



# An imperceptible semi-blind image watermarking scheme in DWT-SVD domain using a zigzag embedding technique

Aree A. Mohammed<sup>1,2</sup>  · Dilman A. Salih<sup>2</sup> · Ari M. Saeed<sup>2</sup> · Mohammed Q. Kheder<sup>1</sup>

Received: 24 March 2020 / Revised: 8 August 2020 / Accepted: 21 August 2020 /

Published online: 25 August 2020

© Springer Science+Business Media, LLC, part of Springer Nature 2020

## Abstract

This research work presents a semi-blind image watermarking scheme based on transforms domain DWT-SVD using an efficient embedding technique. This scheme provides a high level of robustness and imperceptibility for digital image copyright protection. In the embedding process, the watermark data (logo and image in this research) is first transformed into the frequency domain using the DWT algorithm for one pass. Then, the LL-band values are also transformed by the SVD algorithm. S values (diagonal matrix) are prepared for inserting into the cover images. Differently, the cover images (SD and HD quality) are also transformed by DWT for two levels of decomposition. During the insertion process, the watermark bits are embedding into the HL2 and HH2 bands of the cover image using the zigzag technique to improve the imperceptibility. Moreover, the obtained watermarked images are subjected to different attacks (geometric, image processing, and jpeg compression) to show the robustness of the proposed scheme. Finally, the extraction process needs only the watermarked image and the U and V values of SVD transforms (semi-blind watermarking) to reconstruct the original watermark. The performance parameters for the robustness and imperceptibility involved in this work are PSNR and Normalized Correlation Coefficient NCC metrics. Computational cost is also calculated for both embedding and extracting watermark process for different cover image types. Test results indicate that the proposed scheme has a better performance when the watermark data is embedding in a zigzag way.

**Keywords** Semi-blind watermarking · Transform domain · Zigzag embedding · Attacks

---

✉ Aree A. Mohammed  
aree.ali@univsul.edu.iq

<sup>1</sup> Computer Science Department, College of Science, University of Sulaimani, Sulaimani, KRG, Iraq

<sup>2</sup> Computer Science Department, College of Science, University of Halabja, Halabja, KRG, Iraq

## 1 Introduction

Nowadays, digital image copyright protection is required for the rapid growth of the Internet technology, illegal copy distribution of ownership, and multimedia transmission. Copyright protection could overcome these security issues by providing a solution for both image authentication and protection [8]. The main aim of the image watermarking process is to hide watermark secret data (text, image, audio, and video) into the color or gray cover images. Therefore, the ownership can guarantee the copyright protection of the host image by efficiently extracting the secret watermark data [9, 25]. Moreover, watermarking has been developed as a generic technique to offer essential security of these transmitted digital data. There are three types of watermarking applications: (1) to transfer ownership information, (2) to confirm that object content has not altered, and (3) to exchange object-specific data to a community of willing receivers [25, 29].

A powerful watermarking scheme must have the following important parameters such as (Robustness and Imperceptibility). Robustness is measured when the watermarked image is attacked while imperceptibility is the invisibility perception between original and watermarked images [6, 36]. Major attacks applied to the watermarked image can be classified as signal processing (adding noise, filtering, and blurring), signal compression (jpeg), and geometric (rotation, cropping, scaling, and translation) [26]. Over the last decade, most of the developing and proposed watermarking schemes are considerably focused on image and movie files instead of audio files due to the sensitivity of the human auditory system (HAS) than the human visual system (HVS). A high imperceptible audio watermarking requires a robust embedding technique [17].

The use of digital video applications, namely digital TV, video conferencing, digital cinema, videophone, distance learning, and video-on-demand has rapidly developed over the last decade. Nowadays, it is much easier for digital data owners to exchange multimedia data over the Internet; therefore, the data can be perfectly duplicated and quickly redistributed on a wide scale [3]. As a result, the significance of copyright protection for multimedia data has become more critical. In addition, the techniques of image watermarking could be extended effortlessly to watermark video image sequences [21, 27]. It is worth mentioning that video watermarking schemes require to meet some other challenges: a large volume of unnecessary data among frames, unbalance between motion and still locales [3], and real-time broadcasting that makes the video signals highly susceptible to pirate attacks involving frame dropping, averaging, swapping, and statistical analysis [21]. Recently, the digital video watermarking scheme is proposed to insert the watermark in “intra-pictures” of MPEG video sequence through changing the Variable Length Codes (VLCs) directly in order to prevent reverse quantization [3, 17, 23, 24].

Digital image watermarking could be applied in both spatial (original data) and frequency (transform data) domains. In the spatial domain, the watermark directly changes the pixel value of the cover or host image which is lead into low-cost calculations whereas in the frequency domain, the cover image pixel data is transformed to coefficient value instead of pixel value by using forward transformation. Thus, the watermark bits alter these coefficient values. This domain is more robust than the spatial one especially against image processing and compression attacks. On the one hand, the spatial domain shows low resistance against several image-processing operations and is subsequently classified as a weak watermarking. On the other hand, the frequency domain methods such as those applying Discrete Cosine Transforms (DCT), Discrete Wavelet Transforms (DWT) techniques are helpful to identify the potential

locations to embed the watermark in order to get better results. Hence, many watermarking are carried out in the frequency domain is therefore classified as a robust watermarking [10]. This is due to the fact that the insertion of watermark data modifies coefficient values. As a consequence, when the inverse transformation is performed, the watermark data is spread out non-uniformly over the cover image [13]. Some spatial image watermarking schemes are proposed in the literature based on the LSB algorithm for both color and gray images [4, 20, 34].

Other watermarking techniques are based on 3D mesh watermarking which can be simply adapted to the 3D objects. These objects could be represented in different ways including NURBS, voxels, and polygonal meshes [2]. 3D watermarking schemes comprise of embedding directly the watermark data by modifying either the topology of the triangles or the 3D mesh geometry. These techniques are usually not complex and need less computational time. Nevertheless, they are not robust enough to resist different types of attacks. Recently, some watermarking schemes have been developed and proposed for 3D mesh in the frequency domain that are mainly based on multi-resolution mesh analysis (wavelet transform and spectral decomposition) and show better resistance against geometrical attacks [1].

Discrete Fourier Transformation DFT, DCT, DWT, and Singular Value Decomposition SVD is among those techniques that have a significant robustness for almost all types of attacks [5, 12, 18, 19]. Furthermore, hybrid transformation is used such as DCT-DFT [11], DWT-SVD [16, 30, 36, 37], and DCT-DWT-SVD [10, 38] to improve the invisibility and the robustness of the watermark insertion process. In addition, digital image watermarking is also classified as non-blind, semi-blind, and blind methods. In the non-blind method, the host image information, original watermark, and watermarked image are required for extracting the embedded watermark [15, 31] while in semi-blind method, both original watermark and watermarked image are used for the watermark extraction process [33]. The blind watermarking scheme only needs a watermarked image for watermark extraction. Generally, the less the cover image information is used; the more sophisticated the watermarking algorithm becomes [14]. A watermarking scheme is commonly inserted as unrecognizable, however, in some cases, it is intentionally recognizable. The unrecognizable called invisible watermarking and the latter is visible watermarking [7]. Visible and/or transparent image watermarking is said to be visible when the content is visible to the human eye while transparent watermarks are also described as invisible watermarks, in which the content is not visible to the human eye [28].

The rest of the paper is organized as follows: an overview of recent related works of the digital image watermarking in frequency domain has been presented in section 2. In section 3, a brief description of the proposed DWT-SVD based watermarking has been introduced. Section 4 shows the performance evaluation based on PSNR and NCC tested on different image samples (SD and HD) quality for different kinds of attacks. Finally, the conclusions and some suggestions for future work are presented in Section 4.

## 2 Related works

Security provocations and vulnerabilities for the high quality images (1K, 2K, and 4K) transmission via the communication channels give rise to a security issue. Researchers in this field began to develop and implement an efficient image watermarking scheme based on transforms domain in terms of imperceptibility (invisibility of the watermark inside the host

image) and robustness (resist the most type of attacks). Piva Alessandro et al. [23] proposed a new method depending on an image watermarking algorithm which embeds the code in the DWT for each frame. The scheme has been tested on various video sequences, each frame composed of two different objects: the background (Video Object 1), and the player (Video Object 2). After the watermarking process, the frame was sequentially compressed to obtain an MPEG-4 coded video bit-stream with a rate of 500 Kb/s per Video Object Layer (VOL). Next, the video stream was decompressed, and the two objects were separated in each frame obtaining two different images, where the detection process was implemented. They also applied the detection process to the completed frame without choosing the objects. Their result shows that the correlation peak of the tennis player (VO 0) was lower than the response of the background (VO 1) since low watermark energy can be embedded into the tennis player. Moreover, the correct detection of the two objects shows that the system is robust to conversion from MPEG-4 to MPEG-2.

Tay R and J P Havlicek [35] presented an image watermarking scheme used 2D discrete wavelet transform to decompose an image into different frequency channels. A scaled image, which has been used as the watermark, added into a mid-frequency wavelet channel. The watermark embedded image is constructed through taking the inverse 2D discrete wavelet transform of the modified wavelet decomposition. Image size, the channel where the watermark is embedded, non-zero scaling factor, and the wavelet transform filters are used as security keys for the extraction of the inserted watermark. The technique of the proposed watermark extraction is totally independent of the original image. Also, three different types of attacks, such as JPEG compression, image cropping, and median filter are applied via adjusting the scaling factor to achieve a compromise between visually perceptible artifacts and resiliency in preserving the watermark. The paper's results indicate that the technique of the watermark embedding is resilient to the above three types of attacks, and in all case the watermark was successfully recovered which supports the robustness of the image watermarking.

PredaRadu and DragosVizireanu [24] suggested a video watermarking technique based on multi-resolution wavelet decomposition. A binary image is applied for the watermark which is embedded within the wavelet coefficients of the LH, HL, and HH sub-bands of the second wavelet decomposition level through quantization. A unique key is used to spread each bit of the watermark over a number of wavelet coefficients. The proposed method has achieved great resilience against several various attacks in the spatial, temporal, and compressed domains since test results show that the embedded watermark is imperceptible and robust to attack. In addition, the performance of the technique can be improved via using error correction codes and by redundantly embedding the same watermark in different frames of the video.

Singh Siddharth et al. [33] proposed a hybrid semi-blind grayscale image watermarking method based on Wavelet, Contourlet and singular value decomposition. The main objective of the work is to focus attention on the effectiveness of redundant wavelet transforms in digital image watermarking. This is due to the sensitivity of the classical wavelet transformation toward the shift-invariance and directional information which is required for better reconstruction of the watermarked image. For embedding a single watermark, host images are sub-sampled followed by one level of Non-sampled Contour let Transform NSCT and Redundant Discrete Wavelet Transform RDWT decomposition. Furthermore, Singular Value Decomposition SVD has been performed on attained RDWT coefficients. Just the same, image watermark data has been transformed by a hybrid NSCT-RDWT-SVD technique. Differently, inverse SVD-RDWT-NSCT transformation is applied to provide a watermarked image. For

the watermark extraction, the NSCT-RDWT-SVD decomposition and SVD coefficients are needed with the same scaling factor that has been used in the embedding process. While in the dual watermarking, Arnold transform is utilized to encrypt the text watermark before embedding phase. The proposed scheme improved the performance against some geometrical and image processing attacks. Objective and subjective test evaluations using peak signal to noise ratio (PSNR), correlation coefficient (CC), bit error rate (BER) and structural similarity index metric (SSIM) show the robustness of the method and outperform the previous related methods.

VaidyaPrasanth and Chandra Mouli [36] proposed a robust semi-blind watermarking scheme for color images based on multiple decompositions. The main aim is to preserve the copyrights of the original (owner) host image. The gray watermark is inserted into a color image by applying multiple decompositions. To improve security the gray watermark is encrypted with SVD and Arnold transforms via generating secret keys. The luminance component of the given host image is subjected to DWT, Contourlet Transform (CT), Schur decomposition, and SVD sequentially and finally, the watermark is added. Without the aid of the original watermark and image, the watermark is extracted from various attacked images in the semi-blind extraction process. Their results indicate that the proposed watermark guarantees both imperceptibility and robustness against image and signal processing attacks. In addition, the proposed method compared with the related watermarking methods is more secure, robust, and efficient.

Yadav Bandana et al. [37] proposed a robust digital image watermarking scheme relied on Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD). In the paper, they first applied DWT with three levels of decompositions on the cover image. Then, SVD is performed on the third level sub-bands to obtain the diagonal matrices of singular values. The watermark data is then inserted in these singular values. The simulation results show that the PSNR has a better value in term of quality compared to other related approaches. In addition, the acquired test results also demonstrate that the present method can properly extract the watermark image when the watermarked image is subjected to various malicious attacks such as (signal processing, geometric, and compression).

Pal Arup and Soumitra Roy [22] developed a robust and blind watermarking scheme based on DCT for protecting the originality of digital images. In the initial stage, the image is decomposed into non-overlapping blocks, and then DCT is applied on each extracted block to insert a binary bit of watermark into each transformed block via enhancing some middle important AC coefficients by repetition code. Throughout the embedding stage, DC and some higher AC coefficients are saved intact after zigzag scanning of each DCT blocks to confirm the high quality of the watermarked image. Consequently, the proposed method is suitable to preserve the copyright information even in the compressed form of the watermarked image because the scheme exploits middle bands of DCT coefficients for inserting the watermark bits. The obtained results showed that they achieved satisfactory visual quality of the watermarked image.

Gupta Ritu et al. [10] proposed a watermarking scheme that uses a progressed encryption method is commonly known as Elliptic Curve Cryptography (ECC). It is applied to embed a binary image as a watermark in several grayscale images in a semi-blind way. According to their results the ECC technique is a quick encryption method that effectively encrypts the subject with significantly less number of bits as compared to other well-known encryption techniques, namely Rivest Shamir Adleman (RSA) and

Direct Selling Association (DSA). DWT-SVD domains are performed on the grayscale images before the embedding process. Furthermore, the scheme is divided into two parts. In the first part, entropy-based HVS parameters are calculated block-wise to recognize the most suitable blocks in spatial domain. First level DWT is applied for the selected blocks and watermark embedding is performed via applying the calculated SVD parameters. Conducted results showed that the use of hybrid DWT-SVD with ECC had a better performance. In the second part, the model of HVS in the DCT domain is applied, and compared with the entropy-based HVS model used in the transform domain to insert the ECC entropy binary watermark in images. Test results of this part demonstrated that the proposed watermarking scheme got better results in terms of imperceptibility and robustness as compared to other schemes.

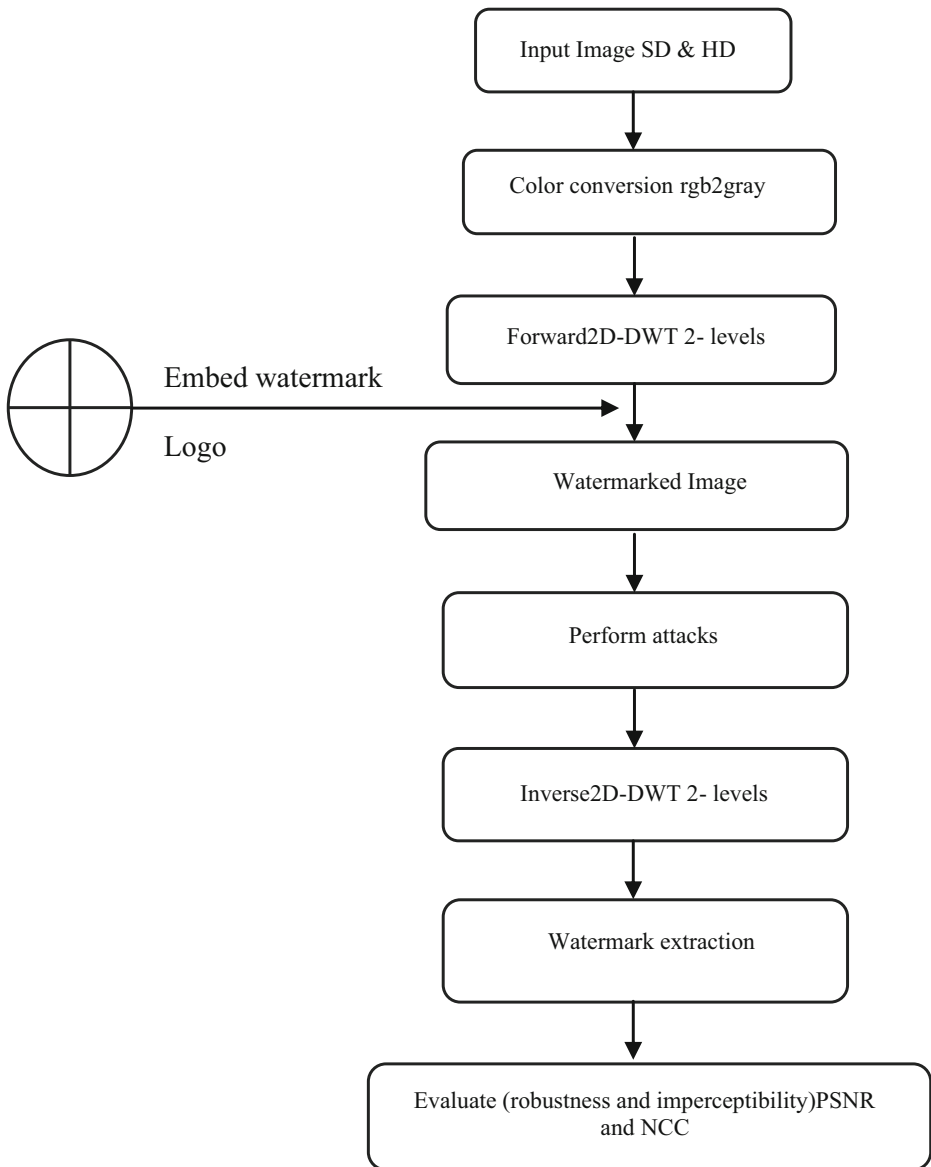
Savakar Dayanand and Anand Ghuli [30] proposed an imperceptible hybrid watermarking algorithm based on blind and non-blind watermarking schemes. The blind scheme is operated as an inner scheme whereas a non-blind scheme utilized as an outer scheme. A watermark secret binary data is embedded in an inner cover image by using (DWT) with the assistance of the blind watermarking method combined with the predefined binary digit sequence block and gain factor  $\alpha$  to obtain the inner watermarked image. Subsequently, the watermarked image is embedded into an outer cover image using DWT and SVD by the non-blind watermarking method to achieve the hybrid watermarked image. On the other hand, the secret binary image is extracted by non-blind and blind watermark extraction techniques. Test results show that the proposed approach has better robustness against various attacks (JPEG compression, image rotation, salt and pepper noise, Gaussian noise, speckle, and Poisson noise).

### 3 The proposed watermarking algorithm

The main aim of developing the proposed semi-blind image watermarking is to improve the robustness and imperceptibility of the embedded watermark before and after applying different kinds of attacks. The watermark (logo of Sulaimani and Halabja universities) is hiding in both standard quality images (Lena, Cameraman, Baboon) and high quality images (1K, 2K, 4K). The host image is first transformed in the frequency domain using two passes of wavelet transformation. Then, the watermark image is also transformed using one pass of wavelet transformation and applying SVD on the LL band of the watermark. Eventually, the watermarked image is subjected to the objective evaluation based on PSNR and Correlation Coefficient. JPEG compression, signal processing, and geometric transformation are used as an attacker tool. The general block diagram of the proposed image watermarking scheme is shown in Fig. 1.

#### 3.1 Color space conversion

There are many reasons for using grayscale instead of color information in image processing. First of all, converting RGB into a gray image is simply reducing the complexity of calculation because the data is fetching from one channel. Another reason is the sensitivity of the human vision system HVS to the brightness than the RGB color. Finally, the grayscale images are mostly used in steganography and watermarking techniques.



**Fig. 1** General diagram of the proposed scheme

### 3.2 Watermark embedding process

In the proposed approach scheme, the hidden watermark must be imperceptible to human eyes and robust against image processing attacks. To get by, the watermark logo must first transform into the frequency domain using wavelet transformation. And then, SVD is applied to the LL band to get the Singular values of the diagonal matrix. In the following subsections, DWT, SVD, and embedding process are described.

### 3.2.1 2D – Wavelet transformation

DWT has a significant multi-resolution property. It decomposes the gray image (both cover and watermark) on a logarithmic scale for the constant frequency bandwidth. DWT transforms the input image into four sub-bands namely LL (Low–Low or approximation), LH (Low–High or horizontal), HL (High–Low or vertical), and HH (High–High or diagonal) at the first level of decomposition. Additional decomposition of LL sub-band provides LL2, LH2, HL2, and HH2 at the second level and others. As a general rule, LL appears for the smooth variations in a color while (LH, HL, and HH) represent the sharp variations of the color level. Differently, the basic structure of an image is composed by the LL, and the edges which give the details are composed by LH, HL, and HH. In this paper, the cover image is transformed by DWT for two levels of decomposition. Moreover, the watermark image is also transformed at the first level.

### 3.2.2 SVD transformation

In this paper, let  $A$  represents a matrix of watermark image. When the SVD transform is applied to  $A$ , it is transformed into three matrices. They are similar in size to the original matrix. On the report of linear algebra, an array of nonnegative elements which can be considered as a matrix can be shown as an image. If an image is denoted by  $A$ , where  $A \in R_{n \times n}$ ,  $R$  is the realnumber domain, then SVD of  $A$  is given by [37]:

$$A = USV^T \quad (1)$$

$U \in R_{n \times n}$  and  $V \in R_{n \times n}$  are orthogonal matrices and  $S \in R_{n \times n}$  is a diagonal matrix given by,

$$S = \begin{bmatrix} \rho_1 & & \\ & \rho_2 & \\ & & \rho_n \end{bmatrix} \quad (2)$$

Here  $\rho$ 's (diagonal elements) are known as singular values which satisfy:

$$\rho_1 \geq \rho_2 \geq \rho_r \geq \rho_{r+1} = \rho_{r+2} \dots = \rho_n = 0 \quad (3)$$

SVD properties are useful in image watermarking schemes. In recent times, image watermarking techniques based on SVD have been combined with other kinds of transformation including DWT, DCT, and DWT. This hybridization improves the robustness and the imperceptibility of the watermark hiding in different image watermarking applications.

### 3.2.3 Proposed embedding scheme

The following steps are performed to embed the watermark data into the host image using zigzag technique.

1. A color image using as a host image ' $T$ ' with different sizes  $256 \times 256$ , 1 K, 2 K, 4 K and a color watermark image ' $w$ ' having the size of  $128 \times 128$  are taken.
2. Both cover and watermark images are converted into a gray scale images.
3. 2nd level DWT decomposition is applied to the host image. 1st level of DWT decomposition is performed on the watermark image.



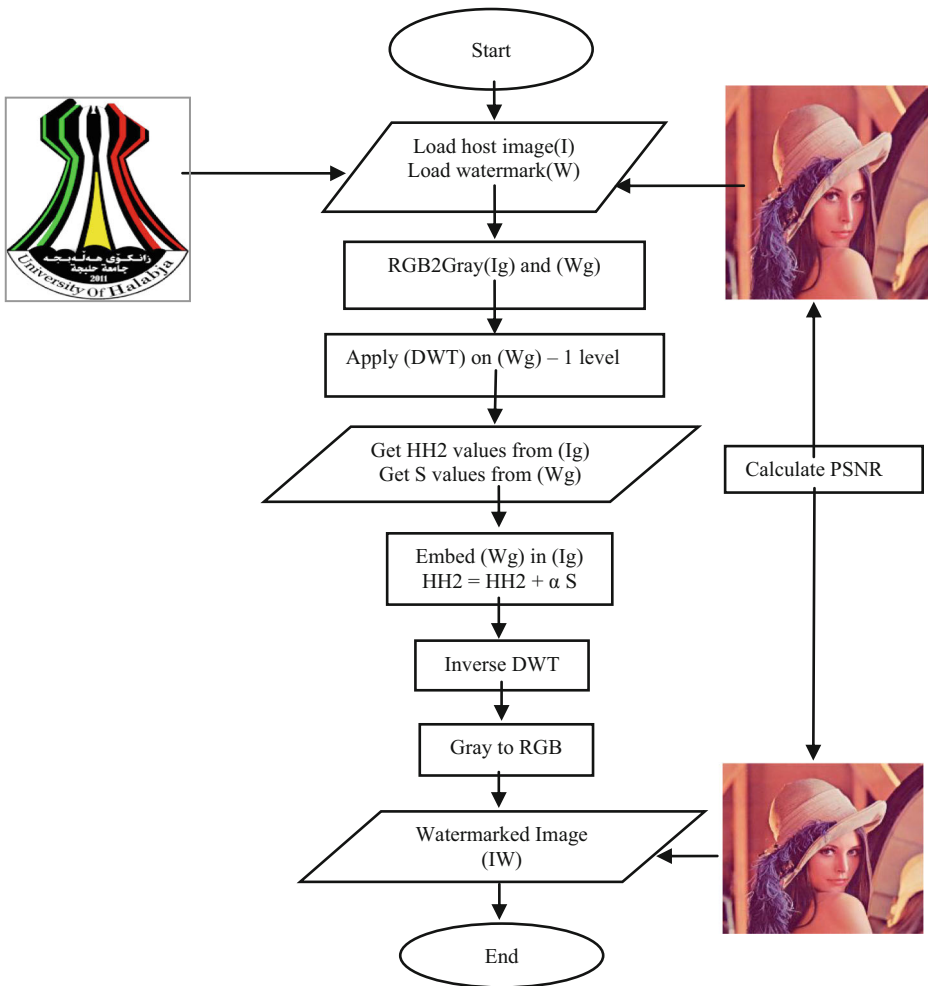


Fig. 2 Watermark embedding flowchart

4. Furthermore, the LL1 band of the watermark is transformed by SVD. It gives  $USV^T$  matrices. Then, the HH2 band of the host image is modified by the singular values of the watermark  $S$ . To keep the proposed scheme semi-blind, only the  $S$  values of the watermark LL1band is embedded in the HH2 band of the host image. Other bands (LH1, HL1, HH1) are set to zero. A copy of the original watermark is saved in HL2 band for the extraction process.

$$HH_2 = HH_2 + \alpha S \tag{4}$$

Where  $\alpha$  represents the scale factor. It is used to control the strength of the watermark to be embedded.

5. Inverse DWT is performed on the modified  $HH_2$ band to obtain the watermarked image  $I_w$ .

Figure 2 shows the proposed embedding process diagram.

### 3.2.4 Zigzag embedding technique

When the singular values of the diagonal matrix (64 values) is embedded into the HH2 band of the host image, the watermark data is visible and clearly appear on the watermarked image. Therefore, a new strategy is followed to embed the watermark based on the zigzag mechanism. The technique distributes the watermark data according to Fig. 3. The figure shows only a block (16\*16) of the HH2 band of the host image. Singular diagonal values  $S$  of the watermark are embedding by starting from the column 20 with a step size 16 as described below.

$$S = \text{diag}(S');$$

$$\text{zigzag\_HH2} = \text{zigzag}(\text{HH2});$$

$$\text{zigzag\_HH2}(20:16:w*h) = \text{zigzag\_HH2}(20:16:w*h) + (\text{alpha}*S);$$

Here,  $S$  is the diagonal matrix of SVD and  $w,h$  represents the width and the height of HH2 band of the cover image.

In Fig. 4, the imperceptibility of the watermarked image is shown with and without zigzag technique.

### 3.3 Watermark extracting process

To extract the watermark from the watermarked image, the following steps are performed.

1. Second order of DWT decomposition is applied to the watermarked image ( $I_w$ ).
2. Reconstruct the singular value  $S$  using the following formula:

$$S = (HH_2 - HL_2) / \rho \tag{5}$$

3. Reconstruct the LL1 of the watermark from  $S, U,$  and  $V^T$  values.
4. Apply one level IDWT to the LL1 and set LH1, HL1, and HH1 to zero.
5. Extract the  $128 \times 128$  watermark image.
6. Compare the similarity between the extracted watermark and the original one using correlation coefficient measurement.

0	1	5	6	14	15	27	28	44	45	65	66	90	91	119	120
2	4	7	13	16	26	29	43	46	54	67	89	92	118	121	150
3	8	12	17	25	30	42	47	63	68	88	93	117	122	149	151
9	11	18	24	31	41	48	62	69	87	94	116	123	148	152	177
10	19	23	32	40	49	61	70	86	95	115	124	147	153	176	178
20	22	33	39	50	60	71	85	96	114	125	146	154	175	179	200
21	34	38	51	59	72	84	97	113	126	145	155	174	180	199	201
35	37	52	58	73	83	98	112	127	144	156	173	181	198	202	219
36	53	57	74	82	99	111	128	143	157	172	182	197	203	218	220
54	56	75	81	100	110	129	142	158	171	183	196	204	217	221	234
55	76	80	101	109	130	141	159	170	184	195	205	216	222	233	235
77	79	102	108	131	140	160	169	185	194	206	215	223	232	236	245
78	103	107	132	139	161	168	186	193	207	214	224	231	237	244	246
104	106	133	138	162	167	187	192	208	215	225	230	238	243	247	252
105	134	137	163	166	188	191	209	212	226	229	239	242	248	251	253
135	136	164	165	189	190	210	211	227	228	240	241	249	250	254	255

Fig. 3 Watermark embedding using zigzag technique



Normal technique

Improved technique

Fig. 4 Imperceptible watermark with zigzag embedding

### 3.4 Attack on the watermarked image

To find the robustness of the proposed scheme, several types of attack must be applied to the watermarked image in order to evaluate the performance of the proposed system in terms of imperceptibility and resistance against attacks. Figure 5 illustrates the attack performed on the watermarked image.

## 4 Test results

In the next subsection 4.1, the test samples of watermark and host image for both SD, and HD qualities are described whereas the performance parameters are presented in subsection 4.2. In subsections (4.3 and 4.4) the imperceptibility and the robustness of the proposed watermarking scheme are calculated by conducting different tests.

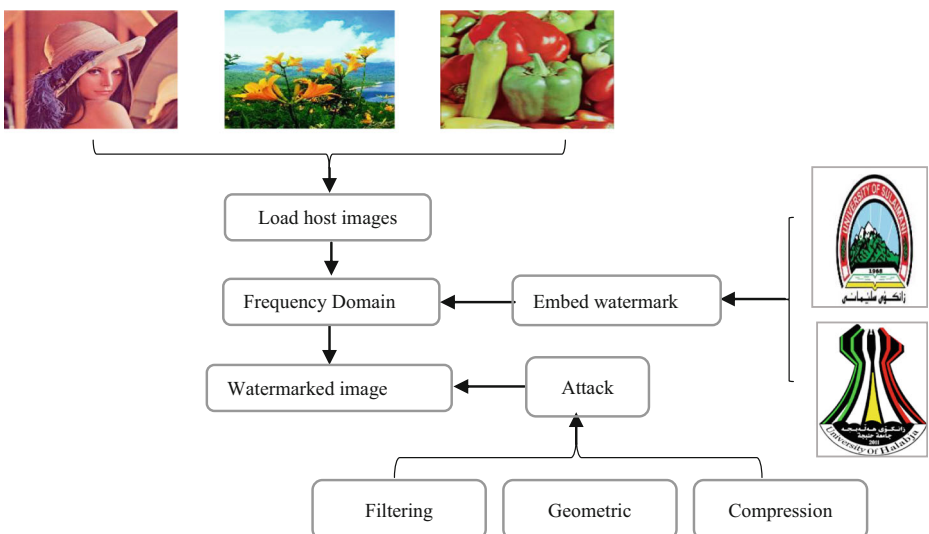


Fig. 5 Signal processing attacks

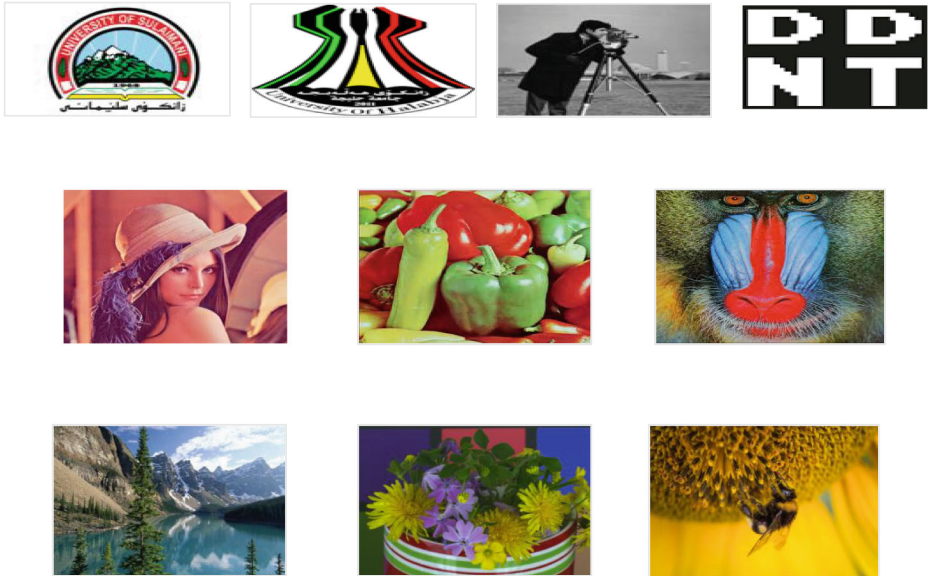


Fig. 6 Test samples

### 4.1 Test samples

In this research work, three images as a watermark of size  $128 \times 128$  (Sulaimani University Logo and Halabja University Logo, Cameraman) plus a binary logo and three standard image qualities as a host of size  $512 \times 512$  (Lena, Pepper, and Baboon) are used. In addition, three high definition image qualities of size 1 K, 2 K, and 4 K (Nature, Flower, and HoneyBees respectively) are also used to carry out optimal results. Figure 6 shows the watermark and the host images.

### 4.2 Performance parameters

The imperceptibility and the robustness of the proposed image watermarking are measured between original, watermarked images and original, extracted watermarks respectively. Peak Signal to Noise Ratio (PSNR) value using Mean Squared Error (MSE) and the similarity using Normalized Correlation Coefficient (CC) are formulated according to the following equations:

$$PSNR = 10 \log \left( \frac{MAX(I_o^2)}{MSE} \right) \tag{6}$$

$$MSE = \frac{1}{n \times m} \sum_{i=1}^n \sum_{j=1}^m \left( I_o(i, j) - I_w(i, j) \right)^2 \tag{7}$$

**Table 1** PSNR (dB) and NCC without attacks

	Watermark Images Image Types																	
	SD (Lena) (512 X 512)			SD (Baboon) (512 X 512)			SD (Pepper) (512 X 512)			HD (1 K) (1920 X 1080)			HD (2 K) (2048 X 1536)			HD (4 K) (4848 X 2808)		
	PSNR	NCC		PSNR	NCC		PSNR	NCC		PSNR	NCC		PSNR	NCC		PSNR	NCC	
Normal Code Only Watermarked Without Attack	Cameraman	42.144	0.968	43.817	0.955	42.516	0.967	51.153	0.968	56.392	0.959	61.585	0.963					
	UoH-Logo	40.278	0.943	41.232	0.926	40.472	0.943	49.219	0.934	52.261	0.935	58.547	0.939					
	UoS-Logo	40.621	0.917	41.879	0.9	40.804	0.915	49.459	0.916	53.536	0.903	59.257	0.91					
Improved Code Only Watermarked Without Attack	Cameraman	54.828	0.968	47.636	0.967	50.69	0.968	58.625	0.968	66.561	0.967	72.611	0.967					
	UoH-Logo	50.659	0.954	46.762	0.952	48.604	0.954	57.155	0.953	63.474	0.946	69.676	0.945					
	UoS-Logo	45.833	0.92	46.888	0.92	49.148	0.92	57.407	0.92	63.816	0.916	70.006	0.916					

**Table 2** PSNR (dB) and NCC without attacks (new logo)

	Watermark Image											
	Lena		Baboon		Pepper		1 K		2 K		4 K	
	PSNR	NCC	PSNR	NCC	PSNR	NCC	PSNR	NCC	PSNR	NCC	PSNR	NCC
Normal Code Only Watermarked Without Attack	41.162	0.979	42.404	0.965	41.221	0.98	49.82	0.981	54.45	0.96	60.076	0.974
Improved Code Only Watermarked Without Attack	53.387	0.9995	47.344	0.9995	50.044	0.999	58.105	0.9996	65.4	0.99	71.532	0.997

**Table 3** NCC for different attacks with improved technique

Image Types							
Attack	Watermark Images	SD (Lena) (512 X 512)	SD (Baboon) (512 X 512)	SD (Pepper) (512 X 512)	HD (1 K) (1920 X 1080)	HD (2 K) (2048 X 1536)	HD (4 K) (4848 X 2808)
		NCC	NCC	NCC	NCC	NCC	NCC
Gaussian	Cameraman	0.9534	0.96	0.9598	0.9619	0.9604	0.9566
Noise (0.0001%)	UoH-Logo	0.9462	0.9489	0.95	0.9464	0.9406	0.9326
	UoS-Logo	0.99164	0.9139	0.9168	0.9139	0.9084	0.9109
Gaussian	Cameraman	0.8529	0.8804	0.8802	0.8796	0.9024	0.8667
Noise (0.001%)	UoH-Logo	0.9005	0.886	0.8789	0.8837	0.8268	0.8528
	UoS-Logo	0.8664	0.8784	0.8198	0.8747	0.8633	0.8114
Gaussian	Cameraman	0.4262	0.6589	0.4078	0.5061	0.5747	0.4979
Noise (0.01%)	UoH-Logo	0.6579	0.5268	0.5356	0.5762	0.6229	0.5946
	UoS-Logo	0.6335	0.5675	0.7002	0.6045	0.5258	0.5251
Gaussian	Cameraman	0.4067	0.4118	0.4201	0.413	0.4189	0.3965
Noise (0.1%)	UoH-Logo	0.2885	0.3091	0.2911	0.2892	0.2891	0.291
	UoS-Logo	0.4054	0.3531	0.3505	0.4174	0.3491	0.3494
Salt & Pepper	Cameraman	0.9598	0.965	0.9682	0.9637	0.9312	0.9671
Noise (0.001%)	UoH-Logo	0.9541	0.9483	0.7822	0.9531	0.9464	0.9457
	UoS-Logo	0.9207	0.9204	0.9208	0.9205	0.9168	0.679
Salt & Pepper	Cameraman	0.8475	0.909	0.4038	0.6893	0.8974	0.8825
Noise (0.01%)	UoH-Logo	0.7639	0.8328	0.9369	0.7983	0.9195	0.8646
	UoS-Logo	0.7898	0.8115	0.7708	0.6302	0.5364	0.6194
Salt & Pepper	Cameraman	0.4163	0.4156	0.4114	0.4092	0.4148	0.5233
Noise (0.1%)	UoH-Logo	0.3045	0.4158	0.2927	0.2909	0.2904	0.2912
	UoS-Logo	0.3525	0.5354	0.3511	0.3511	0.402	0.4869
Median	Cameraman	0.6934	0.4726	0.5808	0.4143	0.9236	0.8835
Filtering (3X3)	UoH-Logo	0.7596	0.4779	0.5696	0.293	0.883	0.8536
	UoS-Logo	0.739	0.5026	0.5386	0.3974	0.8634	0.8286
Median	Cameraman	0.4141	0.4122	0.4121	0.4179	0.5092	0.4102
Filtering (5X5)	UoH-Logo	0.2901	0.2902	0.3559	0.2927	0.4585	0.3347
	UoS-Logo	0.3439	0.348	0.3499	0.3491	0.3777	0.3494









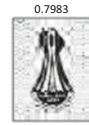





$$NCC = \frac{\sum_{i=1}^n \sum_{j=1}^m (W_o(i, j) - W_e(i, j))}{\sum_{i=1}^n \sum_{j=1}^m (W_o(i, j))^2 * \sum_{i=1}^n \sum_{j=1}^m (W_e(i, j))^2} \tag{8}$$

Here,  $I_o(i, j)$  and  $I_w(i, j)$  are the original and watermarked images respectively. Here,  $W_o(i, j)$  is the original watermark and  $W_e(i, j)$  is the extracted watermark.

### 4.3 Imperceptibility

The proposed image watermarking scheme with normal and zigzag embedding techniques wasted on the all mentioned previously test samples. Table 1 shows the test results of PSNR and NCC when there is no attack performing on the watermarked image. The first part of the test is done with a normal distribution (normal code) of the watermark data within host images while the second part is performed when the zigzag embedding is used (improved code). Test results show that there is a significant improvement in imperceptibility when the improved embedding technique is applied.

**Table 4** NCC between original and extracted watermarks.

Attacks	Watermark Images	Image Types					
		SD (Lena) (512 X 512)	SD (Baboon) (512 X 512)	SD (Pepper) (512 X 512)	HD (1K) (1920 X 1080)	HD (2K) (2048 X 1536)	HD (4K) (4848 X 2808)
		NCC	NCC	NCC	NCC	NCC	NCC
Gaussian Noise 0.0001%	Camerman	0.9543	0.96	0.9598	0.9619	0.9604	0.9566
							
	UoH-Logo	0.7639	0.8328	0.9369	0.7983	0.9195	0.8646
							
	UoS-Logo	0.6481	0.5261	0.5041	0.3487	0.8527	0.8389
							
	Average Filtering 3 X 3						

As illustrated in Fig. 4, the visual perception of the watermarked image has perfect quality in all cases, especially when for the improved embedding technique. For comparison reasons with other related works, a new logo as a watermark has been used. Table 2 presents the PSNR and NCC without applying any attacks. The logo is a simple binary image  $128^*128$  taking from [12].

#### 4.4 Robustness

To evaluate the performance of the proposed watermarking scheme, the watermarked images are subjected to the common attacks for different parameters. In Tables 3, the test results in terms of NCC between the original and the extracted watermarks are presented only when the improved technique is used.

According to the obtained results, the proposed approach has better robustness when the image processing attacks are used. In Table 4 some extracted watermarks with different kinds of attacks are shown.

Tables 3 and 4 show that the proposed approach has higher robustness especially for high quality images (2 K and 4 K) which is a new contribution to the field of image watermarking. Moreover, there are various researches that can be compared with the proposed scheme. However, they are few works tested uniquely on the HD image quality. For that reason, the robustness is also tested with a new logo. In Table 5, the test results in terms of NCC between the original and the extracted watermarks are presented only when the improved technique is used. Test results show that the proposed approach outperforms other works mainly for image compression attack using a jpeg compression factor of 50% and 75%. Furthermore, it could be noticed that the proposed image watermarking scheme indicates an optimal result in term of robustness NCC particularly for HD images (2 K and 4 K). Table 6 presents some extracted watermarks with image compression attack for the binary logo.



**Table 5** NCC for different attacks with improved technique (new logo)

Attack	Watermark Images	Image Types					
		SD (Lena) (512 X 512)	SD (Baboon) (512 X 512)	SD (Pepper) (512 X 512)	HD (1 K) (1920 X 1080)	HD (2 K) (2048 X 1536)	HD (4 K) (4848 X 2808)
		NCC	NCC	NCC	NCC	NCC	NCC
Gaussian Noise (0.0001%)	New Logo	0.994	0.995	0.9951	0.9977	0.9953	0.9929
Gaussian Noise (0.001%)	New Logo	0.9534	0.9464	0.9556	0.9624	0.9347	0.9475
Gaussian Noise (0.01%)	New Logo	0.7405	0.6911	0.7323	0.6529	0.8705	0.7169
Salt & Pepper Noise (0.001%)	New Logo	0.9629	0.9995	0.994	0.9901	0.998	0.9866
Salt & Pepper Noise (0.01%)	New Logo	0.9968	0.9938	0.8934	0.9981	0.815	0.9749
Median Filtering (3X3)	New Logo	0.8288	0.6001	0.689	0.6145	0.8793	0.8621
Average Filtering (3X3)	New Logo	0.772	0.5811	0.6449	0.5245	0.8731	0.8286
Jpeg compression (75%)	New Logo	0.9804	0.9809	0.9782	0.9752	0.9881	0.9895
Jpeg compression (50%)	New Logo	0.9795	0.8385	0.9544	0.934	0.9757	0.9714

### 4.5 Comparison with the existing approaches

The performance evaluation in terms of imperceptibility and the robustness of the proposed approach is compared with some existing research works that used DWT and/or SVD schemes.

**Table 6** Extracted watermarks with jpeg compression attack.

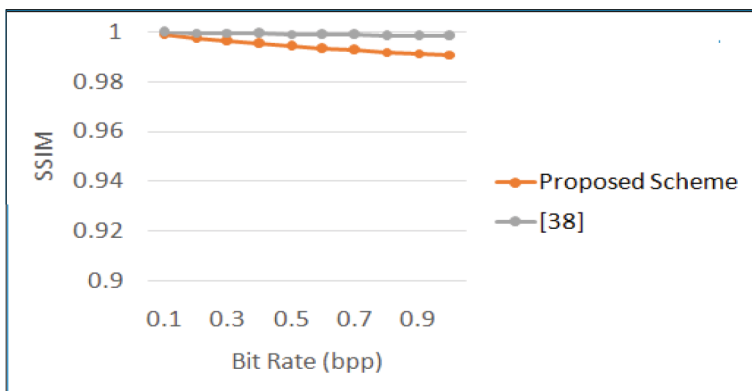
Attack	Watermark Images	Image Types					
		SD (Lena) (512 X 512)	SD (Baboon) (512 X 512)	SD (Pepper) (512 X 512)	HD (1K) (1920 X 1080)	HD (2K) (2048 X 1536)	HD (4K) (4848 X 2808)
Jpeg compression 75%							
Jpeg compression 50%							

**Table 7** Performance comparisons with NCC

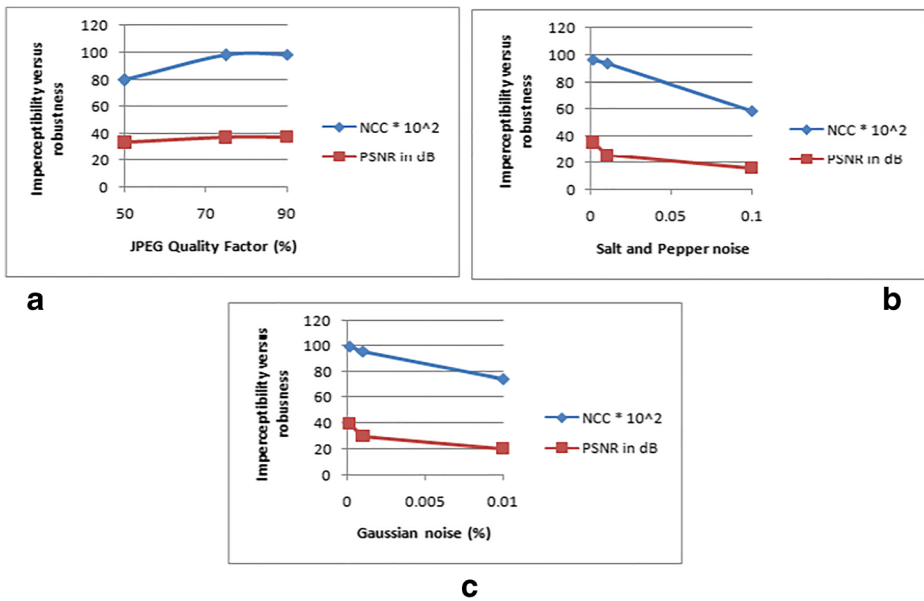
Schemes	Attacks	Image types			
		SD (Lena) HD (1 K)HD (2 K) (512 X 512) (1920 X 1080)(2048 X 1536)	NCC	NCC	NCC
[14]	Gaussian Noise 0.001	0.844	0.999	1.00	
	Low pass Filter 3X3	0.808	0.9944	0.725	
	Jpeg Compression 50%	0.88	0.9960	0.894	
<u>Proposed scheme</u>	Gaussian Noise0.001	<b>0.953</b>	0.962	0.934	
	Low pass Filter 3 X3	<b>0.943</b>	0.8793	<b>0.873</b>	
	Jpeg Compression 50%	<b>0.979</b>	0.934	<b>0.975</b>	
Schemes	Attacks	SD (Lena) HD (1 K)HD (2 K) (512 X 512) (1920 X 1080)(2048 X 1536)	NCC	NCC	NCC
[25]	Gaussian Noise0.01	0.895	0.821		
	Salt & Pepper 0.01	0.256	0.203		
	Jpeg Compression 50	0.950	0.943		
[36]	Gaussian Noise 0.01	0.996	0.999		
	Salt & Pepper 0.01	0.998	0.999		
	Jpeg Compression 50%	0.868	0.858		
[4]	Gaussian Noise 0.01	0.993	0.956		
	Salt & Pepper 0.01	0.971	0.968		
	Jpeg Compression 50	0.887	0.79		
<u>Proposed scheme</u>	Gaussian Noise 0.01	0.953	0.946		
	Salt & Pepper 0.01	<b>0.982</b>	<b>0.999</b>		
	Jpeg Compression 50%	<b>0.979</b>	<b>0.83</b>		

Table 7 consists of NCC measure between the original and extracted watermark data as the robustness metric of the various type of attacks. The robustness performance is measured by the same measurement corresponding to the existing schemes. Therefore, the NCC values of the existing scheme were taken from the corresponding reference.

The first comparison has been done with [14], which is based on DWT-SVD transforms and performed on both SD and HD images. Another comparison is done with [4, 25, 36] which contains different SD quality images. Finally, we found the SSIM of the improved



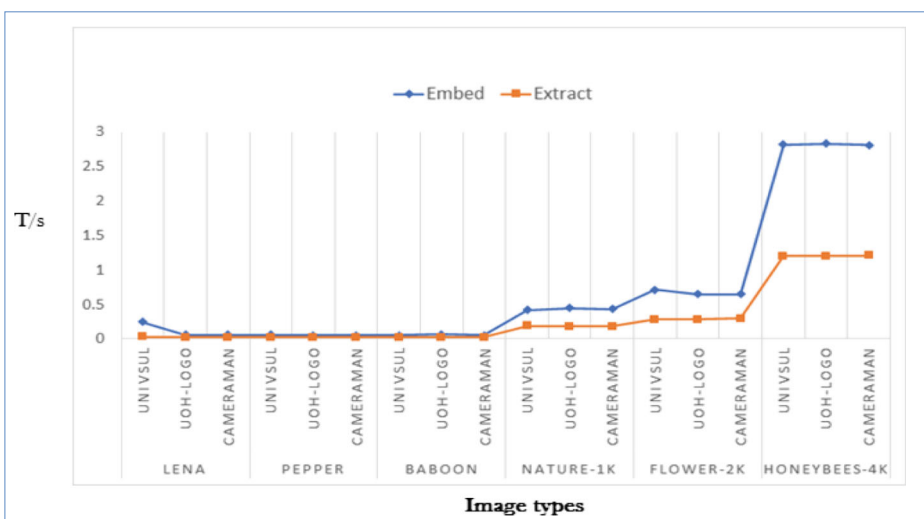
**Fig. 7** SSIM comparison with different embedding rates



**Fig. 8** Effects of attack parameters on PSNR and NCC (a) compression (b) Salt & Pepper noise (c) Gaussian noise

scheme between cover and watermarked image for different bitrates (0:1:0.1) in order to compare with the result given in [32]. Test results in Fig. 7 show that our proposed technique is significantly efficient for the texture images. SSIM values are always greater than 0.99 which can be consider as an accurate watermark embedding system.

The effect of the different type of attack parameters such as (compression, salt & pepper noise, and Gaussian noise) is studied for the performance metrics PSNR and NCC as shown in Fig. 8. In the conducted test, only the improved technique is used and applied to the Lena



**Fig. 9** Computational cost for improved technique

image. Figure 8-A illustrates that a high NCC (almost 1.00) is obtained for jpeg quality factors 75% and 90% respectively while for the QF = 50, the NCC is decreased to ~0.8. Moreover, the imperceptibility PSNR is decreased when the quality of the watermarked image is degraded especially for QF = 50. Figures 8-B and 8-C present the impact of the Salt & Pepper and Gaussian noise parameters on the proposed method performance. Accordingly, it can clearly be seen that both NCC and PSNR are reduced for the larger amount of noise.

#### 4.6 Computational cost for improved technique

It can be clearly seen from the Fig. 8 that the execution time for embedding and extracting processes increases as the quality of the cover image increases, even though the embedded logo size is always constant (128 X 128). This due to the transformation of the cover images into frequency domain using DWT algorithm. When the high quality cover images are used, more time is required to transform them into the frequency domain.

Another equally important point from Fig. 8 is that the embedding time is higher than the extraction time, especially in the case of using high quality cover images, in which embedding requires twice the time of extraction. This is because in the case of embedding the cover images have to go into one more step that the extraction process does not have it, which is 2-level Inverse Discrete Wavelet Transform (IDWT). In other words, after transferring the cover images into frequency domain and adding the diagonal singular values of the logos to them, they have to be reconstructed in order to reconstruct them (i.e. watermarked image).

### 5 Conclusion

In this paper, a semi-blind image watermarking scheme in DWT and SVD transform domain is developed. It mainly emphasizes on improving the imperceptibility using PSNR metric for both SD and HD quality images as presented in Fig. 4 and Table 1. The proposed zigzag embedding technique has increased the invisibility of the watermark data inside the host image for all image types. In most cases, it has better robustness compared with other related works for different kinds of attacks especially for image compression attack as illustrated in Table 6. Furthermore, two types of watermarks are used to show the performance of the developed approach. For instance, high texture and simple binary images are utilized for the embedding process. Test results show that the quality of the watermarked image has attained an optimal value 54.826 dB for SD images and 72.611 dB for HD images. In addition, the optimal NCC has reached for a binary logo watermark when a jpeg compression (50%) attack is performed to the watermarked image and it is 0.975 for 2 K image and 0.979 for SD image. Also, the computational cost of the improved proposing scheme is calculated for both embedding and extracting processes as depicted in Fig. 9. Finally, the improved scheme is compared with references [4, 14, 25, 36] for both SD and HD images as described in Table 7.

**Acknowledgements** This research is a part of the research work between the University of Sulaimani and Halabja in Kurdistan Region of Iraq. Special thanks to the college of science at both universities for providing a healthy environment to fulfill this project. We would also like to express our deep gratitude for generous support and funds by the presidency of Sulaimani and Halabja universities.

## References

1. Abdallah, Emad E, A Ben Hamza, and Prabir Bhattacharya (2007). “Spectral graph-theoretic approach to 3D mesh watermarking”; Proceedings of Graphics Interface
2. Abdallah, Emad E, A Ben Hamza, and Prabir Bhattacharya (2009). “Watermarking 3D models using spectral mesh compression”; Signal, image and video processing
3. Abdallah EE, Hamza AB, Bhattacharya P (2010) Video watermarking using wavelet transform and tensor algebra. *SIViP* 4(2):233–245
4. Abraham J, Paul V (2019) An imperceptible spatial domain color image watermarking scheme. *Journal of King Saud University-Computer and Information Sciences* 31(1):125–133
5. Arora SM (2018) A DWT-SVD based robust digital watermarking for digital images. *Procedia computer science* 132:1441–1448
6. Chrysochos E et al (2014) Hybrid watermarking based on chaos and histogram modification. *Signal, Image and Video Processing* 8.5:843–857
7. IS Coaxial (2008), “Digital Watermarking and Steganography.”Morgan Kaufmann Publisher
8. Ermawan F, Kabir MN (2018) A robust image watermarking technique with an optimal DCT- psychovisual threshold. *IEEE Access* 6:20464–20480
9. Fazli S, Moeini M (2016) A robust image watermarking method based on DWT, DCT, and SVD using a new technique for correction of main geometric attacks. *Optik* 127(2):964–972
10. Gupta R, Mishra A, Jain S (2018) A semi-blind HVS based image watermarking scheme using elliptic curve cryptography. *Multimed Tools Appl* 77(15):19235–19260
11. Hamidi M, Haziti ME, Cherifi H, Hassouni ME (2018) Hybrid blind robust image watermarking technique based on DFT-DCT and Arnold transform. *Multimed Tools Appl* 77(20):27181–27214
12. Hurrh, Nasir N., et al (2017). “A transform domain based robust color image watermarking scheme for single and dual attacks.” 2017 Fourth International Conference on Image Information Processing (ICIIP). IEEE
13. Kumar C, Singh AK, Kumar P (2018) A recent survey on image watermarking techniques and its application in e-governance. *Multimed Tools Appl* 77(3):3597–3622
14. Lee Y-S, Seo Y-H, Kim D-W (2019) Blind image watermarking based on adaptive data spreading in n-level DWT subbands. *Security and Communication Networks* 2019:1–11
15. Minamoto, Teruya, and Ryuji Ohura (2011). “A non-blind digital image watermarking method based on the dyadic wavelet transform and interval arithmetic.” International Conference on Signal Processing, Image Processing, and Pattern Recognition. Springer, Berlin, Heidelberg
16. Moeinaddini E, Afsari F (2018) Robust watermarking in DWT domain using SVD and opposition and dimensional based modified firefly algorithm. *Multimed Tools Appl* 77.19:26083–26105
17. Mohammed AA, Ali NA (2018) Robust video watermarking scheme using high efficiency video coding attack. *Multimed Tools Appl* 77(2):2791–2806
18. Mohammed, Aree Ali, and Haval Mohammed Sidqi (2011). “Robust image watermarking scheme based on wavelet technique.” *IJCSS*, Vol.5, Issue.4, Malaysia
19. Moosazadeh M, Gholamhossein Ekbatanifard (2019) A new DCT-based robust image watermarking method using teaching-learning-based optimization. *Journal of Information Security and Applications* 47:28–38
20. Nasir I et al (2010) Multiple spatial watermarking technique in color images. *SIViP* 4(2):145–154
21. Ntalianis, Klimis S., et al (2002). “Automatic stereoscopic video object-based watermarking using qualified significant wavelet trees.” 2002 Digest of Technical Papers. International Conference on Consumer Electronics (IEEE Cat. No. 02CH37300). IEEE
22. Pal AK, Roy S (2018) A robust and blind image watermarking scheme in DCT domain. *Int J Inf Comput Secur* 10(4):321–340
23. Piva, Alessandro, Roberto Caldelli, and Alessia De Rosa (2000). “A DWT-based object watermarking system for MPEG-4 video streams.” Proceedings 2000 International Conference on Image Processing (Cat. No. 00CH37101). Vol. 3. IEEE
24. Preda RO, Vizireanu DN (2010) A robust digital watermarking scheme for video copyright protection in the wavelet domain. *Measurement* 43(10):1720–1726
25. Rahman, Md Maklachur, et al (2017). “A semi blind watermarking technique for copyright protection of image based on DCT and SVD domain.” *Global Journal of Research In Engineering*
26. Rai, Sandeep, et al. (2019). “Digital Image Watermarking Against Geometrical Attack.” *Data, Engineering and applications*. Springer, Singapore. 129–145
27. Rasti P, Samiei S, Agoyi M, Escalera S, Anbarjafari G (2016) Robust non-blind color video watermarking using QR decomposition and entropy analysis. *J Vis Commun Image Represent* 38:838–847
28. Reddy B, Jadhav A (2015) Visible and Invisible Image Watermarking. *IJERT* 3.1:1–4

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. Savakar DG, AnandGhuli (2019) Robust invisible digital image watermarking using hybrid scheme. *Arab J Sci Eng* 44(4):3995–4008
31. Savakar DG, Ghuli A (2017) Non-blind digital watermarking with enhanced image embedding capacity using DMeyer wavelet decomposition, SVD, and DFT. *Pattern Recognition and Image Analysis* 27(3):511–517
32. C. Shaji and I. Shatheesh Sam (2019). “A new data encoding based on maximum to minimum histogram in reversible data hiding”, of *J Imaging Sci*, Vol. 67, [Issue 4](#)
33. Singh S, Rathore VS, Singh R, Singh MK (2017) Hybrid semi-blind image watermarking in redundant wavelet domain. *Multimed Tools Appl* 76(18):19113–19137
34. Su Q, Chen B (2018) Robust color image watermarking technique in the spatial domain. *Soft Comput* 22(1):91–106
35. Tay, R, and JP Havlicek (2002). “Image watermarking using wavelets.” The 2002 45<sup>th</sup> Midwest Symposium on Circuits and Systems, 2002. MWSCAS-2002.. Vol. 3. IEEE
36. Vaidya P, Chandra Mouli PVSSR (2017) A robust semi-blind watermarking for color images based on multiple decompositions. *Multimed Tools Appl* 76(24):25623–25656
37. Yadav, Bandana, Ashish Kumar, and Yogendera Kumar (2018). “A robust digital image watermarking algorithm using DWT and SVD.” *Soft Computing: Theories and applications*. Springer, Singapore. 25–36
38. Zhou X, Zhang H, Wang C (2018) A robust image watermarking technique based on DWT, APDCBT, and SVD. *Symmetry* 10(3):77

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



**Prof. Aree Ali Mohammed** was born in Sulaimani city–Kurdistan Region Iraq. He obtained BSc degree at the University of Mousle (1995), MSc degree in France in computer Science (2003) and PhD in multimedia system at the University of Sulaimani (2008). He directed Information Technology Directorate for four years (2010–2014) and the head of computer science department/ college of Science / University of Sulaimani for seven years. The main filed of interest is about multimedia system application for processing, compression and security. Many papers have been published in scientific journals throughout the world.



**Dilman Abdalla Salih** is a teaching assistant at the University of Halabja, department of computer science. He received his BSc. in computer science at the University of Sulaimani in 2011 and stood the 1st out of sixty eight graduates. He received his MSc. in Human-Computer Interaction at the University of Birmingham in 2016 under the KRG-HCDT scholarship program for distinguished young men and women to continue their education in internationally renowned universities.



**Ari Muhammad Saeed** is a Lecturer at University of Halabja, department of computer science, college of science; he received BSc. in computer science at university of Sulaimani in 2010 and MSc. in computer engineering at European University of Lefke in 2015. He is working in the field of artificial intelligence.



**Mohammed Qader Kheder** is a lecturer in the computer science department/ college of science at the University of Sulaimani. He graduated high education with Bachelor of Computer Science at Sulaimani University in 2008. After that, in 2011 he went to United Kingdom to continue his master of Advanced Computer Science at Huddersfield University. He also by his researches could pass from Assistant Lecturer to Lecturer at the University of Sulaimani.