

## Hybrid and blind watermarking scheme in DCuT – RDWT domain

Rohit Thanki<sup>a,\*</sup>, Ashish Kothari<sup>b</sup>, Deven Trivedi<sup>c</sup>

<sup>a</sup> Faculty of Technology and Engineering, C. U. Shah University, Wadhwan City, India

<sup>b</sup> Atmiya University, Rajkot, India

<sup>c</sup> Department of ECE, G. H. Patel College of Engineering and Technology, Vallabh Vidyanagar, India



### ARTICLE INFO

#### Keywords:

Arnold scrambling  
Copyright protection  
Discrete curvelet transform (DCuT)  
Image watermarking  
Redundant discrete wavelet transform (RDWT)  
Security

### ABSTRACT

In this paper, a hybrid and blind watermarking scheme is proposed for the protection of copyright of digital images. The scheme based on hybridization of two advance transforms such that discrete curvelet transform (DCuT) and redundant discrete wavelet transform (RDWT). The motivation behind using these two transforms combination to improve the imperceptibility of the watermarking scheme. The imperceptibility requirement of the scheme is achieved using hybrid coefficients which are achieved by applying single level RDWT to the high frequency curvelet coefficients of the cover image. The watermark information is inserted by modifying the coefficients of the wavelet coefficients of LH subband using PN sequences according to watermark bit and gain factor. The security of the proposed scheme is achieved by applying Arnold scrambling to watermark image before embedding. Experiments of the proposed scheme are conducted on various types of natural images. Experiments results show that, compared with existing schemes, the proposed scheme is robust to various attacks while having high imperceptibility. Also, the proposed scheme is performed better than many existing schemes.

© 2019 Elsevier Ltd. All rights reserved.

### 1. Introduction

With the rapid used or social media for sharing of multimedia information using digital devices, the images are easily manipulated, duplicated and transmitted. Therefore, preventing unauthorized use of these images has become more important [1]. For the solution of this issue, robust digital watermarking is used. The basic concept of watermarking is to embed an owner identity within the cover image to secure it from unauthorized usage [2,3]. In general, any watermarking scheme should be fulfilled four requirements such as imperceptibility, robustness, payload capacity and security [4,5]. A good watermarking scheme must provide a good tradeoff between these requirements according to targeted applications. The main and important requirements of any watermarking scheme are imperceptibility and robustness. The imperceptibility refers to the perceptual similarity between the original cover image and watermarked image. If any watermarking scheme does not provide good imperceptibility than it is not preferable for targeted applications. The robustness refers as resistance ability of scheme against watermarking attacks. While

the payload capacity refers as maximum watermark bits can be inserted into host data for given any watermarking scheme. The last requirement is security and refers to its ability to resist against unauthorized extraction of watermark information. To achieve this requirement, various encryption methods are used as an additional step in the watermarking scheme [6].

Digital watermarking can be used in many applications such as copyright protection, ownership authentication, etc. [1–6]. In copyright protection, the goal of the application is secure digital information over transmission networks like the internet and communication channel. While ownership authentication is an application which identifies modification or tampering has been applied to digital information or not. This application is also used for localization of tampered region within digital information. Watermarking can be used in applications where very important digital information such as medical images [7], digital audio signals, speech signals [8], etc. are involved.

The different types of classification for the watermarking scheme are available in the literature [5]. Based on the resistance against watermarking attacks, the scheme can be classified as robust, fragile and semi-fragile. The fragile watermarking scheme is mainly proposed for applications of ownership identification and integrity verification [9]. These schemes are used for identification unauthorized manipulation in digital information. Semi fragile watermarking schemes are implemented for the identification of

\* Corresponding author.

E-mail addresses: [rohitthanki9@gmail.com](mailto:rohitthanki9@gmail.com) (R. Thanki), [amkothari@aits.edu.in](mailto:amkothari@aits.edu.in) (A. Kothari).

unauthorized manipulation [4]. Robust watermarking schemes are provided resistance against various watermarking attacks on digital information. The watermarking scheme can be also classified into spatial domain and transform domain according to process domain. In the spatial domain, the pixel of information of host digital information is directly modified by watermark bits. While in the transform domain, transform coefficients of host digital information is modified by watermark bits. Here, various types transform such as discrete Fourier transform (DFT), discrete cosine transform (DCT), discrete wavelet transform (DWT), and singular value decomposition (SVD), etc. are used [1–9].

According to the extraction ability of watermark, the watermarking scheme can be classified into blind, semi-blind and non-blind [10–13]. In the non-blind scheme, information of original host is required; semi-blind scheme requires some information of host and watermark; blind scheme neither needs information of host nor watermark information. The meaning of blind watermarking is that it extracts watermark information from the watermarked information without prior knowledge of actual cover information. The main advantages of this blind watermarking are that it is not required to cover information and suitable for applications such as copyright protection and security of medical data in telemedicine applications [7,10]. The main disadvantages of blind watermarking are that it is more complex than another type of watermarking and has less payload capacity.

In this paper, a hybrid and blind watermarking scheme based on DCuT, RDWT and PN sequences for copyright protection of digital images is proposed. Here, vertical wavelet coefficients after carrying out the discrete curvelet transform (DCuT) of the original cover image is modified by two PN sequences according to scrambled watermark information. In this proposed scheme, PN sequences are used for blind extraction of the watermark at extractor side. A PN sequence is a deterministic binary sequence where binary values appear in a random manner. For watermarking, this sequence is generated using a pseudorandom number generator. This sequence is performed better than another sequence for watermarking because of the following reasons [14]: (a) it has correlation properties, less effects by noise and interference which makes the proper choice for blind extraction. (b) It is periodic sequences with random nature. (c) It generated by an algorithm which uses a random seed. (d) Unless the generation algorithm and random seed are known, then sequence can be predicted by someone. The choice of using DCuT in the proposed scheme has improved the imperceptibility.

However, it has been found that the imperceptibility of the existing schemes based on, SVD, DCT, DWT, redundant discrete wavelet transform (RDWT) set partitioning in hierarchical tree (SPIHT) and non-subsampled contourlet Transform (NSCT) is weak where the wavelet coefficients are used for watermarking embedding [6,10,15–17]. For enhancement to the security in the proposed scheme, the Arnold scrambling is used to encrypt the watermark information. The improvement is achieved after combining these two transforms in term of imperceptibility and robustness is clearly shown in the experimental results. To evaluate the proposed scheme, the performance of the proposed scheme is compared with existing schemes in term of imperceptibility and robustness. The imperceptibility of the proposed scheme is better than existing schemes available in the literature.

This paper is organized as follows. Section 2 described the related works and main contributions of the proposed work. Section 3 gives a description of various terminologies such as RDWT, DCuT, and Arnold scrambling followed by the proposed scheme given in Section 4. Section 5 gives the experimental setup and results. Section 6 gives the possible application of the proposed scheme. Finally, Section 6 concludes the paper.

## 2. Related work

In the literature, different watermarking schemes using various types of image transform have been proposed [1–17]. The famous scheme based on DCT and pseudo-random noise (PN) sequence is proposed by Cox et al. [5], in which, PN sequence is inserted into largest AC DCT coefficients of the cover image. While Garg et al. [14] proposed a blind DWT based watermarking scheme where the PN sequences are inserted to wavelet coefficients of the medical image according to watermark bits. Das et al. [18] proposed a blind DCT based watermarking scheme where the watermark is inserted based on the correlation between the DCT coefficients of two adjacent blocks. Wang and Lin [19] proposed the DWT based blind watermarking scheme where watermark bits are inserted into quantized wavelet coefficients of the cover image.

Feng et al. [20] proposed DWT – DCT, and Arnold scrambling based watermarking scheme. In this scheme, the scrambled watermark logo is embedded in mid-frequency coefficients of DCT blocks of approximation wavelet coefficients using spread spectrum watermarking. The scrambled watermark logo is generated using Arnold scrambling. Sahraee and Ghofrani [21] proposed the DWT based watermarking scheme, in which distance measurement between quantization of adjacent wavelet coefficients of the cover image. Singh and Singh [22] proposed DWT-SVD and DCT based blind watermarking scheme. In this scheme, DCT coefficients of the watermark logo are inserted into the middle singular value of wavelet coefficients of the hybrid block with a size of  $4 \times 4$  of the cover image. This scheme is robust against common signal processing watermarking attacks.

Note that all these schemes are based on hybridization of conventional image transforms and that they all try to insert the scrambled watermark image into selected coefficients of the cover image to improving robustness and imperceptibility. Also, the conventional image transforms have a shift variant which may lead to failure in watermark extraction. So that, overcome this limitation, researchers are introduced redundant discrete wavelet transform (RDWT) in watermarking [23–34]. On other hands, RDWT has limitation such that it requires more wavelet coefficients for representation of edges and curves in the image. Due to this, wavelet based watermarking schemes have less imperceptibility. So that, overcome this limitation, researchers are introduced DCuT in watermarking [35–46]. The various watermarking scheme based on RDWT and FDCuT are given as per follows:

Hien et al. [23] proposed a blind image watermarking scheme using RDWT and independent component analysis (ICA). Here, watermark embedding is performed in RDWT domain while ICA is used for blind recovering of watermark logo. Mankar et al. [24] proposed RDWT and spread spectrum modulation based blind watermarking scheme. In this scheme, wavelet coefficients of cover image are modified by PN sequences. Oskooei et al. [25] proposed RDWT, ICA and principal component analysis (PCA) based blind watermarking scheme. In this scheme, watermark embedding is performed in RDWT domain while hybridization of ICA-PCA is used for blind recovering of watermark logo. Lagzian et al. [26] proposed RDWT – SVD based non-blind watermarking scheme. Here, S matrix values of selected wavelet coefficients of cover image are modified by the watermark logo and gain factor. Makbol and Khoo [27] proposed RDWT – SVD based blind watermarking scheme.

Bajaj [28] proposed RDWT-DCT-SVD based hybrid and non-blind watermarking scheme. In this scheme, S matrix values of all DCT coefficients of selected wavelet coefficients of cover image are modified by the watermark logo and gain factor. Singh et al. [29] proposed RDWT-SVD and Arnold scrambling based multibiometric watermarking scheme. Here, scramble biometric information is taken as watermark and is inserted into S matrix values of selected wavelet coefficients of the cover image. The scrambled

biometric information is generated using Arnold scrambling in this scheme. Thanki et al. [30] proposed RDWT-SVD and compressive sensing based multiple watermarking scheme. Here, S matrix values of three encrypted watermark images are inserted into S matrix values of selected wavelet coefficients of each channel of the color cover image to generate a color watermarked image with multiple watermark logos.

Jamal et al. [31] proposed RDWT-SVD based non-blind watermarking scheme for color images. Roy and Pal [32] proposed RDWT-DCT and Arnold scrambling based blind watermarking scheme. Here, the scrambled watermark logo is inserted into mid frequency DCT coefficients of horizontal wavelet coefficients of the cover image to generate a watermarked image. Singh et al. [33] proposed NSCT-RDWT-SVD based non-blind watermarking scheme. Here, hybrid coefficients of cover image are modified by hybrid coefficients of the watermark logo and gain factor. Ernawan and Kabir [34] proposed RDWT-SVD based blind watermarking scheme for a grayscale image. In this scheme, U matrix value of LL subband of cover image is modified by an encrypted watermark image. The encrypted watermark image is generated using Arnold scrambling.

Zhang et al. [35] proposed the first DCuT based blind watermarking scheme for grayscale images. In this scheme, medium frequency curvelet coefficients of cover image are modified by a binary image to get watermarked image. This scheme is robust against various types of watermarking attacks. Hien et al. [36] proposed DCuT based non-blind watermarking scheme for grayscale images. Here, watermark logo is inserted into selected curvelet coefficients of the cover image to get watermarked image. Tao et al. [37] proposed DCuT based blind watermarking scheme where PN sequences are inserted into selected curvelet coefficients of the cover image according to watermark bit. In this scheme, the selection of curvelet coefficients and the gain factor was done using just noticeable distortion (JND) model. Leung et al. [38,39] proposed robust and non-blind watermarking scheme using DCuT and hamming code. In this scheme, encrypted watermark image is inserted to curvelet coefficients of a selected wedge of the cover image to generate a watermarked image. Here, the encrypted watermark image is generated using a Hamming code.

Song and Gu [40] proposed a curvelet based adaptive watermarking scheme for color images. In this scheme, the watermark is embedded into the middle-frequency curvelet coefficients to generate a watermarked color image. This scheme is robust against various types of watermarking attacks. Lari et al. [41] proposed a curvelet based watermarking scheme using amplitude modulation for the copyright protection of color images. In this scheme, a watermark is embedded in the color image by modifying the pixel values in the blue channel. Channapragada and Prasad [42] proposed different watermarking schemes using DWT and DCuT for color images. In this scheme, the watermark is embedded in the color image by modifying hybrid coefficients which are generated using hybridization of DWT and DCuT. Jero et al. [43] proposed DCuT based watermarking scheme for the security of the ECG signal. This scheme is non-blind and robust against various watermarking attacks. Thanki and Borisagar [44,45] proposed DCuT based watermarking scheme for the security of biometric images and digital audio signals. Thanki et al. [46] proposed blind and robust watermarking scheme using DCuT, DCT and white Gaussian noise (WGN) sequences for the security of medical images.

The main limitation of these existing schemes using individual RDWT and DCuT is that it is unable to fulfill tradeoff between robustness and imperceptibility. So that, take advantage of hybridization of transforms, a new combination of DCuT and RDWT for watermarking is designed and proposed in this paper. The reason behind the choice of this combination is due to the fact

that this combination to enhance imperceptibility of the proposed scheme for providing better robustness against various watermarking attacks. Here, Arnold scrambling provides security to the watermark logo before inserted into the cover image. Following are the special features of the proposed scheme:

- **Improved robustness and imperceptibility:** In the proposed scheme, the watermark data is inserted into the detail wavelet coefficients of selected curvelet coefficients of the cover image which increases the imperceptibility and robustness of the proposed scheme as compared to Roy's scheme [32] and Ernawan's scheme [34]. Here, high frequency coefficients of curvelet decomposition of cover image are used for improving the imperceptibility, while invariant detail wavelet coefficients of cover image are used for improving robustness. Thus, a combination of DCuT and RDWT is improving imperceptibility and robustness of proposed scheme.
- **Security:** In the Singh's scheme [29], watermark bits are directly inserted in to cover image. Thus, this scheme has less security. In the proposed scheme, PN sequences generated using a secret key are used for scaling the cover image in accordance with the watermark bits. This improves the security in the proposed scheme.
- **Blind Extraction:** It is observed from the literature that many existing schemes [16,28–31,36,38,39,43] are based on non-blind approach requiring original data of the cover image in the extraction process. The proposed scheme is blind, requiring only the secret key in the watermark extraction process.

### 3. Preliminaries

The details on discrete curvelet transform, redundant discrete wavelet transform and Arnold scrambling are given in this section.

#### 3.1. Discrete curvelet transform (DCuT)

Discrete curvelet transform (DCuT) was developed by Candes and his research team around 2004 [47,48]. It is a multiresolution transform and used for the sparse representation of the image with geometrical structure. It also overcomes the limitation of FFT and DWT where are a large number of frequency coefficients and many wavelets basis functions are required for image representation. DCuT of images leads to various frequency coefficients representation [2,47,48]. An important property of DCuT is it represents images into edges or curves. The DCuT is linear and takes as input cartesian array (here, it is a 2D digital image) of the form  $f(x, y)$  which allow us to get the output as a collection of curvelet coefficients obtained by the digital,

$$C^D(j, l, k) := \sum_{0 \leq x, y < n} f(x, y) \overline{\theta_{j,l,k}^D(x, y)} \quad (1)$$

Where  $\theta_{j,l,k}^D$  is a digital curvelet waveform,  $j$  is a scale parameter,  $l$  is an orientation parameter and  $k$  is a translation parameter.

The scale parameter depends on the size of the image and calculated as  $\log_2(\min(M, N)) - 3$ , Where, M and N is the size of row and column of the image. The orientation parameter must be set to a multiplier of 4 and the default value of the orientation parameter is 16 [46,47]. The DCuT is divided into two types such as unequi-spaced fast Fourier transform (USFFT) based and frequency wrapping based. The frequency wrapping based DCuT is easy to implement, less computation time and easy to understand compared to the USFFT based DCuT [46,47]. Therefore, frequency wrapping based DCuT is used in many image processing applications particular in watermarking and compression. The frequency

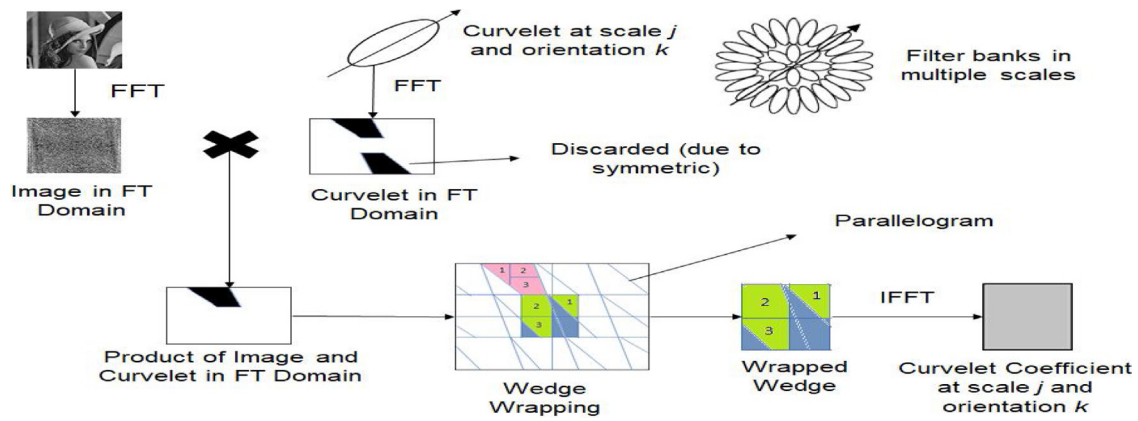


Fig. 1. Frequency wrapping based DCuT [48].



(a) Original Image



(b) Curvelet Coefficients of Image



(c) High Frequency Curvelet Coefficients of Image

Fig. 2. Curvelet coefficients of an image.

wrapping based DCuT is graphically represented in Fig. 1 [49]. The implementing steps of frequency wrapping based DCuT is given below [47–49]:

- Step 1: Take FFT of the image.
- Step 2: Divide FFT into a collection of Digital Corona Tiles
- Step 3: For each corona tile
  - Translate the tile to the origin.
  - Wrap the parallelogram shaped support of the tile around a rectangle centered at the origin.
  - Take the Inverse FFT of the wrapped support.
  - Add the Curvelet array to the Collection of Curvelet coefficients.

The frequency wrapping based DCuT is applied to the image, it produces three different frequency subbands such as Low Frequency (LF), Middle Frequency (MF) and High Frequency (HF). The number of cells depends on the size of the image. For example, an image with a size of  $512 \times 512$  pixels are decomposed using frequency wrapping based DCuT with 6 scale parameters and 16 orientation parameters into different cells, such as  $C(1, 1)$  to  $C(1, 6)$ . Where,  $C(1, 1)$  is a low frequency curvelet coefficient,  $C(1, 2)$  to  $C(1, 5)$  are medium frequency curvelet coefficients, and  $C(1, 6)$  is high frequency curvelet coefficient. The size of the cells  $C(1,$

1) to  $C(1, 5)$  is less than the actual size of image but size of  $C(1, 6)$  is equal to the size of the image. The reason behind chosen high frequency curvelet coefficients in the proposed scheme is that it results in better imperceptibility and achieves good payload capacity compared to other curvelet coefficients. The curvelet coefficients of an image are shown in Fig. 2(b). Fig. 2(c) shows the high frequency curvelet coefficients of an image.

### 3.2. Redundant discrete wavelet transform (RDWT)

The discrete wavelet transform (DWT) is one of the most common transform used in watermarking, which downsamples the original image while making subbands [23,26]. The result is a restriction on the payload capacity of watermarking. Further, the DWT is also shift variant which may lead to failure in watermark extraction. These problems can be overcome by employing RDWT for watermarking. The RDWT provides shift invariance for better extraction of watermark [23,26]. The main difference between DWT and RDWT is given in Fig. 3.

### 3.3. Arnold scrambling

Here, Arnold scrambling [32,50] is used to scrambled the watermark logo before it is inserted into the cover image. So that, im-



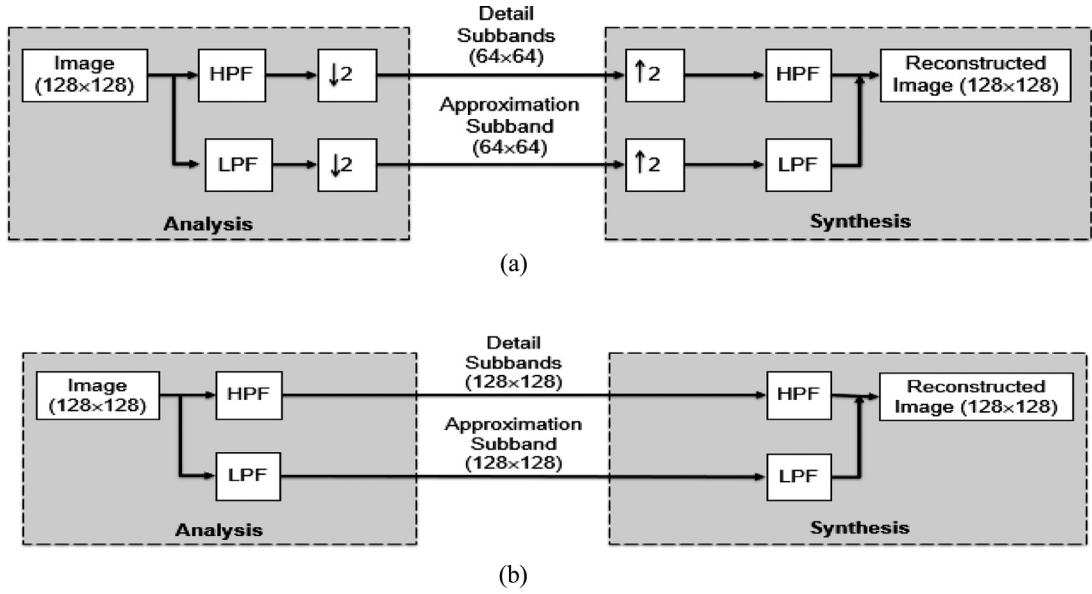


Fig. 3. (a) DWT based decomposition and reconstruction for image (b) RDWT based decomposition and reconstruction for image.



Fig. 4. (a) Original watermark logo (b) Scrambled watermark logo.

poster or unauthorized user can't directly obtain watermark logo from the watermarked image. The resultant scrambled image is secure and can't be recovered without information of the correct security key. Fig. 4 shows the scrambled binary watermark image using Arnold scrambling using secret key  $(k)$ , where (a) is the original watermark logo, (b) is the scrambled watermark logo with a security key  $(k) = 5$ .

#### 4. Proposed scheme

The proposed scheme has two processes: watermark embedding and watermark extraction. The block diagrams of these processes are shown in Figs. 5 and 6, respectively.

##### 4.1. Watermark embedding process

The inputs of the watermarking algorithm being cover image and watermark, and secret seed, the steps involved in the watermark embedding process are given below:

- Step 1: Take watermark image and apply Arnold scrambling with a secret key to watermark image to generate scrambled watermark image.
- Step 2: Apply first level DCuT decomposition on the cover image. Decompose the cover image into curvelet coefficients with different frequencies such as low (C (1,1)), middle (C (1,2), C (1,3), C (1,4), and C (1,5)), and high (C (1,6)).
- Step 3: Select high frequency curvelet coefficients of C (1,6) for watermark embedding. The reason behind chosen these

coefficients is that it is more sparse than other curvelet coefficients and size of these coefficients equal to the actual size of the cover image which improves imperceptibility and payload capacity of the scheme.

- Step 4: First level RDWT applied to the coefficient of C (1,6) to obtain wavelet coefficients of C (1,6) of the cover image. After RDWT decomposition, coefficients of C (1,6) of cover image is decomposed into 4 subbands such as  $W(C)_\psi$ ,  $\psi \in LL, LH, HL, \text{ and } HH$ .
- Step 5: Select horizontal LH wavelet subband of coefficients of C (1,6) of the cover image and convert it into non-overlapped blocks.
- Step 6: Generate two high uncorrelated Pseudorandom Noise (PN) sequences using noise generator and secret seed, each of size equal to the block size.
- Step 7: Embed scrambled watermark bits in chosen wavelet subbands of contourlet subbands based on the following conditions:

- a. If watermark bit is zero, then

$$W(C)'_{LH} = W(C)_{LH} + k \times PN\_Sequence\_0 \quad (2)$$

Where,  $W(C)'_{LH}$  is modified LH subband of coefficients of C (1,6),  $W(C)_{LH}$  is original LH subband of coefficients of C (1,6),  $k$  is the scaling factor, and  $PN\_Sequence\_0$  corresponds to PN sequence of watermark bit 0.

- b. If watermark bit is one, then

$$W(C)'_{LH} = W(C)_{LH} + k \times PN\_Sequence\_1 \quad (3)$$

Where,  $W(C)'_{LH}$  is modified LH subband of coefficients of C (1,6),  $W(C)_{LH}$  is original LH subband of coefficients of C (1,6),  $k$  is the scaling factor, and  $PN\_Sequence\_1$  corresponds to the PN sequence of watermark bit 1.

- c. Repeat this process for all wavelet subbands of each block of the cover image.

- Step 8: Perform first level inverse RDWT on modified LH subband with other original wavelet subbands to get modified coefficients of C (1,6) of the cover image.
- Step 9: Perform first level inverse DCuT on modified curvelet coefficients of C (1,6) with original curvelet coefficients to generate a watermarked image.

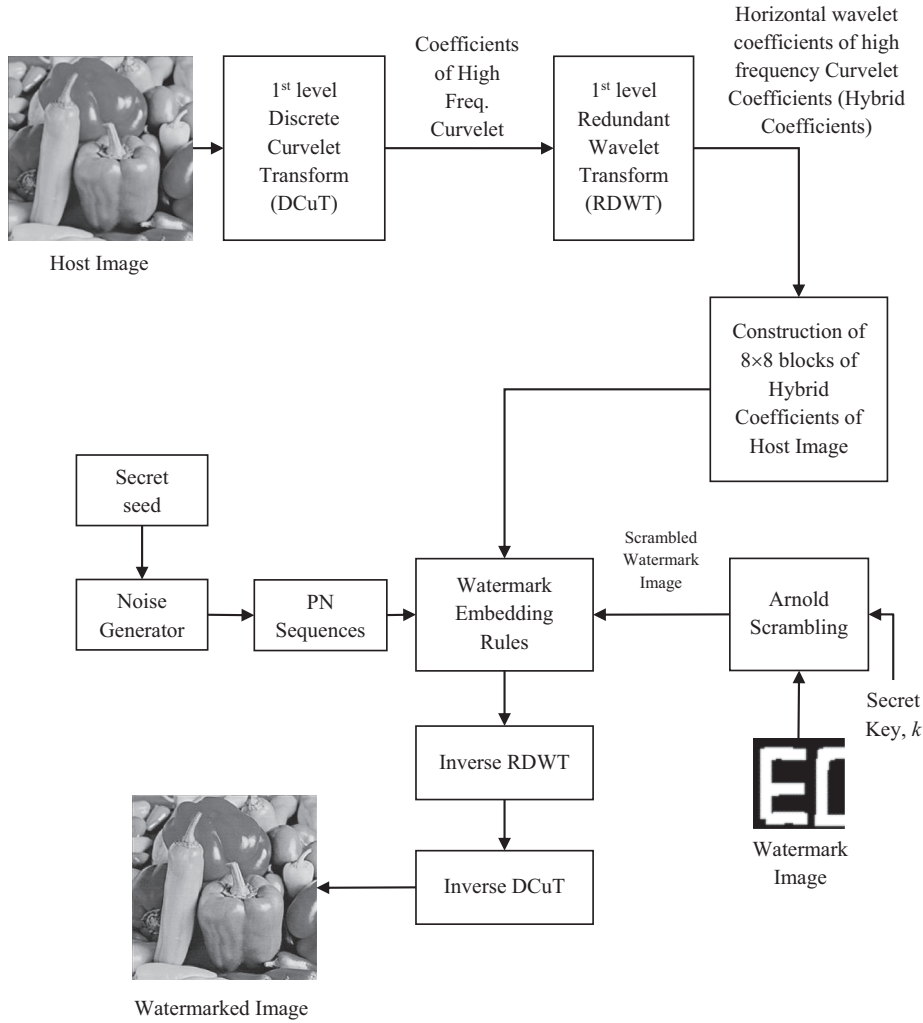


Fig. 5. Watermark embedding process in proposed watermarking scheme.

#### 4.2. Watermark extraction process

The inputs to the watermark extraction process being the test watermarked image and secret key, the steps involved in watermark extraction are given in detail as follows:

- Step 1: Apply first level DCuT decomposition on the watermarked image. Decompose the cover image into curvelet coefficients with different frequencies such as low (WA (1,1)), middle (WA (1,2), WA (1,3), WA (1,4), and WA (1,5)), and high (WA (1,6)).
- Step 2: First level RDWT applied to the coefficient of C (1,6) to obtain wavelet coefficients of C (1,6) of the watermarked image. After RDWT decomposition, coefficients of C (1,6) of cover image is decomposed into 4 subbands such as  $W(WA)_{\psi}$ ,  $\psi \in LL, LH, HL, \text{ and } HH$ . Select the same LH wavelet subband of coefficients of C (1,6) which was selected during the watermark embedding process.
- Step 3: Take the two highly uncorrelated PN sequences which are generated during watermark embedding process using a secret seed.
- Step 4: Extract the scrambled watermark bit from the LH wavelet subband of coefficients of C (1,6) of the watermarked image based on the following conditions:

$$\text{Corr}(0) = \text{corr2}(W(WA)_{LH}, PN\_Sequence\_0) \quad (4)$$

$$\text{Corr}(1) = \text{corr2}(W(WA)_{LH}, PN\_Sequence\_1) \quad (5)$$

- Step 5: Set watermark bit to 0 if  $\text{Corr}(0) > \text{Corr}(1)$ . Otherwise, set watermark bit as bit 1.
- Step 6: Apply to reshape on bits vector to get scrambled watermark image. Then, apply inverse Arnold scrambling to scrambled watermark image to get actual recovered watermark image.

## 5. Results and discussion

The performance of the proposed scheme is analyzed using different types of grayscale images [51] and monochromatic watermark images. In the proposed scheme, the size of the chosen cover image is  $512 \times 512$  pixels and the size of the watermark image is  $64 \times 64$  pixels. The performance of the proposed scheme depends on the LH wavelet subband of the coefficient of C (1,6) of the cover image during watermark embedding. Fig. 7 shows the test cover images and the watermark image.

### 5.1. Evaluation matrices

The peak signal to noise ratio (PSNR) [52] is used to measure the similarity between the original cover image and watermarked image and is given in Eq. (5). The PSNR is measured in dB value.

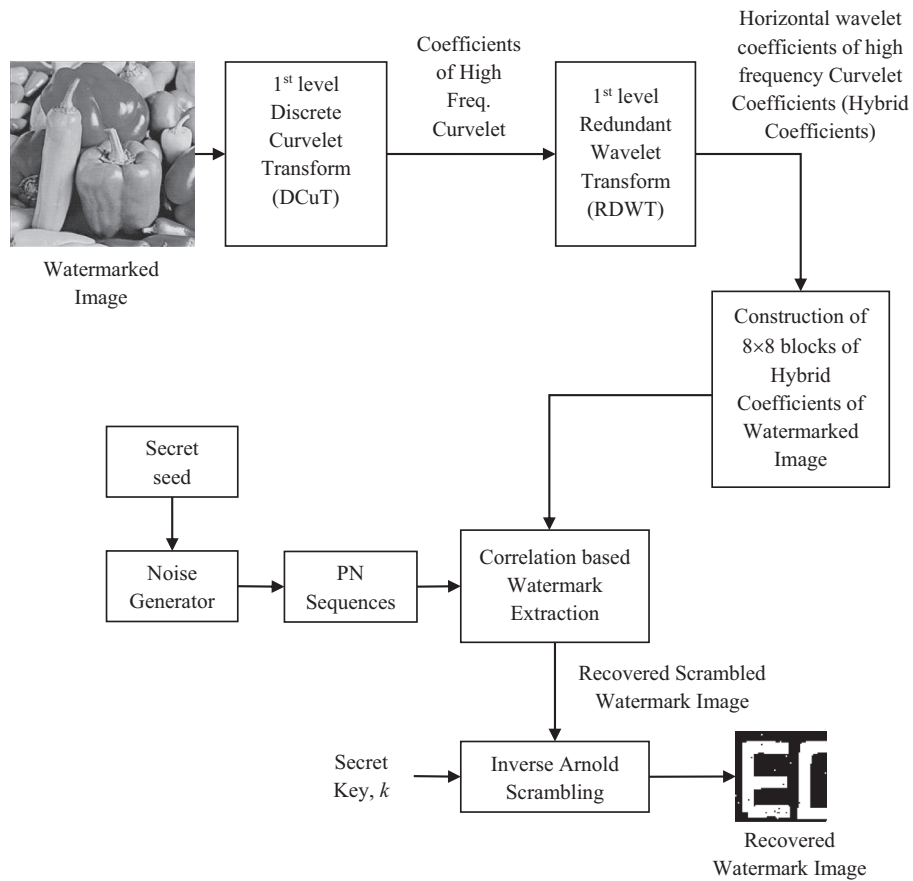
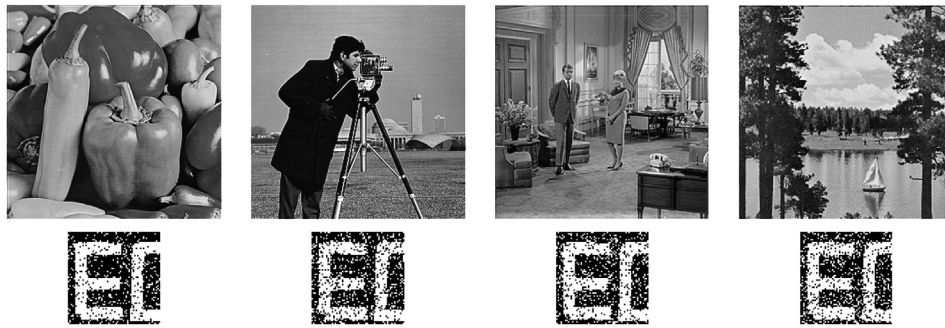


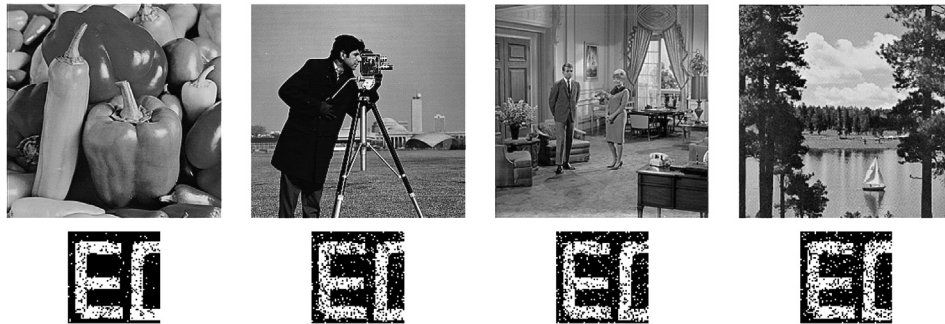
Fig. 6. Watermark extraction process in proposed watermarking scheme.



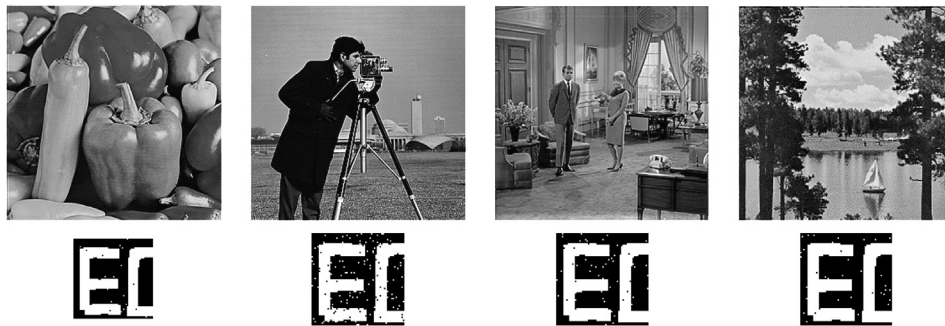
Fig. 7. Test cover images (a) Peppers (b) Cameraman (c) Lean (d) Goldhill (e) Livingroom (f) Lake (g) Watermark image.



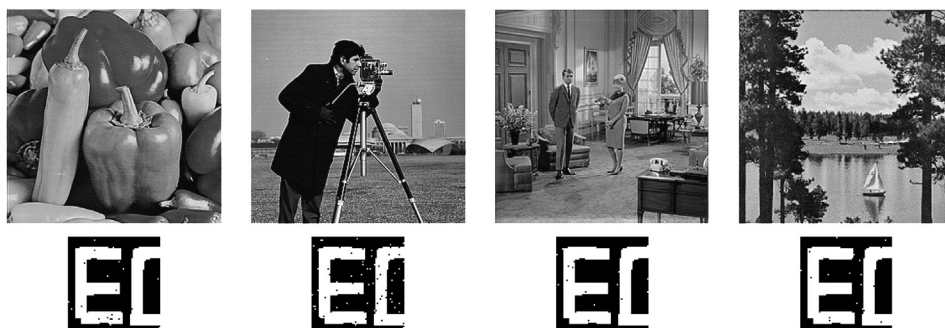
(a) Simulation results with scaling factor  $k = 5$



(b) Simulation results with scaling factor  $k = 15$



(c) Simulation results with scaling factor  $k = 30$



(d) Simulation results with scaling factor  $k = 45$

Fig. 8. Watermarked images and recovered watermark images using the proposed scheme for different scaling factor values.

The MSE is calculated using Eq. (6) which gives real value. The MSE finds error between cover image and watermarked image. A high value of PSNR indicates more similarity of images, indicating high imperceptibility of the hidden watermark.

$$PSNR = 10 \times \log_{10} \left( \frac{255^2}{MSE} \right) \tag{6}$$

$$MSE = \frac{1}{M \times N} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} (C(x, y) - CW(x, y))^2 \tag{7}$$

where,  $C$  is an original cover image and  $CW$  is a watermarked image, respectively.

The robustness of the watermarking scheme can be measured by Normalized Correlation (NC) [52] and Structural Similarity

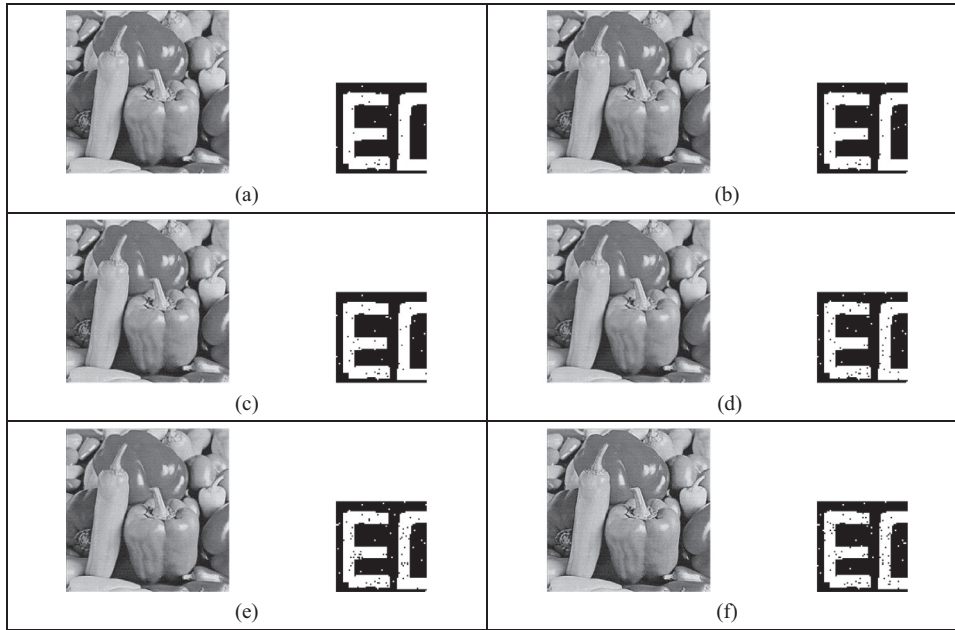


**Table 1**  
PSNR, NC, SSIM, and BER values of the proposed scheme for different scaling factor  $k$ .

Test image	Scaling factor, $k = 5$				Scaling factor, $k = 15$			
	PSNR (dB)	NC	SSIM	BER	PSNR (dB)	NC	SSIM	BER
Peppers	54.6421	0.9097	0.9964	0.1172	46.6618	0.9435	0.9970	0.0754
Cameraman	54.7014	0.8429	0.9943	0.1726	46.7211	0.8825	0.9943	0.1384
Lena	52.9226	0.8940	0.9960	0.1377	44.9423	0.9393	0.9970	0.0784
Goldhill	56.4067	0.8712	0.9937	0.1814	48.4294	0.9586	0.9943	0.1262
Livingroom	57.5145	0.8796	0.9946	0.1589	49.5342	0.9797	0.9949	0.1328
Lake	57.5995	0.8561	0.9937	0.1804	49.6193	0.9688	0.9945	0.1365

Test image	Scaling factor, $k = 30$				Scaling factor, $k = 45$			
	PSNR (dB)	NC	SSIM	BER	PSNR (dB)	NC	SSIM	BER
Peppers	38.9618	0.9952	0.9999	0.0056	35.7938	0.9934	0.9999	0.0054
Cameraman	39.0211	0.9759	0.9992	0.0354	35.8530	0.9831	0.9996	0.0171
Lena	37.2423	0.9988	0.9998	0.0095	34.0742	0.9988	0.9999	0.0024
Goldhill	40.7264	0.9994	0.9999	0.0054	37.5584	1.0000	1.0000	0.0022
Livingroom	41.8342	0.9940	0.9997	0.0132	38.6661	0.9958	0.9999	0.0039
Lake	41.9192	0.9970	0.9998	0.0090	38.7542	0.9946	0.9999	0.0051



**Fig. 9.** Watermarked images and recovered watermark images under JPEG compression attack (a)  $Q=90$  (b)  $Q=80$  (c)  $Q=70$  (d)  $Q=60$  (e)  $Q=50$  (f)  $Q=40$ .

Index Measure (SSIM) [53]. The NC and SSIM can be calculated using Eqs. (7) and (8), respectively. While NC measures the correlation between the original and extracted watermark images, the SSIM measures the similarity between them. The robustness of any watermarking scheme is high if NC and SSIM values are closer to one.

$$NC = \frac{\sum_{x=1}^M \sum_{y=1}^N w(x, y) \times w^*(x, y)}{\sum_{x=1}^M \sum_{y=1}^N w^2(x, y)} \quad (8)$$

where  $w$  is the original watermark image and  $w^*$  is the recovered watermark image.

$$SSIM = \frac{(2\mu_w\mu_{w^*} + C_1)(2\sigma_{ww^*} + C_2)}{(\mu_w^2 + \mu_{w^*}^2 + C_1)(\sigma_w^2 + \sigma_{w^*}^2 + C_2)} \quad (9)$$

where  $\mu_w$  is the average of the original watermark image,  $\mu_{w^*}$  is the average of the recovered watermark image,  $\sigma_{ww^*}$  is the covariance of original watermark image and recovered watermark image, and  $C_1, C_2$  are constant values. Using the above measures, imperceptibility test and robustness test of the proposed scheme

are performed for various tested cover images. While detection performance of the proposed scheme is measured by bit error rate (BER) [54]. It is the number of received watermark bits that have been altered due to noise, divided by the total number of original watermark bits [53]. Its value is range in [0, 1]. The low value of BER indicates high detection performance for a given watermarking scheme.

### 5.2. Imperceptibility test

In the proposed scheme, a standard grayscale images of size  $512 \times 512$  pixels are used as test cover images. The DCuT is applied on cover image followed by application of first level Daubechies (db1) RDWT on coefficients of C (1, 6) of the cover image. The coefficients of LH wavelet subband of coefficients of C (1, 6) of size  $512 \times 512$  are converted into 4096 non-overlapping blocks of size  $8 \times 8$ . The watermark image which is of size  $64 \times 64$  pixels is converted into a vector of size 4096. Then according to the watermark bits, selected hybrid coefficients of each block of cover

image are modified using two PN sequences, and a scaling factor. After watermark embedding, the inverse Daubechies (db1) RDWT, followed by inverse DCuT are applied to get watermarked image. The maximum watermark information that can be inserted by the proposed scheme is calculated using below Eq. (10):

$$\text{Maximum\_Watermark} = \frac{M \times N}{\text{Blocksize}^2} \tag{10}$$

where,  $M$  and  $N$  denote the number of rows and columns of the cover image, respectively.

In the simulations, the number of rows and columns are each 512, and the block size is 8. Thus, the proposed scheme can insert a maximum of 4096 watermark bits. The maximum payload capacity of the proposed scheme can be 1 bit for every 64 pixels of the cover image.

The simulations are repeated on different cover images like peppers, cameraman, livingroom, and lake, to check how the images degrade after watermark embedding. In the proposed scheme, the performance of the watermark embedding process depends on the scaling factor  $k$  used in Eqs. (2) and (3). The amount of degradation on the watermarked image and extracted image is analyzed, by varying the scaling factor  $k$ , and the corresponding subjective and objective results are presented in Fig. 8 and Table 1.

The results indicate the quality of extracted watermark improves with  $k$ , maintaining the visual quality of watermarked images.

Refereeing Table 1, it is indicated the performance of the proposed scheme is better for the high value of scaling factor in term of quality of extracted watermark images while imperceptibility of the proposed scheme is better for the low value of scaling value.

### 5.3. Robustness test

To verify the robustness test of the proposed scheme, various watermarking attacks such as JPEG compression, different filtering attacks, different noise addition attacks, motion blur, sharpening, histogram equalization and geometric attacks are applied on the watermarked images, and then watermark extraction is attempted and the subjective and objective results are given in Figs. 9–13, and Tables 2 to 6. The robustness of the proposed scheme against various watermarking attacks is measured by normalized correlation (NC) and structural similarity index measure (SSIM). For robustness test, the scaling factor  $k$  is set to 45 and peppers image is taken as a cover image.

#### 5.3.1. JPEG compression attack

It is one of common watermarking attack used for evaluation of the performance of the watermarking scheme. It is evaluated the

Corrupted Watermarked image after Median Filter Attack	Filter mask = 3×3 	Filter mask = 5×5 	Filter mask = 7×7 
Recovered Watermark Image			
Corrupted Watermarked image after Average Filter Attack	Filter mask = 3×3 	Filter mask = 5×5 	Filter mask = 7×7 
Recovered Watermark Image			
Corrupted Watermarked image after Gaussian Low Pass Filter Attack	Filter mask = 3×3 	Filter mask = 5×5 	Filter mask = 7×7 
Recovered Watermark Image			

Fig. 10. Watermarked images and recovered watermark images under filtering attack.



Fig. 11. Watermarked images and recovered watermark images under noise addition attack.

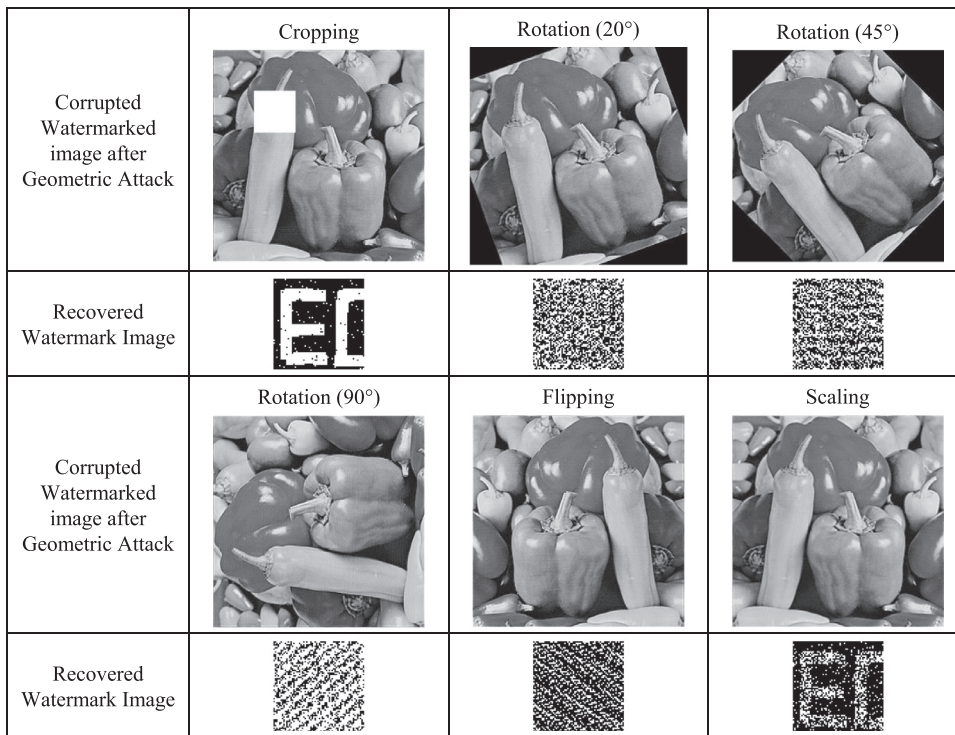


Fig. 12. Watermarked images and recovered watermark images under geometric attack.

performance of scheme when watermarked images are transmitted from one source to another source. Fig. 9 shows corrupted watermarked images by JPEG compression attacks with different quality factors and recovered watermark image from these corrupted images. Table 2 shows the value of NC, SSIM, and BER for robustness checking of proposed scheme against JPEG compression attack. The results indicated that this scheme is robust against this attack.

### 5.3.2. Filtering attack

It is another famous watermarking attack which is used for evaluation of the performance of the proposed scheme. It is a common signal processing attack which is applied watermarked image when it is transferred over the unsecured communication channel. Fig. 8 shows corrupted watermarked images by filtering attacks with different types of the filter with different filter masks and re-



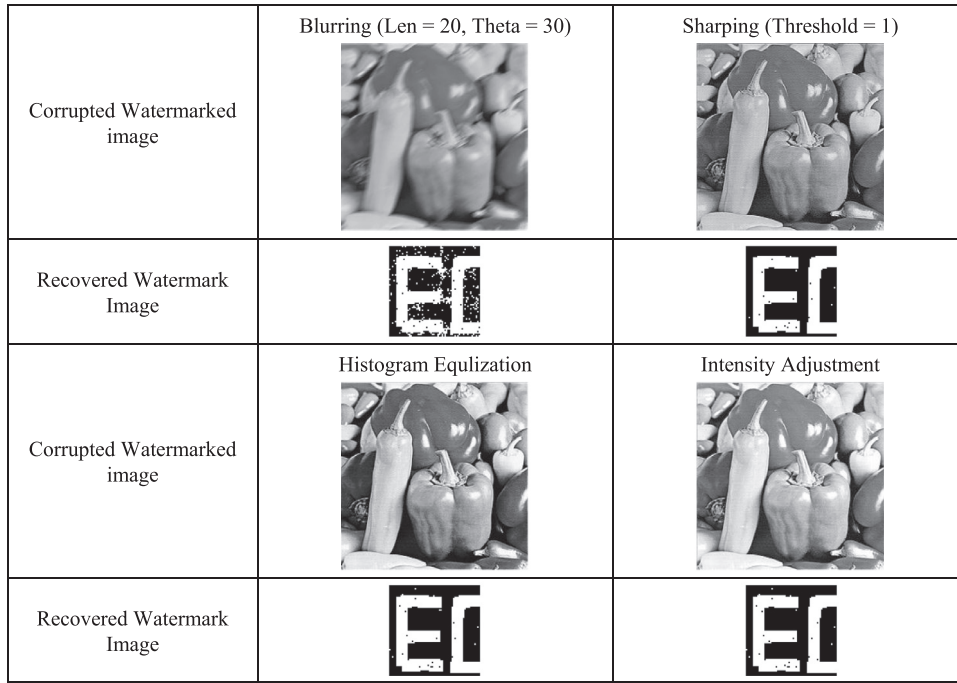


Fig. 13. Watermarked images and recovered watermark images under blurring attack, sharpening attack, histogram equalization attack, and intensity adjustment attack.

**Table 2**  
NC, SSIM and BER values of proposed scheme under JPEG compression attack.

JPEG compression attacks	NC	SSIM	BER
Q = 90	0.9910	0.9998	0.0061
Q = 80	0.9898	0.9998	0.0081
Q = 70	0.9837	0.9997	0.0105
Q = 60	0.9741	0.9996	0.0164
Q = 50	0.9639	0.9994	0.0212
Q = 40	0.9597	0.9994	0.0229

**Table 3**  
NC, SSIM and BER values of proposed scheme under filtering attack.

Filtering attack	NC	SSIM	BER
Median filtering (3 × 3)	0.4576	0.9567	0.6287
Median filtering (5 × 5)	0.1656	0.9285	0.8560
Median filtering (7 × 7)	0.3630	0.9704	0.4075
Average filtering (3 × 3)	0.2258	0.9343	0.7810
Average filtering (5 × 5)	0.0301	0.9130	0.9604
Average filtering (7 × 7)	0.3058	0.9652	0.3682
Gaussian low pass filtering (3 × 3)	0.9916	0.9998	0.0066
Gaussian low pass filtering (5 × 5)	0.9916	0.9998	0.0066
Gaussian low pass filtering (7 × 7)	0.9916	0.9998	0.0066

**Table 4**  
NC, SSIM and BER values of proposed scheme under noise addition attack.

Salt and pepper noise attack	NC	SSIM	BER
$\sigma = 0.001$	0.9831	0.9997	0.0110
$\sigma = 0.005$	0.9934	0.9999	0.0059
$\sigma = 0.01$	0.9843	0.9997	0.0017
$\sigma = 0.02$	0.9657	0.9994	0.0251
$\sigma = 0.1$	0.8314	0.9951	0.1421
Gaussian noise attack	NC	SSIM	BER
$\sigma = 0.001$	0.9837	0.9997	0.0115
$\sigma = 0.005$	0.9922	0.9999	0.0063
$\sigma = 0.01$	0.9500	0.9991	0.0342
$\sigma = 0.02$	0.8832	0.9974	0.0842
$\sigma = 0.1$	0.6827	0.9886	0.2720

**Table 5**  
NC, SSIM and BER values of proposed scheme under geometric attack.

Geometric attacks	NC	SSIM	BER
Cropping	0.9795	0.9994	0.0264
Rotation (20°)	0.4798	0.9705	0.5039
Rotation (45°)	0.4798	0.9712	0.4949
Rotation (90°)	0.6629	0.9681	0.5215
Flipping	0.3149	0.9677	0.4595
Scaling	0.5051	0.9832	0.2510

**Table 6**  
NC, SSIM and BER values of proposed scheme under blurring attack, sharpening attack, histogram equalization attack, and intensity adjustment attack.

Other Attacks	NC	SSIM	BER
Blurring (Len = 20, Theta = 30)	0.9862	0.9969	0.0801
Sharping (Threshold = 1)	0.9916	0.9999	0.0046
Histogram equalization	0.9904	0.9999	0.0061
Intensity adjustment	0.9898	0.9999	0.0061

**Table 7**  
Robustness test of the proposed scheme for benchmark attacks.

Benchmark attacks	Proposed scheme
Compression	0.98
Scaling	0.50
Cropping	0.98
Shearing	0.50
Linear	0.50
Rotation	0.54
Flip	0.31
Random geometrical distortions	0.99
Enhancement	0.99
Average	0.70

covered watermark image form these corrupted watermarked images.

Table 3 shows the value of NC, SSIM, and BER for robustness checking of proposed scheme against filtering attacks. The results



**Table 8**  
Computational time (in seconds) of the proposed scheme for different scaling factor values.

Test image	Watermarking key $k = 5$		Watermarking key $k = 15$	
	Embedding time	Extraction time	Embedding time	Extraction time
Peppers	1.6374	1.1088	1.5948	1.0743
Cameraman	1.6773	1.1092	1.3284	1.0450
Lena	1.6225	1.0659	1.5941	1.0343
Goldhill	1.5827	1.0417	1.6215	1.0271
Livingroom	1.6605	1.0470	1.6900	1.2244
Lake	1.6481	1.0690	1.6118	1.1590

Test image	Watermarking key $k = 30$		Watermarking key $k = 45$	
	Embedding time	Extraction time	Embedding time	Extraction time
Peppers	1.9150	1.0782	1.6090	1.1232
Cameraman	1.6101	1.0761	1.7558	1.1468
Lena	1.6045	1.0547	1.7287	1.1120
Goldhill	1.7198	1.0791	1.7293	1.1294
Livingroom	1.6335	1.0345	1.6654	1.1185
Lake	1.5903	1.0666	1.6847	1.1726

**Table 9**  
Computation time between Makbol scheme, Ernawan scheme, and proposed scheme.

Images	Embedding time (in seconds)			Extraction time (in seconds)		
	Makbol's scheme [57]	Ernawan's scheme [34]	Proposed scheme	Makbol's scheme [57]	Ernawan's scheme [34]	Proposed scheme
Lena	14.2656	84.3218	1.6375	5.7188	25.5313	1.0667
Peppers	14.3594	86.2969	1.6891	5.6563	25.3125	1.0961

**Table 10**  
Comparison of PSNR (dB) of the proposed scheme with existing schemes.

Scheme	Maximum PSNR (dB)
Hien et al. [23]	52.03
Zhang et al. [35]	50.12
Hien et al. [36]	48.73
Mankar et al. [24]	42.05
Tao et al. [37]	39.73
Leung et al. [38]	48.03
Lagzian et al. [26]	37.52
Song et al. [40]	45.81
Lari et al. [41]	40.00
Bajaj et al. [28]	51.00
Channapragada et al. [42]	43.63
Singh et al. [33]	36.98
Roy et al. [32]	51.46
<b>Proposed</b>	<b>52.92</b>

**Table 11**  
Comparative analysis of PSNR (dB) values of proposed scheme with existing schemes [32–34].

Test images	Roy's scheme (2017) [32]	Singh's scheme (2017) [33]	Ernawan's scheme (2018) [34]	Proposed scheme
Lena	51.4581	47.09	44.4558	<b>52.9226</b>
Airplane	47.3052	Not reported	36.9675	<b>55.2546</b>
Barbara	47.9349	39.88	43.4487	<b>52.1565</b>
Peppers	46.9716	45.24	43.8606	<b>54.6421</b>

show that this proposed scheme is partially robust against the median filter and average filter while complete robust against Gaussian low pass filter.

5.3.3. Noise addition attack

The robustness of the proposed scheme is evaluated by adding various noises to the watermarked image. This attack introduces distortion in the watermarked image and tries to recovered watermark images from the corrupted watermarked images. Here, two types of noises such as Gaussian and salt & pepper with different variances are added into the watermarked image to generate a corrupted watermarked image. Fig. 9 shows corrupted watermarked images by noise addition attacks with different types of noises with different variance and recovered watermark image form these corrupted watermarked images.

Table 4 shows the value of NC, SSIM, and BER for robustness checking of proposed scheme against noise addition attacks. The results show that this proposed scheme is robust against noise signals with lower variance value but less robust against noise signals with higher variance value.

5.3.4. Geometric attack

The different geometric attacks such as cropping, rotation, flipping, and scaling are applied to the watermarked image and then recovered watermark image from these corrupted watermarked images. Fig. 10 shows corrupted watermarked images by different geometric attacks and recovered watermark image form these corrupted watermarked images. Table 5 shows the value of NC, SSIM, and BER for robustness checking of proposed scheme against geometric attacks. The results show that this proposed scheme is robust against cropping attack and scaling attack while no robust against rotation attack and flipping attack.

5.3.5. Other attack

Another set of attacks such as sharpening, blurring, intensity adjustment, and histogram equalization are applied to the watermarked images and then recovered watermark image from these corrupted watermarked images. Fig. 11 shows corrupted watermarked images by mentioned attacks and recovered watermark image form these corrupted watermarked images. Table 6 shows the value of NC, SSIM, and BER for robustness checking of the proposed scheme against mentioned attacks. The results show that this proposed scheme is robust against these mentioned attacks.

5.3.6. Benchmark attacks





























































The performance of the proposed scheme is also tested using benchmark attacks which were proposed by Kutter and Pe-

**Table 12**  
Comparative analysis of NC and BER values of proposed scheme with existing schemes [32,34].

Type of Attacks	Extracted Watermark Images			NC and BER Values					
	Roy's Scheme (2017) [32]	Ernawan's Scheme (2018) [34]	Proposed Scheme	Roy's Scheme (2017) [32]		Ernawan's Scheme (2018) [34]		Proposed Scheme	
				NC	BER	NC	BER	NC	BER
JPEG Compression (Q = 90)				0.9639	0.0347	0.6370	0.3574	0.9910	0.0061
JPEG Compression (Q = 80)				0.9404	0.0588	0.6069	0.4148	0.9898	0.0081
JPEG Compression (Q = 70)				0.8916	0.1138	0.5876	0.4509	0.9837	0.0105
JPEG Compression (Q = 60)				0.8067	0.1943	0.6087	0.4729	0.9741	0.0164
JPEG Compression (Q = 50)				0.7502	0.2380	0.6382	0.4819	0.9639	0.0212
JPEG Compression (Q = 40)				0.6978	0.2898	0.6610	0.4907	0.9597	0.0229
Median Filtering (3×3)				0.8055	0.1946	0.6026	0.4216	0.4576	0.6287
Median Filtering (5×5)				0.3721	0.6187	0.5581	0.5029	0.1656	0.8560
Median Filtering (7×7)				0.4070	0.5867	0.5846	0.5034	0.3630	0.4075
Average Filtering (3×3)				0.8266	0.1677	0.5822	0.4434	0.2258	0.7810
Average Filtering (5×5)				0.2444	0.7427	0.5455	0.5085	0.0301	0.9604
Average Filtering (7×7)				0.34444	0.6545	0.5780	0.5020	0.3058	0.3682
Gaussian Low Pass Filtering (3×3)				0.9573	0.0403	0.6960	0.3254	0.9916	0.0066
Gaussian Low Pass Filtering (5×5)				0.9573	0.0403	0.6960	0.3254	0.9916	0.0066
Gaussian Low Pass Filtering (7×7)				0.9573	0.0403	0.6960	0.3254	0.9916	0.0066































(continued on next page)

Table 12 (continued)

Salt & Pepper Noise Attack ( $\sigma = 0.001$ )				0.8790	0.1140	0.7056	0.3081	0.9831	0.0110
Salt & Pepper Noise Attack ( $\sigma = 0.005$ )				0.9524	0.0442	0.7237	0.2957	0.9934	0.0059
Salt & Pepper Noise Attack ( $\sigma = 0.01$ )				0.8152	0.1807	0.7062	0.3125	0.9843	0.0017
Salt & Pepper Noise Attack ( $\sigma = 0.02$ )				0.7574	0.2473	0.6924	0.3218	0.9657	0.0251
Salt & Pepper Noise Attack ( $\sigma = 0.1$ )				0.5852	0.4180	0.5924	0.4194	0.8314	0.1421
Gaussian Noise Attack ( $\sigma = 0.001$ )				0.7092	0.2917	0.5587	0.4692	0.9837	0.0115
Gaussian Noise Attack ( $\sigma = 0.005$ )				0.8459	0.1460	0.5695	0.4221	0.9922	0.0063
Gaussian Noise Attack ( $\sigma = 0.01$ )				0.6412	0.3557	0.5298	0.4658	0.9500	0.0342
Gaussian Noise Attack ( $\sigma = 0.02$ )				0.6075	0.3804	0.5262	0.4719	0.8832	0.0842
Gaussian Noise Attack ( $\sigma = 0.1$ )				0.5569	0.4446	0.5400	0.4827	0.6827	0.2720
Cropping				0.9657	0.0476	0.7357	0.3081	0.9795	0.0264
Rotation (20°)				0.5593	0.5017	0.5864	0.5205	0.4798	0.5039
Rotation (45°)				0.5521	0.5281	0.5960	0.5256	0.4798	0.4949
Rotation (90°)				0.5039	0.4934	0.4076	0.4790	0.6629	0.5215
Flipping				0.5129	0.5022	0.4570	0.5061	0.3149	0.4595
Scaling				0.7483	0.2410	0.5798	0.4490	0.5051	0.2510
Blurring				0.5316	0.4473	0.5629	0.4988	0.9862	0.0801
Sharping				0.9645	0.0315	0.7983	0.2173	0.9916	0.0046
Histogram Equalization				0.9554	0.0459	0.7225	0.3125	0.9904	0.0061
Intensity Adjustment				0.9585	0.0430	0.7182	0.3030	0.9898	0.0061

(continued on next page)

Table 12 (continued)

Cropping				<b>0.9657</b>	<b>0.0476</b>	<b>0.7357</b>	<b>0.3081</b>	<b>0.9795</b>	<b>0.0264</b>
Rotation (20°)				0.5593	0.5017	0.5864	0.5205	0.4798	0.5039
Rotation (45°)				0.5521	0.5281	0.5960	0.5256	0.4798	0.4949
Rotation (90°)				<b>0.5039</b>	<b>0.4934</b>	<b>0.4076</b>	<b>0.4790</b>	<b>0.6629</b>	<b>0.5215</b>
Flipping				0.5129	0.5022	0.4570	0.5061	0.3149	0.4595
Scaling				0.7483	0.2410	0.5798	0.4490	0.5051	0.2510
Blurring				<b>0.5316</b>	<b>0.4473</b>	<b>0.5629</b>	<b>0.4988</b>	<b>0.9862</b>	<b>0.0801</b>
Sharping				<b>0.9645</b>	<b>0.0315</b>	<b>0.7983</b>	<b>0.2173</b>	<b>0.9916</b>	<b>0.0046</b>
Histogram Equalization				<b>0.9554</b>	<b>0.0459</b>	<b>0.7225</b>	<b>0.3125</b>	<b>0.9904</b>	<b>0.0061</b>
Intensity Adjustment				<b>0.9585</b>	<b>0.0430</b>	<b>0.7182</b>	<b>0.3030</b>	<b>0.9898</b>	<b>0.0061</b>

titcolas [52]. Here, StirMark [52] is used for evaluation of the robustness of the proposed scheme. The robustness of the proposed scheme is tested by different types of attacks such as signal enhancement, compression, scaling, cropping, shearing, linear transformations, rotation, row/column removal, and random geometric distortions. For each attack are applicable on watermarked image. For each image, score value in the range of 0 to 1 assign as per quality of extracted watermark image. If extraction of watermark image is done correctly by scheme then assign a score of 1 other it is taken as 0. Finally, calculate the average for the result of each attack and summarized in Table 7.

#### 5.4. Computational time analysis of proposed scheme

The computation time is an important parameter for any watermarking scheme, particularly when it is proposed to used in various applications such as copyright protection of multimedia files such as digital images and videos, digital content authentication, piracy preservation, and forensic. In these all applications, digital content is delivered from one point to another point via a communication channel with high security and in less time. Therefore, watermarking schemes with less computation time is suitable for these types of applications. The computational time, which includes the time required for watermark embedding and extraction is important, particularly when it is used in copyright protection of real time multimedia data.

Table 8 shows the computational time of the proposed watermark embedding and extraction process for different images. This proposed scheme is implemented on 2 GHz processor with 8 GB physical memory, using MATLAB 2016 b software. The average computational time of the watermark embedding process is 1.6465 s and the watermark extraction process is 1.0916 s. Thus,

the average total computational time of the proposed watermarking technique is 2.7381 s, which is satisfactory. The computational time of the proposed scheme is compared with fast existing image watermarking schemes [55,56]. The average computational time of Nguyen et al. [55] is 11.026 s and computational time of Thakkar et al. (2017) [56] is 5.19 s. This indicates that the proposed scheme computes faster than the existing schemes [55,56].

Further, the computational time of proposed scheme is compared with recently published schemes where the same tested images are used. The comparison of average computation time (in seconds) among the Makbol's scheme [57], Ernawan's scheme [34] and the proposed scheme are given in Table 9. Referring to Table 9, the proposed requires a less computational time compared to Makbol's scheme [57] and Ernawan's scheme [34]. It is indicated that this scheme can be used in applications where less computational time is required.

#### 5.5. Comparison of proposed scheme with existing schemes

The PSNR value of the proposed scheme is compared with many existing schemes in Table 10, which are based on solely the RDWT and solely the DCuT. For better comparison of schemes, same test image such as Lena is used. Referring to Table 10, it is indicated that the maximum PSNR value of the watermarked image for the proposed scheme is 52.92 dB while the maximum value of the watermarked image for existing schemes is 51.46 dB. This situation indicated that the proposed scheme better imperceptibility compared to existing schemes.

The proposed scheme not only outperforms over the computational time of fast existing watermarking schemes but also more imperceptible than watermarking schemes based on RDWT and SVD [32–34]. For better comparison of schemes, same test image



**Table 13**  
Comparison of the proposed technique with the existing scheme [29,32–34] with various features.

Features	Singh scheme (2016) [29]	Roy scheme (2017) [32]	Singh scheme (2017) [33]	Ernawan scheme (2018) [34]	Proposed scheme
Type of watermarking technique	Non-blind	Blind	Non – blind	Blind	Blind
Transform used	RDWT and SVD	RDWT and DCT	NSCT, RDWT, and SVD	RDWT and SVD	DCuT and RDWT
Security to watermark data	Arnold scrambling	PN sequences	Using hybridization of NSCT + RDWT + SVD	Arnold scrambling	PN sequences and arnold scrambling
Application of scheme	Copyright protection of images	Copyright protection of images	Copyright protection of images	Copyright protection of images	Copyright protection of images
Maximum PSNR (dB) value	36.98	51.46	54.17	44.46	57.60

database and watermark image are used. The PSNR values of the proposed scheme with Roy's scheme [32], Singh's scheme [33] and Ernawan's scheme [34] for different types of test images are summarized in Table 11. The results in Table 11 indicated that the imperceptibility of the proposed scheme is better than existing schemes [32–34].

For comparison of robustness of schemes, the NC and BER values against various watermarking attacks are considered. The NC and BER values of the proposed scheme with Roy's scheme [32] and Ernawan's scheme [34] for various types of attacks are given in Table 12. Referring to Table 12, it gives subjective as well as an objective comparison of robustness of watermarking schemes. For JPEG compression attack with  $Q=40$ , Roy's scheme [32] and Ernawan's scheme [34] give the NC and BER value as 0.6978, 0.2898 and 0.6610, 0.4907, respectively whereas the proposed scheme gives NC and BER value as 0.9597, 0.0229. For most of the watermarking attacks, the robustness performance of proposed scheme better than Roy's scheme [32] and Ernawan's scheme [34] except median filtering, average filtering, rotation ( $20^\circ$ ,  $45^\circ$ ), flipping and scaling attacks.

The proposed scheme is also compared with the existing schemes [29,32–34] which are proposed for copyright protection of images by various features in Table 13. The average results and comparison indicated that the performance of the proposed scheme is better than the existing schemes in terms of imperceptibility and robustness.

## 6. Medical image security – a possible application of proposed scheme

In this paper, an imperceptible and robust watermarking scheme has been proposed which has different layers of security. The layer of security is achieved by secret values of PN sequences (key 1), scaling factor (key 2) and secret key (key 3). This scheme can be used for different applications where information security is required. One such possible application proposed scheme is the security of medical images in telemedicine application (given in Fig. 14) and described below.

A hospital who is authorized to generate medical images of patients for diagnosis purposed using a variety of medical images as cover image and hospital logo as watermark them based on the proposed scheme and stored at hospital server. On-demand these watermarked medical images can be transmitted or exchanges using local communication channel or internet to different kinds of users as shown in Fig. 14.

Doctor A is authenticated doctor who has copyrights of medical image with all secret keys such as key 1, key 2 and key 3. This doctor can be extracted the watermark from received watermarked medical image via channel using these secret keys. In case if Doctor A can't obtain watermark then the user sends requires to the server to stopping transmission of the medium. Otherwise, water-

marked a medical image with secret watermark transmission via the local channel. Here, Doctor B has key 1 and key 2, Doctor C has key 2 and key 3; Doctor D has key 1. Thus, Doctor A sends the remaining keys to these Doctors for extraction of secret watermark data as per request sends by those Doctors. Thus, security of medical image is maintained when it is transmitted over local communication channel or internet against illegal modification. If Doctor E tries to extract watermark data and modification in the medical image without information of secret keys. But Doctor E can't extract secret watermark, therefore the security of medical image can be maintained against illegal modification in it by impostor Doctor.

Thus, the proposed scheme can be user security of cover medical image in the process of secret transmission of medical images via a communication channel. This scheme is useful for copyright protection of multimedia data such as digital images, videos, and audio. This scheme is also helpful security of biometric images against spoofing attacks.

## 7. Conclusions

In applications such as security of multimedia data and medical images, the watermarking schemes with high complexity are not suitable. Therefore, in this paper, a new robust and blind watermarking scheme based on discrete curvelet transform (DCuT) and redundant discrete wavelet transform (RDWT). This scheme has fast computational with high imperceptibility as well as robust against various types of watermarking attacks. Moreover, copyright protection by this scheme is more due to the different secret key provided by Arnold scrambling and PN sequences. The scheme is tested various types of cover images which have different frequency components in it. The experimental results show that the NC vales of the scheme are above 0.9 for many attacks. It is also observed that the NC value is above 0.99 for attacks such as JPEG compression ( $Q=90$ ), Gaussian low pass filtering, salt & pepper noise ( $\sigma = 0.005$ ), Gaussian noise ( $\sigma = 0.005$ ) and sharpening. The comparison of computational time is indicating that embedding time and extraction time of proposed scheme is around 2.7381 s which is less than fast watermarking scheme proposed in the literature [34,55–57]. Moreover, the comparative analysis shows that the proposed scheme outperforms over the various RDWT and SVD based watermarking schemes proposed in the literature [32,34].

In the proposed scheme, the coefficients of LH wavelet subband of C (1,6) curvelet coefficients of the cover image is modified by two PN sequences and scrambled watermark image in such a way that the blind recovering of the watermark image is possible at extraction side. The Arnold scrambling provides added security to watermark image before embedded into the cover image. The limitations of this proposed scheme are that it has less payload capacity up to 1 bit per 64 pixels and the robustness is poor to attacks such as the median filter, average filter, rotation, flipping, and scal-



- [9] Thanki R, Borra S. Fragile watermarking for copyright authentication and tamper detection of medical images using compressive sensing (CS) based encryption and contourlet domain processing. *Multimed Tools Appl* 2018;1–20.
- [10] Singh AK, Kumar B, Singh G, Mohan A, editors. *Medical image watermarking: techniques and applications*. Springer; 2017.
- [11] Kumar C, Singh AK, Kumar P. A recent survey on image watermarking techniques and its application in e-governance. *Multimed Tools Appl* 2018;77(3):3597–622.
- [12] Thakur S, Singh AK, Ghrera SP, Mohan A. Chaotic based secure watermarking approach for medical images. *Multimed Tools Appl* 2018;1–14.
- [13] Singh AK, Kumar B, Singh SK, Ghrera SP, Mohan A. Multiple watermarking technique for securing online social network contents using back propagation neural network. *Future Gener Comput Syst* 2018;86:926–39.
- [14] Garg S, Singh R. An efficient method for digital image watermarking based on PN sequences. *Int J Comput Sci Eng* 2012;4(9):1550–61.
- [15] Kumar C, Singh AK, Kumar P, Singh R, Singh S. SPIHT-based multiple image watermarking in NSCT domain. *Concurrency Comput* 2018:e4912.
- [16] Kumar C, Singh AK, Kumar P. Improved wavelet-based image watermarking through SPIHT. *Multimed Tools Appl* 2018;1–14.
- [17] Chauhan DS, Singh AK, Adarsh A, Kumar B, Saini JP. Combining Mexican hat wavelet and spread spectrum for adaptive watermarking and its statistical detection using medical images. *Multimed Tools Appl* 2017;1–15.
- [18] Das C, Panigrahi S, Sharma VK, Mahapatra KK. A novel blind robust image watermarking in DCT domain using inter-block coefficient correlation. *AEU-Int J Electron Commun* 2014;68(3):244–53.
- [19] Wang SH, Lin YP. Wavelet tree quantization for copyright protection watermarking. *IEEE Trans Image Process* 2004;13(2):154–65.
- [20] Feng LP, Zheng LB, Cao P. A DWT-DCT based blind watermarking algorithm for copyright protection. In: *Computer science and information technology (ICCSIT)*, 2010 3rd IEEE international conference on, 7. IEEE; July 2010. p. 455–8.
- [21] Sahraee MJ, Ghofrani S. A robust blind watermarking method using quantization of distance between wavelet coefficients. *Signal Image Video Process* 2013;7(4):799–807.
- [22] Singh D, Singh SK. DWT-SVD and DCT based robust and blind watermarking scheme for copyright protection. *Multimed Tools Appl* 2017;76(11):13001–13024.
- [23] Hien TD, Nakao Z, Chen YW. RDWT domain watermarking based on independent component analysis extraction. In: *Applied soft computing technologies: the challenge of complexity*. Berlin, Heidelberg: Springer; 2006. p. 401–14.
- [24] Mankar VH, Das TS, Sarkar S, Sarkar SK. Redundant Wavelet Watermarking using Spread Spectrum Modulation. *ELCVIA Electron Lett Computer Vision Image Anal* 2008;7(2):1–10.
- [25] Oskoei, S.G., Dadgostar, M., Rad, G.R., & Fatemizadeh, E. (2009). Adaptive watermarking scheme based on ICA and RDWT.
- [26] Lagzian S, Soryani M, Fathy M. A new robust watermarking scheme based on RDWT-SVD. *Int J Intell Inf Process* 2011;2(1):22–9.
- [27] Makbol NM, Khoo BE. Robust blind image watermarking scheme based on redundant discrete wavelet transform and singular value decomposition. *AEU-Int J Electron Commun* 2013;67(2):102–12.
- [28] Bajaj A. Robust and reversible digital image watermarking technique based on RDWT-DCT-SVD. In: *Advances in engineering and technology research (ICAETR)*, 2014 international conference on. IEEE; 2014. p. 1–5.
- [29] Singh P, Raman B, Roy PP. A multimodal biometric watermarking system for digital images in redundant discrete wavelet transform. *Multimed Tools Appl* 2017;76(3):3871–97.
- [30] Thanki R, Dwivedi V, Borisagar K, Borra S. A Watermarking algorithm for multiple watermarks protection using RDWT-SVD and compressive sensing. *Informatica* 2017;41(4):479–93.
- [31] Jamal M, Mahmood FS, Mudassar S. Improved robustness of RGB image content watermarking using RDWT-SVD domain. In: *Proceedings of 15th international conference on statistical sciences*; 2017. p. 73–82.
- [32] Roy S, Pal AK. A robust blind hybrid image watermarking scheme in RDWT-DCT domain using Arnold scrambling. *Multimed Tools Appl* 2017;76(3):3577–616.
- [33] Singh S, Rathore VS, Singh R, Singh MK. Hybrid semi-blind image watermarking in redundant wavelet domain. *Multimed Tools Appl* 2017;76(18):19113–37.
- [34] Ernawan F, Kabir MN. A block-based RDWT-SVD image watermarking method using human visual system characteristics. *Visual Computer* 2018;1–19.
- [35] Zhang ZY, Huang W, Zhang JL, Yu HY, Lu YJ. Digital image watermark algorithm in the curvelet domain. In: *Intelligent information hiding and multimedia signal processing*, 2006. IHH-MSP'06. international conference on. IEEE; December 2006. p. 105–8.
- [36] Hien TD, Kei I, Harak H, Chen YW, Nagata Y, Nakao Z. Curvelet-domain image watermarking based on edge-embedding. In: *International conference on knowledge-based and intelligent information and engineering systems*. Berlin, Heidelberg: Springer; September 2007. p. 311–17.
- [37] Tao P, Dexter S, Eskicioglu AM. Robust digital image watermarking in curvelet domain. In: *Security, forensics, steganography, and watermarking of multimedia contents X*, 6819. International Society for Optics and Photonics; March 2008. p. 68191.
- [38] Leung HY, Cheng LM, Cheng LL. A robust watermarking scheme using selective curvelet coefficients. *Int J Wavelets Multiresolution Inf Process* 2009;7(02):163–81.
- [39] Leung HY, Cheng LM, Cheng LL. Robust watermarking schemes using selective curvelet coefficients based on a hvs model. *Int J Wavelets Multiresolution Inf Process* 2010;8(06):941–59.
- [40] Song H, Gu J. Curvelet based adaptive watermarking for images. In: *Computer science and network technology (ICCSNT)*, 2012 2nd international conference on. IEEE; December 2012. p. 1101–5.
- [41] Lari MRA, Ghofrani S, McLernon D. Using Curvelet transform for watermarking based on amplitude modulation. *Signal Image Video Process* 2014;8(4):687–97.
- [42] Channapragada RSR, Prasad MV. Watermarking techniques in curvelet domain. In: *Computational intelligence in data mining-volume 1*. New Delhi: Springer; 2015. p. 199–211.
- [43] Jero SE, Ramu P, Ramakrishnan S. ECG steganography using curvelet transform. *Biomed Signal Process Control* 2015;22:161–9.
- [44] Thanki R, Borisagar K. Biometric watermarking technique based on cs theory and fast discrete curvelet transform for face and fingerprint protection. In: *Advances in signal processing and intelligent recognition systems*. Cham: Springer; 2016. p. 133–44.
- [45] Thanki R, Borisagar K. Watermarking scheme with CS encryption for security and piracy of digital audio signals. *Int J Inf Syst Model Des (IJISMD)* 2017;8(4):38–60.
- [46] Thanki R, Borra S, Dwivedi V, Borisagar K. An efficient medical image watermarking scheme based on FDCuT-DCT. *Eng Sci Technol* 2017;20(4):1366–79.
- [47] Candes E, Demanet L, Donoho D. Fast discrete curvelet transforms. *Appl Comput Math* 2005:1–44.
- [48] Candes E, Donoho D. New tight frames of curvelets and optimal representations of objects with piecewise-C2 singularities. *Comm Pure Appl Math* 2004;57:219–26.
- [49] Sayed U, Mofaddel MA, Abd-Elhafiez WM, Abdel-Gawad MM. Image object extraction based on curvelet transform. *Int J Appl Math Inf Sci* 2013;7(1):133–8.
- [50] Li M, Liang T, He YJ. Arnold transform based image scrambling method. 3rd international conference on multimedia technology; 2013.
- [51] The University of South Carolina SIPI Image Database: <http://sipi.usc.edu/database/database.php>. Last Access Year: 2018.
- [52] Kutter M, Petitcolas FA. Fair benchmark for image watermarking systems. In: *Security and watermarking of multimedia contents*, 3657. International Society for Optics and Photonics; April 1999. p. 226–40.
- [53] Wang Z, Bovik AC, Sheikh HR. Structural similarity based image quality assessment. *Digital Video Image Qual Percept Coding* 2005:225–41.
- [54] Zhang F, Zhang X, Cao K, Li D, Li C. Information theory applications in error bit rate analysis of digital image watermarking. *Comput Elect Eng* 2013;39(2):309–18.
- [55] Nguyen C, Tay D, Deng G. A fast watermarking system for H.264/AVC video. In: *Asia specific IEEE conference on circuits and systems*; 2006. p. 81–4.
- [56] Thakkar F, Srivastava V. A Fast watermarking algorithm with enhanced security using compressive sensing and principle components and its performance analysis against a set of standard attacks. *Multimed Tools Appl* 2017;76(14):15191–219.
- [57] Makbol NM, Khoo BE, Rassem TH. Block-based discrete wavelet transform-singular value decomposition image watermarking scheme using human visual system characteristics. *IET Image Proc* 2016;10(1):34–52.