Multimedia Tools and Applications (2021) 80:13975–13999
https://doi.org/10.1007/s11042-020-10397-4

An improved watermarking scheme for color image using alpha blending

Sanjay Kumar[1] · **Binod Kumar Singh**[1]

Received: 8 May 2020 / Revised: 14 September 2020 / Accepted: 22 December 2020 /
Published online: 20 January 2021

Abstract
This paper proposes a robust and secure watermarking method for a color image in YC_bC_r color space. In this study, watermarking is performed using Lifting Wavelet Transform (LWT). Here, edge entropy and information entropy is used to find the block to embed watermark. In this work alpha blending scheme is used for embedding and extraction of watermarks in the LWT domain. The use of LWT makes the proposed scheme faster and more efficient. The Arnold Cat Map (ACM) is used to enhance watermark security. Numerous tests are presented to illustrate the feasibility of the proposed scheme. The experimental results obtained are compared to state-of-the-art schemes, which demonstrate the superiority of the proposed scheme.

Keywords Watermark · Entropy · Color image · LWT · Arnold cat map

1 Introduction

1.1 Motivation

The advent of computer networks and the Internet has made digital media production and distribution (e.g. audio, video, image, etc.) quite easy these days [16, 17, 33]. Because of this, authentication and copyright protection of digital media has became a prime concern. To address this issue, digital watermarking can be used [1, 10, 20]. Digital watermarking is the procedure by which the signal (watermark) is embedded into the cover signal. Digital watermarking include two main phases: watermark embedding and watermark extraction [15, 16]. The watermarking scheme can be divided into two classes: spatial domain and frequency domain[17, 34, 36]. Various transform domain-based techniques, such as Discrete Wavelet Transform (DWT), Singular Value Decomposition (SVD), Discrete Cosine

✉ Sanjay Kumar
2017rscs001@nitjsr.ac.in

Binod Kumar Singh
bksingh.cse@nitjsr.ac.in

[1] Computer Science & Engineering, National Institute of Technology Jamshedpur, Jamshedpur, India

Transform (DCT), and Lifting Wavelet Transform (LWT) etc. are used. In comparison with traditional wavelet transform LWT is faster and more effective [13, 34]. The frequency domain is more robust but spatial domain schemes are simpler to implement [6, 23]. One of the key issues about digital image watermarking techniques is the security of a watermark. The appropriate encryption of the watermark is thus necessary in the watermarking system [21, 26].

There is always a trade-off between the features of watermarking [17]. Robustness, imperceptibility security, and complexity are the four major features of the watermarking scheme. Watermarking scheme must have to satisfy two opposing properties of robustness and transparency. To balance these two properties selection of block to embed watermark embedding plays a vital role [25]. Alpha blending techniques can also be used to address this trade-off. [9]. It can be used to incorporate invisible watermarks into the image's salient characteristics. Alpha blending scheme is resilient against the attacks and provides high protection [2, 4, 5]. Frequency domain methods are helpful in locating the watermark embedding region which ensures the watermarking scheme is more robust. The traditional wavelet transform has high computational and memory requirements using convolution-based implementation. Lifting wavelet transform has been designed to address these disadvantages. LWT provides strong efficiency in digital watermarking as opposed to conventional wavelet transform [34]. To ensure robustness against the number of attacks, YC_bC_r color space is used for watermarking. YC_bC_r channel is also desirable for watermarking, as it closely models the HVS [27].

1.2 Literature review

Various works have been done in the watermarking to date. In recent years, researchers have studied to improve the color image watermarking scheme. In this section, some of them are briefly discussed.

Kang et al. [12] has proposed a secure and robust color image watermarking scheme. Here, to create the zero watermark, the proposed scheme uses Frobenius norm in the DWT-SVD domain and majority voting. Experimental results shows that this scheme is not robust against the geometric attacks. Pandey et al. [26] proposed a stable hybrid lossless, reliable color watermarking technique lifting method and GWO. In addition, scrambling of the watermark was also achieved by using Arnold transform to improve security and robustness. Robustness of this scheme is comparatively very poor in comparison with other color image watermarking schemes.

For authentication using LWT and SVD, Kejgir et al. [13] has proposed a color image watermarking. Using LWT transform, the cover image is decomposed, and the watermark is inserted into LL subband. Moreover, false positive problem is its main drawback as embedding is carried out in singular component. Liu et al. [20] present a blind color image watermarking based on Schur's decomposition. In this scheme, color watermark is used for the embedding while affine transform was used to encrypt the watermark. Moreover, both imperceptibility and robustness of this scheme is low.

Wang et al. [38] based on the Fuzzy Least Square Support Vector Machine (FLS-SVM) and Bessel K (BKF) distribution have proposed a robust color image watermarking method. Bessel K's shape parameter and scale parameter is used as a function vector to train the model. In [30] a hybrid robust watermarking scheme based on is proposed. Here, watermarking is carried out in Y component of YC_bC_r color space.

Vaidya et al. [36] suggested a robust and semi-blind watermarking method for color images. Arnold Transform was used to encrypt the watermark author. Although, this scheme is robust against different attacks but gives poor imperceptibility. Koley [14] suggests watermarking of color images in the LWT domain using $\alpha - \beta$ blending. The technique infuses the watermark with the factors 'α' and 'β' according to the PC feature map by changing the diagonal information coefficients of the cover image. Experimental results shows that this techniques is not robust against JPEG compression attack.

Chowdhury et al. [3] proposes a blind symmetric watermarking approach in both canonical and cepstrum domains. Using the four-connected t-o'clock process, the security fiber mark is scrambled. Roy et al. [31] have suggested a non-blind, hybrid watermarking technique based on DWT and SVD. Here, component Y is chosen for embedding the watermark. In [28] using Walsh Hadamard Transform (WHT), a color image watermarking scheme is presented. To encrypt watermark 2D-Logistic Sine Coupling Map encryption scheme is used.

Hu et al. [11] developed an SVD-based watermarking scheme which implements mixed modulation to ensure successful extraction of watermarks. For watermarking the color watermark is used here. In [29] DCT based color image watermarking technique is proposed. Here, binary watermark is inserted in Blue and green component of RGB color space. In this scheme computational cost is high. A blind hybrid domain watermarking scheme for color image is proposed in [35], however, the security of this scheme is needed to analyze.

Wang et al. [39] propose a novel blind color image watermarking scheme in DCT domain based on JND. In contrast masking effect, the diversity of orientation between the various blocks is further considered. Laur et al. [19] proposed a watermarking scheme using entropy for imperceptible and robust color image watermarking. Chirp z-transform, orthogonal-triangular decomposition, and SVD are used to embed a watermark in color image DWT. In [8] DFT based color image watermarking is proposed. Here, random sequence are used as a watermark. From its results it can been observed that this techniques is relatively less robust than other frequency domain scheme like DWT, DCT, SVD etc.

Over the past few decades, watermarking methods has come out as authentic method for authentication of data and copyright protection. The literature of watermarking reveals that there is always a trade-off between the various features of watermarking. It is very challenging for research to address these trade-off. Also, to develop a watermarking scheme which is robust against all attacks is very challenging . Wavelet based watermarking technique is comparatively more robust than other frequency domain watermarking techniques. Moreover, in comparison with traditional wavelet transform LWT is computationally efficient. In this work, watermarking is carried out in the Y component of YC_bC_r color space. The proposed method involves LWT, entropy, ACM, and alpha blending techniques.

1.3 Contributions and organization

The main objective of this paper is to develop a watermarking scheme which can address the trade-off between the various features of watermarking.

The main contributions to this work can be summarized as follows:

1) A robust and secure color image watermarking using LWT in YC_bC_r color space is proposed in this work.
2) Block is selected adaptively for watermark insertion in the Y component of the cover image using the visual entropy and the edge entropy.

3) Alpha blending technique is used to balance the trade-offs between imperceptibility and robustness of the watermarking techniques.
4) For better robustness and less computation time LWT domain is used for watermarking, whereas Arnold's Cat Map is used to enhance the security of watermarking technique.

The rest of the paper is structured as follows. The preliminaries of LWT, ACM, and Image entropy are discussed in Section 2. Section 3 describes the proposed scheme and examines the experimental result in Section 4. The conclusion is drawn up in Section 5.

2 Background

2.1 Lifting wavelet transform

W. Sweldens proposed an advancement of DWT called Lifting Wavelet Transform. In the lifting wavelet transformation, sampling up and down is simply replaced by splitting and merge into each of the stages [13]. LWT split down the images in four sub-bands [14]. The forward and the reverse LWT are shown in Figs. 1 and 2 correspondingly. In general, the lifting scheme consists of three steps: Divide, Dual lifting, and Primal lift [32].

Divide: Here the original signal A(i, j) is split into two samples: even sample $A_e(i, j)$ and odd samples $A_o(i, j)$ and is represented by (1) and (2) respectively.

$$A_e(i, j) = A(i, 2j) \tag{1}$$

$$A_o(i, j) = A(i, 2j + 1) \tag{2}$$

Dual Lifting (Predict): We can view this step as a high-pass filtering process. Here, even samples are used to predict odd samples, and the abstract difference is produced as follows:

$$a(i, j) = A_o(i, j) - P[A_e(i, j)] \tag{3}$$

where P[.] is the predict operator.

Primal Lifting (Update): TThis wavelet lifting step can be viewed as a low-pass filtering procedure. The a_l(i,j) low frequency part is a coarse approximation to the original signal A(i, j), and this is done by applying U[.] as follows:

$$a_l(i, j) = A_e(i, j) - U[a(i, j)] \tag{4}$$

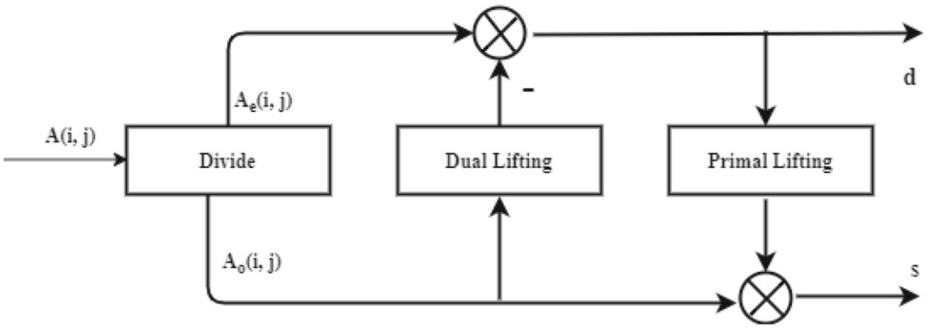

Fig. 1 Block diagram of forward lifting

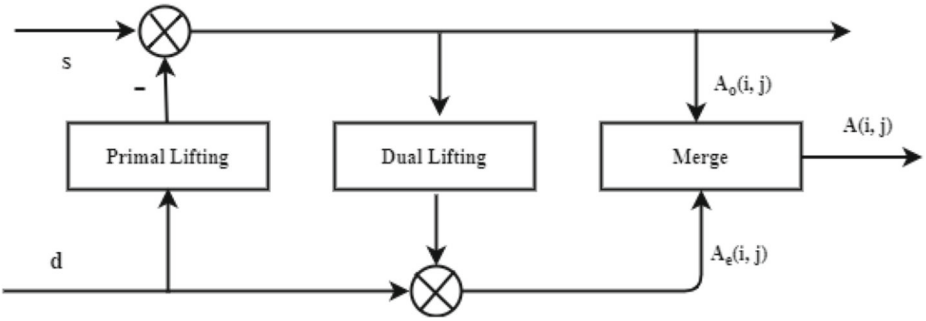

Fig. 2 Block diagram of reverse lifting

2.2 Arnold cat map

ACM also known as Arnold Transform is a form of chaotic encryption which can give watermark security [36]. This encryption technique named after Vladimir I. Arnold. Substantially ACM shears image by a factor of 1 in both vertical and horizontal directions. Further, folds the image collected back to itself [14]. Since ACM retains the size of the watermark even after encryption, this means that the encryption process does not affect the ability of the payload. ACM can be denoted as:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \mod N \tag{5}$$

where N is order of image matrix and (x_n, y_n) and (x_{n+1}, y_{n+1}) represents the pixel value before and after scrambling. Figure 3 illustrate the original watermark and the encrypted watermark image for various iterations of ACM.

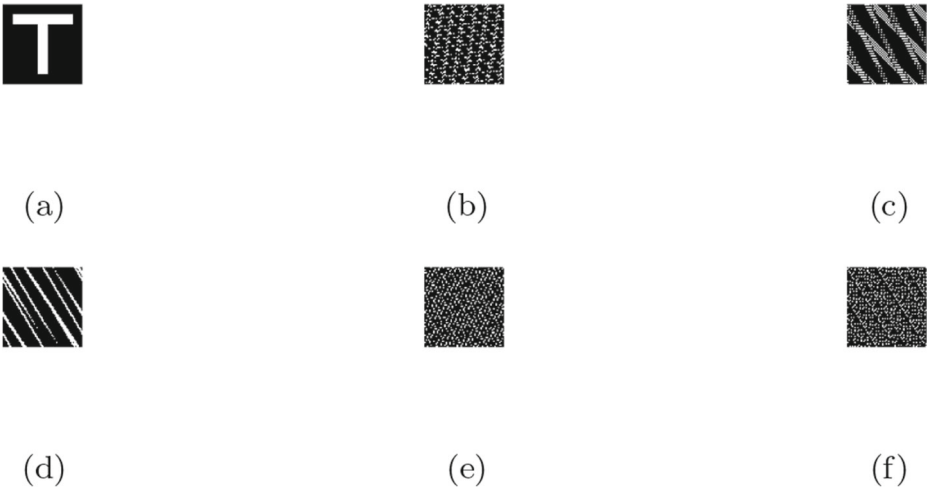

Fig. 3 **a** Original grayscale watermark **b** Encrypted watermark for 10 iterations **c** Encrypted watermark for 25 iterations **d** Encrypted watermark for 50 iterations **e** Encrypted watermark for 75 iterations **f** Encrypted watermark for 100 iterations

2.3 Image entropy

The concept of entropy can be extended to two classes: Visual entropy and edge entropy [7, 22, 23]. Visual entropy and edge entropy consider human visual characteristics. Therefore, it offers the most important host image region for embedding a watermark [6]. Entropy is a proper indicator of adjacent pixel spatial correlation. An image's visual entropy is described as

$$E_v = -\sum_{i=1}^{L-1} p_i \log p_i \tag{6}$$

Edge entropy is an exponential type of entropy capable of holding the image in two dimensional spatial correlations. The edge entropy gives more information about pixels dispersion and edges of the images. Edge entropy or average edge information can be defined as

$$E_e = \sum_{i=1}^{L-1} p_i e^{1-p_i} \tag{7}$$

Here 'p_i' represents the occurrence probability of event i and '1-p_i' represents the uncertainty of the pixel value i.

3 Proposed techniques

In this section, an improved color watermarking techniques in the LWT domain is presented. Here, block block is selected using visual entropy and edge entropy to embed watermark. The block having the optimal entropy value B_E is selected to embed the watermark. The optimal entropy value is calculated using (8). The proposed technique is classified into the following two stages: watermark embedding and watermark extraction. Figures 4 and 5 shows the overview of the watermark embedding and the watermark extraction process respectively. In the embedding process, ACM image scrambling is used to improve robustness and security. Whereas, its inverse transformation is used in the process of extraction. In the proposed scheme we have taken 50 iterations to encrypt the watermark.

$$B_E = max(E_v - E_e) \tag{8}$$

3.1 Watermark embedding

In this work, watermark embedding is carried out in the Y component of YC_bC_r color space using LWT. Here, cover image is transformed into YC_bC_r color space from RGB color space. Y component is selected and first level of LWT is applied over it. Y component is selected because in comparison of C_b and C_r, inserting watermark in Y components yields better robustness. Further, Y component is divided into non overlapping block of size 32×32. To embed watermark, block in HH component of cover image (Y component) is selected adaptively using visual entropy and edge entropy. A grayscale watermark of size 64×64 is taken and is encrypted using ACM to enhance the security of watermark.

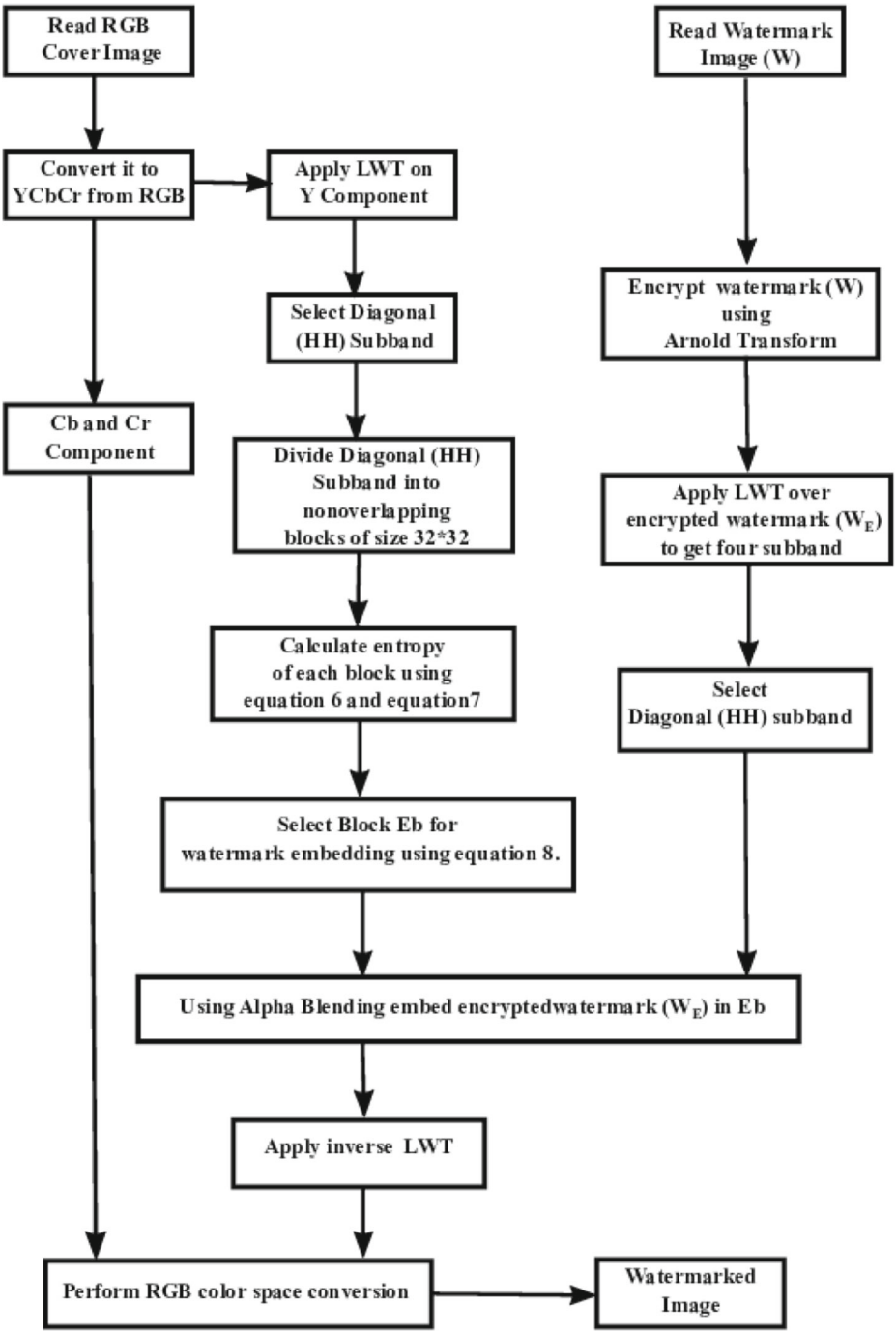

Fig. 4 Watermark embedding process

First level of LWT is applied over the encrypted watermark. Further, using alpha blending technique HH component of watermark is embedded into the selected block of cover image. To balance the trade-off between robustness and imperceptibility alpha blending technique is used. The steps of proposed color image watermark embedding scheme is discussed in Algorithm 1.

Algorithm 1 Pseudo- Code for Watermark Embedding Algorithm.

Input: Color Cover Image , Watermark, Key
Output: Watermarked Image
1. Read the RGB Color Cover Image (X_{RGB}) of size $m_1 \times n_1$.
2. Transform X_{RGB} into YC_bC_r color space. Converted X_{RGB} from RGB to YC_bC_r color space and separate it into three channels Y, C_b and C_r . The Y, C_b and C_r channel of Cover image is represented by X_Y, X_{Cb}, and X_{Cr} respectively.
[X_Y, X_{Cb}, and X_{Cr}] = $YC_bC_rConversion(X_{RGB})$
3. Select Y channel and apply LWT transform. One level of LWT transform is applied over it to get approximation Ψ_Y^A(x,y), horizontal Ψ_Y^H (x,y), vertical Ψ_Y^V (x,y) and diagonal Ψ_Y^D (x,y) components .
[Ψ_Y^A (x,y), Ψ_Y^H (x,y), Ψ_Y^V (x,y), Ψ_Y^D (x,y)] = LWT (X_Y)
4. Divide Diagonal component Ψ_Y^D (x,y) into non-overlapping block and of size 32×32 and calculate the visual entropy and edge entropy of all non overlapping block using (6) and (7) respectively.
5. Select the block (B_E) having optimal entropy value to insert the watermark using (8) .
6. Read a grayscale watermark 'W' of size $m_2 \times n_2$. To increase the security of watermark encrypt the watermark using ACM.
W_E = Arnold Cat Map(W)
7. On encrypted watermark (W_E) apply one level of LWT is applied to get get approximation W_E^A(x,y), horizontal W_E^H (x,y), vertical W_E^V (x,y) and diagonal W_E^D (x,y) components .
[W_E^A (x,y), W_E^H (x,y), W_E^V (x,y), W_E^D (x,y)] = LWT (W_E)
8. Embed the diagonal component of encrypted watermark (W_E^D) in block (B_E) using sing (9).

$$WM^D(x, y) = (\alpha \times B_E(x, y)) + (1 - \alpha) \times W_E^D(x, y) \tag{9}$$

9. Apply Inverse Lifting Wavelet Transom (ILWT) to get Watermarked Image
WM_Y = ILWT [X^A (x,y), X^H (x,y), X^V (x,y), WM^D (x,y)]
10. Transform the watermarked image (WM_{YCbCr}) from YC_bC_r to get RGB watermarked image (WM_{RGB}).
WM_{RGB} = RGBConversion(W_Y, X_{Cb}, X_{Cr})

3.2 Watermark extraction

Let WM_{RGB} represents watermarked image of size $m_1 \times n_1$. To extract the watermark, firstly cover image and watermarked image is transformed into YC_bC_r color space. Further, one level of LWT is applied over Y component of cover image and watermarked image. Alpha blending technique is used to extract the watermark from the watermarked

image. Finally, Inverse ACM is applied to decrypt the extracted watermark to get original watermark. LWT based watermark extraction steps shown in Fig. 5 is discussed below in Algorithm 2.

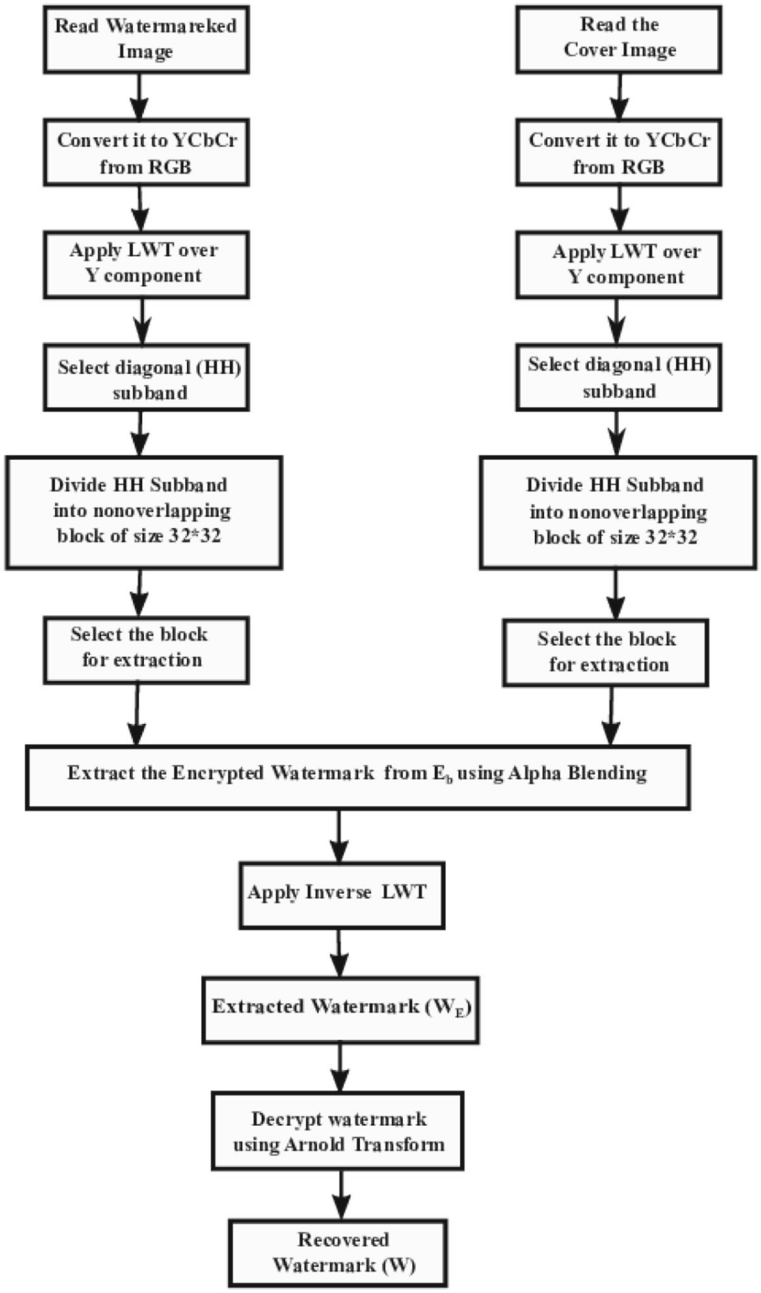

Fig. 5 Watermark extraction process

Algorithm 2 Pseudo- Code for Watermark Extraction.

Input: Watermarked Image, Cover Image, Key
Output: Watermark Image
1. Read the watermarked image WM_{RGB} and cover image X_{RGB} .
2. Convert Watermarked Image and Cover image color space from RGB to YC_bC_r
$[WM_Y, WM_{Cb}, WM_{Cr}] = YC_bC_rConversion(WM_{RGB})$
$[X_Y, X_{Cb}, X_{Cr}] = YC_bC_rConversion(\mathrm{X})$
3. Select Y component of watermarked image and cover image and apply first level of LWT .
$[WM_Y^A\ (\mathrm{x,y}), WM_Y^H\ (\mathrm{x,y}), WM_Y^V\ (\mathrm{x,y})\ WM_Y^D\ (\mathrm{x,y})] = \mathrm{LWT}\ (\mathrm{WM}_Y)$
$[\Psi_Y^A\ (\mathrm{x,y}), \Psi_Y^H\ (\mathrm{x,y}), \Psi_Y^V\ (\mathrm{x,y}), \Psi_Y^D\ (\mathrm{x,y})] = \mathrm{LWT}\ (\mathrm{X}_Y)$
4. Divide both cover image and watermarked image into non-overlapping block of size 32×32 and the selected the block B_E where the watermark is inserted.
5. Extract the watermark using (10)

$$W_E^D(x, y) = \frac{WM_Y(x, y) - (\alpha \times B_E)}{1 - \alpha} \tag{10}$$

6. Apply ILWT to get back the encrypted watermark.
$W_E = \mathrm{ILWT}\ [W_E^A\ (\mathrm{x,y}), W_E^H\ (\mathrm{x,y}), W_E^V\ (\mathrm{x,y}), W_E^D\ (\mathrm{x,y})]$
7. Apply Inverse Arnold Cat Map over extracted watermark W_E with same key value to obtain final watermark (W).
$\mathrm{W} = \text{Inverse Arnold Cat Map}\ (W_E)$

4 Result & discussion

In this section, the result of the proposed scheme is discussed. In this work, seven standard color cover images size 512×512 and a grayscale watermark image of size 64×64 is used to determine the performance of the proposed scheme. Figure 6 depicts the cover image and watermark used in this work. Table 1 depicts the cover image used in the experiment along with its size and extensions. Throughout this study, to balance the trade-off between imperceptibility and robustness of the proposed scheme value of 'α' (scaling factor) in (9) and (10) is taken as 0.70.

4.1 Imperceptibility analysis

Imperceptibility means the visual consistency of the original image in the presence of a watermark will stay the same as the watermarked image [14, 17]. To evaluate the imperceptibility

Table 1 Features of cover images used in proposed scheme

Sl. No	Image	Size	Extension
1	Lena	512×512	.tif
2	Mandrill	512×512	.tif
3	Peppers	512×512	.bmp
4	Girl	512×512	.bmp
5	Jetplane	512×512	.bmp
6	Lake	512×512	.bmp
7	Barbara	512×512	.jpg

Table 2 Imperceptibility result of the proposed scheme

Image	PSNR	SNR	SSIM	NCC	MAE	MSE
Lena	44.7457	39.6081	0.9990	0.9994	0.0768	2.1803
Mandrill	44.1330	38.3912	0.9991	0.9996	0.0872	2.5106
Peppers	44.5948	38.6706	0.9987	0.9995	0.0804	2.2574
Girl	45.3858	43.5498	0.9992	0.9988	0.0642	1.8815
Jetplane	44.6589	41.9709	0.9959	0.9993	0.0800	2.2243
Lake	44.6409	39.4898	0.9985	0.9997	0.0806	2.2335
Barbara	44.3955	37.9881	0.9967	0.9995	0.0839	2.3633

of the proposed scheme various objective performance metrics like PSNR, MSE, SSIM, SNR, NCC, and MAE of cover and watermarked images are used. Table 2 depicts the imperceptibility of the proposed scheme. The PSNR value of the watermarked image ranges in between 44.1330 to 45.3858. The average PSNR value of the proposed scheme is 44.6506. Whereas the SSIM value ranges in between 0.9959 to 0.9991. SSIM value closes to 1 specifies the high perceptual excellence of watermarked images. NCC values range from 0.9989 to 0.9997. NCC values close to 1 depicts a better result. In Table 2, higher value of PSNR, SNR, SSIM and NCC denotes better imperceptibility. Conversely, lower value of MAE and MSE denotes better imperceptibility.

4.2 Robustness analysis

Robustness is the major metric used to determine the effectiveness of watermarking schemes. The watermarking scheme's robustness is its ability to withstand the multiple attacks upon it. The watermarked images endured several attacks to test the robustness of our proposed system. In [37] Stirmark benchmark is depicted as a benchmark for watermarking. Here, the attacks are categorized in some classes like scaling, cropping, geometric distortion, etc. Whereas, in [18] these attacks are classified based on their properties. The robustness of the proposed scheme is checked over the image of Lena and grouped in four key groups [31]:

i) noise addition attack ii) image enhancement attack iii) geometric transformation attack iv) compression attack

Further in noise addition attack robustness is have tested over salt & pepper noise, Gaussian noise, speckle noise, and poisson noise. sharpening, histogram equalization, Gaussian filtering, median filtering, and gamma correction are used to test the robustness of enchantment techniques attack. To evaluate the robustness of geometric transformation attacks, cropping, scaling, and rotation attack is used in proposed work. By adjusting the quality factor of the watermarked images, the proposed scheme is tested against JPEG compression. The robustness of the proposed scheme is calculated using metrics like PSNR, NCC, and BER . The attacked images and the recovered watermarks against various attacks are shown in Figs. 7 and 8 respectively, where [a-o] represents, no attack, salt & pepper noise (m=0,v=0.05), Gaussian noise (m=0,v=0.05), speckle noise, poisson noise, sharpening, histogram equalization, Gaussian filtering, median filtering, Wiener filtering, gamma correction (gamma=0.5), rotation 10°, scaling (0.5), cropping 10%, JPEG compression (QF=90%). Table 3 depicts the PSNR value between the attacked images and watermarked images. From Table 3 its clear that after applying various attacks over watermarked images,

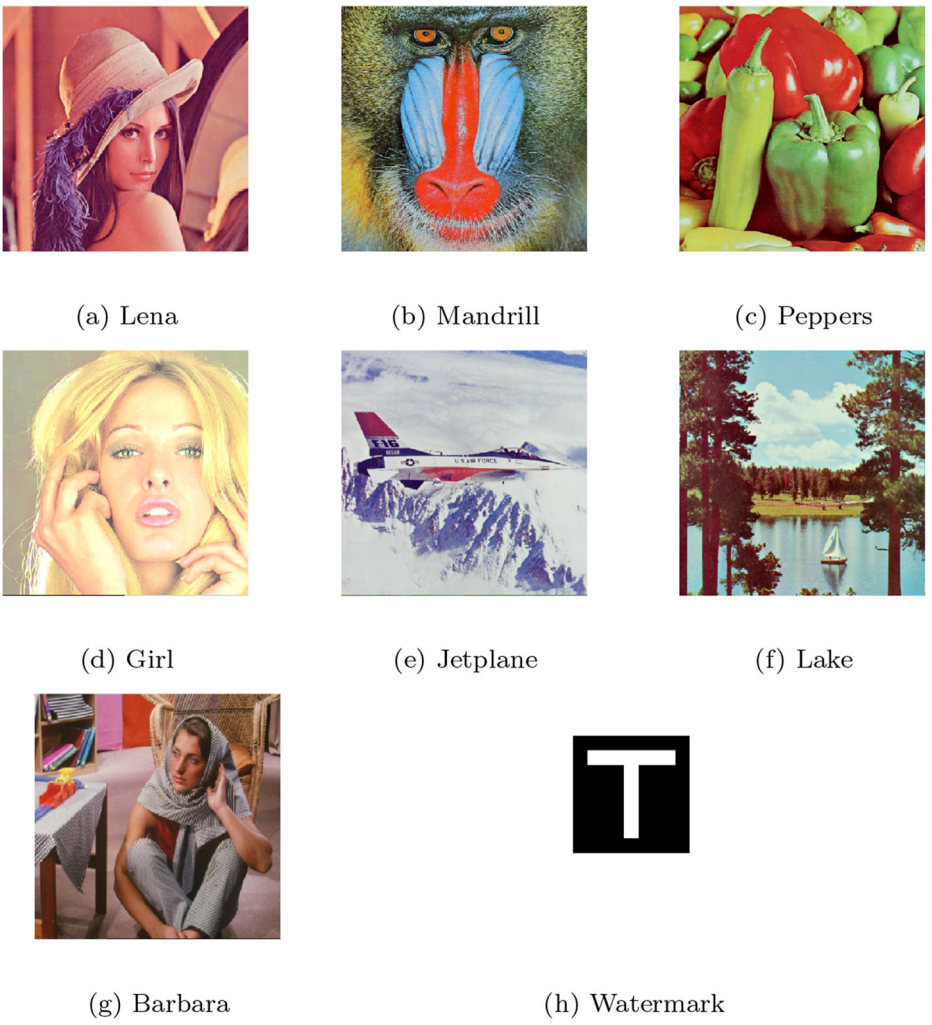

Fig. 6 Cover Images and Watermark

it got distorted and the PSNR value decreases. Tables 4, 5, and 6 illustrate the NCC, BER, and PSNR of the original watermark and recovered watermark under various attacks respectively. Experimental results depicted in Tables 4, 5, and 6 shows that that the proposed scheme is robust against attacks. Whereas, in Table 7 NCC, BER and PSNR value of original watermark and the recovered watermark under multiple attacks are depicted. From the result of Table 7 it is evident that the proposed scheme is also robust against combination attacks. The variation of NCC and BER value of watermark and the recovered watermark against salt & peppers noise, Gaussian noise, speckle noise, median filtering, gamma correction attack, rotation attack, and JPEG compression attack with variation in attack parameters is depicted in Figs. 9–16 respectively. From Figs. 9, 10 and 11 it is clear that with the increase in noise density the NCC value decrease and the BER value increases. Whereas, Fig. 12 depicts that with the varying window size from 3×3 to 11×11 there is very small difference

Fig. 7 Sample Attacked Lena Images

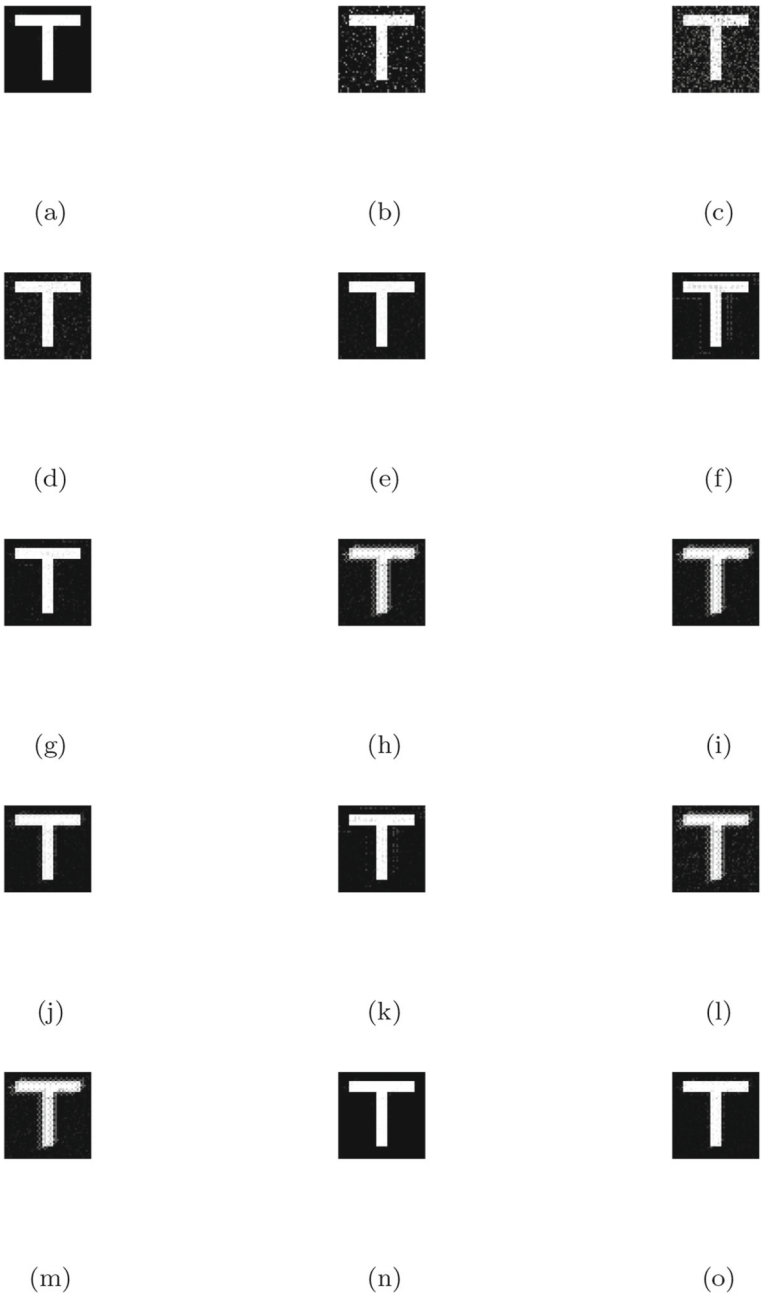

Fig. 8 Recovered watermark under different attacks

in NCC and BER values. Similarly, Fig. 13 depicts the change in NCC and BER value for eight different gamma values. Figure 14 shows the variation in NCC and BER value against varying degrees in both clockwise and anticlockwise. Whereas, the variation in NCC and

Table 3 PSNR values of attacked image

Attack	Lena	Mandrill	Peppers	Girl	Jetplane	Lake	Barbara
No attack	44.7457	44.1330	44.5948	45.3858	44.6589	44.6409	44.3955
Salt & pepper noise(m=0,v=0.05)	18.1932	18.2295	17.8873	17.3946	17.8448	17.9501	18.2738
Gaussian Noise(m=0,v=0.05)	13.8395	13.8256	14.0570	14.4428	14.1828	14.0869	13.7712
Speckle noise(m=0,v=0.05)	18.7704	19.1565	19.1912	16.3757	16.4185	18.6832	19.5610
Poisson noise	27.0626	27.3483	27.6113	25.8983	25.4938	27.1590	27.6324
Sharpening	34.1677	25.3803	33.2720	34.5916	32.6006	30.6531	30.4195
Histogram equalization	22.7765	21.5130	22.2248	10.8440	11.2334	27.8408	18.8975
Gaussian filtering(3×3)	40.3274	30.5978	38.3098	39.3555	40.2331	35.9350	36.9592
Median filtering (3×3)	33.7449	22.6021	31.9333	32.3552	34.1905	28.8363	28.7613
Wiener filtering (3×3)	25.6396	25.9392	34.3102	35.2958	37.0325	31.6698	33.6998
Gamma correction(gamma=0.5)	14.1331	13.8378	14.2893	18.7473	17.4322	14.4457	13.5933
Rotation(10°)	12.5441	12.6178	11.4431	12.6581	10.9812	10.7855	12.3794
Scaling(0.5)	31.8754	22.2597	29.9519	30.1386	29.9426	27.3108	28.1161
Cropping(10%)	15.8038	16.8019	15.6110	12.6714	12.8004	16.5285	17.2334
JPEG(QF=90)	37.0235	27.4300	34.7244	37.5112	39.4649	32.0967	41.5288
JPEG(QF=50)	32.4896	22.4795	30.7991	32.6109	32.6906	27.1322	32.0784

BER value with the 10 different scaling factors is depicted in Fig. 15. From Fig. 16 and Tables 3, 4 and 5 it is clear that robustness decreased against JPEG compression attack with decrease in QF from (QF=90) to (QF=50).

Table 4 NCC values of recovered watermark against various attacks

Attack	Lena	Mandrill	Peppers	Girl	Jetplane	Lake	Barbara
No attack	1	1	1	0.9981	1	1	1
Salt & pepper noise(m=0,v=0.05)	0.9729	0.9769	0.9770	0.9635	0.9819	0.9684	0.9801
Gaussian Noise(m=0,v=0.05)	0.9715	0.9707	0.9681	0.9702	0.9699	0.9692	0.9684
Speckle noise(m=0,v=0.05)	0.9861	0.9635	0.9672	0.9268	0.9554	0.9777	0.9576
Poisson noise	0.9966	0.9943	0.9944	0.9867	0.9942	0.9959	0.9933
Sharpening	0.9955	0.9879	0.9931	0.9970	0.9936	0.9946	0.9920
Histogram equalization	0.9987	0.9966	0.9999	0.9902	0.9968	0.9994	0.9972
Gaussian filtering	0.9910	0.9898	0.9918	0.9875	0.9918	0.9912	0.9919
Median filtering (3×3)	0.9646	0.9513	0.9629	0.9609	0.9643	0.9621	0.9609
Wiener filtering (3×3)	0.9961	0.9903	0.9927	0.9863	0.9929	0.9889	0.9935
Gamma correction(gamma=0.5)	0.9976	0.9970	0.9995	0.9895	0.9966	0.9979	0.9967
Rotation(10°)	0.9599	0.9450	0.9617	0.9589	0.9592	0.9586	0.9570
Scaling(0.5)	0.9622	0.9507	0.9635	0.9610	0.9620	0.9619	0.9625
Cropping(10%)	0.9998	0.9804	1	0.9981	1	0.9999	1
JPEG(QF=90)	0.9996	0.9984	0.9998	0.9978	0.9999	0.9995	0.9999
JPEG(QF=50)	0.9974	0.9976	0.9956	0.9934	0.9980	0.9965	0.9949

Table 5 BER values of recovered watermark on various attacks

Attack	Lena	Mandrill	Peppers	Girl	Jetplane	Lake	Barbara
No attack	0.0246	0.0130	0.0125	0.0547	0.0119	0.0170	0.0127
Salt & pepper noise(m=0,v=0.05)	0.0974	0.0942	0.909	0.1137	0.0831	0.0952	0.0932
Gaussian noise(m=0,v=0.05)	0.1570	0.1526	0.1543	0.1641	0.1524	0.1547	0.1557
Speckle noise(m=0,v=0.05)	0.1347	0.1570	0.1564	0.1861	0.1662	0.1355	0.1590
Poisson noise	0.1091	0.1172	0.1170	0.1437	0.1205	0.1122	0.1224
Sharpening	0.0890	0.1396	0.1018	0.0985	0.0855	0.0976	0.1165
Histogram equalization	0.0879	0.1083	0.0558	0.1135	0.1269	0.0741	0.1136
Gaussian filtering	0.1193	0.0996	0.0890	0.0867	0.0986	0.0971	0.0989
Median filtering(3×3)	0.1476	0.1925	0.1529	0.1470	0.1403	0.1511	0.1784
Wiener filtering(3×3)	0.1139	0.1625	0.1386	0.1384	0.1166	0.1343	0.1554
Gamma correction(gamma=0.5)	0.0748	0.1242	0.0927	0.1216	0.1032	0.0823	0.1198
Rotation(10°)	0.1695	0.1997	0.1682	0.1667	0.1671	0.1699	0.1773
Scaling(0.5)	0.1469	0.1972	0.1532	0.1515	0.1426	0.1542	0.1767
Cropping(10%)	0.0246	0.0765	0.0125	0.0547	0.0119	0.0172	0.0127
JPEG(QF=90)	0.0781	0.1189	0.0730	0.0994	0.0581	0.0933	0.0507
JPEG(QF=50)	0.1258	0.1826	0.1371	0.1354	0.1235	0.1506	0.1447

4.3 Security analysis

Watermark protection is an essential precondition for ensuring the efficient implantation of the watermarking scheme. In this paper, we have used ACM for securing the watermark. To evaluate the security of the watermark performance metrics like NCC, PSNR, SSIM, and

Table 6 PSNR values of recovered watermark on various attacks

Attack	Lena	Mandrill	Peppers	Girl	Jetplane	Lake	Barbara
No attack	42.5857	55.0793	56.3445	32.1752	56.5903	46.0642	56.0197
Salt & pepper noise(m=0,v=0.05)	24.3753	24.6931	26.5267	23.1293	26.1224	24.8370	26.0908
Gaussian noise(m=0,v=0.05)	20.9209	21.5430	21.6329	19.7149	22.6200	20.2978	22.1413
Speckle noise(m=0,v=0.05)	24.9800	24.0892	25.2729	23.6558	25.3462	25.0149	25.1699
Poisson noise	26.8631	25.5487	23.0815	19.0716	21.5641	24.6787	21.9300
Sharpening	32.8256	30.8284	30.9978	26.1913	30.65688	32.1807	30.1940
Histogram equalization	28.5397	23.7975	26.6521	30.0613	27.1113	27.7066	25.7581
Gaussian filtering	33.5186	29.2072	43.1945	25.0942	20.5503	37.0549	30.2187
Median filtering(3×3)	24.9800	24.0892	25.2729	23.6558	25.3462	25.0149	25.1699
Wiener filtering(3×3)	19.5700	18.0687	19.3759	19.1833	19.5616	19.2807	18.9834
Gamma correction(gamma=0.5)	18.9565	17.5551	19.1839	18.9237	18.9285	18.8593	18.6458
Rotation(10°)	42.5857	22.4041	56.3445	32.1752	56.5903	46.0642	56.0197
Scaling(0.5)	19.2988	17.9828	19.4230	19.1613	19.3061	19.2549	19.1407
Cropping(10%)	38.8600	31.9140	41.6249	31.1749	44.5519	36.6979	46.5702
JPEG(QF=90)	34.6500	24.5062	32.9435	29.0103	36.9493	27.8275	35.8477
JPEG(QF=50)	29.9978	19.6038	27.7740	26.2536	31.1088	23.3657	27.0913

Table 7 NCC, BER and PSNR value on multiple attacks

Attack	NCC	BER	PSNR
Histogram Equalization + Gamma Correction(gamma=0.5)	0.9968	0.0957	29.7098
Histogram Equalization + Rotation(10°)	0.9586	0.1714	18.8112
Wiener Filtering(3×3) + Gamma Correction (gamma=0.5)	0.9973	0.1153	29.8962
Wiener Filtering(3×3) + JPEG(QF=50)	0.9893	0.1404	24.3311
Salt & Pepper Noise(m=0,v=0.05) + Rotation(10°)	0.9549	0.1791	18.4795
Salt & Pepper Noise(m=0,v=0.05) + JPEG(QF=50)	0.9596	0.1671	19.0174
Gaussian Noise(m=0,v=0.05) + Cropping(10%)	0.9424	0.1879	17.2696
Gaussian Noise(m=0,v=0.05) + Scaling(0.5)	0.9620	0.1492	19.2780
Speckle Noise(m=0,v=0.05) + Histogram Equalization	0.9880	0.1468	23.7882
Rotation(10°) + Scaling(0.5)	0.9619	0.1495	19.2514
Rotation(10°) + Cropping(10%)	0.9599	0.1695	18.9565
Rotation(10°) + JPEG (QF=50)	0.9602	0.1678	19.0060
Scaling(0.5) + JPEG(QF=50)	0.9620	0.1487	19.2852
JPEG(QF=50) + Gamma Correction(gamma=0.5)	0.9967	0.1200	29.1785
JPEG(QF=50) + Histogram Equalization	0.9963	0.1272	28.6036
JPEG(QF=50) + Wiener Filtering(3×3)	0.9932	0.1325	26.1935

BER are used. Table 8 shows the performance compassion of ACM on various iterations. Lower value of NCC, PSNR and SSIM and the higher BER value in Table 8 indicates better security of watermark.

4.4 Payload analysis

The payload or embedding capacity is a metric that describes the number of bits of information that can be inserted in the cover image [12, 21, 27]. In this proposed scheme color

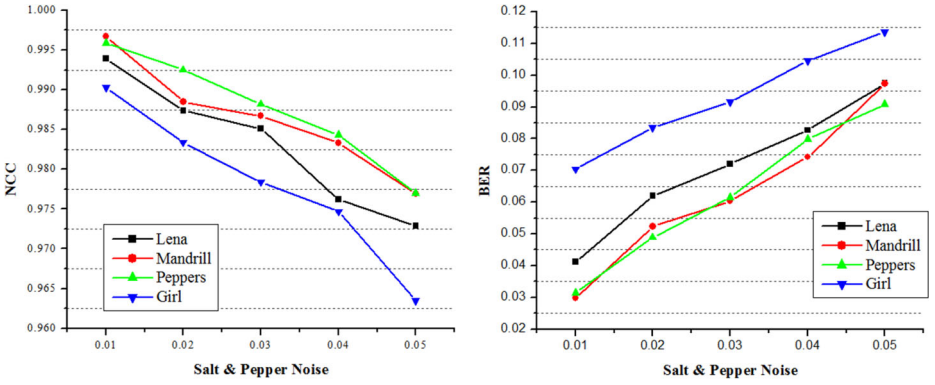

Fig. 9 NCC and BER values variation with different salt & pepper noise density

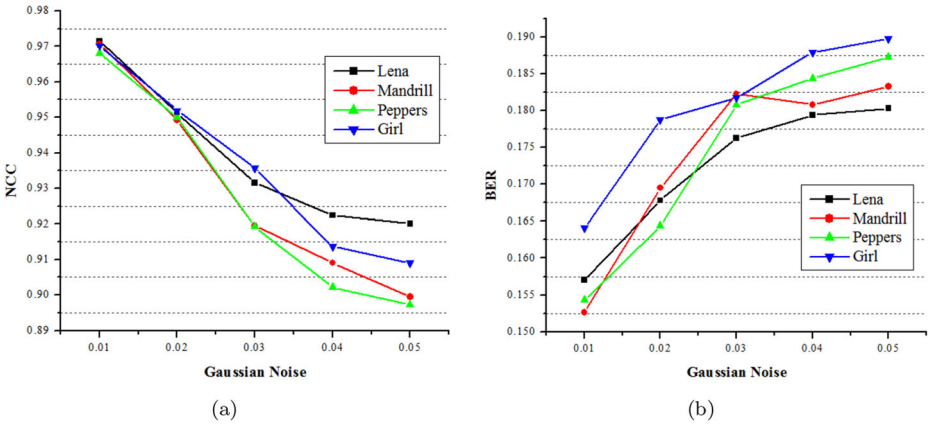

Fig. 10 NCC and BER values variation with different Gaussian noise density

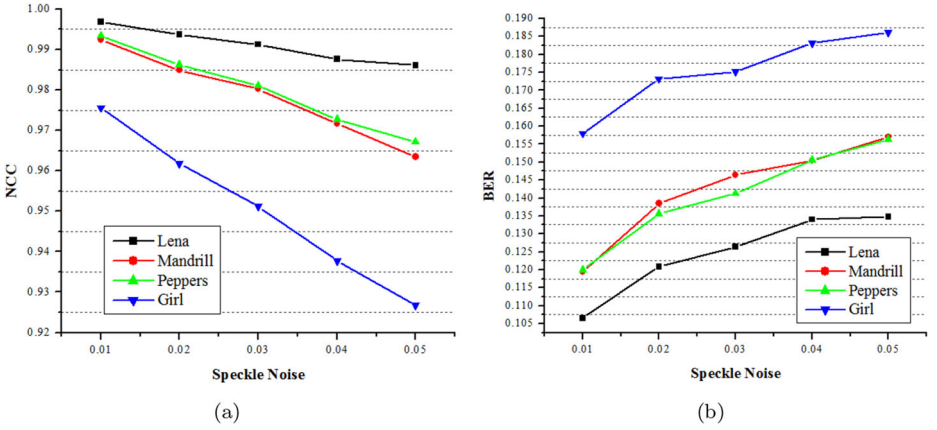

Fig. 11 NCC and BER values variation with different speckle noise density

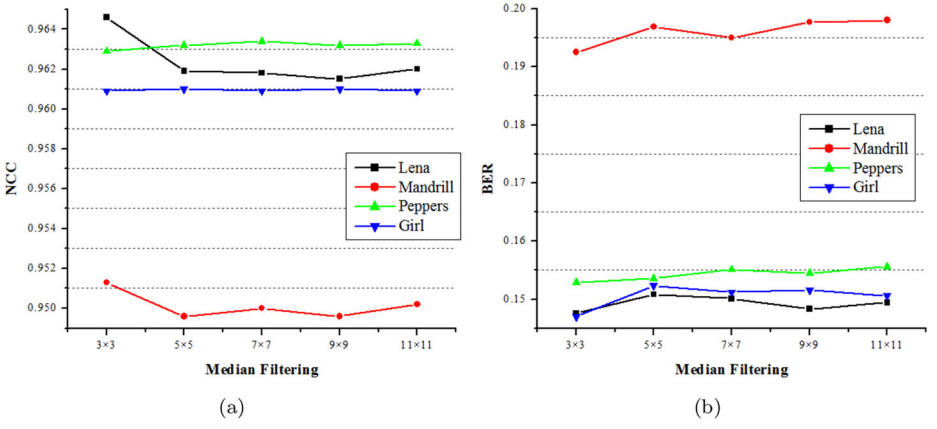

Fig. 12 NCC and BER values variation for median filtering attack with increase in filter size

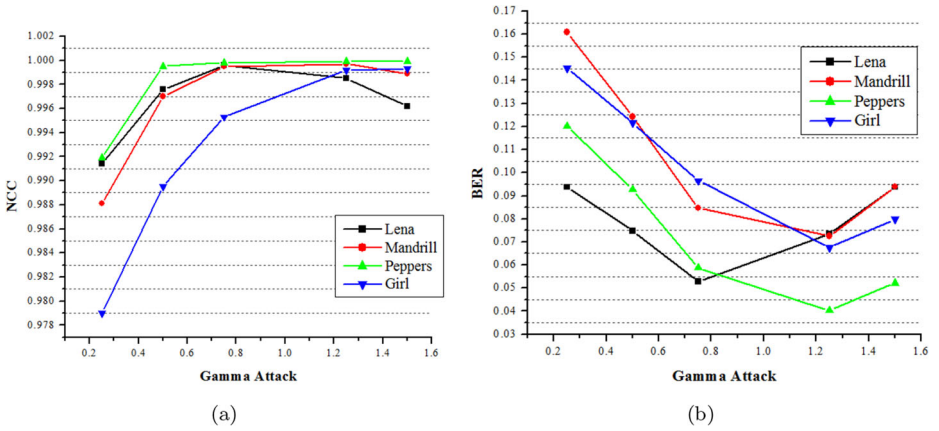

Fig. 13 NCC and BER variation in gamma correction attack with varying gamma value

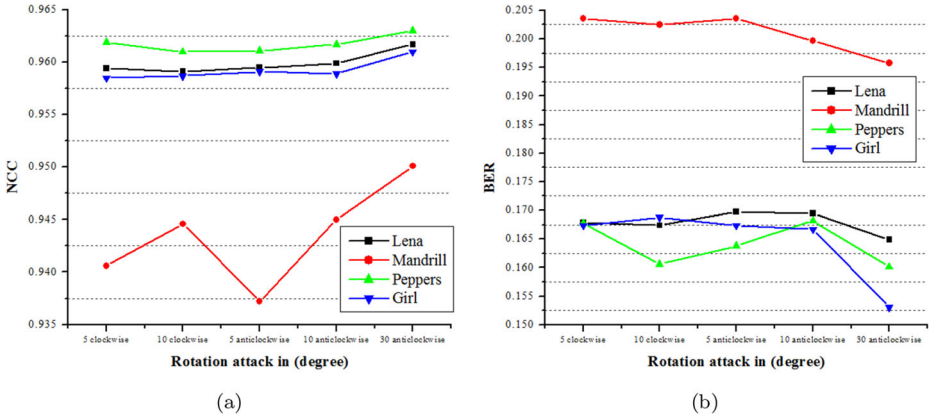

Fig. 14 NCC and BER value variation of rotation attack with varying degree

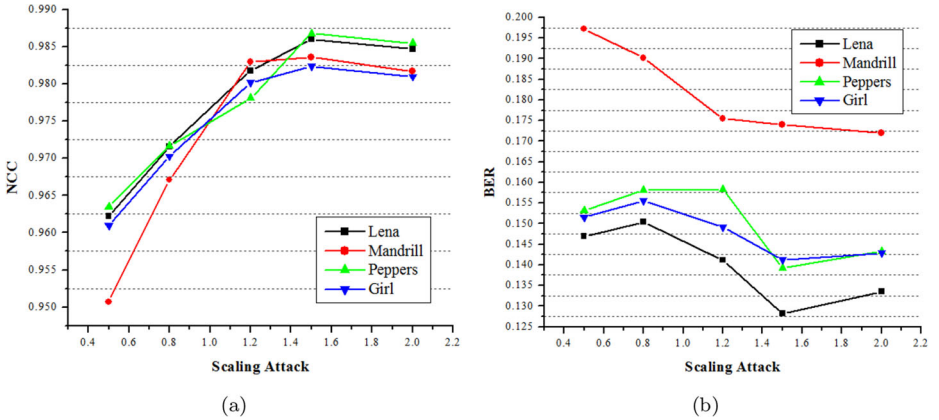

Fig. 15 NCC and BER of value variation for scaling attack with varying scaling factor

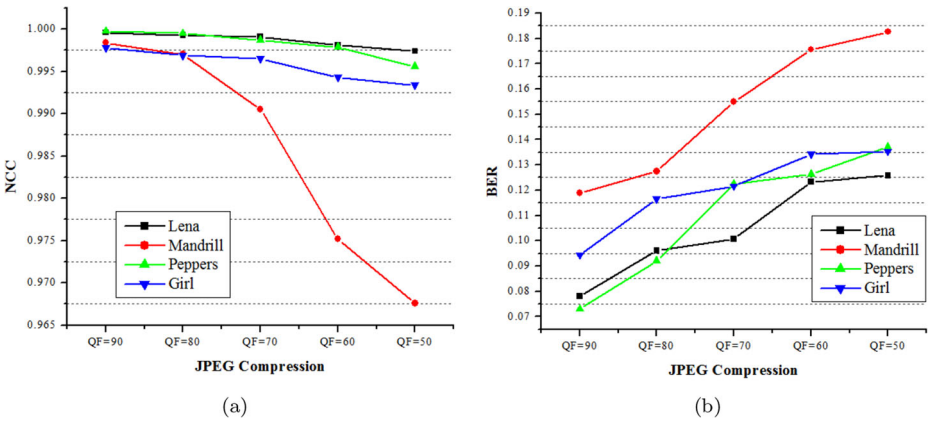

Fig. 16 NCC and BER value variation for JPEG compression attack with varying QF

Table 8 Security analysis of watermark

No. of Iteration	NCC	PSNR	SSIM	BER
10	0.0545	5.4048	- 0.0032	0.2881
25	0.0910	5.4195	0.0580	0.2871
50	0.1166	5.3390	0.0619	0.2925
75	0.0343	5.4269	- 7.3470 e^{-04}	0.2866
100	0.0382	5.4641	0.0023	0.2842

Table 9 Comparison of execution time in (sec) of proposed scheme and Kang et al. scheme [12]

Sl. No	Image	Proposed	[12]
1	Lena	0.223489	1.0605
2	Mandrill	0.216176	1.0608
3	Pepper	0.232826	1.1228
4	Girl	0.217994	—
5	Jetplane	0.224171	1.0851
6	Lake	0.223485	1.0674
7	Barbara	0.218092	—

Table 10 Perceptual Comparison of Lena Image of Size 512 × 512 with state-of-the-art

	Proposed	[36]	[31]	[14]	[29]	[28]	[30]
PSNR	44.7457	33.21	51.1464	54.94	42.2198	39.976	31.708
SSIM	0.9990	0.9989	—	1	—	0.9874	—

cover image of size 512×512 is used. Also, gray-scale watermark image of size 64×64 is used. So, the embedding payload of the proposed scheme is

$$(64 \times 64 \times 8)/(512 \times 512 \times 3) = 0.04166 \text{ bpp}$$

4.5 Computational complexity

In LWT, the wavelet transform can be computed without allocating the auxiliary memory therefore the LWT based watermarking scheme is memory efficient [24]. The watermark bits are inserted in the chosen blocks, further reducing the expense of the computation.

The average execution time of the proposed LWT based scheme is 0.221461 sec. Table 9 depicts the execution time of the proposed scheme and Kang et al. scheme [12] on the various test images. The average execution time of Kang et al. scheme [12] and Hu et al. scheme [11] is 1.07033 sec and 1.954 sec respectively. Therefore, the proposed scheme is nearly 5 times computationally efficient from Kang et al. scheme [12] and nine-time computationally efficient than Hu et al. scheme [11].

4.6 Comparative analysis

In this section comparative analysis of the proposed scheme with the recent state-of-the-art is illustrated. Table 10 demonstrates the imperceptibility comparison between the proposed scheme and some of existing schemes. In Table 11, the robustness comparison with the state-of-the-art of the proposed scheme on the Lena image is performed. From Table 11, it is clear that the proposed scheme is more robust in comparison with the other state-of-the-art schemes. Whereas, Table 12 offers a detailed analysis of the suggested technique with the recent existing schemes.

Table 11 NCC comparison of Proposed and state-of-the-art methods Attack

Attack	Proposed	[36]	[31]	[14]	[29]	[28]	[30]
No attack	1	1	0.9992	1	1	1	0.9976
Salt & pepper noise (m=0,v=0.05)	0.9729	0.9780	0.9583	0.9893	—	—	—
Gaussian noise(m=0,v=0.05)	0.9715	0.9072	0.9294	0.9382	0.9122	—	0.8339
Speckle noise (m=0,v=0.05)	0.9861	0.9046	0.9625	—	0.8838	0.9194	—
Sharpening	0.9955	—	0.9385	0.9686	1	0.9596	0.8560
Histogram equalization	0.9987	—	0.9233	1	0.9313	0.9186	0.8812
Gaussian filtering	0.9910		—	0.9611	—	1	0.8186
Median filtering (3×3)	0.9646	0.9420	0.9796	1	0.9950	—	0.8271
Wiener filtering(3×3)	0.9961	—	0.9732	—	0.9955	—	0.7293
Gamma correction (gamma=0.5)	0.9976	—	0.8400	—	1	1	—
Rotation (10°)	0.9599	—	—	0.9389	—	0.9569	—
Cropping (10%)	0.9998	0.9997	—	—	—	0.9438	—
Scaling(0.5)	0.9622	0.9998	—	—	—	—	0.9862
JPEG(QF=90)	0.9996	0.9921	—	—	—	0.9979	0.9479

Table 12 Performance comparison of the proposed scheme with state-of-the-art

	Proposed	[36]	[31]	[14]	[29]	[28]	[30]
Cover Image Size	512×512	512×512	512×512	512×512	512×512	512×512	512×512
Cover Image Type	color	color	color	color	color	color	color
Watermark Size	64×64	64×64	64×64	70×70	64×64	128×128	256×256
Watermark Image Type	grayscale	grayscale	grayscale	grayscale	binary	binary	grayscale
Operating Domain	Frequency	Frequency	Frequency	Frequency	Frequency	Frequency	Frequency
Technique Used	LWT	DWT+CT+SD+SVD	DWT+SVD	LWT+PC	DCT	WHT	SVD+RDWT
Embedding Color Domain	YCbCr	YCbCr	YCbCr	RGB	RGB	TVT	YCbCr
Embedding Color Component	Y	Y	Y	B	B and G	W	Y
Limitations	less robust against median filtering attack	poor imperceptibility	low robustness & high computational cost	poor robustness against JPEG compression attack	poor robustness against noise addition attack	poor robustness against noise addition attack	poor robustness against attack

5 Conclusion

In this work, a color image watermarking based on the LWT is suggested. As a color image watermarking scheme, the proposed scheme is more appropriate for real-life applications. The suggested approach uses a blending of Alpha to infuse the watermark. Use of LWT makes the proposed technique faster and efficient. Using Arnold transform has improved watermark efficiency. The optimum range of blocks and the alpha blending scheme tackle the trade-off between imperceptibility and robustness. Comprehensive performance analysis of the proposed scheme is conducted including imperceptibility analysis, robustness analysis, security analysis, payload analysis, and computational complexities. The execution time of the proposed scheme is very less as compared to the state-of-the-art. The robustness of the proposed scheme is also tested over various combinations of attacks. Experimental findings suggest the excellence of the proposed scheme is compared to existing schemes. As watermarking is carried out in HH subband, robustness of the proposed scheme against median filtering attack is low. In future, nature based optimization techniques can be used to calculate the optimal α value. Also, robustness against median filtering attack can be improved.

References

1. 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
2. Bajaj A (2014) Robust and reversible digital image watermarking technique based on rdwt-dct-svd. In: 2014 International Conference on Advances in Engineering & Technology Research (ICAETR-2014), pp 1–5. IEEE
3. Chowdhury FS, Dhar PK, Deb K, Koshiba T (2020) Blind image watermarking in canonical and cepstrum domains based on 4-connected t-o'clock scrambling. Symmetry 12(2):266
4. Degadwala SD, Kulkarni M, Vyas D, Mahajan A (2020) Novel image watermarking approach against noise and rst attacks. Procedia Computer Science 167:213–223
5. Desai SD, Pudakalakatti NR, Baligar VP (2017) A survey on intelligent security techniques for high-definition multimedia data. In: Intelligent Techniques in Signal Processing for Multimedia Security, pp 15–45. Springer
6. Ernawan F, Kabir MN (2018) A robust image watermarking technique with an optimal dct-psychovisual threshold. IEEE Access 6:20464–20480
7. Ernawan F, Kabir MN (2020) A block-based rdwt-svd image watermarking method using human visual system characteristics. Vis Comput 36(1):19–37
8. Fares K, Amine K, Salah E (2020) A robust blind color image watermarking based on fourier transform domain. Optik 208:164562
9. Fragoso-Navarro E, Cedillo-Hernández M, Nakano-Miyatake M, Cedillo-Hernández A, Pérez-Meana HM (2018) Visible watermarking assessment metrics based on just noticeable distortion. IEEE Access 6:75767–75788
10. Hosny KM, Darwish MM (2019) Resilient color image watermarking using accurate quaternion radial substituted chebyshev moments. ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM) 15(2):1–25
11. Hu H-T, Hsu L-Y, Chou H-H (2020) An improved svd-based blind color image watermarking algorithm with mixed modulation incorporated. Inf Sci
12. Kang X-B, Lin G-F, Chen Y-J, Zhao F, Zhang E-H, Jing C-N (2020) Robust and secure zero-watermarking algorithm for color images based on majority voting pattern and hyper-chaotic encryption. Multimedia Tools and Applications 79(1):1169–1202
13. Kejgir SG, Kokare MB (2014) Robust multichannel colour image watermarking using lifting wavelet transform with singular value decomposition. Int J Comput Sci Eng 9(4):371–385

14. Koley S (2019) A feature adaptive image watermarking framework based on phase congruency and symmetric key cryptography. Journal of King Saud University-Computer and Information Sciences
15. Kumar S, Dutta A (2016) A novel spatial domain technique for digital image watermarking using block entropy. In: 2016 International Conference on Recent Trends in Information Technology (ICRTIT), pp 1–4, IEEE
16. Kumar S, Dutta A (2016) A study on robustness of block entropy based digital image watermarking techniques with respect to various attacks. In: 2016 IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), pp 1802–1806. IEEE
17. Kumar S, Singh BK, Yadav M A recent survey on multimedia and database watermarking. Multimedia Tools and Applications, pp 1–49
18. Kutter M, Petitcolas FabienAP (1999) Fair benchmark for image watermarking systems. In: Security and Watermarking of Multimedia Contents, vol 3657, pp 226–239. International Society for Optics and Photonics
19. Laur L, Rasti P, Agoyi M, Anbarjafari G (2015) A robust color image watermarking scheme using entropy and qr decomposition. Radioengineering 24(4):1025–1032. https:doi.org/10.13164/re.2015.1025
20. Liu D, Yuan Z, Su Q (2019) A blind color image watermarking scheme with variable steps based on schur decomposition. Multimedia Tools and Applications 79:7491–7513. https://doi.org/10.1007/s11042-019-08423-1
21. Loan NA, Hurrah NN, Parah SA, Lee JW, Sheikh JA, Bhat GM (2018) Secure and robust digital image watermarking using coefficient differencing and chaotic encryption. IEEE Access 6:19876–19897
22. Maity SP, Kundu MK (2010) Dht domain digital watermarking with low loss in image informations. AEU-International Journal of Electronics and Communications 64(3):243–257
23. 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 processing 10(1):34–52
24. Mehta R, Rajpal N, Vishwakarma VP (2016) Lwt-qr decomposition based robust and efficient image watermarking scheme using lagrangian svr. Multimedia Tools and Applications 75(7):4129–4150
25. Moeinaddini E (2019) Selecting optimal blocks for image watermarking using entropy and distinct discrete firefly algorithm. Soft Comput 23(19):9685–9699
26. Pandey MK, Parmar G, Gupta R, Sikander A (2019) Lossless robust color image watermarking using lifting scheme and gwo. Int J Syst Assur Eng Manag 11:320–331. https://doi.org/10.1007/s13198-019-00859-w
27. Patvardhan C, Kumar P, Lakshmi CV (2018) Effective color image watermarking scheme using ycbcr color space and qr code. Multimedia Tools and Applications 77(10):12655–12677
28. Prabha K, Sam IS (2020) A novel blind color image watermarking based on walsh hadamard transform. Multimedia Tools and Applications 79(9):6845–6869
29. Roy S, Pal AK (2017) A blind dct based color watermarking algorithm for embedding multiple watermarks. AEU-International Journal of Electronics and Communications 72:149–161
30. Roy S, Pal AK (2018) An svd based location specific robust color image watermarking scheme using rdwt and arnold scrambling. Wirel Pers Commun 98(2):2223–2250
31. Roy S, Pal AK (2019) A hybrid domain color image watermarking based on dwt–svd. Iranian Journal of Science and Technology, Transactions of Electrical Engineering 43(2):201–217
32. Shi G, Liu W, Zhang L, Li F (2009) An efficient folded architecture for lifting-based discrete wavelet transform. IEEE Transactions on Circuits and Systems II: Express Briefs 56(4):290–294
33. Singh R, Ashok A, Saraswat M (2020) Optimised robust watermarking technique using ckgsa in dct-svd domain. IET Image Process 14(10):2052–2063
34. Singh SP, Bhatnagar G (2019) A simplified watermarking algorithm based on lifting wavelet transform. Multimedia Tools and Applications 78(15):20765–20786
35. Su Q, Wang H, Liu D, Yuan Z, Zhang X (2020) A combined domain watermarking algorithm of color image. Multimedia Tools and Applications 79:30023–30043. https://doi.org/10.1007/s11042-020-09436-x
36. Vaidya P, PVSSR CM (2017) A robust semi-blind watermarking for color images based on multiple decompositions. Multimedia Tools and Applications 76(24):25623–25656
37. Voloshynovskiy S, Pereira S, Pun T, Eggers JJ, Su JK (2001) Attacks on digital watermarks: classification, estimation based attacks, and benchmarks. IEEE communications Magazine 39(8):118–126
38. Wang C, Wang X, Zhang C, Xia Z (2017) Geometric correction based color image watermarking using fuzzy least squares support vector machine and bessel k form distribution. Signal Process 134:197–208

39. Wang J, Wan WB, Li XX, De Sun J, Zhang HX (2020) Color image watermarking based on orientation diversity and color complexity. Expert Syst Appl 140:112868