

An Enhanced Digital Image Watermarking Scheme for Medical Images using Neural Network, DWT and RSA

¹**Sujata Nagpal**

¹Chandigarh Engineering College, Landran, Mohali, 140307, India
Email: nagpalsujata@gmail.com

²**Shashi Bhushan and** ³**Manish Mahajan**

²Professor, Department of CSE, Chandigarh Engineering College, Landran, Mohali

³Associate Professor, Department of CSE, Chandigarh Engineering College, Landran, Mohali
Email: cecm.infotech.shashi@gmail.com, hod.coecse@cgce.edu.in

Abstract—Image watermarking is the process of the hiding the one image into other image for the copyright protection. The process of watermarking must be done in this way that the pixels of the original image must remain in its original HD form. A lot of work has been done in this context in previous years but some techniques have their own applications, drawbacks as well as advantages. So, this paper will utilize three techniques i.e. Discrete Wavelet Transform (DWT), Neural Network (NN) and RSA encryption for image watermarking. In the end the performance of the proposed technique will be measured on the basis of PSNR, MSE, BCR, BER and NCC in MATLAB R2010a environment.

Index Terms—Digital Image watermarking, DWT, Neural Network, Encryption, RSA.

I. INTRODUCTION

Digital form products like video, audio, text etc. are being transmitted in everyday of our lives [1, 2]. In the field of digital multimedia communication, some techniques has helped a lot for storing, editing and accessing of these products [3]. But, security during the transferring communication is very crucial. As lack of security leads to the loss in property rights. So to solve this problem, digital watermarking is very good [4]. Fig. 1 shows the progression of watermark embedding. Digital watermarking is the process of embedding an image with secret data for the communication. The embedded image can only be extracted by person who has authentication.

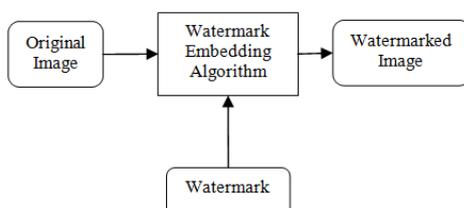


Fig.1. Watermark embedding process

Basically there are two methods for watermarking i.e. spatial and transform domain [5, 6]. Each technique has its own advantages as well as disadvantages. But the main advantage of transform domain method is that it is more robust, so in proposed work transform domain based method will be applied [7]. Fig. 2 shows the watermark extraction process.

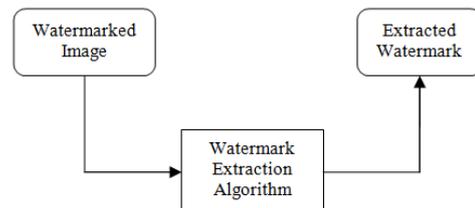


Fig.2. Watermark extraction process

There are two types of image watermarking, one is blind and the other one is non-blind. In blind image watermarking, there is no requirement of original content and it is also called as public image watermarking. In non-blind image watermarking, there is requirement of original content and it is also known as private image watermarking.

A. Medical Images

The amount of digital images in the internet has been increasing day by day. The need of secure diagnosis in the medical field is very necessary. As these days transmission of images has become common, so security is needed at high rate.

Medical images are used to view tissues, organs or body parts of a person. These images are used for disease diagnosis and treatment of the disease. Medical images play a major role in the classification of diseases. These are also helpful in monitoring disease activity. Several machines are accessible today that can generate images of internal organs of a person. There are different types of imaging methods such as x-ray, ultrasound, MRI scans, CT scans, Nuclear medicine scans etc [16]. Electromagnetic waves are also called x-rays. X-rays are

the common form of medical imaging. X-rays are passed through the body of a person to produce images of internal structure of body. X-rays are commonly used for checking swallowed objects, blood vessels, broken bones etc. Ultrasound is also known as medical sonography. Sound waves are used in this method to check internal organs. It is used in pregnancy or to check organs in abdomen and pelvis etc. MRI stands for Magnetic Resonance Imaging. Radio waves and magnetic field are used in this method so that organs and tissues of the body can viewed in much more detail. It is useful to check spinal injuries, abnormal tissues, blood vessels etc. CT scans are similar to X-rays but in this technique, multiple X-rays are projected from different angles to obtain a 3-D view of different organs. Medical images must be taken care of to confirm the identity as all diagnose depends on the obtained medical image. In order to fulfill the security and convenience issues of the patients watermarking is used in this field.

B. Noise and Distortions

Images are vulnerable to various types of noises. Noise is any degradation in the signal of an image. It is caused due to external disturbance during transmission of an image from one place to another. Different types of devices like network cable, satellites etc. can be used for transmission of image. There are different types of noise that can occur during transmission such as Gaussian, Poisson, Salt & Pepper etc.

In digital images, Gaussian noise can be aroused during attainment or communication. This noise is additive in temperament. Additive means that each pixel in the noised image is the addition of original pixel and some random value. Gaussian noise is the type of the noise in which PDF is equal to the normal distribution. Sometimes it is also known as the Gaussian distribution noise. The modified values of Gaussian distribution lead to this type of noise. The various sources of Gaussian noise are sensor noise, high temperature and electronic circuit noise. Poisson noise is also known as shot noise. It is a form of electronic noise which can be molded by a Poisson development. In this noise, diverse pixels of picture endure autonomous noise values. Salt & Pepper noise is also termed as impulse noise. In this, black and white dots are sprinkled on the pixels of the image. Pointed and abrupt changes in the signal of the image ground this type of noise. An effective noise reduction method for this type of noise is a median filter or a morphological filter. Speckle Noise is created when original pixel values of the image are multiplied by some arbitrary values. Speckle noise is the outcome of the patterns of constructive and destructive interference shown as bright and dark dots in the image. Localvar noise is the Zero-mean Gaussian white noise with intensity-dependent variance variables. It can be written as following using MATLAB:

$$K = \text{imnoise}(O, 'localvar', B) \quad (1)$$

It adds zero-mean, Gaussian white noise of local variance B to the image O . B is an array of the same size as O . Rotation attack is the most common attack that has been found these days in an image. The obtained image is rotated through several angles like 90 degree, 180 degree and 360 degree [8].

In this paper, a new method is proposed in which encrypted watermark is embedded in the medical image by using DWT and Neural Network approach. Section II describes previous work done in this field. Section III describes the techniques used in proposed work. Section IV describes the stimulation model. Results and comparisons are presented in section V. Finally, section VI describes conclusion and future scope [17].

II. RELATED WORKS

Digital watermarking is an outstanding field of research. A lot of researchers have proposed large number of algorithms in this field. The main purpose of all these algorithms is to provide imperceptibility and robustness against different attacks. Several types of watermarking techniques found in the academic literature are presented in this section.

Wang, B. et al. [9] proposed digital watermarking process based on the usage of DWT, DCT and SVD. From result evaluation it has been seen that the proposed algorithm has good rate of performance. It is more robust to all types of noises. Also the usage of the Arnold transform made the results better. Lai, C. et al. [10] proposed a hybrid method for image watermarking based on two methods i.e. Discrete Wavelet Transform (DWT) along with Singular Value Decomposition (SVD). In proposed work DWT will be used to decompose the image into 4 parts and then embedding will be done using SVD method. From the result analysis it has been concluded that proposed method worked well for all types of images. Jain, Y. et al. [11] proposed an improved method based on the SVM technique that will improve the rate of training. In addition to this usage of SVM is also very helpful as it is also invariant to various types of attacks. The experimental results reveal that the proposed algorithm can achieve the desired result and high stoutness to general image processing technique & geometric distortion.

Saxena, P. et al. [12] proposed a method for watermarking based on the usage of the SVD-DWT. The main advantage of this method is that it is robust to various types of attacks. In proposed work the watermark is embedded in high frequency band by SVD. Kaur, R. et al. [14] presented the new watermarking algorithm based on the usage of DWT-SVD techniques. In proposed work 4 sub-bands will be obtained using DWT and then watermarking will be done using Singular Value Decomposition method. From experiments it has been concluded that proposed method has better efficiency. Sridevi, T. et al. [15] proposed the watermarking method in which instead of taking an original image a reference

image has been taken. Then with the help of fuzzy logic the image is watermarked in the reference image. Here use of fuzzy logic is done to embed the image and the use of SVD is done to enhance the embedding process after the application of DWT for the decomposition of an image into 4 levels. In the end results are performed using NCC and PSNR metrics.

Koley, S. et al. [16] proposed a new type of information hiding ability in biomedical images by using the combination of cryptography and digital watermarking to attain the improvement in confidential and authenticated data storage and secured transmission. They use patient's name and doctor's name as patient's information and it is encrypted using cryptography and embedded in the patient image by using watermarking. Higher order bit LSB replacement technique is used for embedding the information and RSA is used for encryption. The private keys are also embedded in the cover image to have enhanced security and precise recovery of the concealed information. The outcome of the proposed methodology shows that the concealed information doesn't influence the cover image and it can be recovered efficiently even from several noisy images. The strength of the proposed embedding scheme is also supported by numerous image quality matrices. Solanki, N. et al. [17] proposed an algorithm in which work is divided in two main stages; initially image is divided into two parts: Region of Interest i.e. defined as informational piece of image and Region of Non Interest i.e. defined as non-informational piece. They have used Region of Non Interest to conceal the data so that the informational part of the image remains protected. RSA is used for encryption of watermark. A Discrete Wavelet Transform based approach is utilized for embedding the encrypted data in Region of Non Interest part of image for improving data security. The experimental result demonstrates that watermark embedded by the proposed algorithm gives better security and can survive successfully under different attacks.

Anita, et al. [18] presented a review on watermark coding and decoding technique for image security. DWT technique is utilized for coding as DWT have broad range of functionalities. Two images are used, one as a host image and second as a watermark image. Then the image is extracted to retrieve the watermark image. This all is done under DWT technique. They basically evaluate the DWT technique, its improvement, and its challenges and also result are analyzed on MATLAB tool by computing SSIM, PSNR and SSR values of extracted image. Sridhar, S. et al. [19] combine the features of watermarking, image encryption in addition to image steganography to give consistent and protected data transmission. The fundamentals of data hiding and encryption are enlightened. The initial step entails inserting the mandatory watermark on the image at the best possible bit plane. The next step is to utilize RSA hash to encrypt the image. The last step entails attaining a cover image and hiding the encrypted image inside this cover image. A set of metrics will be used for evaluation of the effectiveness of the digital watermarking. The list

incorporates Mean Squared Error, Peak Signal to Noise Ratio and Feature Similarity.

Venkatram, N. et al. [20] proposed an algorithm for authentication of medical images. Medical images restrain extremely susceptible information. Watermarking medical images entail cautious amendments protecting the data in the images. RSA algorithm is used for encryption and decryption of patient image. Medical images like MRI, CT and Ultrasound scans of body parts of patients are used as a cover image. 2D DWT (Discrete Wavelet Transform) is used to watermark the encrypted patient image. The medical cover image and watermark image are transformed into wavelet domain and are diverse using two scaling factors alpha as well as beta. At last these watermarked medical images are passed on through the internet in conjunction with the secret key which will be used for decryption. On the receiving end the embedded encrypted watermark is extracted using 2D DWT and decryption key. The robustness of the projected watermarking techniques is tested with various attacks on the watermarked medical images. Peak-Signal-to-Noise ratios (PSNR) and Normalized cross correlation (NCC) coefficients are computed to access the eminence of the watermarked medical images and extracted patient images. The results are evaluated for three types of medical images with one patient image watermarks using single key by using four wavelets (haar, db, symlets, bior) on four diverse levels (1,2,3,4).

III. TECHNIQUES USED IN PROPOSED WORK

A. Discrete Wavelet Transform (DWT)

The discrete wavelet transform is a valuable way designed for signal exploration as well as picture handling, chiefly in multi-resolution description. It can crumble signal into different components in the frequency sphere. It divides an image into 4 sub-bands i.e. HL, HH, LH and LL. One-dimensional discrete wavelet transform (1-D DWT) decomposes an input into two components (the average component and the detail component). The 2-dimensional (2-D) DWT distributes an input picture into four type of sub-bands, single average component (LL) and three detail components (LH, HL, HH) as shown in Fig. 3.

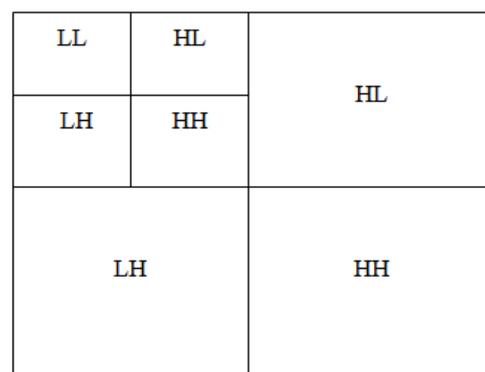


Fig.3. DWT second level decomposition

The utilization of wavelets is done mainly for the denoising of an image or to decompose the image into its constituent forms [11, 12]. Detailed has LL and LH. Image consists of pixels that are arranged in two dimensional matrix, each pixel represents the digital equivalent of image intensity. DWT transforms the spatial domain into frequency domain. Below equations shows the mathematical portion of a discrete signal:

$$gI[n1] = \frac{1}{\sqrt{M1}} \sum_{k1} W1\phi[j1o, k1]\phi1j0, k[n1] + \frac{1}{\sqrt{M1}} \sum_{j1=j1o}^{\infty} \sum_{k1} W1\psi[j1, k1]\psi1j, k[n1] \tag{2}$$

Here, $gI[n1]$, $\phi1j0, k[n1]$ and $\psi1j1, l1$ are discrete functions which are defined in $[0, M-1]$, totally $M1$ points. For the reason that the sets $\{\phi1j1o, k1[n1]\}_{k1 \in EC}$ and $\{\psi1j1, k1[n1]\}_{(j1, k1) \in C1^2, j1 \geq k1o}$, are orthogonal to each other.

B. RSA Algorithm

RSA stands for Rivest, Shamir and Adelman. It turned out 1st for sale in 1978 among the 1st public key cryptographic programs. RSA can be used pertaining to key alternate along with digital signatures. Currently, RSA is generally utilized to encrypt your procedure key useful for secret key encryption (message integrity) or message's hash value (digital signature). It is the most widely used algorithm in the world for cryptography. It can be used for public key cryptography as well as digital signatures. In this, Party A send the message to party B without prior knowledge to party B then using decrypt key B can extract and read the message sent by party A.

Within cryptography, RSA is an algorithm pertaining to public key cryptography. The particular RSA algorithms entail the application of two keys. A public key which is often known by everyone, in addition to enable you to encrypt statement. A private key, acknowledged simply because of the receiver, in addition utilizing to decrypt communication. To produce a great RSA public/private key match, there are some principle measures:

Step 1: Opt for two prime numbers, $p1$ as well as $q1$. Commencing these numbers we can compute the modulus, $n=p1*q1$.

Step 2: Choice a third number, e , which is reasonably prime to (i.e., it doesn't distribute uniformly into) the product $(p1-1) (q1-1)$. The number e may be the public exponent.

Step 3: Compute an integer d through the quotient $(ed-1)/ [(p1-1) (q1-1)]$. The number d may be the private exponent.

Step 4: Compute an integer d through the quotient $(ed-1)/ [(p1-1) (q1-1)]$. The number d may be the private exponent.

Step 5: The public key may be the number pair (n, e) . Although these kinds of valuations are generally widely acknowledged, it truly is computationally infeasible to

discover d from n addition to e if $p1$ in addition to $q1$ are generally big enough.

To encrypt a communication message, M , while using the public key, build your cipher text, C , while using the equation:

$$C = M^e \text{ mod } n \tag{3}$$

The receiver after that decrypts your cipher text while using private key using the equation:

$$M = C^d \text{ mod } n \tag{4}$$

C. Neural Network

The Back Propagation neural network is artificial neural network based on error back propagation algorithm. The Back Propagation (BP) neural network model consists of an input layer, more or less hidden layers as well as an output layer. Each connection connecting neurons has a distinctive weighting value. In training the network, the nodes in the BP neural network obtain input information from exterior sources, and then go by to hidden layer which is an interior information processing layer and is answerable for the information conversion, and then the nodes in the output layer supply the required output information. After that, the back-propagation of error is transported by distinct the actual output with wanted output.

BP neural network consists of many neurons that are arranged in a form of three layers: input, hidden and output. The neurons are linked by weights W y In training the network with a given architecture, the back propagation approach, finds a single best set weight values by minimization of suitable error function. In a multi-layer feed forward neural network, the processing elements are arranged in layers and only the elements in adjacent layers are connected. It has a minimum of three layers of elements (i.e., input layer, the middle or hidden layer, and the output layer).

The name "back propagation" (BP) derives from the fact that computations are passed feed forward from the input layer to the output layer, resulting which computed errors are broadcasted back in other direction to change the weights to obtain a better performance. BP algorithm is an extension of the least mean square algorithm that can be used to train multi-layer networks.

Once the network weights and biases are preliminary, the linkage is prepared for training. The preparation process necessitates a group of instances for proper network behavior, such as network inputs p and destination outputs t . For the duration of training the weights as well as biases of the network are iteratively adjusted to minimize the network performance function. The number of hidden layer is always difficult to determine in ANN creation. It is generally agreed that one hidden layer is sufficient for most of purposes. In the present study, only 1 hidden layer will, thus, be used in the BP network for simplicity.

Neural network consists of various no. of neurons and their working is similar to the brain neuron structure. There are various types of neural networks but commonly used neural network is Back Propagation Neural network [14]. The normal Back propagation is the mainly applied to train Multilayer FNN.

IV. STIMULATION MODEL

The proposed idea will be implemented in MATLAB which is extensively utilized in all regions of applied mathematics, in education as well as research by universities, and in the industry. The flowchart for proposed work is shown in Fig. 4. The methodology of proposed work is given as:

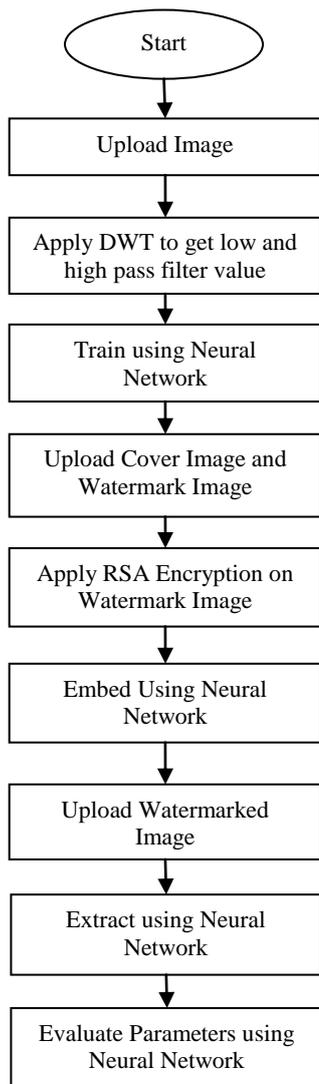


Fig.4. Flowchart of proposed work

A. Training Panel

Initially images are uploaded for Training. After that calculation of image bits has done. Now the lower and upper DWT values are calculated. Load DWT values for training and after that training is done using Neural

Network. Fig. 5 shows the Neural Network training process.

B. Testing Panel

In testing panel, initially cover image is uploaded. After that watermark image is uploaded. Now implementation of RSA will be done to encrypt watermark. The encrypted watermark is embedded in cover image.

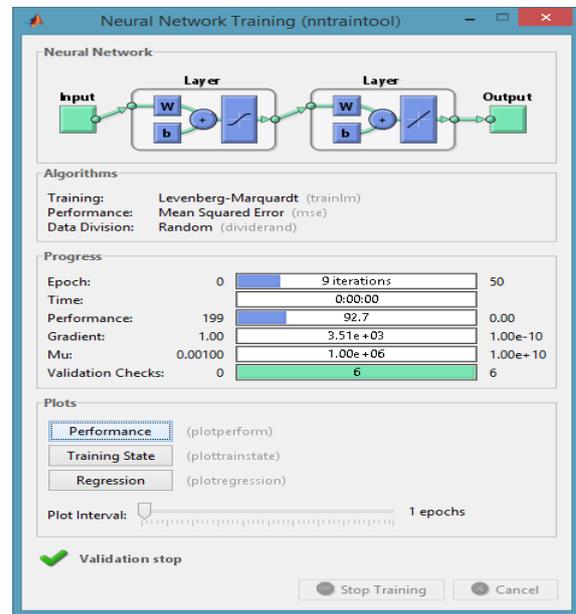


Fig.5. Neural Network training process

C. Extraction Panel

In extraction panel, watermarked image is uploaded and neural network is applied to obtain extracted watermark. In the end parameter evaluation will be done using five metrics i.e. PSNR, MSE, BCR, BER and NCC.

V. RESULTS AND DISCUSSIONS

In this section, experimental results of the proposed algorithm are evaluated. The imperceptibility and robustness are evaluated by using different parameters and different attacks are applied to test the robustness of the proposed algorithm.

A. Results

The proposed scheme is implemented in MATLAB 7.10.0 (R2010a). The proposed scheme is tested on six gray scale and six colored medical images with size 512x512. A gray scale watermark of size 64x64 is used. The performance of the proposed scheme is evaluated on the basis of PSNR, MSE, NCC, BER and BCR. These parameters are used to check the quality of the watermarked image. Different attacks are applied on the watermarked image to check the robustness. Table 1 show the gray scale watermarked medical images and watermarked medical images with different attacks. Different parameters are evaluated for watermarked

image and watermarked image with different attacks to check the imperceptibility and robustness of the proposed algorithm. Similarly, table 2 shows the colored watermarked medical images and watermarked medical

images with different attacks. Different parameters are evaluated for watermarked image and watermarked image with different attacks to check the imperceptibility and robustness of the proposed algorithm.

Table 1. Experimental results of gray scale medical images

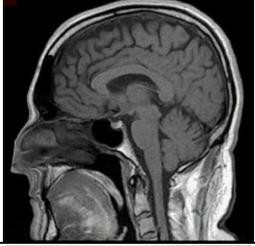
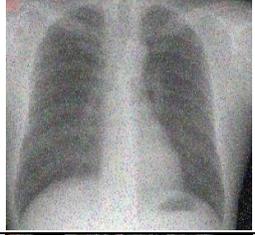
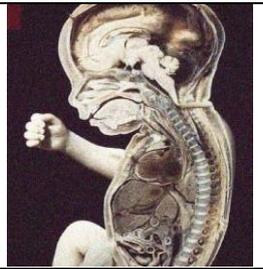
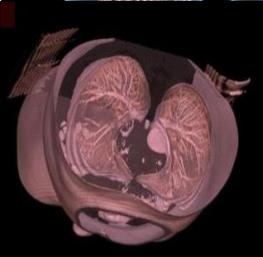
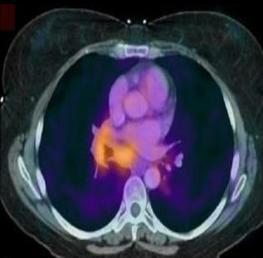
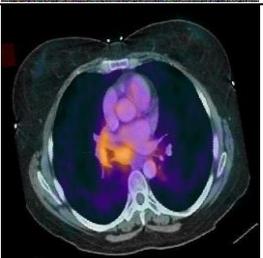
WATERMARKED IMAGE	PARAMETERS	WATERMARKED IMAGE WITH ATTACKS	PARAMETERS
	MSE =0.2899		MSE =0.5687
	PSNR =54.5382		PSNR =51.7634
	BER =0.3298		BER =0.2663
	BCR =4.6129		BCR =4.9221
	NCC =0.9985		NCC =0.9941
	MSE =0.4676		MSE =0.6953
	PSNR =52.9416		PSNR =50.4185
	BER =0.5589		BER =0.5812
	BCR =5.0266		BCR =5.1838
	NCC =0.9955		NCC =0.9964
	MSE =0.4219		MSE =0.5198
	PSNR =53.9430		PSNR =52.8832
	BER =0.3827		BER =0.4453
	BCR =5.0484		BCR =5.3625
	NCC =0.9942		NCC =0.9940
	MSE =0.5064		MSE =0.6368
	PSNR =51.8941		PSNR =50.5347
	BER =0.6570		BER =0.6609
	BCR =4.8782		BCR =5.3688
	NCC =0.9901		NCC =0.9929
	MSE =0.5301		MSE =0.6120
	PSNR =52.6875		PSNR =51.3476
	BER =0.6736		BER =0.4624
	BCR =5.0112		BCR =5.0881
	NCC =0.9969		NCC =0.9948
	MSE =0.5124		MSE =0.5899
	PSNR =52.1182		PSNR =51.4627
	BER =0.5172		BER =0.5358
	BCR =5.0486		BCR =5.0314
	NCC =0.9914		NCC =0.9919

Table 2. Experimental results of colored medical images

WATERMARKED IMAGE	PARAMETERS	WATERMARKED IMAGE WITH ATTACKS	PARAMETERS
	MSE =0.2885		MSE =0.6393
	PSNR =54.5670		PSNR =51.0726
	BER =0.3298		BER =0.2666
	BCR =4.6115		BCR =4.9927
	NCC =0.9915		NCC =0.9928
	MSE =0.5828		MSE =0.7084
	PSNR =51.6083		PSNR =50.8047
	BER =0.5593		BER =0.5842
	BCR =5.1417		BCR =5.2331
	NCC =0.9985		NCC =0.9958
	MSE =0.4642		MSE =0.5807
	PSNR =53.1430		PSNR =50.9606
	BER =0.3829		BER =0.5779
	BCR =5.0907		BCR =4.9292
	NCC =0.9973		NCC =0.9988
	MSE =0.3047		MSE =0.5742
	PSNR =54.7452		PSNR =52.0150
	BER =0.5290		BER =0.6738
	BCR =4.7648		BCR =5.2506
	NCC =0.9955		NCC =0.9945
	MSE =0.5874		MSE =0.6667
	PSNR =51.4436		PSNR =50.6501
	BER =0.5940		BER =0.4588
	BCR =5.2307		BCR =5.1949
	NCC =0.9956		NCC =0.9937
	MSE =0.5831		MSE =0.7561
	PSNR =51.4919		PSNR =49.9271
	BER =0.4292		BER =0.6155
	BCR =5.4859		BCR =5.3961
	NCC =0.9926		NCC =0.9937

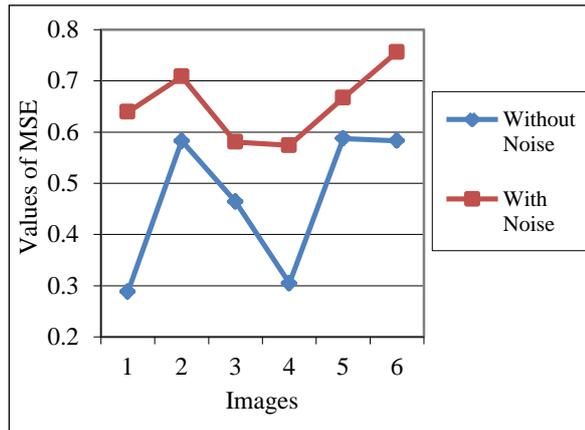


Fig.6. Graph of MSE values

Values of MSE for different colored medical images are shown in Fig. 6. Robustness is tested by applying different attacks on the watermarked images. These attacks are Gaussian Noise, Poisson Noise, Salt & Pepper Noise, Speckle Noise, Localvar Noise and Rotation attack. From the above graph, it can be observed that the values of MSE for all watermarked images are between 0.2 and 0.6 and the values of MSE for all watermarked images with different attacks are between 0.5 and 0.8. Lesser value of MSE gives enhanced results. This shows that the proposed scheme has good imperceptibility and robustness.

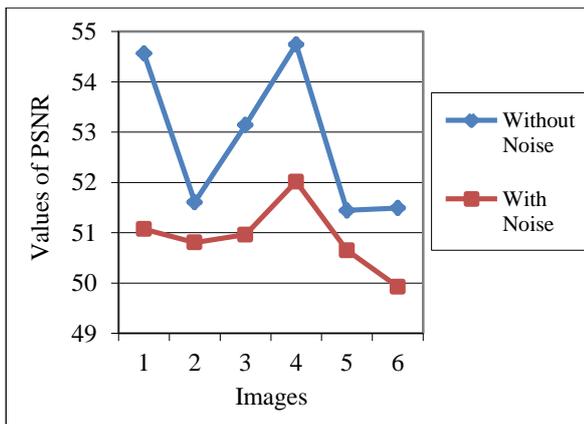


Fig.7. Graph of PSNR values

Values of PSNR for different colored medical images are shown in Fig. 7. Different attacks are applied on watermarked images to test the robustness of the proposed algorithm. These attacks are Gaussian Noise, Poisson Noise, Salt & Pepper Noise, Speckle Noise, Localvar Noise and Rotation attack. From the above graph, it can be observed that the values of PSNR for all watermarked images are between 49 and 52 and the values of PSNR for all watermarked images with different attacks are between 51 and 55. Higher value of PSNR gives superior results. This shows that the proposed scheme has good imperceptibility and robustness.

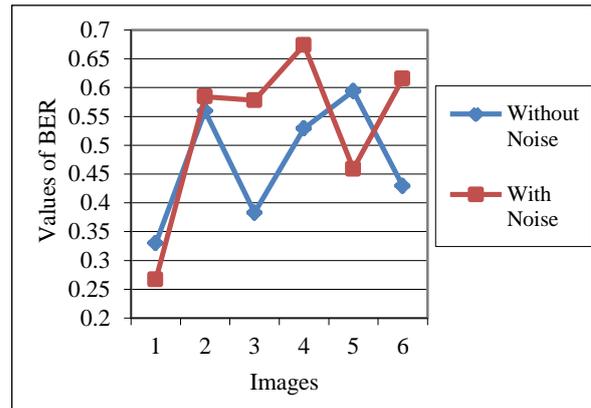


Fig.8. Graph of BER values

Values of BER for different colored medical images are shown in Fig. 8. Imperceptibility of the proposed algorithm is evaluated on the basis of parameters of watermarked images and robustness of the proposed algorithm is evaluated on the basis of different attacks applied on these watermarked images. From the above graph, it can be observed that the values of BER for all images are between 0.2 and 0.7 and lesser value of BER gives enhanced results. This shows that the proposed scheme has good imperceptibility and robustness.

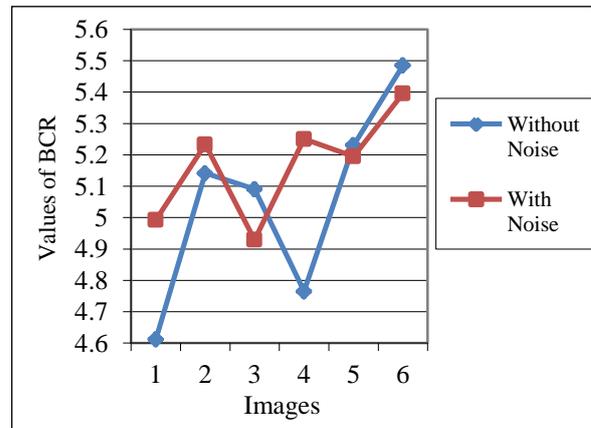


Fig.9. Graph of BCR values

Values of BCR for different colored medical images are shown in Fig. 9. Different attacks are applied on the watermarked images to check the robustness of the proposed algorithm. This robustness ensures that the data can be transmitted securely despite various attacks they might be subjected to. The embedded watermark cannot be tampered easily by using different attacks. Imperceptibility is also important so that informational part of the image does not get distorted. From the above graph, it can be observed that the values of BCR for watermarked images and watermarked images with different attacks are between 4.6 and 5.6 and larger value of BCR gives improved results. This shows that the proposed scheme has good imperceptibility and robustness.

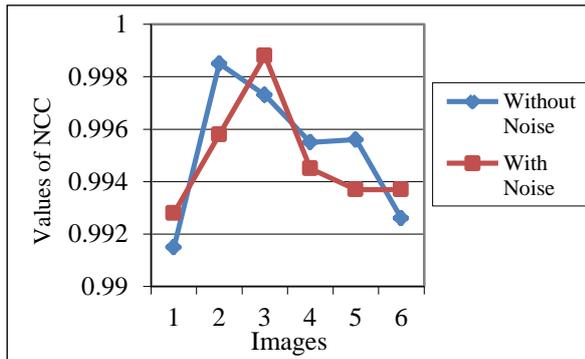


Fig.10. Graph of NCC values

Values of NCC for different colored medical images are shown in Fig. 10. From the above graph, it can be observed that the values of NCC for all images are close to 1 and higher value of NCC gives enhanced results. This shows that the proposed scheme has good robustness.

B. Comparison of Results

The comparison of existing scheme and proposed scheme is shown in table 3 [20]. The values of NCC for the proposed algorithm are higher than the existing method and higher value of NCC gives better results. These results demonstrate that the proposed scheme has more robustness.

Table 3. Comparison of results

Type of Attack	NCC (Existing Method)	NCC (Proposed Method)
Without Noise	0.9835	0.9985
Salt & Pepper Noise	0.6038	0.9959
Gaussian Noise	0.6061	0.9971
Rotation Attack	0.9653	0.9936

Fig. 11 shows the graph of NCC for existing and proposed method. It can be observed that the values of NCC for proposed method are higher than the existing method and values of NCC which are close to 1 gives better results. Therefore, the proposed algorithm gives enhanced results than the existing method.

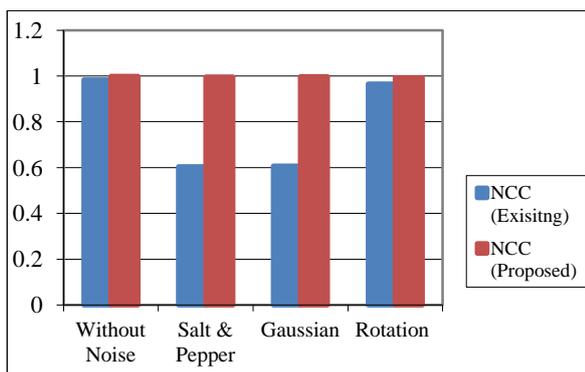


Fig.11. Comparison of results

The comparison of existing scheme and proposed scheme is shown in table 4 [21]. Three medical images are used for testing and values of PSNR for all three images are higher than the existing method. These results demonstrate that the proposed scheme has more imperceptibility.

Table 4. Comparison of results

Type of Attack	PSNR (Existing Method)	PSNR (Proposed Method)
Image 1	42.48	56.96
Image 2	48.46	50.31
Image 3	42.52	50.85

Fig. 12 shows the graph of PSNR for existing and proposed method. It can be observed that the values of PSNR for proposed method are higher than the existing method. Therefore, proposed method gives enhanced results than the existing method because higher value of PSNR gives better results.

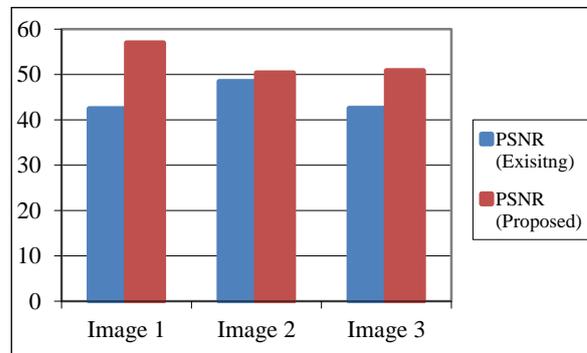


Fig.12. Comparison of results

The comparison of existing scheme and proposed scheme is shown in table 5 [21]. The values of PSNR for proposed method are higher than the existing method. These results demonstrate that the proposed scheme has more robustness and imperceptibility.

Table 5. Comparison of results

Type of Attack	PSNR (Existing Method)	PSNR (Proposed Method)
Without Noise	42.52	50.85
Salt & Pepper Noise	31.94	50.56
Gaussian Noise	30.03	50.34
Rotation Attack	35.87	50.32

Fig. 13 shows the graph of PSNR for existing and proposed method. It can be observed that the values of PSNR for proposed method gives enhanced results than the existing method because higher value of PSNR gives better results.

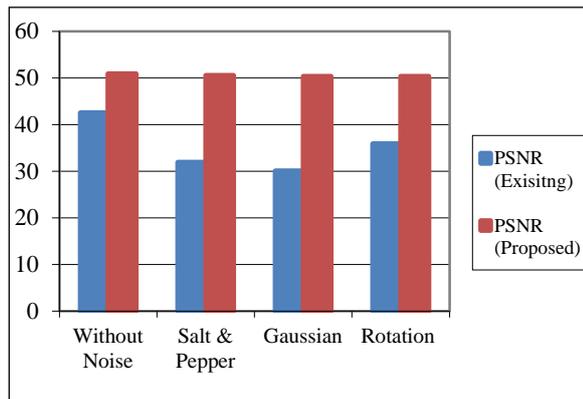


Fig.13. Comparison of results

VI. CONCLUSION AND FUTURE SCOPE

In this paper, DWT is used to get low and high pass filter values. Then, training of images is done using Neural Network. RSA algorithm has been used for encryption of watermark to make it more secure. After that, embedding and extraction of watermark is done using Neural Network. Results are evaluated using five parameters such as PSNR, MSE, BCR, BER and NCC.

In future, hybridization of different techniques can be used to enhance results.

ACKNOWLEDGMENT

The authors wish thanks to all research experts of the Information Technology Department of CEC and Computer Science Department of CGC, Landran, Mohali, Punjab, India.

REFERENCES

- [1] David J. Coumou, and Athimoottil Mathew, "A Fuzzy Logic Approach to Digital Image Watermarking", Rochester Institute of technology, Sept 2014.
- [2] G. Bhatnagar and R. Balasubramanian, "A New Robust Reference Watermarking Scheme Based on DWT-SVD", Computer Standards & Interfaces vol. 31, issue 5, Sept 2009, pp. 1002-1013, doi:10.1016/j.csi.2008.09.031.
- [3] J.L. Liu, D.C. Lou, M.C. Chang, H.K. Tso, "A Robust Watermarking Scheme Using Self-Reference Image", Computer standards and interfaces, vol. 28, issue 3, Jan 2006, pp. 356-367, doi:10.1016/j.csi.2005.07.001.
- [4] V. Gupta, A. Barve, "A Review on Image Watermarking and Its Techniques", International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE), vol. 4, issue 1, January 2014, pp. 92-97.
- [5] M. Kaur and V. K. Attri, "A Survey on Digital Image Watermarking and Its Techniques" International Journal of Signal Processing, Image Processing and Pattern Recognition, vol. 8, no. 5, Sept 2015, pp. 145-150.
- [6] N. Divecha and N. N. Jani, "Implementation and Performance Analysis of DCT-DWT-SVD Based Watermarking Algorithms for Color Images", International Conference on Intelligent Systems and Signal Processing (ISSP), March 2013, pp.204-208, doi:10.1109/ISSP.2013.6526903.
- [7] Z. Yuefeng and L. Li, "Digital Image Watermarking Algorithms Based On Dual Transform Domain and Self-Recovery" International Journal On Smart Sensing And Intelligent Systems, vol. 8, no. 1, March 2015, pp. 199-219.
- [8] R. Verma and J. Ali, "A Comparative Study of Various Types of Image Noise and Efficient Noise Removal Techniques," International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE), vol. 3, issue 10, October 2013.
- [9] B. Wang, J. Ding, Q. Wen, X. Liao and C. Liu, "An Image Watermarking Algorithm Based On DWT, DCT And SVD", IEEE International Conference on Network Infrastructure and Digital Content, IC-NIDC, Nov. 2009, pp.1034-1038, doi:10.1109/ICNIDC.2009.5360866.
- [10] C. C. Lai and C. C. Tsai, "Digital Image Watermarking Using Discrete Wavelet Transform and Singular Value Decomposition", IEEE Transactions on Instrumentation and Measurement, vol. 59, issue 11, Nov. 2010, pp. 3060 – 3063, doi:10.1109/TIM.2010.2066770.
- [11] Y. K. Jain and S. Tiwari, "An Enhanced Digital Watermarking for Color Image using Support Vector Machine" International Journal of Computer Science and Information Technologies (IJCSIT), vol. 2, no. 5, 2011, pp. 2233 – 2236.
- [12] P. Saxena, S. Garg and A. Srivastava, "DWT-SVD Semi-Blind Image Watermarking Using High Frequency Band", 2nd International Conference on Computer Science and Information Technology (ICCSIT), April 2012, pp. 28-29.
- [13] S. R. Anjum and P. Verma, "Performance Evaluation of DWT Based Image Watermarking Using Error Correcting Codes", International Journal of Advanced Computer Research, vol. 2, no. 4, Dec. 2012, pp.151-156.
- [14] R. Kaur, and S. Jindal, "Semi-Blind Image Watermarking Using High Frequency Band Based on DWT-SVD", 6th International Conference on Emerging Trends in Engineering and Technology (ICETET), Dec. 2013, pp.19-24, doi:10.1109/ICETET.2013.5.
- [15] T. Sridevi and S. S. Fatima, "Digital Image Watermarking using Fuzzy Logic approach based on DWT and SVD" International Journal of Computer Applications, vol. 74, no.13, July 2013, pp. 16-20.
- [16] S. Koley, K. Pal, G. Ghosh and M. Bhattacharya, "Secure Transmission and Recovery of Embedded Patient Information from Biomedical Images of Different Modalities through a Combination of Cryptography and Watermarking" International Journal of Image, Graphics and Signal Processing, March 2014, pp. 18-31, doi: 10.5815/ijgisp.2014.04.03.
- [17] N. Solanki and S. K. Malik, "ROI Based Medical Image Watermarking with Zero Distortion and Enhanced Security" International Journal of Modern Education and Computer Science, October 2014, pp. 40-48, doi:10.5815/ijmecs.2014.10.06.
- [18] Anita and Arachana, "Discrete Wavelet Transform Technique for Digital Image Watermarking: A Review" International Journal of Advanced Research in Computer Science and Software Engineering, vol. 5, issue 7, July 2015, pp. 495-498.
- [19] Sridhar, S., "A Comprehensive Approach to Image Watermarking, Encryption and Steganography" Canadian Center of Science and Education, vol. 8, no. 4, November 2015, pp. 32-39, doi: 10.5539/cis.v8n4p32.
- [20] N. Venkatram, L.S.S. Reddy, P.V.V. Kishore and CH. Shavya, "RSA-DWT Based Medical Image Watermarking for Telemedicine Applications" Journal of Theoretical and Applied Information Technology (JATIT), vol. 65, no. 3, July 2014, pp. 801-812.

- [21] B.L. Gunjal and S.N. Mali, "ROI Based Embedded Watermarking of Medical Images for Secured Communication in Telemedicine" International Journal of Computer, Electrical, Automation, Control and Information Engineering, vol. 6, no.8, 2012, pp. 997-1002.

Authors' Profiles



Sujata Nagpal is a student of Masters of Information Technology in Chandigarh Engineering College, Landran (Mohali), Punjab. She has completed her Bachelor degree in Information Technology from Rayat & Bahra College of Engineering and Bio-tech. for Women, Kharar (Mohali), Punjab. Her research area is image

processing.



Dr. Shashi Bhushan is Head of Department in Chandigarh Engineering College, Landran (Mohali), Punjab.



Mr. Manish Mahajan is Associate Professor and Head of Department in Chandigarh Group of Colleges, College of Engineering, Landran (Mohali), Punjab. His area of interest is Image Processing, Cloud Computing and Networking.