b)	Pepper	512 × 512	JPEG	Homogenous zones
(c)	Sailboat	512 × 512	TIFF	Textured zones with high frequency component
(d)	Tiffany	512 × 512	TIFF	Variant brightness and high frequency component
(e)	Girl	768 × 512	PNG	High contrast in the face and clothes
(f)	Hats	768 × 512	PNG	Smooth zones in the sky area but textured with high frequency component in the other areas
(g)	Lighthouse	768 × 512	PNG	Complex texture in the rocks area
(h)	Flower	768 × 512	PNG	Weak intensity luminance
(m)	Door	960 × 1280	JPEG	Textured zones with high frequency component
(n)	MosqueLight	1280 × 960	JPEG	Larges homogenous zones and textured in the roof
(o)	BinWidane	2560 × 1536	JPEG	Larges homogenous zones with poor and not clear content
(p)	Ifrane	2560 × 1536	JPEG	Larges homogenous zones but textured in trees area
(q)	Thorax	512 × 512	JPEG	Larges homogenous zones
(r)	Anonymized	512 × 512	JPEG	Larges homogenous zones

Fig. 5 The binary original watermark



$$PSNR = 10 \log_{10} \left(\frac{(X_{max})^2}{\frac{1}{3MN} \sum_c \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} [\{X(i,j) - Y(i,j)\}^2]} \right) \quad (24)$$

Where: X_{max} is the maximum possible value for a pixel.

The denominator expression in Eq. (24) represents the mean squared error for image X (original image) and image Y (watermarked image) of size $M*N$.

After extracting the watermark, the Normalized Coefficient (NC) is computed using the original watermark W_{orig} and the extracted one W_{ext} . As defined in Eq. (25):

$$NC(W_{orig}, W_{ext}) = \frac{\sum_i \sum_j W_{orig}(i,j) W_{ext}(i,j)}{\sum_i \sum_j [W_{orig}(i,j)]^2} \quad (25)$$

The NC value is between 0 and 1. In principle, if the NC value is 0.7 and get closer to 1, the extracted watermark is getting more similar to the original one [44, 58].

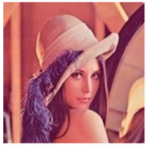


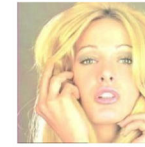














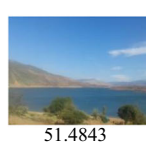






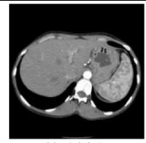


4.1 Visibility experiments

Table 3 shows the obtained watermarked images and their PSNR value as well as the extracted watermark and their NC value.

As it is clear from Table 3, all the PSNR values are higher than 30 db and the visual quality of the watermarked image is very good without any perceptible distortions even after embedding in a random block. This quality is also improved by using an adaptive scaling factor using JND function. Because, to embed into an image, but still invisible, the scaling factor has to consider how the human eye perceives disturbs in order to fit the behavior of the HVS (Human Visual System) to the watermarking problem. Since the eye is less sensitive to noise in areas where brightness is high or low and also in textured area while it is more sensitive near the edges. Based on these considerations, the JND function is computed using the product of three terms: the frequency, local brightness and image texture masking.

The LL sub-band contains most of the image energy, so embedding the watermark in it guarantees robustness against various attacks. However, it may cause visible distortions. This

Table 3 Visual representation, PSNR and NC value of the watermarked and extracted images

Watermarked image PSNR(db)	 52.0156	 52.1921	 51.8874	 52.0231
Extracted watermark (NC)	 NC=0.9866	 NC=0.9866	 NC=0.9833	 NC=0.9866
Watermarked image PSNR(db)	 52.770	 52.770	 52.2451	 52.1742
Extracted watermark (NC)	 NC=0.9716	 NC=0.9716	 NC=0.9716	 NC=0.9716
Watermarked image PSNR(db)	 52.1465	 52.3956	 51.4843	 52.1350
Extracted watermark (NC)	 NC=1	 NC=1	 NC=1	 NC=1
Watermarked image PSNR(db)		 57.7864	 60.1021	
Extracted watermark (NC)		 NC=0.9866	 NC=0.9866	

is why the SVD is applied to the random block from the *LL* sub-band where only its singular values are modified. Furthermore, with the reuse of the block eigenvectors which contains most of details such as texture and edges information, the invisibility of watermarking is ensured with a good similarity between original and watermarked images which is proved with high PSNR values even when the image has flat and homogeneous zones such as “*BinWidane, Ifrane, Sailboat*” where the modifications can easily be perceived.

Concerning the extraction, the NC metric is used to compute the similarity between the original and the extracted watermark and it is supposed to be between 0 and 1. If the NC value of the extracted watermark is closer to 1, then it is getting more similar to the original one.

Otherwise, if the NC value tends to be closer to 0, then the extracted watermark does not look like the original watermark or even destroyed.

Note that in Table 3, all the NC values of the extracted watermark are close or equal to 1. Thanks to embedding in the original image low frequencies sub-band which are robust against different attacks and the use of the original watermark eigenvectors in order to get the extracted watermark even after resizing and encrypting the original one. These operations may cause a loss of information from the beginning. However, in our proposed method, the algorithm kept the most of the watermark information.

4.2 Robustness experiments

4.2.1 Attacks experiments

In order to test the robustness of our method, we applied two attack categories [50]. The first one is the removal attacks (noise, filter, compression, sharpening...), while the second category concerns geometric attacks (rotation, resizing, scaling...) [50]. In Table 4, a brief description is presented of the attacks used in our watermarking technique.

The removal attacks aim to remove the watermark from the watermarked image without attempting to break the security of the watermarking algorithm. On the other side, the geometric attacks try to desynchronize the watermarking content in the image and detector for extraction [50, 55]. So despite the presence of the watermark, the extracted bits are different to those that have been hidden.

For these reasons, the attacks above are applied to test the robustness of the proposed approach. Table 5 shows the NC values of the extracted watermark.

As noticed in Table 5, all the NC value of the extracted watermark are higher than 0.9. However, there is a slight difference depending on the images since each one has different features. In order to compare the obtained results, the used images are divided into two categories: the first one includes images with textured zone and high frequency components (*Sailboat, Tiffany, Girl, Hats and Lighthouse*), while the second category includes images

Table 4 Brief description of used attacks

Attack index	Attack name	Description
SP [50]	Salt & Pepper Noise (0.01)	Randomly transform the image pixel to black and white
GB [50]	Gaussian Noise (0.01)	Adding successive values generated randomly to each pixel of the image
GF [50]	Gaussian filter (3×3)	Replace the value of each pixel in an image by the weighted average of the intensity levels in the neighborhood defined by the filter mask. The filter mask is defined by the Gaussian function
RO [50]	Rotation 45°	Reverse the image according to a certain degree
CA [50]	Contrast adjustment (20%)	Improve the image contrast by gamma correction and histogram equalization
JPG [55]	Compression JPG 50%	Apply a sub-sampling and quantization to the image in which the major part of information is lost.
RS [50]	Reduce the image to its half size and resize again it to its original size	Stretch or reduce the image size
SH [50]	Sharpening (0.8)	Apply a high-pass filter to sharpen edges.

Table 5 NC values of the extracted watermark against different attacks

Image/Attack	SP	GB	GF	RO	CA	JPG	RS	SH
Lenna	0.9401	0.9851	0.9866	0.9750	0.9850	0.9866	0.9833	0.9900
Pepper	0.9867	0.9834	0.9842	0.9842	0.9833	0.9816	0.9858	0.9900
Sailboat	0.9867	0.9858	0.9842	0.9809	0.9866	0.9866	0.9783	0.9892
Tiffany	0.9892	0.9883	0.9842	0.9833	0.9866	0.9917	0.9858	0.9917
Girl	0.9732	0.9716	0.9765	0.9724	0.9699	0.9800	0.9765	0.9783
Hats	0.9725	0.9741	0.9765	0.9709	0.9699	0.9800	0.9757	0.9775
Lighthouse	0.9749	0.9741	0.9765	0.9797	0.9716	0.9766	0.9774	0.9792
Flower	0.9766	0.9699	0.9765	0.9725	0.9699	0.9766	0.9757	0.9785
Door	0.9933	0.9925	0.9916	0.9933	0.9899	0.9883	0.9933	0.9925
MosqueLight	0.9891	0.9891	0.9899	0.9815	0.9816	0.9800	0.9899	0.9891
BinWidane	0.9958	0.9958	0.9958	0.9908	0.9917	0.9917	0.9958	-
Ifrane	0.9958	0.9958	0.9958	0.9958	0.9917	0.9917	0.9958	-
Thorax	0.9842	0.9833	0.9842	0.9783	0.9816	0.9866	0.9815	0.9909
Anonymized	0.9891	0.9900	0.9842	0.9850	0.9766	0.9933	0.9858	0.9900

with large homogenous zones (*Lenna*, *MosqueLight*, *BinWidane*, *Ifrane*, *Thorax*, *Anonymized*).

For the removal attacks and specially noise attacks where the noise is dominant in image high frequencies, in other word, details that repeat frequently in a small amount of pixels like edges. We found that NC values for the extracted watermark of the images with high frequencies are lower than images with homogenous zones and lower frequency component with $NC = 0.9732$ for the image *Girl* against *salt&pepper* noise attack, $NC = 0.9725$ for the image *Hats*, $NC = 0.9749$ for the image *Lighthouse*. While the extracted watermark NC value for the image *MosqueLight* is $NC = 0.9958$, $NC = 0.9958$ for the images *BinWidane* and *Ifrane* against the same attack.

In the second category that includes large homogenous zones images, there are images from our personal data base and images from the medical data base DICOM. We noticed that NC values of the extracted watermark from the medical watermarked images are lower than NC value of the extracted watermark from the personal watermarked image because even if they both have homogenous areas, the medical images have clearer high frequencies than the personal images (sudden change in the black background and gray color of scanned thorax and the body of the Anonymized image). This is due to the use of the *LL* sub-band which contains low frequencies. Thus, embedding in the *LL* sub-band is more robust against the removal attack since it has the most of the image energy and details. This explains the difference of the NC value of the extracted watermark from the watermarked images with high and low frequency components.

When embedding, the eigenvectors U_I and V_I of the original watermark are saved as secret key in order to be used for extraction. Those eigenvectors contain the detail information of the watermark and are used to reconstruct the extracted watermark. Hence, even after applying the geometric attacks, the extracted watermark still similar to the original for all the watermarked images and their NC values are close to 1.

4.2.2 Comparison with other schemes

In order to evaluate the performance of the proposed algorithm, the obtained results are compared with those presented in [4, 6]. Their main features are described in Table 6.

Table 6 The main characteristics of presented schemes in [4, 6] and the proposed one

Description	[4] (2013)	[6] (2016)	Proposed
Scheme type	Non-blind	Semi-blind	Semi-blind
Used domain	DWT-SVD	IWT-SVD	DWT-SVD
Embedding mode	Static	Static	Dynamic/Random
Original image color	Gray level	Gray level	RGB
Original image size	512 × 512	512 × 512	Variant
Watermark size	64 × 64	256 × 256	32 × 32
False positive detection	No	No	No
Scaling factor	Optimized by DE	Optimized by ABC	Adaptive with JND

All the methods described in Table 6 use a hybrid technique combining between DWT and SVD or IWT (Integer Wavelet Transform) and SVD. But embedding the watermark is done in static way. While in the proposed scheme, the watermarking is dynamic by using a random embedding position for every execution. In Table 7, the NC values of the extracted watermark against the attacks presented in Table 4 for the image ‘Lenna’. The purpose of using ‘Lenna’ is that it has mixed features of high contrast, textured areas and change of the frequency components in its hat area. For these reasons, the image ‘Lenna’ is very used in the image processing studies.

In [4], Ali embedded the watermark in the *LL* and *HH* sub-bands of the 3 level DWT applied on the original image. While in [6], Ansari used 1 level of IWT to embed the watermark in *LL* and *LH* sub-bands. To embed in the image high frequencies (*HH* sub-band) makes the watermark invisible but less robust against the removal attacks and can be removed easily. Thus, in our method, the watermark is embedded by modifying the singular values of the *LL* sub-band known by its energy compact which makes the watermarking scheme robust against attack and imperceptible. Beside, a small alteration in singular values does not perturb the visual quality of the watermarked image. So, the robustness is proved by the NC values: 0.9851, 0.9866, 0.9850 and 0.9900 for attacks: salt & pepper noise, Gaussian filter, contrast adjustment and sharpening respectively. The same results for geometric attacks where the NC values of the proposed scheme exceed 0.9 with slight difference compared with the other methods. This difference is due to the dynamic watermarking where watermark is embedded in a random block of the *LL* sub-band. This explains why some NC values of the other methods are higher than ours, because embedding every time in a different position with different coefficients does not give always the

Table 7 The NC value of the extracted watermark form the image ‘Lenna’ against different attacks

Attack/Scheme	[4] (2013)	[6] (2016)	Proposed
SP	No	0.9989	0.9401
GB	0.9805	0.9446	0.9851
GF	No	No	0.9866
RO	0.9922	0.9881	0.9750
CA	No	0.9797	0.9850
JPG	0.9961	0.9996	0.9866
RS	0.9996	0.9885	0.9833
SH	No	0.9481	0.9900

same results and the same NC values of the extracted watermark. However, all NC values are close to 1 and the extracted watermark is recognizable even against attacks. Let's clarify that in [4, 6], the test images are gray scale level images, while the image test in our algorithm are RGB 24 byte/pixel and are converted to YCbCr color space. Hence, some information loss is mandatory while converting back to the original color space to reconstruct the watermarked image.

4.2.3 Multiple attacks experiments

Multiples attacks are applied on the watermarked images (one image from each database). It is very important to experiment multiples attacks since pirates always try to use them in order to detect the watermark. The results are shown in Table 8.

According to Table 8, when the noise attacks are combined with other type of attack, the PSNR values of the watermarked image are low. This is because the noise attacks aim at changing the black and white pixels, luminance and chrominance of the image causing visible alterations for the watermarked images. For example the PSNR value for 'Lenna' is 16.6836db when combining Gaussian noise and JPG compression (GN + JPG). The same low PSNR value for the multiple attacks (SP + CA + JPG) that combine between Salt & pepper noise, contrast adjustment and JPG compression. However, it does not affect the algorithm robustness for extracting the watermark since NC values are higher than 0.7, with: 0.9633 for *Lenna*, 0.9332 for *GIRL*, 0.9082 for *Door* and 0.9766 for *Thorax* against the GN + JPG attack.









For attack that combines between sharpening and Gaussian filter (SH + GF), both of them tend to improve the image quality, this why it is noticed that the PSNR value are higher than 30db. Therefore the visual disturbs of the watermarked images are more or less invisible. Beside, the NC values of the extracted watermark against the same multiple attack (SH + GF) are 1 for *Lenna*, 0.9449 for *Girl*, 0.9232 for *Door* and 0.9950 for *Thorax*.

All the experimental results discussed above prove that the novel proposed approach based on DWT and SVD is robust even with the dynamic embedding. Due to the multi-resolution of the DWT and its energy concentration in the approximation coefficients combining with SVD known by geometric attacks invariance and singular values stability. In addition, the original watermark eigenvectors are very useful to reform the extracted watermark since they preserve the most of watermark details.

Table 8 PSNR and NC values after multiple attacks (GN Gaussian Noise [50], JPG compression JPEG [55], RS resizing $\frac{1}{2}$ [50], SH Sharpening [50], GF Gaussian Filter [50], SP Salt & pepper Noise [55], Contrast Adjustment [50])

Attaques	PSNR				NC			
	Lena	Girl	Door	Thorax	Lena	Girl	Door	Thorax
GN + JPG	16.6836	17.5092	16.4229	17.1428	0.9633	0.9332	0.9082	0.9766
RS + JPG	32.2582	29.8868	33.2229	31.6889	0.9816	0.9449	0.9098	0.9633
SH + GF	32.8717	33.5560	34.9273	35.4620	1	0.9449	0.9232	0.9950
GN + GF + JPG	15.4525	16.1778	15.1660	16.4447	0.9800	0.9315	0.9115	0.9699
SP + CA + JPG	19.2686	15.7826	19.2719	14.5851	0.8798	0.8998	0.7379	0.9616

Table 9 Extracted watermark according to different keys availability

RSA private key	True	True	True	True	False	False	False	False
AES private key	True	True	False	False	True	True	False	False
Secret key used for random block selection	True	False	True	False	True	False	True	False
Extracted watermark								

4.3 Security experiments

In this section, we will experiment the ownership of different private keys used in this algorithm for extracting the watermark in order to evaluate its security. The results are presented in Table 9.

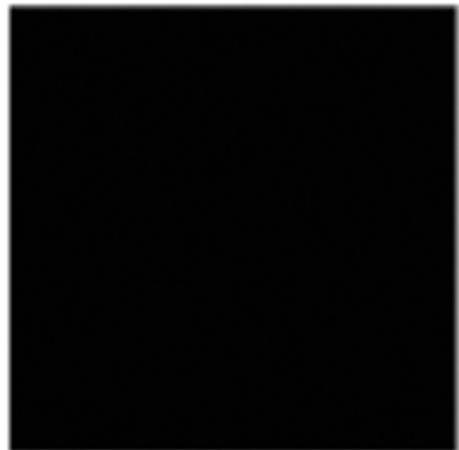
As shown in Table 9, the extracted watermark can not be detected and extracted without using the appropriate encryption keys and the same secret key to select the extracting block.

4.4 False positive detection

The false positive error is detected when a wrong watermark (which has never been embedded) is extracted.

Let's suppose that a pirate could find the RSA and AES private keys used for extraction, and he wants to modify the U_{IW} and V_{IW} by his eigenvectors in order to get his own watermark. Before getting to the extraction process, a verification test is performed computing the correlation between the secret saved information and those sent to the user for extraction. If the correlation value is higher than a predefined threshold then continue the extraction process otherwise, the program will stop and displays a black image as illustrated in Fig. 6. In this case, the predefined threshold value is $T = 0.9$ since the necessary information needed for extraction can go through

Fig. 6 Displayed image after a failed verification test



some small modifications during their transfer (Otherwise the threshold value should equal 1). Thus, the proposed method ensures the user authentication and avoids the detection false positive error, so the pirate will get a black image if he tried to extract a wrong watermark.

5 Conclusion

The novelty in this paper is the use of a random embedding position for watermarking based on HSV model in order to choose an adaptive scaling factor. The original watermark is resized according to block size used for each image and encrypted using AES algorithm in order to improve its security. The RSA algorithm is used to encrypt all the private and secret keys used in this scheme. The watermarked images have a very good quality and the extracted watermark is robust against different attacks and similar to the original one, thanks to the hybrid combination between DWT and SVD. However, the SVD is known by the false positive error detection by changing the original eigenvectors by those of the pirate. Thus, in our proposed method, a verification test is performed in extraction phase in order to ensure the user authentication and identity and avoid the false positive error. In our future work, we will focus on a dynamic watermarking for color watermarks and experiment the random move of the embedded watermark for the sender and the recipient.

References

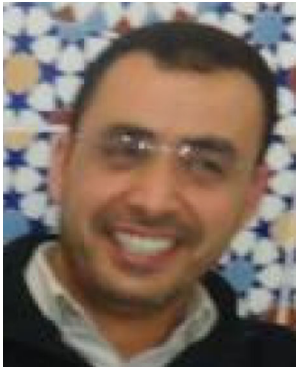
1. Acharya R, Niranjan UC, Iyengar SS, Kannathal N, Min LC (2004) Simultaneous storage of patient information with medical images in the frequency domain. *Comput Methods Prog Biomed* 76(1):13–19
2. Agreste S, Andaloro G, Prestipino D, Puccio L (2007) An image adaptive, wavelet-based watermarking of digital images. *J Comput Appl Math* 210(1):13–21
3. Ali M, Ahn CW, Pant M (2014) A robust image watermarking technique using SVD and differential evolution in DCT domain. *Optik-International Journal for Light and Electron Optics* 125(1):428–434
4. Ali M, Ahn CW, Siarry P (2014) Differential evolution algorithm for the selection of optimal scaling factors in image watermarking. *Eng Appl Artif Intell* 31:15–26
5. Ali M, Ahn CW, Pant M, Siarry P (2015) An image watermarking scheme in wavelet domain with optimized compensation of singular value decomposition via artificial bee colony. *Inf Sci* 301:44–60
6. Ansari IA, Pant M, Ahn CW (2016) Robust and false positive free watermarking in IWT domain using SVD and ABC. *Eng Appl Artif Intell* 49:114–125
7. Baker K (2013) Singular Value Decomposition Tutorial
8. Barni M, Bartolini F, Piva A (2001) Improved wavelet-based watermarking through pixel-wise masking. *Image Processing, IEEE Transactions on* 10(5):783–791
9. Bas P, Chassery JM, Macq B (2002) Geometrically invariant watermarking using feature points. *IEEE Trans Image Process* 11(9):1014–1028
10. Bhatnagar G, Raman B (2009) A new robust reference watermarking scheme based on DWT-SVD. *Computer Standards & Interfaces* 31(5):1002–1013
11. Bouslimi D, Coatrieux G (2015) Encryption and Watermarking for medical Image Protection. In *Medical Data Privacy Handbook (pp. 493–526)*. Springer International Publishing
12. Chen CC, Tsai YH, Yeh HC (2016) Difference-expansion based reversible and visible image watermarking scheme. *Multimedia Tools and Applications*, 1–20
13. Cox JJ, Kilian J, Leighton FT, Shamoon T (1997) Secure spread spectrum watermarking for multimedia. *IEEE Trans Image Process* 6(12):1673–1687

14. Daemen J, Rijmen V (2002) The design of Rijndael. Information security and cryptography. Text and Monographs, Springer Verlag
15. Das C, Panigrahi S, Sharma VK, Mahapatra KK (2014) A novel blind robust image watermarking in DCT domain using inter-block coefficient correlation. *AEU - Int J Electron Communicat* 68(3):244–253
16. Dicom Viwer Database: www.dicomlibrary.com
17. Fisher Ronald Aylmer, Yates Frank (1949) Statistical tables for biological, agricultural and medical research. Ed. 3
18. Ford A, Robert A, (1998) Color Space Conversions
19. Gan J, Zhang Y (2003) A study of singular value decomposition of face image matrix. In *Neural Networks and Signal Processing, 2003. Proceedings of the 2003 International Conference on* (Vol. 1, pp. 197–199). IEEE
20. Golea NEH, Seghir R, Benzyd R (2010). A blind RGB color image watermarking based on singular value decomposition. In *Computer Systems and Applications (AICCSA), 2010 IEEE/ACS International Conference on* (pp. 1–5). IEEE
21. Grettillat J-D (2006) Modification de l'algorithme de la décomposition en ondelettes discrète pour l'obtention d'une représentation invariante sous rotation
22. Gupta AK, Raval MS (2012) A robust and secure watermarking scheme based on singular values replacement. *Sadhana* 37(4):425–440
23. Hu HT, Hsu LY (2016) Collective blind image watermarking in DWT-DCT domain with adaptive embedding strength governed by quality metrics. *Multimedia Tools and Applications*, 1–20
24. Huynh-Thu Q, Ghanbari M (2008) Scope of validity of PSNR in image/video quality assessment. *Electron Lett* 44(13):800–801
25. Jia SL (2014) A novel blind color images watermarking based on SVD. *Optik-International Journal for Light and Electron Optics* 125(12):2868–2874
26. Kalra GS, Talwar R, Sadawarti H et al. (2014) Adaptive digital image watermarking for color images in frequency domain. *Multimed Tools Appl*:1–21
27. Kamran AK, Malik SA (2014) A high capacity reversible watermarking approach for authenticating images: exploiting down-sampling, histogram processing, and block selection. *Inf Sci* 256:162–183
28. Khalili M, Asatryan D (2013) Colour spaces effects on improved discrete wavelet transform-based digital image watermarking using Arnold transform map. *Signal Processing, IET* 7(3):177–187
29. Kodak database: <http://r0k.us/graphics/kodak/>
30. Kumari GRN, Jeeru SS, Maruthuperumal S. (2014) Color Image Watermarking Using Wavelet Transform Based on HVS Channel. In *ICT and Critical Infrastructure: Proceedings of the 48th Annual Convention of Computer Society of India-Vol I* (pp. 59–67). Springer International Publishing
31. Lang J, Zhang ZG (2014) Blind digital watermarking method in the fractional Fourier transform domain. *Opt Lasers Eng* 53:112–121
32. Li Q, Yuan C, Zhong YZ (2007) Adaptive DWT-SVD domain image watermarking using human visual model. In *Advanced Communication Technology, The 9th International Conference on* (Vol. 3, pp. 1947–1951). IEEE
33. Li J, Li X, Yang B, Sun X (2015) Segmentation-based image copy-move forgery detection scheme. *IEEE Trans Inf Forensics and Secur* 10(3):507–518
34. Li C, Yang R, Liu Z, Li J, Guo Z (2016) Semi-fragile self-recoverable watermarking scheme for face image protection. *Comput Electr Eng* 54:484–493
35. Liu F, Qian Y (2011) A Novel Robust Watermarking Algorithm Based On Two_Levels DCT and Two_Levels SVD. In *2011 Third International Conference on Measuring Technology and Mechatronics Automation* (Vol. 1, pp. 206–209). IEEE
36. Lou DC, Chou CL, Tso HK, Chiu CC (2012) Active steganalysis for histogram-shifting based reversible data hiding. *Opt Commun* 285:2510–2518
37. Loukhaoukha K, Chouinard JY, Taieb MH (2011) Optimal image watermarking algorithm based on LWT-SVD via multi-objective ant colony optimization. *Journal of Information Hiding and Multimedia Signal Processing* 2(4):303–319
38. Lusson F, Bailey K, Leeney M, Curran K (2013) A novel approach to digital watermarking, exploiting colour spaces. *Signal Process* 93(5):1268–1294
39. Mallat S (1999) A wavelet tour of signal processing. Academic press
40. Mishra A, Agarwal C, Sharma A, Bedi P (2014) Optimized gray-scale image watermarking using DWT-SVD and firefly algorithm. *Expert Syst Appl* 41(17):7858–7867
41. Munib S, Khan A (2017) Robust image watermarking technique using triangular regions and Zernike moments for quantization based embedding. *Multimed Tools Appl* 76(6):8695–8710

42. Naderahmadian Y, Hosseini-Khayat S (2014) Fast and robust watermarking in still images based on QR decomposition. *Multimed Tools Appl* 72(3):2597–2618
43. Pakdaman Z, Saryazdi S, Nezamabadi-pour H (2017) A prediction based reversible image watermarking in Hadamard domain. *Multimed Tools Appl* 76(6):8517–8545
44. Raghavender Ra Y, Prathapani Nikhil, Nagabhooshanam E (2014). Application of normalized cross correlation to image registration. *International Journal of Research in Engineering and Technology IJERT*, vol 4
45. Roy A, Maiti AK, Ghosh K (2015) A perception based color image adaptive watermarking scheme in YCbCr space. In *Signal Processing and Integrated Networks (SPIN), 2015 2nd International Conference on* (pp. 537–543). IEEE
46. Shi H, Lv F, Cao Y (2014) A blind watermarking technique for color image based on SVD with circulation. *J Softw* 9(7):1749–1756
47. Singh AK (2016) Improved hybrid algorithm for robust and imperceptible multiple watermarking using digital images. *Multimedia Tools and Applications*, 1–18
48. Singh RK, Shaw DK, Alam MJ (2015) Experimental studies of LSB watermarking with different noise. *Procedia Computer Science* 54:612–620
49. SIPI database: <http://sipi.usc.edu/database/>
50. Song C, Sudirman S, Merabti M, Llewellyn-Jones D (2010) Analysis of digital image watermark attacks. In *2010 7th IEEE Consumer Communications and Networking Conference* (pp. 1–5). IEEE
51. Su Q, Niu Y, Liu X, Zhu Y (2012) Embedding color watermarks in color images based on Schur decomposition. *Opt Commun* 285(7):1792–1802
52. Su Q, Niu Y, Liu X, Yao T (2013) A novel blind digital watermarking algorithm for embedding color image into color image. *Optik-International Journal for Light and Electron Optics* 124(18):3254–3259
53. Su Q, Niu Y, Wang G, Jia S, Yue J (2014) Color image blind watermarking scheme based on QR decomposition. *Signal Process* 94:219–235
54. Su Q, Wang G, Jia S, Zhang X, Liu Q, Liu X (2015) Embedding color image watermark in color image based on two-level DCT. *SIViP* 9(5):991–1007
55. Subramanyam AV, Emmanuel S (2011) Robust watermarking of compressed JPEG images in encrypted domain. In *Transactions on data hiding and multimedia security VI* (pp. 37–57). Springer Berlin Heidelberg
56. Sun G, Yu Y (2007) DWT based watermarking algorithm of color images. In *Industrial Electronics and Applications, 2007. ICIEA 2007. 2nd IEEE Conference on* (pp. 1823–1826). IEEE
57. Tirkel AZ, Rankin GA, Van Schyndel RM, Ho WJ, Mee NRA, Osborne CF (1993) *Electronic Water Mark. DICTA*, Macquarie University. p. 666–673
58. Tsai DM, Lin CT (2003) Fast normalized cross correlation for defect detection. *Pattern Recogn Lett* 24(15):2625–2631
59. Tsui TK, Zhang X-P, Androutsos D (2008) Color image watermarking using multidimensional fourier transforms. *IEEE Trans Inform Forensics Security* 3(1):16–28
60. Vahedi E, Zoroofi RA, Shiva M (2007) On optimal parameter selection for multiresolution based image watermarking. In *Intelligent and Advanced Systems, 2007. ICIAS 2007. International Conference on* (pp. 641–646). IEEE
61. Vahedi E, Zoroofi RA, Shiva M (2012) Toward a new wavelet-based watermarking approach for color images using bio-inspired optimization principles. *Digital Signal Process* 22(1):153–162
62. Verma AK, Patvardhan C, Lakshmi CV (2012) Robust color image watermarking scheme using JFIF-YCbCr color space in wavelet domain. In *Wireless Networks and Computational Intelligence* (pp. 187–192). Springer Berlin Heidelberg
63. Wang YR, Lin WH, Yang L (2011) An intelligent watermarking method based on particle swarm optimization. *Expert Syst Appl* 38(7):8024–8029
64. Yadav N, Singh K (2015) Robust image-adaptive watermarking using an adjustable dynamic strength factor. *SIViP* 9(7):1531–1542
65. Yang CT, Chu WC, Huang HN, Chen ST, Chen DF, Lin CC, Chang CH (2015) Optimizing PSNR for Image Watermarking Using Summation Quantization on DWT Coefficients. In *Computer Software and Applications Conference (COMPSAC), 2015 I.E. 39th Annual (Vol. 1, pp. 68–74)*. IEEE
66. Zhao X, Luo H, Lu ZM, Pan JS (2011) Reversible data hiding based on multilevel histogram modification and sequential recovery. *Int J Electron Commun* 65:814–826
67. Zheng Y, Jeon B, Xu D, Wu QM, Zhang H (2015) Image segmentation by generalized hierarchical fuzzy C-means algorithm. *J Intell Fuzzy Syst* 28(2):961–973
68. Zhou X, Tang X (2011) Research and implementation of RSA algorithm for encryption and decryption. In *Strategic Technology (IFOST), 2011 6th International Forum on* (Vol. 2, pp. 1118–1121). IEEE



Youssra Lakrissi obtained her MS degree from Faculty of Sciences and Technologies, University Sultan Moulay Slimane, Morocco in 2013. Currently, she is a PhD student in Computer sciences at Sidi Mohammed Ben Abdellah University, Fez, Morocco. Her research interests include image watermarking and information security.



Abderrahim Saaidi received the PhD degree from SMBA-Fez University in 2010. He is currently a professor of computer sciences at SMBA-Taza University. He is member of the LIHAN and LSI Laboratories. His research interests include camera self-calibration, image mosaicing, image matching, 3D reconstruction, people tracking, face recognition, image encryption, image watermarking and real-time rendering.



Abdelouahed Essahlaoui is a professor at Sidi Mohamed Ben Abdellah University since 2003. He is a master degree in electronic from university of Meknes (Morocco) in 1997 and a deeper study diploma from university of Metz (France) in 1998. He received his Ph.D in optoelectronic at university of Metz in 2002. His current research interests include cryptography, watermarking and E-learning security.