Multimedia Tools and Applications (2021) 80:27593–27613
https://doi.org/10.1007/s11042-021-11064-y

Hybrid, blind and robust image watermarking: RDWT – NSCT based secure approach for telemedicine applications

Rohit Thanki[1] · Ashish Kothari[2] · Surekha Borra[3]

Received: 10 February 2020 / Revised: 20 February 2021 / Accepted: 5 May 2021 /
Published online: 21 May 2021

Abstract
Images frequently are helpless to burglary and copyright encroachment. There are numerous events where pictures were illegally copied from websites for utilization or monetary profit and were gotten away from equity, prompting misfortunes for the battled proprietors or innovators. Techniques for securing and recognizing digital pictures and their owners from adversaries are thus required. In this paper, a watermarking procedure in hybrid domain is proposed for copyright assurance of images. The strategy inserts watermarks in Non-Subsampled Contourlet Transform (NSCT) and Redundant Discrete Wavelet Transform (RDWT) areas to accomplish better invisibility, and robustness. The blind extraction of watermark can be performed associating the arbitrarily produced PN arrangements. The experimental results demonstrate that the combination of NSCT – RDWT improves the nature of watermarked image when tried on standard and medical images. The experimental results indicated that the proposed scheme provides good imperceptibility and robustness against various kind of watermarking attacks. The main strength of proposed scheme is that it provides good imperceptibility for watermarked images up to 58 dB along with good robustness for watermark image up to 0.99 against various types of attacks and equally works for various kind of images such as greyscale and medical images. Further, the performance of proposed scheme indicated that the quality of generated watermarked medical image has fulfilled all parameters and benefits for secure telemedicine applications.

Keywords Blind · Non-subsampled Contourlet transform (NSCT) · Medical image · Redundant discrete wavelet transform (RDWT) · Robustness · Watermarking

✉ Rohit Thanki
rohitthanki9@gmail.com

[1] Prognica Labs Tech FZCO, Dubai, UAE

[2] Atmiya University, Rajkot, India

[3] ECE Department, K. S. Institute of Technology, Bangalore, India

1 Introduction

Prior to the advanced time, the image takers or associations generally sign their photographs or structures utilizing their mark or decorating seals to help recognize the proprietors of the pictures, particularly if the Licensed innovation (IP) gets shared. Watermarking is another method for marking the picture by the proprietor for destroying the endeavors of assailants. A watermark is a superimposed logo put over an image with an aim of recognizing the proprietor of the image. Analog watermarks existed for quite a long time which are unmistakable and are generally simpler to recreate. Advanced Watermarking as a major aspect of digital right management (DRM) framework allows concealing the copyright proprietor/wholesaler/circulation chain/buyer in the pictures as a proof of ownership if there should arise an occurrence of copyright security and copyright law requirement [6–8]. A few tasks associated with putting away/altering/transmitting may contort, erase, or generally may meddle with watermarks. Although there are a lot of watermarking methods that are accessible web-based, watermarking is yet a difficult errand when managing attacks [9, 42]. Tools, for example, Checkmark, Optimark, and StirMark are the couple of programming techniques that evaluate the watermarking techniques [9].

In the literature, different sorts of schemes are proposed for image watermarking [1, 9, 12–14, 27, 28, 30, 35, 41–44, 46, 51–53]. The transform-based schemes are well known and are more focused as they exhibit better characteristics [28]. As of late, hybrid image watermarking strategies have been proposed to check their viability in watermarking. A large portion of these strategies are non-blind, require cover image for watermark extraction, which might be hard to deliver. The blind watermarking strategies do not require original images for watermark extraction and are adaptable to be utilized in numerous applications including image verification, copyright insurance, and electronic frameworks. The robust watermarking is the technique can example, duplicate control; authentication and copyright insurance as they get by against a wide scope of attacks and when the watermarks get non-damaging in the event of attacks [14].

Recently, many medical information is exchange from one healthcare centre to other healthcare center. When this medical information (particularly medical image) is transfer using open communication channel then it is vulnerable against manipulation in it. Thus, security and privacy of medical image is required when it transmits over communication channel. For integrity and privacy issue of medical image in telemedicine applications, researchers were show the useful of watermarking for security of medical images in telemedicine applications [2, 4, 19, 20, 36, 39–41]. The main requirements of watermarking for telemedicine applications are that scheme should be provided higher imperceptibility, better robustness against watermarking attacks and extraction of watermark information done using blind approach [41, 46].

The various types of proposed watermarking schemes for integrity and security of medical images in recent time are discussed here. Thakkar et al. [41] proposed blind medical image watermarking using discrete wavelet transform (DWT) and singular value decomposition (SVD) for security of medical image for telemedicine applications. This scheme equally works for grayscale as well as color medical images. Singh et al. [36] proposed redundant discrete wavelet transform (RDWT) based hybrid medical image watermarking scheme. But the limitation of this scheme is that it has less imperceptibility for watermarked medical images. Aparna et al. [4] proposed blind crypto- watermarking scheme for security of medical images. This scheme was developed using advanced encryption standard (AES) and arithmetic encoding algorithm along additive watermarking approach. This scheme was generated watermarked medical image with less imperceptibility. Kahlessenane et al. [19] proposed blind watermarking scheme using DWT for security of medical images.

Anand et al. [2] proposed non-blind watermarking scheme using combination of DWT – SVD for security of medical images. The main limitation of this scheme is that at receiver side, original cover image requires for extraction of watermark image from the watermarked image. Swaraja et al. [40] proposed blind and optimized watermarking scheme using DWT and schur transform with combination of optimization algorithm such as particle swarm bacterial for-aging (PSBF) for security of medical image. In this scheme, optimization algorithm was used to get optimized watermarked medical images. Singh et al. [39] proposed blind watermarking scheme using polar harmonic Fourier transformation (PHFT) for security of medical image. The scheme differs than other schemes because it uses different kind of transform for generation of watermarked images. Kahlessenane et al. [20] proposed blind watermarking scheme using non-subsample contourlet transform (NSCT) and schur transform for security of medical images. The limitation of this scheme is that it generates watermarked medical images with low imperceptibility.

In this paper, a blind and robust image watermarking scheme dependent on non-subsampled contourlet transform (NSCT) and redundant discrete wavelet transform (RDWT) is proposed for security of general images and medical images. The main strength of this proposed scheme is that it provides higher imperceptibility along with better robustness and blind extraction possible which shows that the proposed scheme has achieved all basic requirements of watermarking for security of medical images in telemedicine applications. Also, this scheme is equally working on general images. This is beauty of this proposed scheme without any minor changes, it works good for any kind of images.

In this scheme, a watermark (binary logo or monochromic image) is inserted into the wavelet sub band of contourlet sub band of the cover image in such a way that blind extraction is possible. The proposed scheme is tested and analyzed over several general images and medical images and its performance in term of imperceptibility and robustness is compared with existing watermarking schemes in the literature [11, 20, 33, 37, 38]. Following are some few other contributions provided by the proposed scheme.

- **Improved imperceptibility and robustness:** The high frequency contourlet coefficients are utilized to achieve better imperceptibility, while coefficients of wavelet sub-band of host are utilized for better robustness. In this way, combination of these two transforms is used in this proposed scheme to improves the limitations of existing schemes [11, 20, 33, 37, 38].
- **Improved Security:** In the existing schemes [11, 20, 33, 37, 38], watermark or secret information is straightaway inserted into the cover image. Therefore, these schemes provide lesser security for watermark or secret information. To overcome this limitation, in this proposed scheme, the PN patterns are produced using a secret key. Here, the PN pattern are inserted into cover image according to value of watermark image. Therefore, security of watermark or secret information is achieved in the scheme without inserted actual value of watermark image into cover image.
- **Blind Extraction:** Many existing scheme [2, 17, 18, 23, 29, 37, 38, 45, 49, 50] are non-blind, where cover image information is required at extraction of watermark.

This proposed scheme is blind where it requires only the secret key for extraction of watermark.

The remainder of the paper is composed as pursues: the related works are examined in section 2. The working of proposed watermarking scheme is given in section 3, followed by results in Section 4. At last, section 5 concludes the research work.

2 Related Works

In this section, the overview of various related watermarking schemes is provided.

2.1 NSCT based Watermarking Schemes

Kumar et al. [21] provide non-blind watermarking scheme using NSCT for security of multiple watermark images. Jayalakshmi et al. [18] modified high frequency contourlet coefficients of cover image create watermarked image, followed by non-blind extraction approach. Yang et al. [50] proposed support vector regression (SVR) and NSCT based non-blind watermarking scheme for copyright protection of grayscale images. In this scheme, low frequency contourlet sub-band is changed for watermark inserting. This system gives robustness strength against geometric attacks. C. Narasimhulu and K. Prasad [29] proposed another comparable hybrid non-blind image watermarking system using CT and SVD domains. Alternately, an NSCT based color watermarking scheme is proposed by Sadreazami et al. [34].

S. Das and M. Kundu [11] proposed blind medical image watermarking scheme which embeds AES encrypted watermark in DCT coefficients of NSCT low pass subband of cover image using secret key. In Patil and Rindhe [32] non-blind approach, first, NSCT is applied on cover image and contourlet coefficients of low pass subband of it are altered by bits of watermark to get watermarked version of cover image. V. Ananthaneni and U. Nelakuditi [3] proposed blind medical image watermarking utilizing NSCT, DCT, and SVD. The contourlet coefficients of two sub-bands are separated into 16×16 non-overlapping squares. The DCT is applied to the squares of these coefficients to get hybrid coefficients of cover image, followed by the SVD application to estimate hybrid coefficients of cover image into which the watermark picture is embedded utilizing secret keys. In this method, the watermark picture is additionally isolated into 16×16 non-covering squares. Singh et al. [38] proposed a similar approach, where the contourlet coefficients of all the sub-bands of cover image are utilized for watermark inserting.

2.2 RDWT based Watermarking Schemes

Bajaj et al. [5] proposed watermarking scheme combining RDWT – DCT – SVD for images. It employs non-blind extraction which demands for original cosine frequency coefficients of chosen wavelet sub-band of cover image. A RDWT – SVD based Arnold scrambled biometric watermarking is proposed by Singh et al. [37]. Thanki et al. [45] proposed another non-blind CS based encryption and RDWT – SVD based watermarking scheme where three types of watermarks are inserted into each channel of color cover image. Independent component analysis (ICA) based blind watermarking scheme is proposed by Hien et al. [16] where in watermark is inserted in RDWT domain. The wavelet sub-band of cover image is altered by PN patterns in accordance with the watermark bits in Mankar et al. [25] method. A principal component analysis (PCA) based watermarking scheme where in RDWT is utilized for watermark insertion, and the ICA – PCA for non-blind watermark extraction is proposed by Oskooei et al. [31].

Yet another RDWT and SVD based scheme for non-blind extraction is proposed by Lagzian et al. [23]. Makbol and Khoo [24] proposed blind image watermarking scheme using the same domains. Here, singular estimations of all wavelet sub-band of cover image are changed by watermark and watermarking key. Roy et al. [33] proposed watermarking scheme utilizing mixture of RDWT – DCT for images where encrypted bits of watermark inserted into selected hybrid coefficients of host to get watermarked image.

3 Background

In the proposed blind watermarking scheme, the watermark inserting, and extraction are performed in mixture of NSCT and RDWT. Therefore, in this section, the information of these two transforms is covered.

3.1 Non-Subsampled Contourlet Transform (NSCT)

The NSCT is a one of the types of contourlet transform (CT) [15]. The properties such as repetitive change and invariant moving of this transform makes it a decent possibility for usage in the process of watermark inserting. This transform converts image in to multiscale and multidirectional dimension by utilizing various filter channel banks such as laplacian pyramid (LP) and directional channel (DC). Here, the LP provides multiscale portrayal while DC provides multidirection portrayal to image. The output coefficients after these two filter channel banks process are known as contourlet coefficients. The coefficients provide rich directional information and smooth shapes of image compared to wavelet transform [10, 15, 26]. This transform also overcomes sub-band blending issue of wavelet transform. Figure 1 shows 1st level NSCT decomposition of image where image decomposed into two different sub-bands such as lowpass and bandpass. The frequency of lowpass sub-band is low and has visual information of image, while frequency of bandpass sub-band is high and has smooth as well as edges information of image. Figure 2 shows sample image and its contourlet coefficients. Here, 1st level decomposition provides one lowpass sub-band and five bandpass sub-bands.

3.2 Redundant Discrete Wavelet Transform (RDWT)

The most common transform used for watermarking is DWT, which down samples the original image while making sub bands [16, 23]. 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 redundant discrete wavelet transform (RDWT) for watermarking. The RDWT provides shift invariance for better extraction of watermark. The RDWT eliminates downsampling and the upsampling process of discrete wavelet transform. The difference between discrete wavelet transforms (DWT) and redundant discrete wavelet transform (RDWT) is shown in Fig. 3.

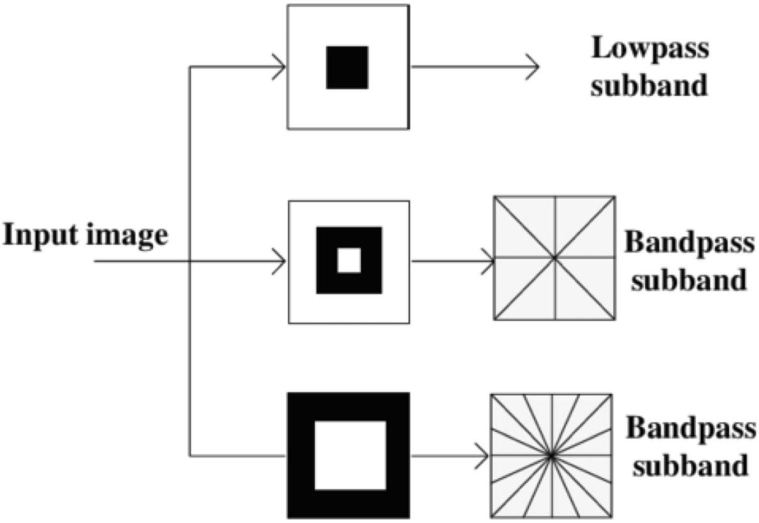


Fig. 1 NSCT Decomposition of Image

4 Proposed Watermarking Scheme

The proposed scheme is based on combination of two transform NSCT and RDWT. In this scheme, first 1st level NSCT after that 1st RDWT is applied on cover image to get its hybrid

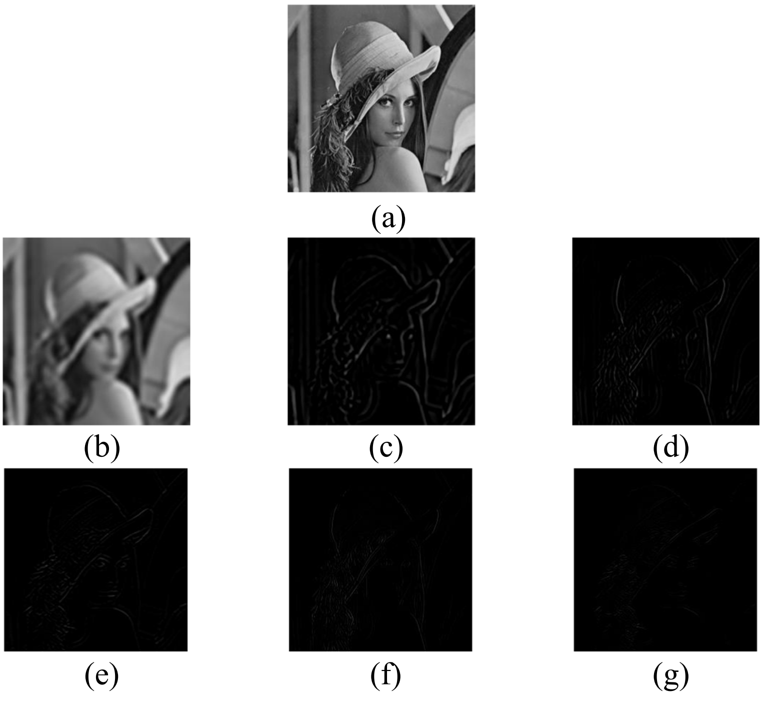


Fig. 2 (**a**) Lena image, (**b**) Low pass contourlet coefficients, (**c**) – (**g**) Band pass contourlet coefficients

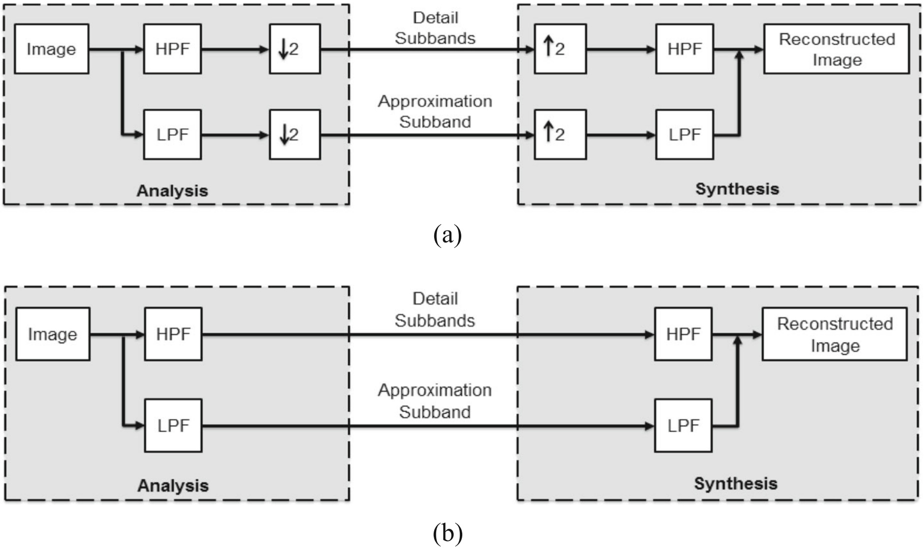


Fig. 3 Main difference between DWT and RDWT (**a**) Image Analysis and Synthesis using DWT (**b**) Image Analysis and Synthesis using RDWT

coefficients. After that, the PN patterns are inserted into hybrid coefficients of cover image according to value of watermark image such way that extraction of watermark image is done blindly at extraction side. The various combinations of these coefficients are tried to use to generated watermarked image. The proposed watermarking scheme incorporates two processes: inserting (shown in Fig. 4) and extraction (shown in Fig. 5). The details of these processes are given in next subsections.

4.1 Inserting Process

The steps of this process are given below:

Step 1: Decompose cover image into its contourlet sub-bands, 1st level NSCT is applying on it.

Step 2: Select any bandpass contourlet sub-bands of cover image. Then, apply 1st level RDWT to get wavelet sub-bands of selected contourlet sub-band of cover image. After RDWT decomposition, contourlet sub-band of cover image is decomposed into 4 sub-bands, for example, C_{ψ}, $\psi \in$ LL, LH, HL, and HH.

Step 3: Choose any sub-band of wavelet sub-bands and divide it into non-covered blocks with size of 8×8.

Step 4: With the help of secret seed and noise generator, generate two PN patterns which are uncorrelated in the nature.

Step 5: Insert a bit of watermark in each block of selected wavelet sub-band of contourlet sub-band of cover image using following equations:

a. If watermark contains zero bit, then:

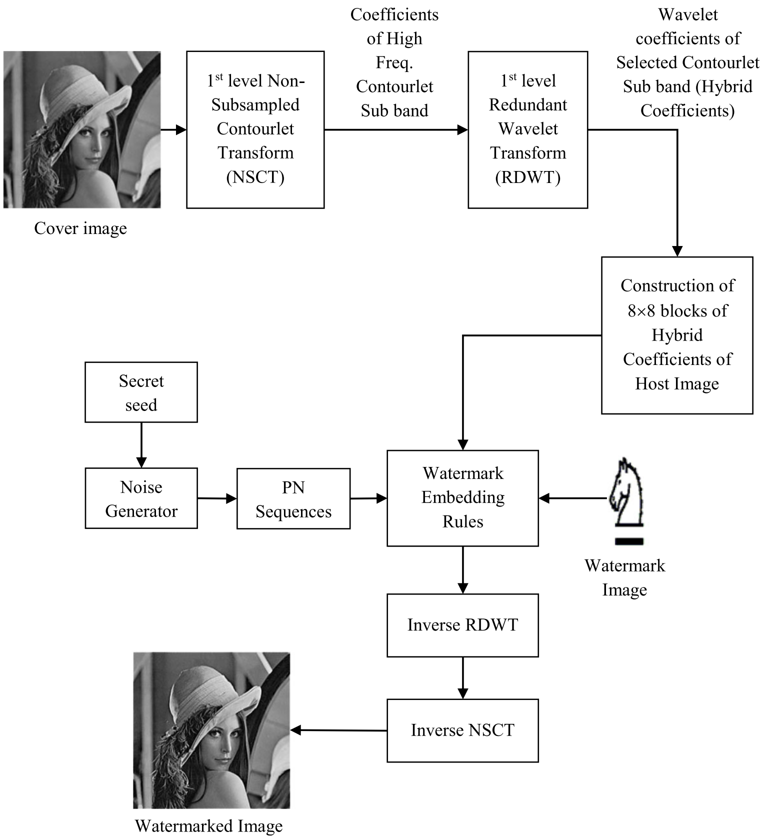


Fig. 4 Block Diagram of Watermark Inserting Process

$$WC_{S\psi} = WC_{S\psi} + k \times P_0 \tag{1}$$

else

$$WC_{S\psi} = C_{S\psi} + k \times P_1 \tag{2}$$

Where, $WC_{S\psi}$ is modified selected wavelet sub-band, $C_{S\psi}$ is originally selected wavelet sub-band of contourlet sub-band of cover image, k is the scaling factor, P_0 corresponds to PN pattern for bit 0, and P_1 corresponds to the PN pattern for bit 1.

Step 6: Perform 1st level IRDWT on modified selected wavelet sub-band to get modified selected contourlet sub-band. Then perform 1st level INSCT on it to generate a watermarked image, *WI*.

4.2 Extraction Process

The steps of this process are given below:

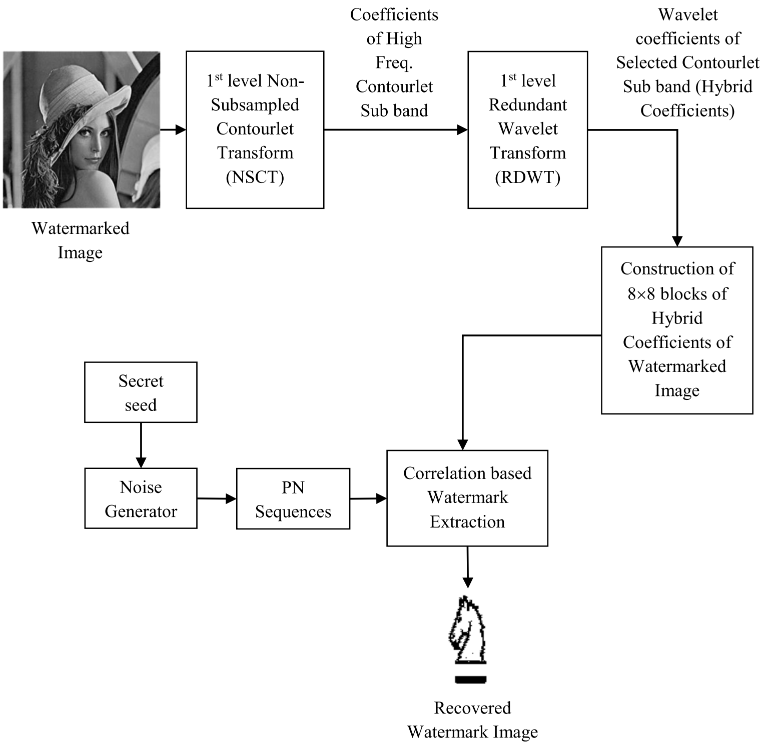


Fig. 5 Watermark Extraction Process in Proposed Watermarking Technique

Step 1: The watermarked image decomposed into its contourlet sub-bands such as lowpass and bandpass with the help of 1st level NSCT decomposition. Then, select a similar high frequency contourlet sub-band that was chosen during watermark inserting process.

Step 2: Perform 1st level RDWT to get modified wavelet coefficients of contourlet sub-band of watermarked image.

Step 3: Select a similar wavelet sub-band of contourlet sub-band of watermarked image ($WI_{S\psi}$) which was chosen during inserting process. Convert this sub-band into non-covered blocks.

Step 4: Take two PN patterns which was generated during inserting process.

Step 5: Calculate the parameters CS1 and CS2 using correlation process (corr2) such that:

$$CSI = corr^2\left(WI_{S\psi}, P_0\right) \tag{3}$$

$$CS2 = corr^2\left(WI_{S\psi}, P_1\right) \tag{4}$$

If $CS1 < CS2$, assign watermark bit as 1, else as 0.

Step 6: After getting all bits of watermark, the reshaping operation is applied on vector of these bits to get recovered watermark.

5 Results and discussion

The performance for the proposed scheme is tested on grayscale host [47] and watermark image [33]. The size of cover image and watermark is 256 × 256 pixels and 8 × 8 pixels. The performance relies upon the choice of subbands during watermark inserting. Figure 6 demonstrates the test cover image and watermark.

5.1 Performance Measures

The peak signal to noise ratio (PSNR) [22] is used to measure the similarity between original cover image and watermarked image and is given in eq. 5. The PSNR is measured in dB value. The MSE is calculated using eq. 6 which gives a 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 hidden watermark.

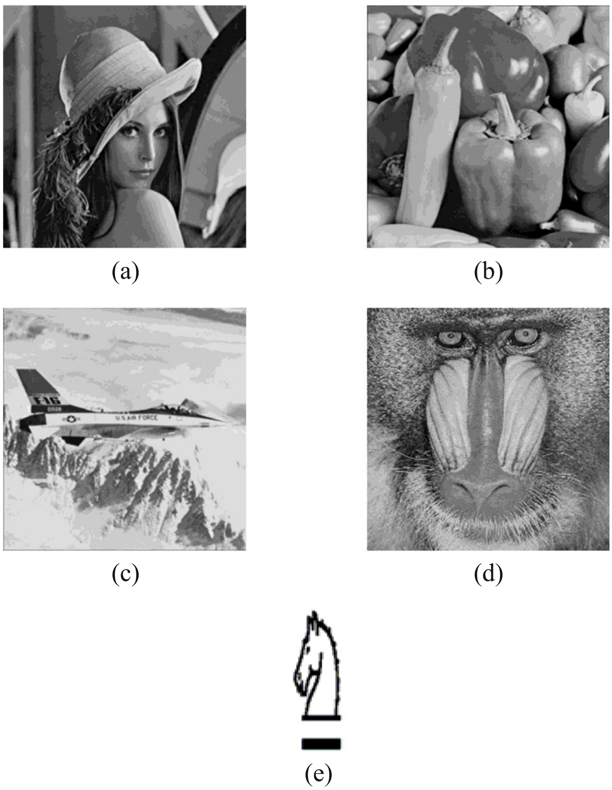


Fig. 6 Test Cover images (**a**) Lena (**b**) Peppers (**c**) Airplane (**d**) Baboon and (**e**) Watermark

Table 1. Performance of proposed scheme for various combination of NSCT – RDWT sub-bands

Contourlet Sub-band	Wavelet Sub-band	PSNR (dB)	NC	Watermark Extraction from Smoothed Watermarked Image (NC)	Watermark Extraction from Sharped Watermarked Image (NC)
C (1, 2)	LL	47.18	0.6617	0.6530	0.6743
C (1, 3) (1, 1)		45.90	0.8200	0.7732	0.7890
C (1, 3) (1, 2)		46.35	0.7315	0.7273	0.7289
C (1, 4) (1, 1)		48.66	**0.9318**	**0.8672**	**0.8931**
C (1, 4) (1, 2)		48.33	**0.8859**	**0.8378**	**0.8730**
C (1, 2)	LH	58.67	0.5538	0.5771	0.5745
C (1, 3) (1, 1)		56.01	0.7376	0.7040	0.7302
C (1, 3) (1, 2)		49.92	0.6472	0.6284	0.6443
C (1, 4) (1, 1)		51.72	**0.9842**	**0.9447**	**0.9622**
C (1, 4) (1, 2)		42.13	**0.9632**	**0.9703**	**0.9771**
C (1, 2)	HL	53.15	0.5955	0.6006	0.6023
C (1, 3) (1, 1)		46.33	0.7990	0.7331	0.7696
C (1, 3) (1, 2)		54.39	0.6346	0.6620	0.6737
C (1, 4) (1, 1)		39.95	**0.9926**	**0.9603**	**0.9625**
C (1, 4) (1, 2)		51.69	**0.9577**	**0.8992**	**0.9367**
C (1, 2)	**HH**	70.57	0.5241	0.5089	0.5105
C (1, 3) (1, 1)		59.05	0.7696	0.6992	0.7299
C (1, 3) (1, 2)		58.53	0.6420	0.6026	0.6174
C (1, 4) (1, 1)		43.49	**0.9997**	**0.9961**	**0.9987**
C (1, 4) (1, 2)		43.07	**0.9997**	**0.9974**	**0.9997**

$$PSNR = 10 \times \log_{10}\left(\frac{255^2}{MSE}\right) \tag{5}$$

$$MSE = \frac{1}{M \times N}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}\left(C(x,y) - CW(x,y)\right)^2 \tag{6}$$

Where, C is original cover image and CW is watermarked image, respectively.

The robustness of the watermarking scheme can be measured by Normalized Correlation (NC) [22] and Structural Similarity Index Measure (SSIM) [48]. The NC and SSIM can be calculated using Eqs. 7 & 8, respectively. While NC measures the correlation between 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.

$$NC = \frac{\sum_{x=1}^{M}\sum_{y=1}^{N} w(x,y) \times w^*(x,y)}{\sum_{x=1}^{M}\sum_{y=1}^{N} w^2(x,y)} \tag{7}$$

Where, w is the original watermark image and w^* is the recovered watermark image.

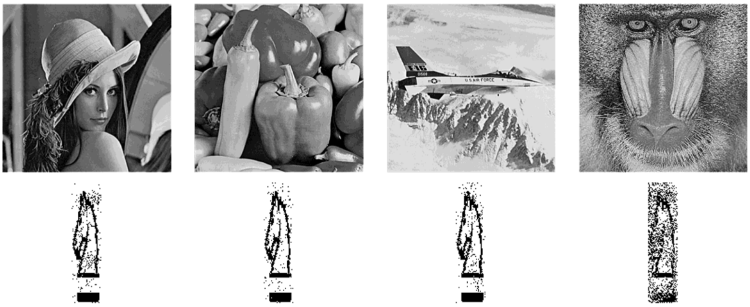
$$SSIM = \frac{(2\mu_w\mu_{w*} + C_1)(2\sigma_{ww*} + C_2)}{\left(\mu_w^2 + \mu_{w*}^2 + C_1\right)\left(\mu_w^2 + \mu_{w*}^2 + C_2\right)} \tag{8}$$

Where, μ_w is the average of original watermark image, μ_{w*} is the average of recovered watermark image, σ_{ww*} is the covariance of original watermark image and recovered watermark image, and C_1, C_2 are constant values.

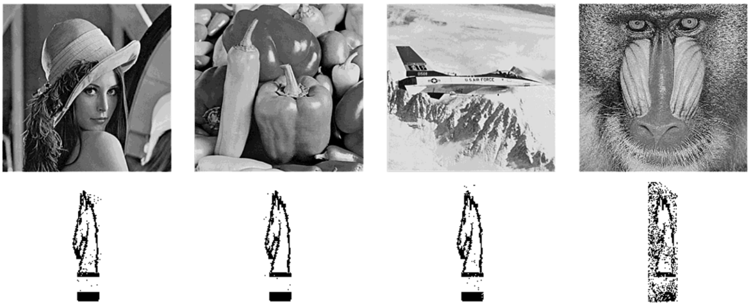
Using above measures, imperceptibility test and robustness test of proposed scheme are performed for various tested cover images.

5.2 Selection of Coefficients for Inserting Watermark Image in to Cover Image

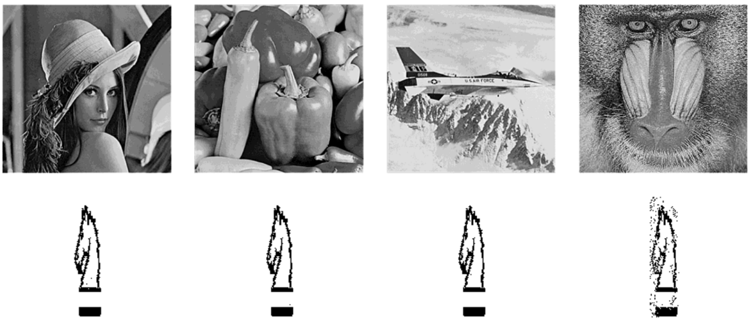
In the proposed scheme, the NSCT breaks down cover image into six diverse contourlet sub-bands. Out of these sub-bands, low frequency contourlet coefficients (C (1, 1)) cannot be



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



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



(c) Subjective results with scaling factor $k = 25$

Fig. 7 Watermarked Images and Extracted Watermarks for Different Scaling Factor Values using Proposed Scheme. (**a**) Subjective results with scaling factor $k = 5$. (**b**) Subjective results with scaling factor $k = 15$. (**c**) Subjective results with scaling factor $k = 25$

Table 2. Objective results for variation in scaling factors

Test Cover Image	*k*=25			*k*=15			*k*=5		
	PSNR (dB)	NC	SSIM	PSNR (dB)	NC	SSIM	PSNR (dB)	NC	SSIM
Lena	41.77	0.9994	1.0000	46.55	0.9832	0.9994	55.88	0.9263	0.9977
Peppers	43.49	0.9997	1.0000	48.27	0.9955	0.9999	57.60	0.9577	0.9991
Airplane	42.33	0.9997	1.0000	47.12	0.9913	0.9997	56.44	0.9457	0.9986
Baboon	43.26	0.9428	0.9985	48.04	0.7861	0.9934	57.37	0.6943	0.9901

utilized for inserting process as it contains enormous visual data of cover image. The RDWT breaks any high frequency contourlet sub-band into four distinctive wavelet sub-bands. A total of 20 combinations of NSCT and RDWT are available in the proposed scheme, and the performance varies for each combination. The PSNR and NC are estimated for each combination of NSCT – RDWT and are listed in Table 1. The robustness of the proposed scheme is high for the combinations of C (1, 4) (1, 1) and C (1, 4) (1, 2) sub-bands with any wavelet sub-band. Subsequently, to accomplish better robustness with the proposed scheme, the combination of C (1, 4) (1, 1) contourlet sub band – HH wavelet sub-band is utilized for watermark inserting process.

5.3 Imperceptibility Test

In the proposed scheme, a cover image of size 512 × 512 is taken as cover image. The 1st level NSCT followed by 1st Daubechies (db1) RDWT is applied on cover image to get its hybrid coefficients with size of 512 × 512. After that, these coefficients are divided into 4096 non-overlapping blocks with size of 8 × 8. The watermark image which is of size 32 × 128 pixels is converted into a vector of size 4096. Then according to the watermark bits, selected hybrid

Table 3. Performance Comparison

Scheme	Maximum PSNR (dB)
Hien et al. [16] (2006)	52.03
Jayalakshmi et al. [18] (2006)	47.00
Mankar et al. [25] (2008)	42.05
Oskooei et al. [31] (2009)	54.62
Lagzian et al. [23] (2011)	37.52
Narasimhulu et al. [50] (2011)	37.7705
Yang et al. [29] (2011)	45.167
Das et al. [11] (2011)	41.5895
Singh et al. [38] (2011)	36.8402
Makbol et al. [24] (2013)	54.16
Bajaj et al. [5] (2014)	51.00
P. Singh et al. [37] (2017)	36.98
Roy et al. [33] (2017)	51.46
Jamal et al. [17] (2017)	24.72
Singh et al. [36] (2017)	54.8135
Zhong et al. [54] (2020)	42.47
Kahlessenane et al. [20] (2021)	44.98
Proposed	57.60

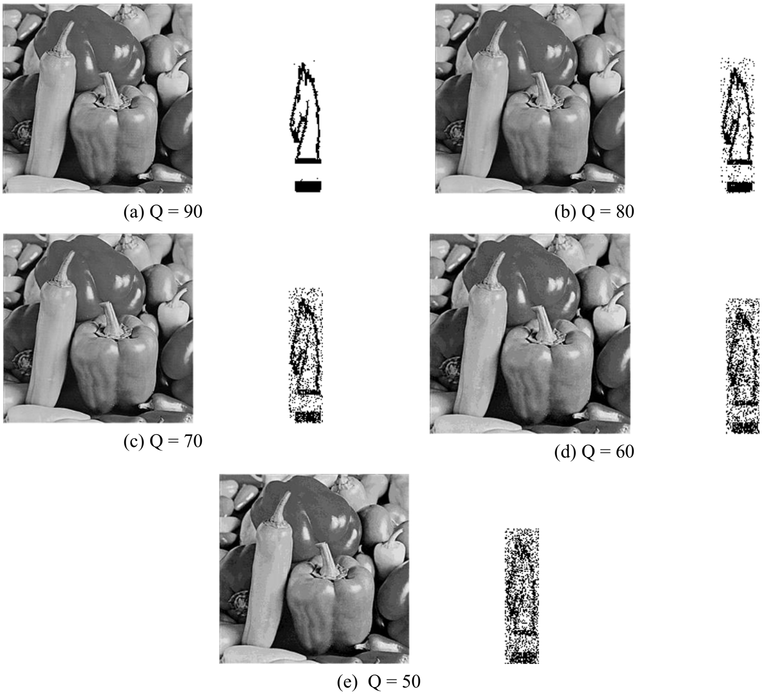


Fig. 8 Subjective Results of Proposed Scheme against Compression Attacks

coefficients of each block of cover image are modified using two PN sequences, and a scaling factor. After watermark embedding, the inverse 1st db1 RDWT, followed by inverse 1st level NSCT are applied to get watermarked image.

The proposed scheme is tested using different general images to check how the image degrade after inserting process. The performance of inserting process depends on the scaling

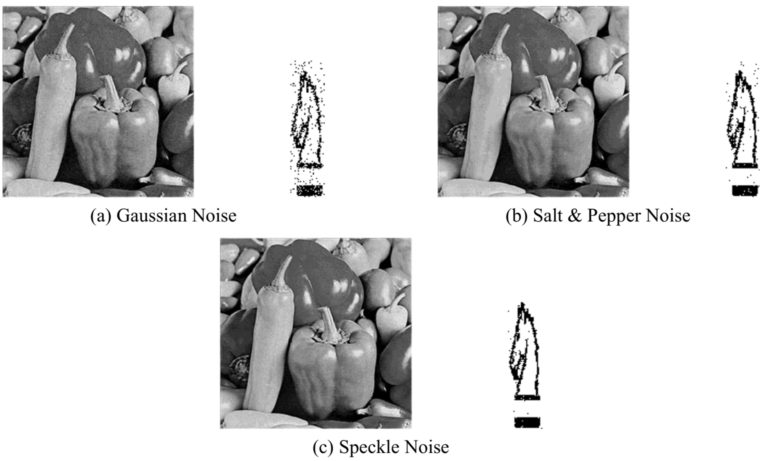
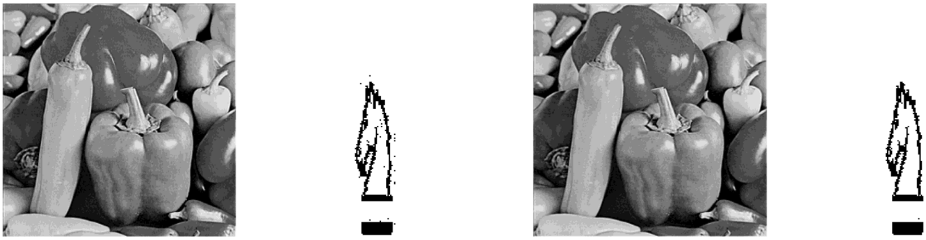


Fig. 9 Subjective Results of Proposed Scheme against Noise Addition Attacks



(a) Median Filter (b) Gaussian Low Pass Filter

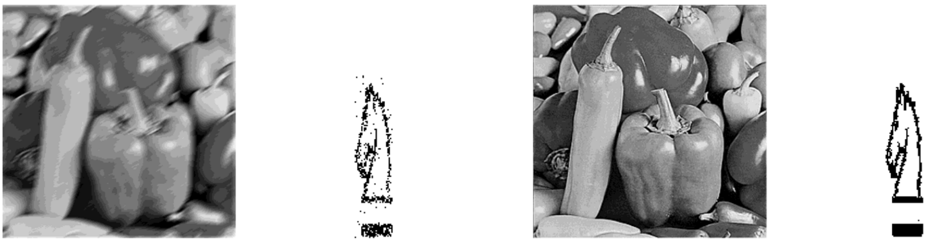
Fig. 10 Subjective Results of Proposed Scheme against Filter Attacks

factor k used in Eq. 2. 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. 7 and Table 2. The results indicate the quality of extracted watermark improves with k, maintaining the visual quality of watermarked images.

In Table 3, the imperceptibility performance of proposed scheme is compared with other existing RDWT and NSCT based schemes in the literature. It is to be noted that the maximum PSNR achieved using proposed scheme is 57.60 dB which is comparatively high compared to PSNR achieved by existing schemes in the literature.

5.4 Robustness Test

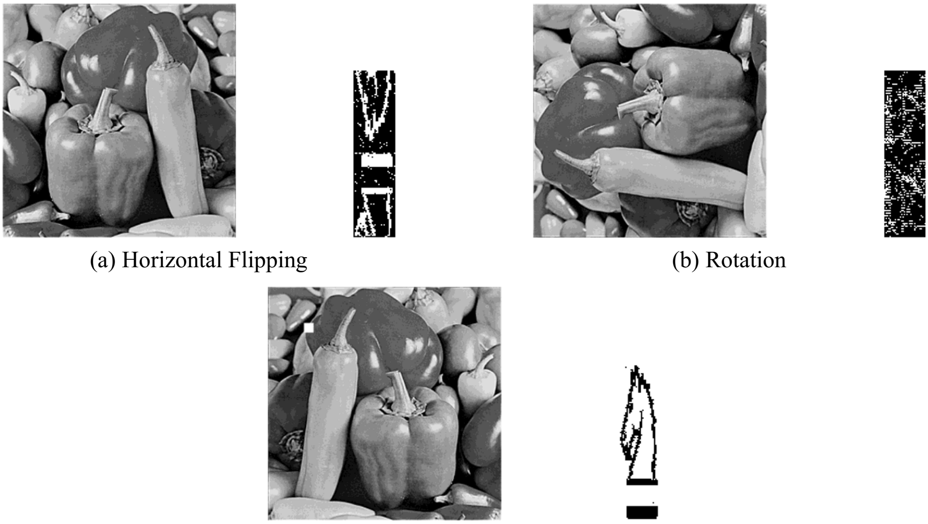
To verify the robustness test of the proposed scheme, various watermarking attacks such as JPEG compression, different filtering attacks, different noise addition attacks, motion blur, sharpening, histogram equalization and geometric attacks are applied on the watermarked images, and then watermark extraction is attempted and the subjective and objective results are



(a) Motion Blur (b) Sharpening

(c) Histogram Equalization

Fig. 11 Subjective Results of Proposed Scheme against various types of Attacks



(a) Horizontal Flipping (b) Rotation

(c) Cropping

Fig. 12 Subjective Results of Proposed Scheme against various types of Geometric Attacks

given in Figs. 8, 9, 10, 11 and 12, and Table 4. The robustness of 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 25.

5.5 Application of Proposed Scheme for Security of Medical Images in Telemedicine

The proposed scheme is additionally analyzed for its applicability to medical images [11] [54] in telemedicine applications, for example, CT, MRI, and US which are shown in Fig. 13. The subjective results (shown in Fig. 14) and objective results (shown in Figs. 15 and 16) for medical images show that this scheme is effectively works for security of medical images.

Table 4 Quantitative Results of Proposed Scheme against Various Types of Attacks

Test image	Lena	Peppers	Airplane	Baboon	Lena	Peppers	Airplane	Baboon
JPEG Compression Attack	NC				SSIM			
Q=50	0.6733	0.6772	0.6630	0.6029	0.9884	0.9884	0.9875	0.9850
Q=60	0.7325	0.7283	0.7134	0.6304	0.9910	0.9913	0.9901	0.9866
Q=70	0.7939	0.7974	0.7784	0.6743	0.9939	0.9941	0.9929	0.9898
Q=80	0.8785	0.8973	0.8808	0.7677	0.9971	0.9977	0.9968	0.9934
Q=90	0.9968	0.9984	0.9990	0.9296	0.9999	1.0000	0.9999	0.9985
Motion Blur	0.9664	0.9780	0.9800	0.7861	0.9968	0.9970	0.9972	0.9912
Sharpening	0.9987	0.9997	0.9994	0.9351	0.9999	1.0000	0.9999	0.9985
Histogram Equalization	0.9958	0.9994	0.9929	0.9296	0.9998	1.0000	0.9996	0.9983
Median Filter (3 × 3)	0.9838	0.9929	0.9848	0.8607	0.9997	0.9999	0.9997	0.9967
Gaussian Low Pass Filter (3 × 3)	0.9961	0.9997	0.9987	0.8947	0.9999	1.0000	0.9999	0.9974
Speckle Noise (variance=0.005)	0.9948	0.9948	0.9819	0.9173	0.9997	0.9998	0.9992	0.9979
Salt & Pepper Noise (variance= 0.005)	0.9835	0.9851	0.9800	0.9225	0.9994	0.9995	0.9994	0.9980
Gaussian Noise (variance=0.005)	0.9386	0.9467	0.9447	0.8801	0.9976	0.9979	0.9979	0.9964

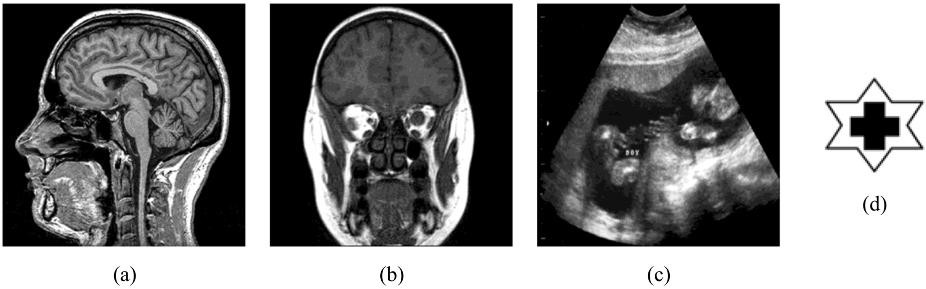


Fig. 13 Test Cover Medical Images (**a**) CT (**b**) MRI (**c**) US (**d**) Watermark image

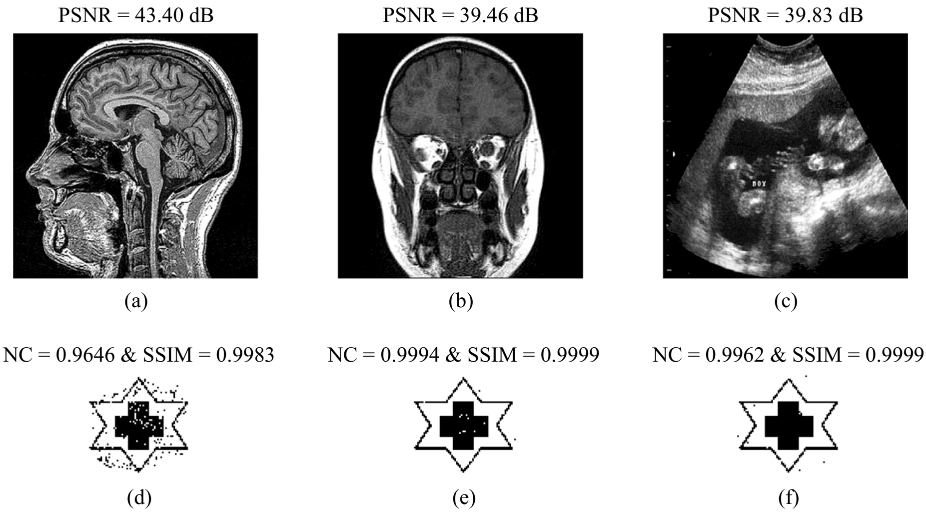


Fig. 14 (**a**) – (**c**) Watermarked medical image (**d**) – (**f**) Extracted watermark image using watermarking key k = 25.

Figures 15 and 16 shows that the NC and SSIM estimations of recovered watermark image from watermarked medical images against different watermarking attacks. The qualities show

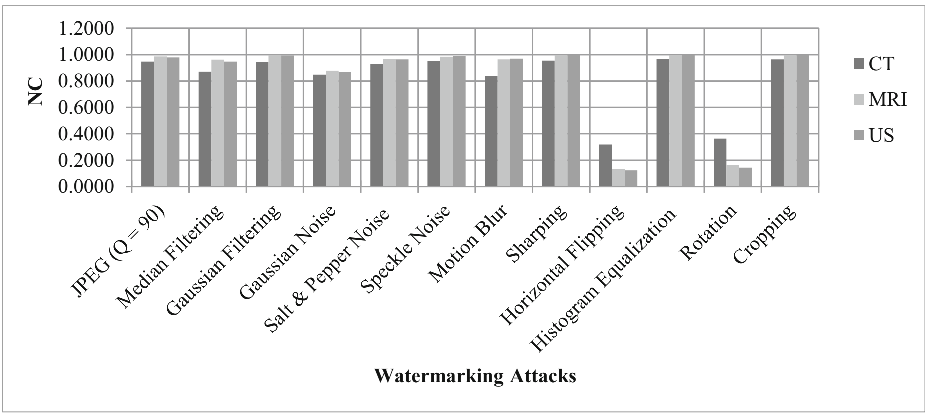


Fig. 15 NC values of proposed scheme against various attacks for various medical images

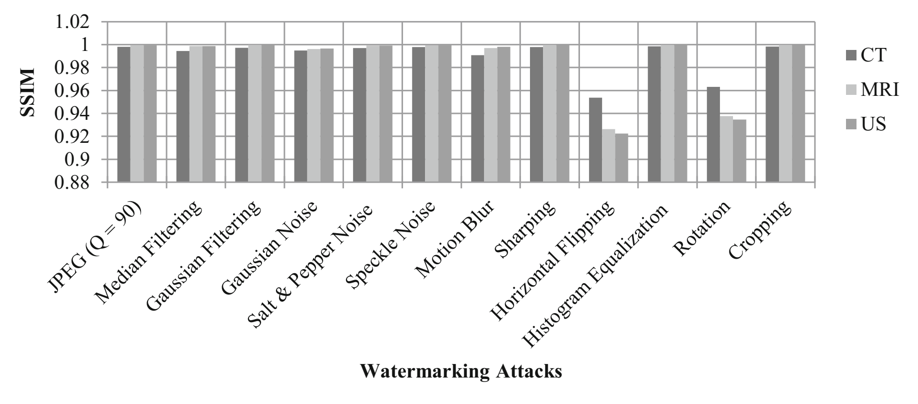


Fig. 16 SSIM values of proposed scheme against various attacks for various medical images

Table 5. Performance comparison of the proposed scheme with existing RDWT based schemes

(a) Comparison of Maximum PSNR (dB) values of schemes			
Test Images	**P. Singh et al. [37]**	**Roy et al. [33]**	**Proposed**
Lena	36.85	51.4581	**55.88**
Peppers	35.43	46.9716	**57.60**
Airplane	Not Reported	47.3052	**56.44**
Baboon	34.21	Not Reported	**57.37**
(b) Comparison of NC values of schemes			
Watermarking Attacks	**P. Singh et al. [37]**	**Roy et al. [33]**	**Proposed**
Gaussian Filtering (3 × 3)	Not Reported	1.0000	0.9997
Median Filtering (3 × 3)	Not Reported	0.7452	**0.9929**
Sharpening	0.8804	0.9995	**0.9997**
Histogram Equalization	0.9822	0.9964	**0.9994**
Salt & Pepper Noise (variance=0.005)	0.8264	0.9496	**0.9851**
Speckle Noise (variance=0.005)	Not Reported	0.8791	**0.9948**
Gaussian Noise (variance=0.005)	Not Reported	0.9030	**0.9467**
Blurring	0.8836	Not Reported	**0.9780**

that this proposed scheme is robust to a large portion of the basic attacks. This recommends the proposed scheme for its use in security of medical images in telemedicine applications.

Table 6. Performance comparison of the proposed scheme with existing NSCT based schemes

(a) Comparison of Maximum PSNR (dB) values of schemes			
Test Medical Images	Singh et al. [38]	Das et al. [11]	Proposed
MRI Image	18.5950	41.5713	**39.46**
CT Image	19.2730	41.5157	**43.40**
US Image	Not Reported	41.4776	**39.83**
(b) Comparison of NC values of schemes			
Watermarking Attacks	Kahlessenane et al. [20]	Proposed	
Median Filtering	0.9179	**0.9988**	
Salt & Pepper Noise	0.8741	**0.9991**	
Cropping	0.7115	**0.9999**	
Sharping	0.7644	**0.9999**	
JPEG Compression	0.9430	**0.9853**	

5.6 Performance Comparison with Performance of Existing Schemes

The performance comparison of the proposed scheme with RDWT and NSCT based existing schemes [11, 20, 33, 37, 38] is given in Tables 5 and 6 with respect to PSNR and NC. The comparison is performed after considering the same test cover image. The comparison demonstrated that proposed scheme provides better imperceptibility and robustness compared to existing schemes [11, 20, 33, 37, 38].

6 Conclusions

This paper proposed hybrid, robust and blind watermarking scheme for security of general images and medical images. The proposed scheme is used combination of NSCT and RDWT to achieved high imperceptibility when PN patterns are used to achieved blind extraction of watermark image at extraction side. The proposed scheme is tested on different kinds of cover images and performance of scheme is compared with many existing schemes in the literature. It is observed that the proposed scheme showed superiority to the existing schemes as far as imperceptibility and robustness is concerned. The proposed scheme is also contrasted with existing watermarking schemes, to suit applications for example, copyright assurance in telemedicine and E-commerce. In future, this scheme will be tested on DICOM version of medical images.

References

1. American Hospital Association (2015) The promise of telehealth for hospitals, health systems and their communities. Trend Watch.
2. Anand A, Singh AK (2020) An improved DWT-SVD domain watermarking for medical information security. Comput Commun 152:72–80
3. Ananthaneni V, Nelakuditi UR (2017) Hybrid Digital Image Watermarking using Contourlet Transform (CT), DCT and SVD. Intl J Image Process (IJIP) 11(3):85–93
4. Aparna P, Kishore PVV (2020) A blind medical image watermarking for secure e-healthcare application using crypto-watermarking system. J Intell Syst 29(1):1558–1575
5. Bajaj A (2014) Robust and reversible digital image watermarking technique based on RDWT-DCT-SVD. In Advances in Engineering and Technology Research (ICAETR), 2014 International conference on (1 – 5). IEEE
6. Borra S, Swamy G (2013) Sensitive digital image watermarking for copyright protection. Intl J Network Secur 15(2):113–121
7. Borra S, Swamy G (2014) Lossless Watermarking technique for copyright protection of high-resolution images. In Region 10 Symposium. IEEE 2014:73–78
8. Borra S, Swamy G, Reddy K (2012) A novel copyright protection scheme based on visual secret sharing. In Computing Communication & Networking Technologies (ICCCNT), Third International Conference on, 1–5, IEEE (2012).
9. Borra S, Lakshmi H, Dey N, Ashour A, Shi F (2017) Digital image watermarking tools: state-of-the-art. Front Artificial Intell Appl 296:450–459
10. Da Cunha A, Zhou J, Do M (2006) The nonsubsampled Contourlet transform: theory, design, and applications. IEEE Trans Image Process 15(10):3089–3101
11. Das S, Kundu M (2011) Hybrid contourlet – DCT based robust image watermarking technique applied to medical data management. In: International Conference on Pattern Recognition and Machine Intelligence. Springer, Berlin, pp 288–292

12. Dey N, Biswas D, Roy A, Das A, Chaudhuri S (2012) DWT-DCT-SVD based Blind Watermarking Technique of Gray Image in Electrooculogram Signal. 2012 12th International Conference on Intelligent Systems Design and Applications (ISDA), 680–685
13. Dey N, Das P, Roy A, Das A, Chaudhuri S (2012) DWT-DCT-SVD based Intravascular Ultrasound Video Watermarking. 2012 World Congress on Information and Communication Technologies (WICT), 224–229
14. Dey N, Ashour AS, Chakraborty S, Banerjee S, Gospodinova E, Gospodinov M, Hassanien AE (2017) Watermarking in biomedical signal processing. In intelligent techniques in signal processing for multimedia security (pp. 345-369), Springer International Publishing
15. Do M, Vetterli M (2005) The Contourlet transform: an efficient directional multiresolution image representation. IEEE Trans Image Process 14(12):2091–2106
16. Hien TD, Nakao Z, Chen YW (2006) RDWT Domain Watermarking based on Independent Component Analysis Extraction. In: Applied Soft Computing Technologies: The Challenge of Complexity (401–414). Springer, Berlin
17. Jamal M, Mahmood FS, Mudassar S (2017) Improved Robustness of RGB Image Content Watermarking Using RDWT-SVD Domain. In Proceedings of 15th International Conference on Statistical Sciences (73–82)
18. Jayalakshmi M, Merchant SN, Desai UB (2006) Digital watermarking in contourlet domain. In Pattern Recognition, 2006. ICPR 2006. 18th International Conference on (Vol. 3, 861–864). IEEE.
19. Kahlessenane F, Khaldi A, Kafi R, Euschi S (2020) A DWT based watermarking approach for medical image protection. J Ambient Intell Humanized Comput 1-8
20. Kahlessenane F, Khaldi A, Kafi R, Euschi S (2021) A robust blind medical image watermarking approach for telemedicine applications. Clust Comput:1–14
21. Kumar C, Singh AK, Kumar P, Singh R, Singh S (2020) SPIHT-based multiple image watermarking in NSCT domain. Concurrency Comput: Pract Experience 32(1):e4912
22. Kutter M, Petitcolas FA (1999) Fair benchmark for image watermarking systems. Secur Watermark Multimed Contents 3657:226–239
23. Lagzian S, Soryani M, Fathy M (2011) A new robust watermarking scheme based on RDWT-SVD. Intl J Intell Inform Process 2(1):22–29
24. Makbol NM, Khoo BE (2013) Robust blind image watermarking scheme based on redundant discrete wavelet transform and singular value decomposition. AEU-Intl J Electronics Commun 67(2):102–112
25. Mankar VH, Das TS, Sarkar S, Sarkar SK (2008) Redundant wavelet watermarking using spread Spectrum modulation. ELCVIA: Electronic Lett Comput Vis Image Analys 7(2):1–10
26. MedPixTM Medical Image Database (2017) available at http://rad.usuhs.mil/medpix/medpix.html, https://medpix.nlm.nih.gov/home, Last Access Year
27. Mohanpurkar A, Joshi M (2016) A traitor identification technique for numeric relational databases with distortion minimization and collusion avoidance. Intl J Ambient Comput Intell 7(2):114–137
28. Mousavi SM, Naghsh A, Abu-Bakar SAR (2014) Watermarking techniques used in medical images: a survey. J Digital Imaging 27(6):714–729
29. Narasimhulu C, Prasad K (2011) A robust watermarking technique based on non-subsampled Contourlet transform and SVD. Intl J Comput Appl 16(8):27–36
30. Nyeem H, Boles W, Boyd C (2013) A review of medical image watermarking requirements for teleradiology. J Digit Imaging 26(2):326–343
31. Oskooei SG, Dadgostar M, Rad GR, Fatemizadeh E (2009) Adaptive watermarking scheme based on ICA and RDWT
32. Patil HM, Rindhe BU (2016) Study and overview of combined NSCT-DCT digital image watermarking. In Global Trends in Signal Processing, Information Computing and Communication (ICGTSPICC), 2016 International conference on (302 – 307). IEEE
33. Roy S, Pal A (2017) A robust blind hybrid image watermarking scheme in RDWT – DCT domain using Arnold scrambling. Multimed Tools Appl 76(3):3577–3616
34. Sadreazami H, Ahmad MO, Swamy MS (2015) A robust multiplicative watermark detector for color images in sparse domain. IEEE Trans Circuits Syst II: Express Briefs 62(12):1159–1163
35. Singh A (2015) Some new techniques of improved wavelet domain watermarking for medical images. Ph.D. Thesis, NIT Kurukshetra
36. 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
37. Singh P, Raman B, Roy PP (2017) A multimodal biometric watermarking system for digital images in redundant discrete wavelet transform. Multimed Tools Appl 76(3):3871–3897
38. Singh S, Singh R, Singh AK, Siddiqui T (2018) SVD – DCT based medical image watermarking in NSCT domain. In: Quantum Computing: An Environment for Intelligent Large Scale Real Application. Springer, Cham, pp 467–488

39. Singh MK, Kumar S, Ali M, Saini D (2021) Application of a novel image moment computation in X-ray and MRI image watermarking. IET Image Process 15(3):666–682
40. Swaraja K, Meenakshi K, Kora P (2020) An optimized blind dual medical image watermarking framework for tamper localization and content authentication in secured telemedicine. Biomed Signal Process Control 55:101665
41. Thakkar FN, Srivastava VK (2017) A blind medical image watermarking: DWT-SVD based robust and secure approach for telemedicine applications. Multimed Tools Appl 76(3):3669–3697
42. Thanki R, Kothari A (2016) Digital watermarking: technical art of hiding. Intelligent Analysis of Multimedia Information, 431–465
43. Thanki R, Borra S, Dwivedi V, Borisagar K (2017) An efficient medical image watermarking scheme based on FDCuT – DCT. Eng Sci Technol Intl J 20(4):1366–1379
44. Thanki R, Borra S, Dwivedi V, Borisagar K (2017) A steganographic approach for secure communication of medical images based on DCT-SVD and compressed sensing (CS) theory. Imaging Sci J 65(8):458–468
45. Thanki R, Dwivedi V, Borisagar K, Borra S (2017) A Watermarking Algorithm for Multiple Watermarks Protection Using SVD and Compressive Sensing. Informatica 41(4)
46. Thanki R, Borra S, Borisagar K (2018) A hybrid watermarking technique for copyright protection of medical signals in teleradiology. Handbook Res Inform Secur Biomed Signal
47. University of South Carolina SIPI Image Database (2017): http://sipi.usc.edu/database/database.php, Last Access Year
48. Wang Z, Bovik AC, Sheikh HR (2005) Structural similarity-based image quality assessment. Digital Video image quality and perceptual coding, 225–241
49. Wang Z, Sun X, Zhang D (2007) Novel watermarking scheme based on PSO algorithm. In: Li K (ed) LSMS 2007, LNCS 4688. Springer-Verlag, Berlin, pp 307–314
50. Yang HY, Wang XY, Chen LL (2011) Geometrically invariant image watermarking using SVR correction in NSCT domain. Comput Electric Eng 37(5):695–713
51. Yassin N (2015) Digital watermarking for telemedicine applications: a review. Intl J Comput Appl 129(17): 30–37
52. Yuan XC, Li M (2018) Local multi-watermarking method based on robust and adaptive feature extraction. Signal Process 149:103–117
53. Zhang Y, Qin C, Zhang W, Liu F, Luo X (2018) On the fault-tolerant performance for a class of robust image steganography. Signal Process 146:99–111
54. Zhong Z, Gao W, Khattak AM, Wang M (2020) A novel multi-source image fusion method for pig-body multi-feature detection in NSCT domain. Multimed Tools Appl 79(35):26225–26244 MedPix™ medical image database available at http://rad.usuhs.mil/medpix/medpix.html, https://medpix.nlm.nih.gov/home, last access year: 2017