ROI Based Medical Image Watermarking with Zero Distortion and Enhanced Security

Neha Solanki, Sanjay K. Malik
Hindu College of Engineering/CSE Department, Sonepat, 131001, India
Email: solanki.neha08@gmail.com, skmalik9876@gmail.com

Abstract—Medical Image Watermarking has been considered as an appropriate method for enhancing the data security and content verification in medical science. For the purpose of achieving better security it is recommended to hide the data in the medical image itself that will improve the reliability of medical information system. In our paper, the work is divided in two main stages, first of all image is divided into two parts: Region of Interest that is defined as informational part of image and Region of Non Interest that is defined as non-informational part. In our work we have used Region of Non Interest to hide the data so that the informational part of the image kept safe. Watermark is encrypted by using RSA. A Discrete Wavelet Transform based approach is used for embedding the encrypted data in Region of Non Interest part of image for enhancing data security. The experimental result shows that watermark embedded by the proposed algorithm provides better security and can survive successfully under different attacks.

Index Terms—ROI (Region of Interest), RONI (Region of Non Interest), IWT (Integer Wavelet Transform), DWT (Discrete Wavelet Transform), IWT with AT (IWT with Arnold Transform), DWT with RST (DWT with RSA, Subtraction and Threshold).

I. INTRODUCTION

The need of sharing secret messages in distributed communication increase the use of data embedding methods into multimedia documents like images, text files, audio files, video etc. The hiding process is not as simple as it sounds, a message can be hidden in cover document if the content of the document has high redundancy. One of the techniques for hiding data is called watermarking [13]. Watermarking is the process of embedding a special kind of data into media, which may be image, audio and video. This special kind of data known as watermark that can be extracted later and used for supporting copyright protection, ownership verification and covert communication. Watermarking is an antique technique but digital technology give it a new direction so that it can hide information in digital images and signals in such a way that data can be safely transferred over channel and not perceived by other unsuspecting users [12]. During the last few years as advancements in information and communication technologies are growing rapidly, medical data management systems have changed immensely. Advancements in medical information system is changing the way patient records are stored, accessed and distributed. The integrity of the records such as medical images, patient text records etc. needs to be protected from unauthorized modification or destruction of information on the medical images [3].

Initially, data encryption is being used on the Internet to protect sensitive data during transmission. It is also being used to protect medical images in the form of digital signature. The problem with digital signature is that it needs to be transmitted together with the image in a separate file or in the image header. There is also a risk of losing the signature during transmission. The signature will also be lost if the image file is converted to another format that does not allow headers. Data embedding is where related information such as digital signature or any other information can be inserted into the medical images as a watermark.

There are three objectives of using watermark for medical images:-

- Data hiding, way to hide the information to make it more secure.
- Integrity control prevents the image from being modified by unauthorized user.
- Authentication, verifies that the image is really what the user suppose it is.

The watermark has been embedded into the medical image to provide more authenticity and integrity. Then RONI and ROI [1] concept is used that provides more security because it hides the message in the background part (RONI) by keeping the informational part (ROI) secure. First of all, the ROI and NROI part is separated. The information is watermarked by using various watermarking techniques like DWT, IWT. Then, the watermarked information is embedded into the NROI part of the medical image. The process is to be done make the information more secure, authentic and keeping the main information part secure [6]. Various approaches have been proposed that uses ROI with different techniques.

In this paper, we propose a new reliable method by hiding the encrypted watermark in the RONI part of the medical image using DWT approach. In section II Literature Review is discussed and in section III Methodology is discussed. The proposed algorithm and

experimental results related to it is presented in section IV and section V. Finally conclusion and future work is in section VI and References are listed.

II. LITERATURE REVIEW

B. M. Planitz [2] proposed a novel model in conceptual form whereby medical image regions are watermarked differently so that perceptual degradation due to watermarking is limited in 2005. Results on MR and CT images demonstrate that less visually sensitive areas on images can be watermarked using more robust techniques.

In the year 2005, A. J. Maeder [3] described an approach to ensure that impact on the image quality is well below the threshold of visual perceptibility. The principles on which this approach rests are the choice of a suitably light payload, and the use of different watermarking methods and parameters for different medical image types.

M. Kallel performed a work Medical Image Watermarking Scheme for preserving the image history [4] that presents a multiple watermarking application in spatial domain to preserve the historic of the medical image by embedding medical diagnosis.

N. A. Memon proposed the scheme embeds robust watermark in region of non interest (RONI) for achieving security and confidentiality in 2009 [5]. The image visual quality as well as tamper localization has been evaluated. Author have used weighted peak signal to noise ratio (WPSNR) for measuring image quality after watermarking.

In Year 2010, M. K. Kundu performed a work "Lossless ROI Medical Image Watermarking Technique with Enhanced Security and High Payload Embedding". In this article, a new fragile, blind, high payload capacity, ROI (Region of Interest) preserving Medical image watermarking (MIW) technique in the spatial domain for gray-scale medical images is proposed [6]. Article presents a watermarking scheme that combines lossless data compression and encryption technique in application to medical images.

N. V. Dharwadkar [7] presented a reversible (distortion free), fragile, spatial domain watermarking scheme for medical images. The proposed scheme uses the second mode of operation which extracts the watermark from the unaltered pixel components of image. The scheme is robust to different types of attacks. The fragility and robustness of the scheme is analyzed considering different types of image processing attacks.

In the year 2010, R.Velumani [8] presented a reversible blind watermarking scheme to watermark a medical image with the patient's photograph in an invisible manner such that it is available to the respective physician only on extraction with a key.

B. W. T. Agung [9] performed a work, "Medical Image Watermarking with Tamper Detection and Recovery Using Reversible Watermarking with LSB Modification

and Run Length Encoding (RLE) Compression". This paper will study and test a watermarking scheme using LSB Modification to perform tamper detection and recovery in the ROI. To make this watermarking scheme reversible, RLE is used to embed the original LSBs in the RONI to get higher embedding capacity. As the embedding capacity is high but there are some security related problems.

Y. Liu [10], proposed a robust watermarking algorithm for medical image authentication and protection. The scheme obtains the visual feature vectors of the medical image using DWT-DCT. The watermarking image is encrypted by Logistic Map to strengthen its security. By using the DWT-DCT concept, more security is achieved but there are some problems related to the performance.

Prabakaran proposed a viable steganography technique using Integer Wavelet Transform (IWT) [11] to protect the MRI medical image into a single container image. The container image was taken and flip left was applied and the dummy container image was obtained. It is observed that the quality parameters are improved with acceptable PSNR compared to the existing algorithms.

All the above cited techniques that have been reviewed have some problems related to security; performance etc. so to overcome these problems we have proposed a new technique that provides more security; better performance relative to the above cited techniques.

III. METHODOLOGY

A. Pre-processing

First of all the medical image is loaded. The loaded medical image is DICOM. DICOM [10] images define the format for medical images that can be exchanged with the data and quality necessary for the clinic use. Image Enhancement is done on loaded medical image. And then, subtraction is applied by subtracting the original image from the negative image for the separation of ROI and RONI. Original image is the loaded medical image. Negative image is obtained by subtracting the medical image from 255. After that, thresholding is done to find the high intensity areas where we want to hide the data. High intensity areas can be found by assigning the min and max weight. We will hide the encrypted data in the high intensity areas. To hide the encrypted data in the high intensity areas make the informational part secure.

B. Watermark Encryption

To provide secure watermarking first of all the watermark is encrypted by RSA [3]. The purpose of using RSA is that it is more secure, easy to understand, easy to implement and modify. Two types of keys are used in RSA [14]: First key is public for encryption and second key is private for decryption. RSA is a secure encryption technique as it uses the concept of private key for decrypting the encrypted data.
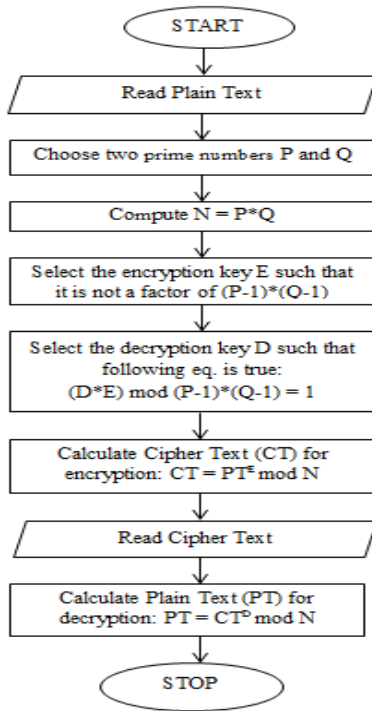
Fig. 1: Steps for using RSA

Algorithm for Encryption:

Step 1: Firstly choose two large prime numbers. Let the prime numbers be P and Q. The prime are the numbers that are divisible by 1 and itself.

Step 2: Then, N is computed by N=P*Q.

Step 3: Choose the encryption key E which is public key such that it is not a factor of (P-1)*(Q-1). RSA algorithm uses two keys. For encryption public key is used.

Step 4: Calculate the Cipher Text (CT) from Plain Text (PT) such that $CT = PT^E \bmod N$.

Encryption is done by using the public key.

Algorithm for Decryption:

Step 1: For decryption choose the decryption key D which is private key such that the following equation is true:

$$(D*E) \bmod (P-1)*(Q-1) = 1 \qquad (1)$$

Step 2: Calculate the Plain Text (PT) from Cipher Text (CT) such that $PT = CT^D \bmod N$.

And decryption will be done using the private key.

C.   DWT (Discrete Wavelet Transform)

The frequency domain transform that we have applied in our paper is Haar DWT. There are two operations for 2D Haar DWT: One is the horizontal and other is the vertical [10]. There are two operations related to these operations:

Step 1: First of all pixels are scanned from left to right in horizontal direction. Then, the addition and subtraction operations are performed on the neighboring pixels. The sum is stored on the left and difference is stored on the right as shown in Fig. 2 Repeat this operation until all the rows are processed. The sum of the pixels represents the low (L) frequency part while difference represents the high (H) frequency part of the original image.
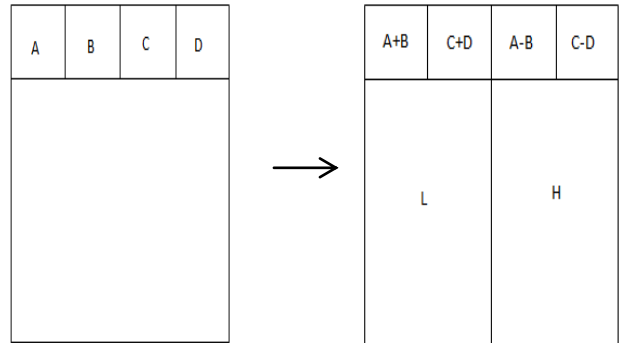

Fig. 2: Horizontal Operation

As the pixels are divided into low and high frequency part then next task is to divide them into LL, LH, HL, HH sub-bands such that we can hide the information in only high frequency parts.

Step 2: Secondly, the pixels are scanned from top to bottom in vertical direction. Then, the addition and subtraction operations are performed on the neighboring pixels. The sum is stored on the top and difference is stored on the bottom as shown in Fig 4. Repeat these operations until all columns are processed. Finally we obtain 4 sub-bands named as LL, HL, LH and HH. The LL sub-band is the low frequency sub-band which looks like similar to the original image. The Fig. 3 shows division of pixels into 4 sub-bands.
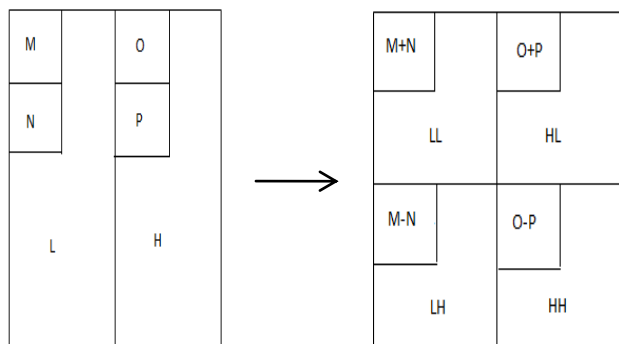

Fig. 3: Vertical Operation

Steps for Watermark Embedding using DWT: There are some steps to be followed for embedding the watermark using DWT [15] and that are presented in Fig. 4. Inverse DWT is used to round off the values. Pseudo number is generated to modify the detailed coefficients like horizontal and vertical coefficients of wavelet decomposition by adding Pn when message bit = 0.

Read Cover Image (Ic)

↓

Calculate size of Ic

↓

Read the secret message m

↓

Prepare m as message vector

↓

Decompose Ic by Haar DWT

↓

Generate pseudo-random number (Pn)

↓

Modify the coefficients of decomposition by adding Pn when message bit = 0.

↓

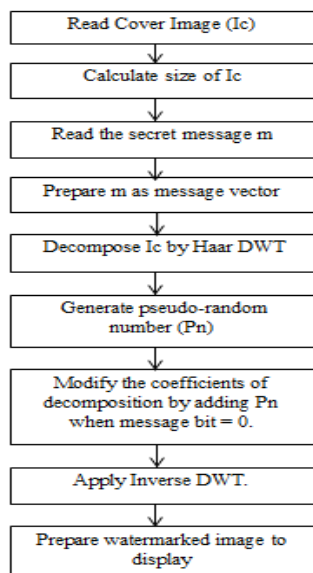Apply Inverse DWT.

↓

Prepare watermarked image to display

Fig. 4: Watermark Embedding using DWT

Steps for Watermark Extraction using DWT: There are some steps to be followed for extracting the watermark using DWT and that are as follows:

Read Cover Image (Ic)

↓

Read the watermarked image (Is)

↓

Decompose Ic and Is by Haar DWT

↓

Generate message vector of all ones

↓

Find correlation b/w modified and original coefficients

↓

Turn the message vector bit to 0 if the correlation value is greater than mean correlation value

↓

Prepare message vector to display secret message
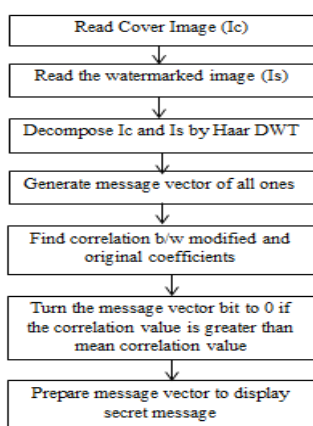
Fig. 5: Watermark Extraction using DWT

The correlation between the modified and original coefficients is found and then message vector bit is turned to 0 if the correlation value is greater than mean correlation value.

IV. PROPOSED ALGORITHM

The proposed algorithm is to design a RONI medical image watermarking by using RSA and DWT. It provides a two-way security by encrypting the watermark and then applying DWT. First of all medical image is loaded. Then image enhancement will be done. After that subtraction and thresholding will be applied to separate ROI and NROI and to find the high intensity areas. The watermark is encrypted and then embedded using DWT and then recovery will be performed.

A. *Algorithm for Watermark Embedding* (CImage, himage) /*

CImage is the cover dicom image and himage is the object that is to hide in cover image*/

Step 1: Load the medical image and perform image enhancement on it. Image enhancement is done by using function histogram equalization.

Step 2: Separate the Background and foreground by performing area subtraction.

Step 3: Identify High intensity foreground area as ROI cover area.

Step 4: himage = RSAEncode(himage). Encryption of the secret message is done using RSA.

Step 5: Cover image is analysed under min-max intensity analysis approach.

Step 6: Analyse the image pixels based on weighted values respective to global best and local best intensities.

Step 7: Shift the pixels in global best or local best areas based on intensity analysis.

Step 8: Identify high intensity gbest area as the main cover ROI.

Step 9: For i=1 to length (himage) [Read the hide image data to perform data hiding in cover ROI].

Step 10: Perform Block wise Wavelet Decomposition over the image.

Step 11: Use the diagonal coefficient vector to take the decision about data storage.

Step 12: Identify High Intensity Diagonal coefficient Area to store 0.

Step 13: Identify Low Intensity Diagonal coefficient Area to store 1.

Step 14: Perform Inverse Wavelet Decomposition over Image and EImage is generated.

Step 15: Return EImage.

B. *Algorithm for Watermark Extraction* (EImage, himage) /*

EImage is the Embedded dicom image and himage is the object that is to hide in cover image*/

Step 1: Analyse the Eimage under min-max intensity analysis approach.

Step 2: Analyse the image pixels based on weighted values respective to global best and local best intensities.

Step 3: Shift the pixels in global best or local best areas based on intensity analysis.

Step 4: Identify High intensity gbest area as the main cover ROI

Step 5: For i=1 to length (himage). [Read the hide image data to perform data hiding in cover ROI].

Step 6: Perform Block wise Wavelet Decomposition over the image.

Step 7: Identify diagonal coefficient vector to take the decision about hidden info area.

Step 8: If high intensity area found extract 0 and store in simage.

Step 9: If low intensity area found Extract 1 and store in simage.

Step 10: Perform Inserve Wavelet Decomposition over Image

Step 11: simage=RSADec(simage). [Decode the hide object using RSA cryptography]
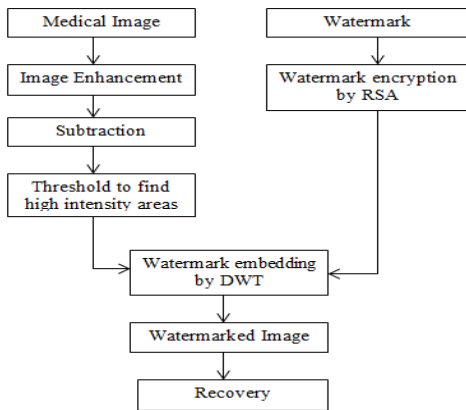
Step 12: Return simage.

Fig. 6: Block diagram of Proposed Algorithm

V. EXPERIMENTAL RESULTS

The performance of the proposed method can be evaluated by using Matlab R2010a and 7.10 versions. In our experiment we have tested 15 medical images (512 X 512). Let us take one example in which we have one medical image 1.jpeg, the watermark to be hidden is encrypted by RSA. The watermarked image is attacked and recovered.
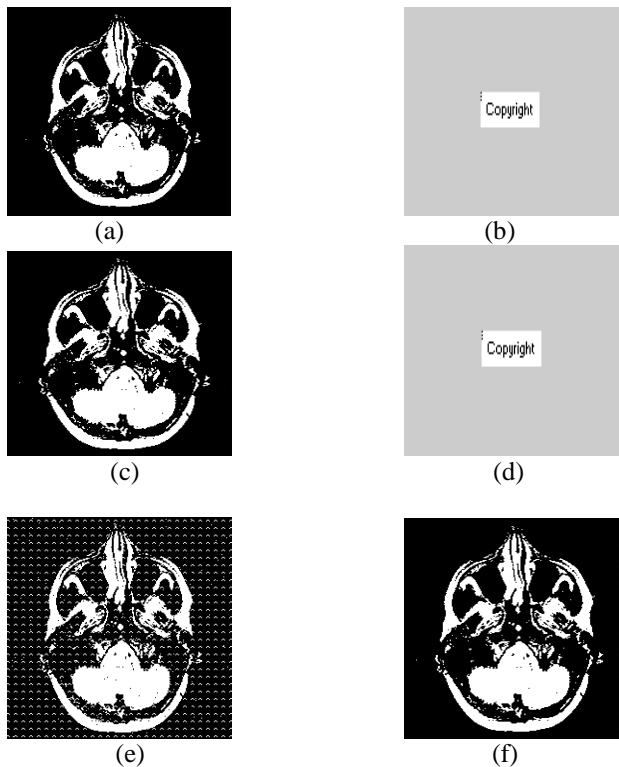

Fig. 7: shows (a) MRI image taken as cover image (b)Watermark we have used, (c) Watermark is encrypted and embedded using DWT resulted as watermarked image, (d) recovered watermark from watermarked image, (e) Salt and Pepper Noise attack on image, (f) Image recovered from attack.

Similarly as above example various images have been tested and analysed.

A. Statistical Analysis

The experimental results that we have obtained are subjected to various statistical techniques to evaluate the performance. The parameters used are as:

MSE: Mean Square Error (MSE) is defined as mean squared distance between the cover image and the watermarked image.

$$MSE = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} (aij - bij)^2 \qquad (2)$$

Aij means the pixel value at position (i, j) in the cover image and bij means the pixel at same position in the corresponding watermarked image.

PSNR: The quality of the image can be determined by PSNR value (Peak Signal to Noise Ratio).

$$PSNR = 10 \ \log_{10} \frac{255^2}{MSE} \qquad (3)$$

Higher the PSNR value higher will be the quality of the image.

BCR: The correlation between the embedded and extracted watermarks measured by Bit Correct Rate (BCR).

$$BCR = 1 - \frac{1}{M_W \times N_W} \sum_{i=1}^{M_W} \sum_{j=1}^{N_W} [W(i,j) \oplus W'(i,j)] \qquad (4)$$

Where W and W' are embedded and extracted watermarks respectively, with size of $M_W \times N_W$ and $\oplus$ denotes the exclusive- or (XOR) operation. The larger value of BCR is gives the better result.

NCC: Normalized Cross Correlation (NCC) used as a measure for calculating the degree of similarity between two images [11].

$$NCC = \sum_{j=1}^{M} \sum_{k=1}^{N} (X_{j,k} - X'_{j,k}) \frac{1}{\sum_{j=1}^{M} \sum_{k=1}^{N} (X_{j,k})^2} \qquad (5)$$

Thus NCC is used as a similarity measure to measure the degree of similarity. Higher the value of NCC gives better result.

SR: A Comparison between extracted watermark and original watermark can be done by computing the Similarity Ratio (SR) between the two patterns as defined in equation 5 which is the metric used for identifying robustness of the watermarking process[12].

$$SR = \frac{S}{S+D} \qquad (6)$$

Where 'S' denotes number of matching pixels and 'D' denotes number of different pixel values.

SSIM: SSIM is ideal for testing for similarities in medical images because it focuses on local rather than global image similarity. SSIM performs a luminance comparison (LC), contrast comparison (CC), and structure comparison (SC) between two image regions. The structural similarity of two images regions R_x and R_y which are on images x and y respectively, is given by

$$SSIM(R_x, R_y) = LC(R_x, R_y)^\alpha . CC(R_x, R_y)^\beta . SC(R_x, R_y)^\gamma$$
(7)

Where $\alpha, \beta, \gamma, \geq 1$ and are used to weight the importance of each of the three components. In the perceptual model used in the experiments presented in this article, each of the three SSIM components was weighted equally i.e. $\alpha = \beta = \gamma = 1$. SSIM values > 0.95 are typically regarded as visually imperceptible for the parameter choices indicated.

B. Results and Discussions

Table 1: Comparison of Existing and Proposed Scheme without Attack

Technique	Image	MSE	PSNR	BCR	NCC	SR	SSIM
IWT with AT[11]	1.jpeg	1.89	45.35	5.44	1.05	0.78	0.96
	2.jpeg	1.78	45.60	5.42	1.02	0.81	0.97
	3.jpeg	1.18	47.32	5.68	1.07	0.76	0.96
	4.jepg	1.23	48.81	5.23	1.06	0.65	0.98
DWT with RST(Our Scheme)	1.jpeg	1.02	48.04	5.82	1.09	0.97	0.99
	2.jpeg	0.85	48.82	5.84	1.07	0.86	0.99
	3.jpeg	1.14	47.56	5.88	1.09	0.94	0.98
	4.jpeg	0.74	50.48	6.34	1.08	0.89	0.99

Four watermarked medical images are taken (1.jpeg, 2.jpeg, 3.jpeg, 4.jpeg). The performance of the proposed algorithm (DWT with RST) and existing algorithm (IWT with AT) is evaluated and compared by using parameters like MSE, PSNR, BCR, NCC, SR and SSIM as shown in Table I. The graphical representation of results is shown as:
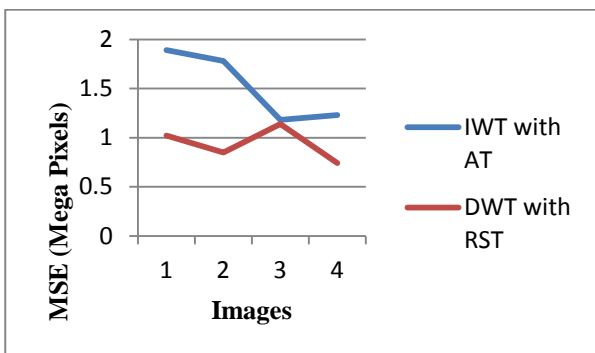
Fig. 8: Comparison according to MSE value of 4 images

Fig. 8 shows the comparison of proposed and existing algorithm according to MSE values of 4 images. It is observed that MSE values of proposed algorithm (DWT with RST) is less than the existing algorithm (IWT with AT). Lesser the value of MSE gives better result.
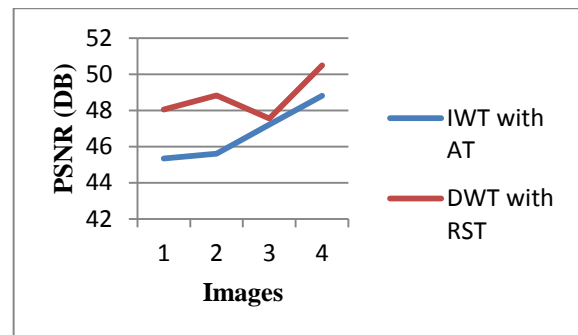

Fig. 9: Comparison according to PSNR value of 4 images

It is observed that PSNR values of proposed algorithm (DWT with RST) is more than the existing algorithm (IWT with AT). More the value of PSNR gives better result. Fig. 9 shows the comparison of proposed and existing algorithm according to PSNR values of 4 images.
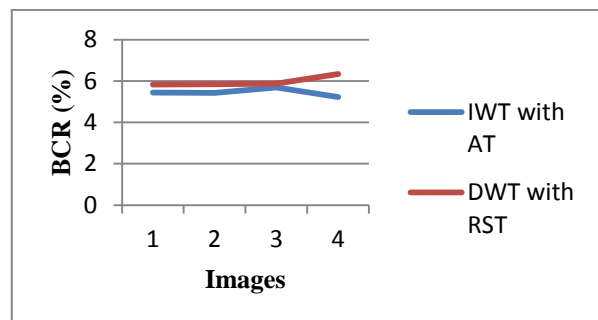

Fig. 10: Comparison according to BCR value of 4 images

Fig. 10 shows the comparison of proposed and existing algorithm according to BCR values of 4 images. It is observed that BCR values of proposed algorithm (DWT with RST) is more than the existing algorithm (IWT with AT). More the value of BCR gives better result.
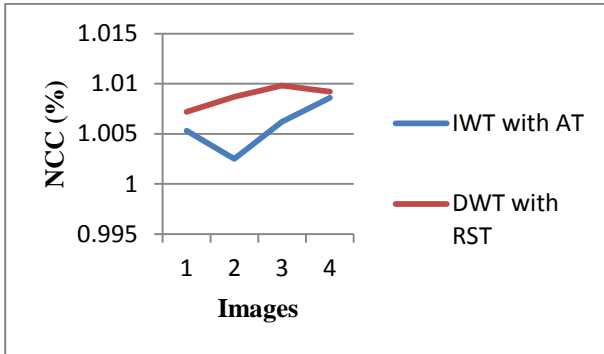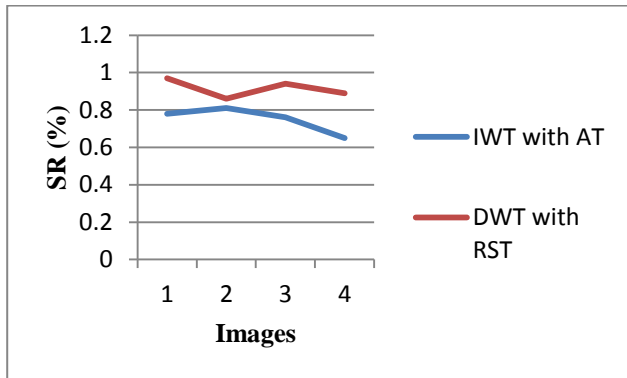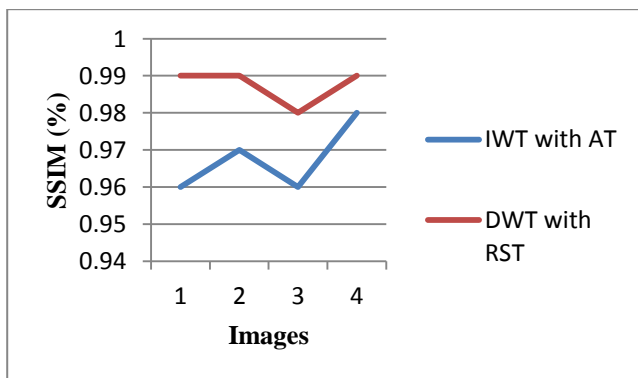

Fig. 11: Comparison according to NCC value of 4 images

It is observed that NCC values of proposed algorithm (DWT with RST) is more than the existing algorithm (IWT with AT). More the value of NCC gives better result. Fig. 11 shows the comparison of proposed and existing algorithm according to NCC values of 4 images.

Fig. 12: Comparison according to SR value of 4 images

Fig. 12 shows the comparison of proposed and existing algorithm according to SR values of 4 images. It is observed that SR values of proposed algorithm (DWT with RST) is more than the existing algorithm (IWT with AT). More the value of SR gives better result.

Fig. 13: Comparison according to NCC value of 4 images

It is observed that SSIM values of proposed algorithm (DWT with RST) is more than the existing algorithm (IWT with AT). More the value of SSIM gives better result. Fig. 13 shows the comparison of proposed and existing algorithm according to SSIM values of 4 images.

From the above analysis it is perceived that the proposed technique (DWT with RST) is better than existing technique (IWT with AT) in all parameters MSE, PSNR, BCR, NCC, SR, SSIM. The proposed technique is an improvement over existing technique.

The watermarked image is subjected to distortions like salt and pepper noise, Gaussian noise attack, image adjustment, scaling, rotation. Median filtering and linear filtering has been applied on the watermarked image. The imperceptibility and robustness of watermark has been evaluated and the assessment of the parameters (PSNR, BCR, NCC, SR, SSIM) under the different attacks has been shown in the Tables below.

Table 2: Assessment of PSNR under Different Attacks

Attacks		PSNR	
		IWT with AT [11]	DWT with RST (proposed)
Adding Gaussian Noise Attack (mean, variance)	0.01, 0	44.50	48.32
	0.001	42.52	45.60
Adding Salt and Pepper Noise	0.002	41.23	43.54
Median Filtering	3X3	35.26	37.45
Liner Filtering	3X3	33.45	35.68
Image Adjustment		22.34	25.67
Scaling		51.23	56.67
Rotation	5 degree	18.94	19.23
	10 degree	19.56	19.98

Table 3: Assessment of BCR under Different Attacks

Attacks		BCR	
		IWT with AT [11]	DWT with RST (proposed)
Adding Gaussian Noise Attack (mean, variance)	0.01, 0	5.42	5.84
	0.001	5.32	5.67
Adding Salt and Pepper Noise	0.002	5.10	5.21
Median Filtering	3X3	4.23	4.35
Liner Filtering	3X3	4.16	4.20
Image Adjustment		5.13	5.39
Scaling		5.23	5.67
Rotation	5 degree	4.10	4.56
	10 degree	4.02	4.09

Table 4: Assessment of NCC under Different Attacks

Attacks		NCC	
		IWT with AT [11]	DWT with RST (proposed)
Adding Gaussian Noise Attack (mean, variance)	0.01, 0	1.05	1.07
	0.001	1.03	1.06
Adding Salt and Pepper Noise	0.002	1.02	1.03
Median Filtering	3X3	1.03	1.04
Liner Filtering	3X3	1.05	1.07
Image Adjustment		1.02	1.04
Scaling		1.03	1.06
Rotation	5 degree	1.01	1.3
	10 degree	1.00	1.01

Table 6: Assessment of SSIM under Different Attacks

Attacks		SSIM	
		IWT with AT [11]	DWT with RST (proposed)
Adding Gaussian Noise Attack (mean, variance)	0.01, 0	0.98	0.99
	0.001	0.97	0.99
Adding Salt and Pepper Noise	0.002	0.92	0.94
Median Filtering	3X3	0.94	0.98
Liner Filtering	3X3	0.91	0.93
Image Adjustment		0.89	0.90
Scaling		0.95	0.98
Rotation	5 degree	0.86	0.89
	10 degree	0.82	0.85

For the assessment of parameters, the watermarked medical image is subjected to Gaussian noise attack with mean and variance of 0.01,0 and 0.001. Salt and Pepper noise attack is added with density of 0.002. Watermarked image is smoothed with 3X3 median filter. Rotation is performed with 5 degree and 10 degree. Scaling and image adjustment attack is also applied on the watermarked image to perceive the chances of recovery of attacked image. The imperceptibility of the proposed scheme is evaluated by the assessment of PSNR under different attacks. The robustness of the proposed work is evaluated with the help of SR, SSIM. The correlation between the embedded and the extracted watermark is evaluated by the assessment of the BCR and NCC. All the results show that the proposed method is more robust, more imperceptible and more secure than the existing scheme.

Table 5: Assessment of SR under Different Attacks

Attacks		SR	
		IWT with AT [11]	DWT with RST (proposed)
Adding Gaussian Noise Attack (mean, variance)	0.01, 0	0.81	0.92
	0.001	0.76	0.93
Adding Salt and Pepper Noise	0.002	0.71	0.76
Median Filtering	3X3	0.64	0.69
Liner Filtering	3X3	0.69	0.71
Image Adjustment		0.71	0.79
Scaling		0.82	0.88
Rotation	5 degree	0.52	0.59
	10 degree	0.50	0.54

VI. Conclusion And Future Work

We have presented a reliable watermarking scheme applied to medical images with good imperceptibility, high PSNR and enhanced security. Our scheme can be used for different medical image modalities. The experimental results indicate that the proposed scheme is feasible and given its relative simplicity, it can be applied to the medical images at the time of acquisition to serve in many medical applications concerned with privacy protection, safety and management. The result shows that our proposed technique is an improvement over the existing technique in terms of image quality, security and imperceptibility. In our work we have used images of 512 X 512 resolutions. In future the algorithm can be applied on the high resolution images with better quality.

Acknowlegement

The authors would like to thank the anonymous reviewers for their careful reading for this article and for their helpful comments.

References

[1] H. K. Lee, "ROI Medical Image Watermarking Using DWT and Bit-plane", in proceedings of IEEE Asia-Pacific Conference on Communications, Perth, Western Australia, vol. 16, pp. 512-515, 2005.

[2] B. M. Planitz, "A Study of Block-based Medical Image Watermarking Using a Perceptual Similarity Metric", in proceedings of IEEE Digital Imaging Computing Techniques and Applications (DICTA), vol. 13, pp.600-612, 2005.

[3] A. K. Navas, M. Sasikumar and S. Sreevidya "A Benchmark for Medical Image Watermarking", in proceedings of International Conference on Image Processing, vol. 33, pp. 237-240, 2007 .

[4] N. A. Memon and S.A.M. Gilani, "Multiple Watermarking of Medical Images for Content

Authentication and Recovery", in proceedings of World Academy of Science, Engineering and Technology, vol. 38, pp. 347-350, 2009.

[5] S. C. Liew and J. Mohamad, "Reversible Medical Image Watermarking For Tamper Detection and Recovery", Computerized Medical Imaging and Graphics, vol. 27, pp. 185-196, 2010.

[6] M. K. Kundu and S. Das, "Lossless ROI Medical Image Watermarking Technique with Enhanced Security and High Payload Embedding", in proceedings of IEEE International Conference on Pattern Recognition, vol. 38, pp. 1457-1460, 2010.

[7] N. V. Dharwadkar and B. B. Amberker, " Reversible Fragile Medical Image Watermarking with Zero Distortion", in proceedings of IEEE International Conference on Computer & Communication Technology, vol. 21, pp. 248-254, 2010.

[8] B. W. T. Agung and F. P. Permana, "Medical Image Watermarking with Tamper Detection and Recovery Using Reversible Watermarking with LSB Modification and Run Length Encoding (RLE) Compression", in proceedings of28th IEEE Annual International Conference, New York, USA, vol. 30 pp. 3270-3273, 2010.

[9] C. Dhong and L. Jingbing, "The Watermarking Medical Image Algorithm with Encryption by DCT and Logistic" in proceedings of9thWeb Information Systems and Applications Conference, vol. 6072, San Jose, CA, pp. 1-13, 2012.

[10] L. Yaoli and L. Jingbing, "The Medical Image Watermarking Algorithm Using DWT-DCT and Logistic", in proceedings of9thIEEE Web Information Systems and Applications Conference, vol. 30, pp. 119-124, 2012.

[11] G. Prabakaran and R. Bhavani, "Multi Secure and Robustness for Medical Image Based Steganography Scheme", in proceedings of IEEE International Conference on Circuits, Power and Computing Technologies, vol.28, pp. 947-951, 2013.

[12] Hongmei Liu, JunhuiRao, and Xinzhi Yao, "Feature Based Watermarking Scheme for Image Authentication", IEEE, pp.229-232, 2008.

[13] J. Dittmann, "Content-fragile Watermarking for Image Authentication", Proc. of SPIE, Security and Watermarking of Multimedia Contents III, vol. 4314, pp. 175-184, 2001.

[14] Kil-Sang Yoo, Mi-Ae Kim, and Won-Hyung Lee "A Robust image watermarking technique for JPEG images using quadtrees", Lecture Notes in Computer Science, Vol. 3332, pp. 34-41, 2004.

[15] Thai DuyHien Zensho Nakao, and Yen-Wei Chen, "Robust Multi-logo watermarking by RDWT and ICA", Signal Processing, Elsevier, Vol. 86, pp. 2981-2993, 2006.

Authors' Profiles

Neha Solanki was born in Sonepat (Haryana), India, received Bachelor's Degree in Information Technology from M.D. University, Rohtak, Haryana in 2012 and Master's Degree in Computer Science and Engineering from Deenbandhu Chhotu Ram University of Science and Technology, Murthal, Sonepat, Haryana in 2014. Her research interests are Image processing and Information security.

Sanjay Kumar Malik obtained the B.E degree in Computer Science and Engineering from Vaish College of Engineering, Rohtak, Haryana, India in 1999 and M.Tech degree in Computer Science and Engineering from JanardanRai Nagar Rajasthan Vidyapeeth University, Udaipur, Rajasthan, India in 2005. Ph.D. degree in Computer Science and Engineering from Deenbandhu Chhotu Ram University of Science and Technology, Murthal (Sonepat), Haryana, India in the area of Wireless Sensor Networks. He is presently working as Assistant Professor in Department of Computer science and Engineering at Hindu College of Engineering, Sonepat with more than 14 years' experience of academic and administrative affairs.