RONI Medical Image Watermarking using DWT and RSA

Neha Solanki
PG Student
Hindu College of Engineering
Sonepat, Haryana, India

Sanjay Kumar Malik
Faculty
Hindu College of Engineering
Sonepat, Haryana, India

Sonam Chhikara
Dept. of Computer Science
DCRUST Murthal
Sonepat, Haryana, India

ABSTRACT
In this paper, the proposed work is about to store the patient information in the medical image itself that can be a CT scan or the MRI image. Medical records are extremely sensitive patient information and require uncompromising security during both storage and transmission. In the traditional way, the patient information and patient test reports are kept in different tables or databases or locations. But, this kind of data management can have some human oriented errors such as transfer of wrong report to a patient. Errors can be prevented by hiding the data in scan report itself. It will improve the reliability of the medical information system. In our paper the work is divided in two main stages, first to identify the ROI and RONI of the image. Here, the ROI is defined in terms of information part of medical image and RONI is defined in terms of non-information part of the MRI image. It will avoid the user to destroy the valuable information from the image. Watermark is encrypted by using RSA. The second stage is about to hide the image in RONI. A DWT based approach is used to hide such information.

General Terms
To provide a two-way security to the medical images by using DWT and RSA along with the preservation of ROI.

Keywords
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).

1. INTRODUCTION
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 los t 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.

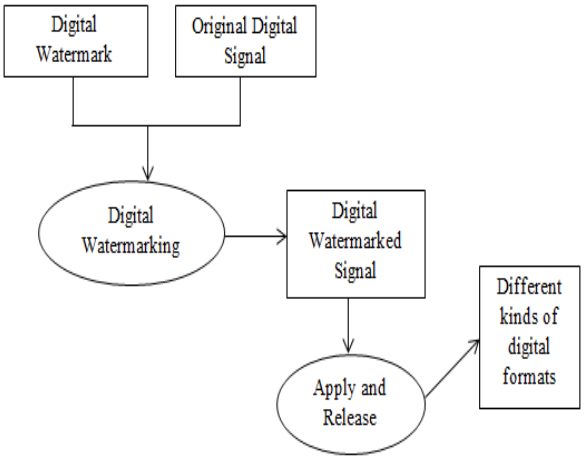


Fig. 1: Watermarking process

The watermark has been embedded into the medical image to provide more authenticity and integrity. Then RONI and ROI [11] 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 is in section VI and References is in section VII.

2. LITERATURE REVIEW
The exchange of database between hospitals requires efficient transmission and storage. Various approaches have been proposed for the purpose of securing the medical information using watermarking.
In 2005, H.K. Lee et al., [1] proposed a digital watermarking technique for medical image that prevents illegal forgery that

can be caused after transmitting medical image data remotely. Author embed the watermark into some area of medical image, except the decision area that makes a diagnosis so called region of interest (ROI) area in Presented paper, to increase invisibility.

M. Kallel et al., [2] performed a work in 2006 that presents a multiple watermarking application in spatial domain to preserve the historic of the medical image by embedding medical diagnosis. This paper provides an overview of watermarking application and Author present the used watermarking insertion domains.

N. A. Memon et al., [4] in 2009 proposed a multiple watermarking method. The scheme embeds robust watermark in region of non interest (RONI) for achieving security and confidentiality. 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.

Siau-Chuin Liew and J. M. Zain [5] discussed the usage of watermarking for medical images in 2010 to ensure the authenticity and integrity of the image and reviewed some watermarking schemes that had been developed. Watermark embedded can be used to detect tampering and recovery of the image can be done. The watermark is also reversible.

Nagaraj V. Dharwadkar and B. B. Amberker [7] performed a work that presents a reversible (distortion free), fragile, spatial domain watermarking scheme for medical images in 2010. 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.

T. Agung et al., [8] in 2012 performed a work that 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.

Prabakaran G et al., [11] proposed a viable steganography technique in 2013 using Integer Wavelet Transform (IWT) 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. lt 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.

3. METHODOLOGY

3.1 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 data in the high intensity areas.

3.2 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: First key is public for encryption and second key is private for decryption.

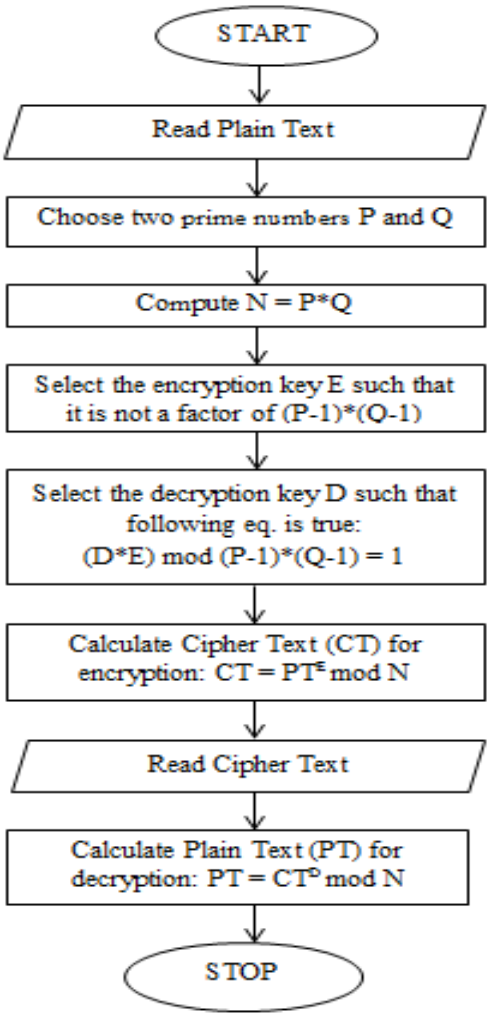


Fig. 2: Steps for using RSA

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) mod (P-1)*(Q-1) = 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.

3.3 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. 3 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.

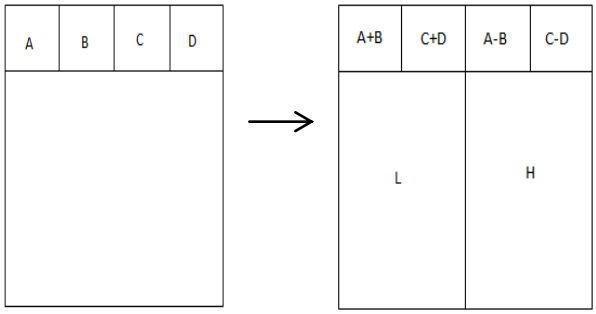


Fig. 3: Horizontal operation

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. 4 shows division of pixels into 4 sub-bands.

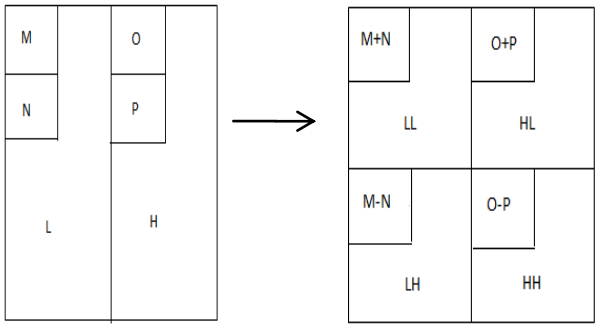


Fig. 4: Vertical operation

Steps for Watermark Embedding using DWT: There are some steps to be followed for embedding the watermark using DWT and that are presented in Fig. 5.

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.

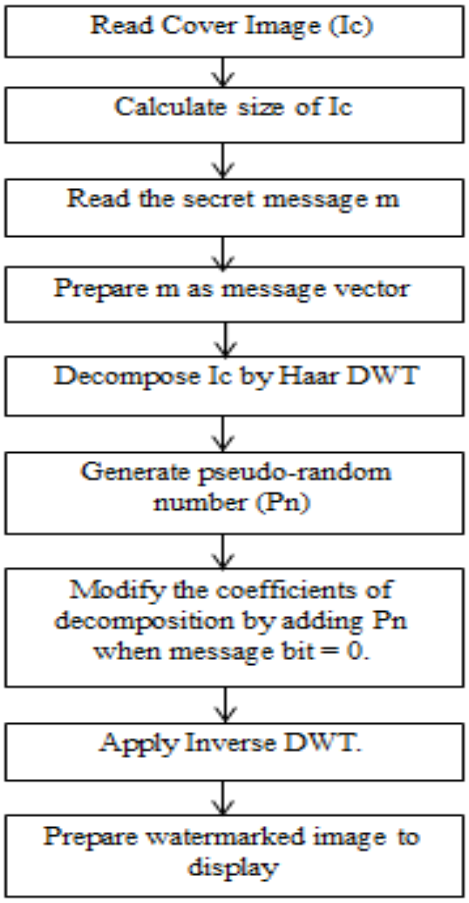


Fig. 5: Watermark Embedding using DWT

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

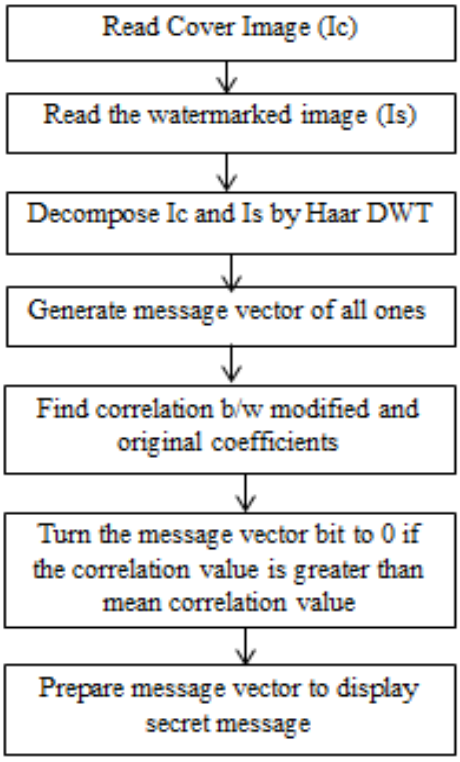


Fig. 6: Watermark Extraction using DWT

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.

4. 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.

4.1 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.

4.2 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.

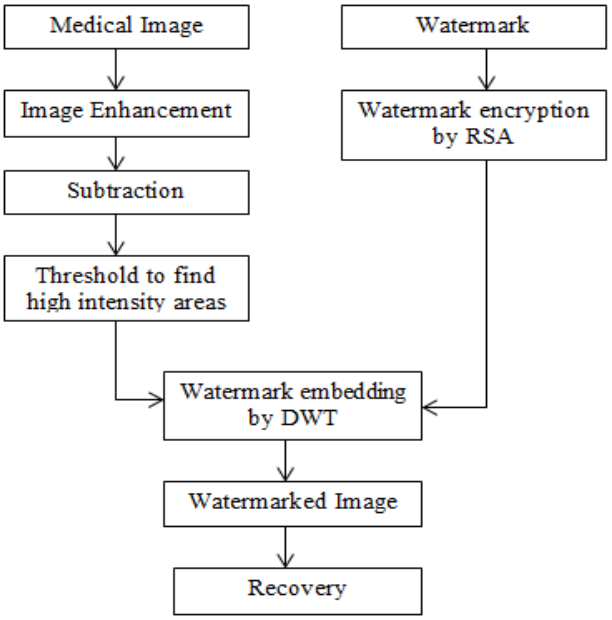
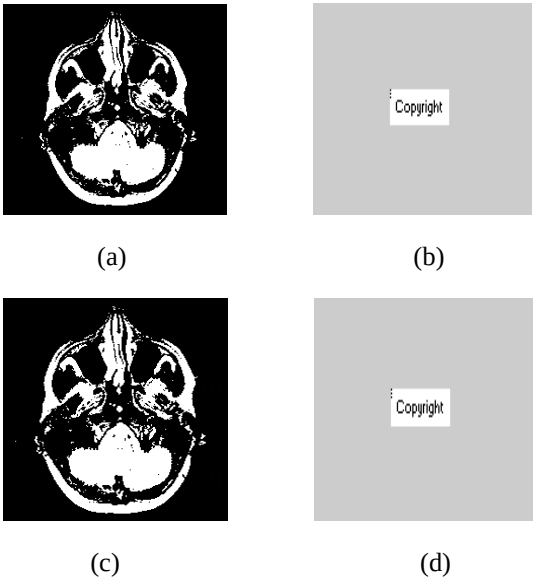


Fig. 7: Block diagram of Proposed Algorithm

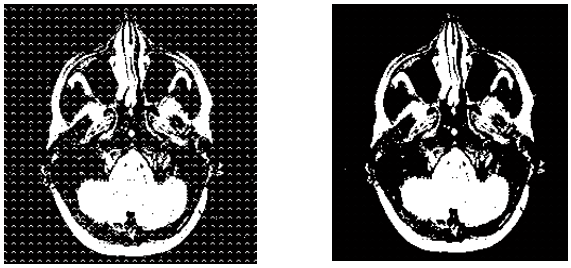
5. EXPERIMENTAL RESULTS

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.



(a) (b)

(c) (d)



(e) (f)

Fig. 8: 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.

5.1 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.

$$\text{MSE} = \frac{1}{\text{M X N}} \sum_{i=1}^{M} \sum_{j=1}^{N} (aij - bij)^2 \quad \ldots (1)$$

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).

$$\text{PSNR} = 10 \log_{10} \frac{255^2}{\text{MSE}} \quad \ldots (2)$$

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).

$$\text{BCR} = 1 - \frac{1}{M_W \text{ X } N_W} \sum_{i=1}^{M_W} \sum_{j=1}^{N_W} [W(i,j) \oplus W'(i,j)] \quad \ldots (3)$$

where W and W′ are embedded and extracted watermarks respectively, with size of M_W X 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].

$$\text{NCC} = \sum_{j=1}^{M} \sum_{k=1}^{N} (X_{j,k} - X'_{j,k}) \frac{1}{\sum_{j=1}^{M} \sum_{k=1}^{N} (X_{j,k})^2} \quad \ldots (4)$$

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

5.2 Results and Discussions

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 and NCC

Table I: Comparison of Existing and Proposed Scheme

Techniques	Images	MSE	PSNR	BCR	NCC
IWT with AT[11]	1.jpeg	1.89	45.35	5.44	1.0053
	2.jpeg	1.78	45.60	5.42	1.0025
	3.jpeg	1.18	47.22	5.68	1.0091
	4.jpeg	1.23	48.81	5.23	1.0086
DWT with RST (Our Scheme)	1.jpeg	1.02	48.04	5.82	1.0072
	2.jpeg	0.85	48.82	5.84	1.0080
	3.jpeg	1.14	47.56	5.88	1.0035
	4.jpeg	0.74	50.48	6.34	1.0092

We have taken 4 medical images and calculated the value of parameters.

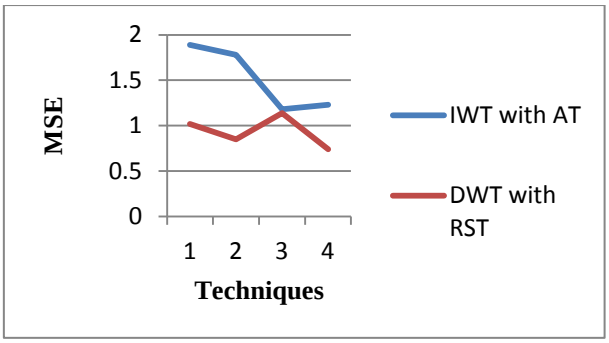


Fig. 9: Comparison according to MSE value of 4 images

Fig. 9 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.

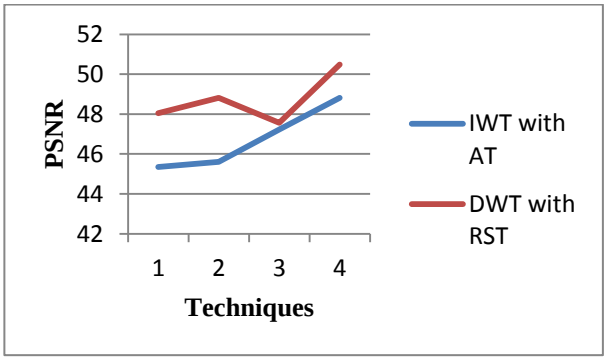


Fig. 10: Comparison according to PSNR value of 4 images

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. 10 shows the comparison of proposed and existing algorithm according to PSNR values of 4 images.

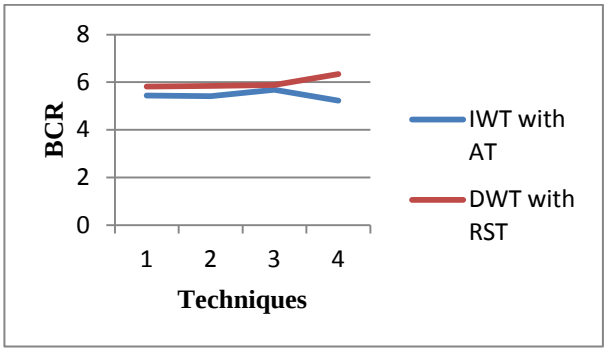


Fig. 11: Comparison according to BCR value of 4 images

Fig. 11 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.

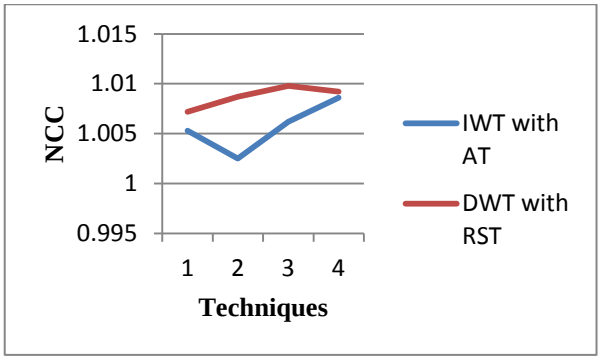


Fig. 12: Comparison according to NCC value of 4 images

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. 12 shows the comparison of proposed and existing algorithm according to NCC 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. The proposed technique is an improvement over existing technique.

6. CONCLUSION

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 image we have used is 512X512 resolutions. In future algorithm can be improved so that it can be applied to the high resolution images with better quality.

7. 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, 2003, vol. 27, pp. l85-196, 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 of.

28th Annual International Conference of the IEEE, 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 of Ninth Web 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 of IEEE Ninth 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 2013 IEEE International Conference on Circuits, Power and Computing Technologies, vol.28, pp. 947-951, 2013.