Journal of Data Acquisition and Processing
ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.776707

WATERMARKING SCHEME FOR MEDICAL IMAGES WITH ENHANCED ROBUSTNESS BASED ON DISCRETE WAVELET TRANSFORM AND NEURAL NETWORK

Raj Vikram Singh[1]
Department of Electronics, College of Engineering Science, and Technology, Lucknow

Dr. Subodh Wariya[2]
Professor
Institute of Engineering and Technology, Lucknow

Dr. Rajiv Kumar Singh[3]
Assistant Professor, Institute of Engineering and Technology, Lucknow

Abstract
Medical data has become increasingly sensitive in the world today, and the necessity for privacy has become more important. The digital watermarking method is used to offer privacy and verification to medical information, which comprises a patient's medical information. The goal of the paper is to use digital watermarking technology with neural networks to validate medical information. The host information is analyzed using a four-level DWT before being fed into a back propagation neural network, which contains the secret image as well as various noise attacks. DWT is used to process the acquired image, which is then either saved or sent. The process of disguising one image in another for copyright protection is known as image watermarking. The watermarking process should be carried out in such a way that the original image's pixels stay in their original HD format. Although much work was done in this area in recent years, each technique has its own set of applications, disadvantages, and benefits. As a result, this study will employ two strategies, namely, Image watermarking using Neural Network (NN) and Discrete Wavelet Transform (DWT). Finally, the suggested technique's efficiency will be evaluated using MSE, PSNR, BER, NCC, and BCR in the MATLAB R2010a environment.

Keywords: Discrete Wavelet Transform, neural network, watermarking, digital, security

1. Introduction
Digital medical pictures can now be exchanged globally for services like teleradiology, telemedicine, teleconsultation, and telediagnosis because of the extensive use of digital technology and the prominence of electronic health records management. By allowing remote accessibility, transfer, and analysis of medical pictures for disease recognition, these e-Health services are offering new practices for the profession and also for patients. Instant diagnosis and comprehension of a condition, as well as a reduction in the incidence of misdiagnoses, have had significant societal and economic consequences, demonstrating the importance of effective patient data sharing between experts in various hospitals. [1-3] The key concern in the handling of medical photographs is to ensure that the patient's records are protected from

unauthorized manipulation. This includes image preservation and fraud, confidentiality, professional liability, licensing, and credentialing. As a result, the primary concern of the current electronic medical system is to provide a standard solution for preserving the integrity and authenticity of medical source images.

Digital imaging technology has permeated the medical industry due to the ongoing growth of multimedia technologies and online image processing. [4] The health-care system, digital diagnostic imaging, and PACS based on communication systems have all been hot topics in

recent research. However, as PACS becomes more popular and widely used, information security becomes more vulnerable. When compared to the conventional picture of the film, the treatment is predicated on the electronic healthcare image. If an exception takes place, including counterfeiting, tampering with illness data, etc., not only will it not be as solid evidence of healthcare malpractice, but it will also defer the patient's diagnosis and possibly misdiagnose him or her.

Because meeting the PACS data security criteria has been hard due to encryption and security systems, data security technology solutions are urgently needed. Watermarking technology offers a viable solution to this issue. [5] The purpose of digital watermarking tech is to embed iconic digital data into multimedia digital files, and its unique resilience and security characteristics can secure the data's integrity and dependability following information transmission. As a result, it can determine the materials' legitimacy and also copyright laws.

Electronic document security was and continues to be one of the most pressing issues in scientific research. Intruders are unlawfully reproducing, authenticating, and disseminating digital materials as Internet capabilities advance. [6] As a result, watermarking technologies were researched for many applications, like transmitting, monitoring, intellectual property rights, document validation, and copying limitation. Copyright violations, unauthorized usage, replication, and online media theft became more common as a result of the widespread uploading and dissemination of electronic material on the Internet.

Digital photographs are high-value-added resources, and their intellectual property copyrights must be protected. Digital watermarking, on the other hand, is a modern and useful tool for image security. The owner's data can be encoded using the watermarking technique (WM), which is then preserved or distributed on the Internet. According to existing tech, specific uses, and other digital platform-based systems, this method is utilized to assert proprietorship by obtaining the encoded watermark information as required. [7-9] For digital watermarking photos, just a few studies have been conducted. Different ways of watermark embedding were implemented, including algorithmically retrieving the WM from the digital image or modifying it.

In general, watermarking can be vulnerable to malicious attacks aiming at damaging or eliminating the encoded WM information, and also non-malicious attacks aimed at preserving or distributing the information. [10-12] As a result, WM embedding might be done either

algorithmically or mechanically. The circumstances for WM removal, on the other hand, are quite different. [13] non-malicious or malicious assaults may damage the WM-incorporated host data, and the embedded WM information may be erased. As a result, retrieving the WM programmatically or sequentially could be ineffective, and a statistical method may be more beneficial.

Video, music, text, and other digital forms of goods are communicated in our daily life [14]. Some strategies have greatly aided in the storage, editing, and retrieving of digital multimedia interaction goods. However, security during the transport of communication is quite important. As a result of a lack of security, property rights are lost. As a result, digital watermarking is an excellent solution to this problem. [15] The process of inserting hidden data into an image for transmission is known as digital watermarking. Only someone with authentication can retrieve the embedded picture.

2. Proposed Method 2.1.Digital watermarking

The practice of embedding data, including a watermark, into a digital multimedia entity so that the watermark could be recognized or retrieved later to make a statement about the object is known as digital watermarking. Watermarking has shown to be an effective method of copyright security and digital media validity confirmation.

Two steps make up the watermarking system.

1. Embedding
2. Extracting

Embedding is the process of putting watermark information into the host signal. A secret key is employed, which adds to the level of security. Detection or extraction refers to the process of extracting watermark information from watermarked images.

Discrete wavelet transform

The Wavelet Series is simply a sampled form of CWT, and based on the resolution needed, its computation might take a long time and demand a lot of resources. The Wavelet Transform can be computed quickly using DWT, which is dependent on sub-band coding. It is simple to use and decreases the amount of time and resources needed for computation. The DWT is the wavelet sequence of a discrete-time signal if the signal, scaling factors, and wavelets are all discrete in time. The DWT of a series is made up of 2 series expansions, one for the estimation and the other for the sequence's features. The technical definition of DWT for an N-point series x [n], $0 \leq n \leq N-1$ is as follows:

$$DW\{f(t)\} = W_{\emptyset}(j_o, k) + W_{\varphi}(j, k) \quad \text{----------> (1)}$$

$$W_{\emptyset}(j_o, k) = \frac{1}{\sqrt{N}} \sum_{n=0}^{n=n-1} [n]\emptyset_{j_o,k}[n] \quad \text{----------> (2)}$$

$$W_{\emptyset}(j, k) = \frac{1}{\sqrt{N}} \sum_{n=0}^{n=n-1} [n]\varphi_{j,k}[n], j \geq j_o \quad \text{----------> (3)}$$

The sequence $[n],0 \leq n \leq N-1$ can be recovered from the DWT coefficients $W\varphi$ and $W\psi$ as given by

$$X[n] = \frac{1}{\sqrt{N}} \sum_{n=0}^{n=n-1} x[n]\emptyset_{jo,k}[n] + \frac{1}{\sqrt{N}} \sum_{n=0}^{n=n-1} [n]\varphi_{j,k}[n] - - - - - - - - - - - -> (4)$$

In the second summation of the preceding equation, the scale factor has an unlimited number of terms. However, in reality, the scale parameter's upper limit is normally set to some value, such as J. The initial scale value j0 is normally zero, which correlates to the original signal. Thus, for j = 0, 1,..., J 1 and k = 0, 1,...,2J 1, the DWT coefficients for x [n],0 n N 1 are determined. N is also usually a power of two, as in N = 2J.

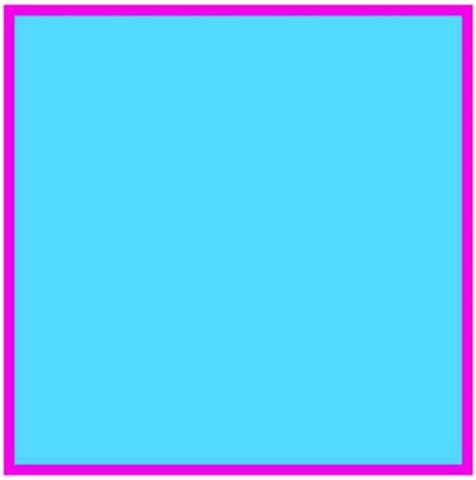


Fig. 1. The layout of the Original Picture

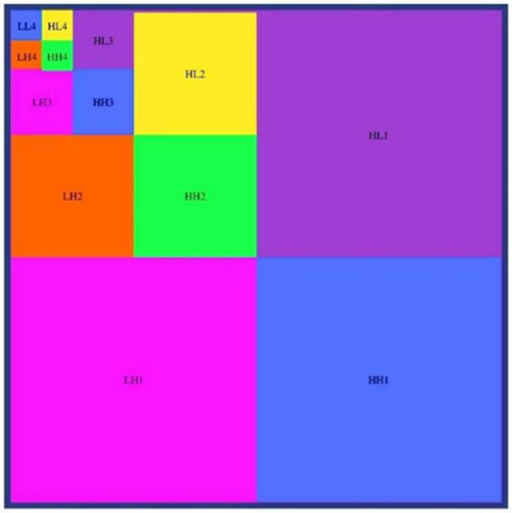


Fig. 2. DWT picture layout with four levels

DWT Algorithm:

Step 1. Apply DWT to the original host image in order to decompose it into four non-overlapping multi-resolution sub-bands: LL1 , HL1 , LH1 , and HH1 .
Step 2. Apply DWT again to the HL1 sub-band to get four smaller sub-bands, and choose the HL2 sub-band. Or apply DWT to the HH1 sub-band to get four smaller sub-bands, and choose the HH2 sub-band.
Step 3. Reformulate the grey-scale watermark image into a vector of zeros and ones.

Step 4. Generate a uniformly distributed, highly uncorrelated, zero-mean, two-dimensional pseudorandom sequence (PN) using a secret seed value. The PN sequence is used to embed the zero watermark bit in the host image.
Step 5. Embed the pseudorandom sequence PN in the selected DWT sub-band with a gain factor α. Number of elements in the selected sub-band and the pseudorandom sequence PN must be equal for embedding to take place. If we donate X as coefficients matrix of the selected sub-band, then embedding is done
Step 6. Apply the inverse DWT (IDWT) on the DWT transformed image, including the modified sub-band, to produce the watermarked host image.
Step 7. Apply DWT to decompose the watermarked image into four nonoverlapping multiresolution subbands: LL1 , HL1 , LH1 , and HH1 .
Step 8. Apply DWT to the HL1 subband to get four smaller subbands, and choose the subband HL2 . Or apply DWT to the HH1 subband to get four smaller subbands, and choose the subband HH2 .
Step 9. Regenerate the pseudorandom sequence (PN sequence) using the same seed used in the watermark embedding procedure described previously.
Step 10. Calculate the correlation between the watermarked subband HL2 (or HH2) and the generated pseudorandom sequence (PN sequence). This step is repeated m times, where m is number of bit elements in the watermark vector.
Step 11. Compare each correlation value with the mean correlation value. If the calculated value is greater than the mean, then the extracted watermark bit will be taken as a 0; otherwise, it is taken as a 1. A mean correlation value of 0.75 is used.
Step 12. Reconstruct the watermark image using the extracted watermark bits, and compute the similarity between the original and extracted watermarks.

Healthcare Images

The number of digital photos on the internet is growing every day. In the medical field, it is critical to have a reliable diagnosis. As image communication has become more widespread in recent years, increased security is required. Medical pictures are used to examine a person's tissues, organs, or body parts. These photos are utilized in the diagnosis and therapy of various diseases. Medical images serve an important role in disease classification. These are also useful for keeping track of illness activity. Several technologies that can give access to a person's interior organs are now available. Ultrasound, nuclear medicine scans, x-rays, CT scans, MRI scans, and other imaging modalities are available. X-rays are another name for electromagnetic radiation. The most prevalent type of medical imaging is X-rays. X-rays are used to create images of a person's interior anatomy by passing them through their body. X-rays are frequently

used to examine ingested objects, blood vessels, and shattered bones, among other things. Medical sonography is another name for the ultrasound. Internal systems are checked using sound waves in this procedure. It's used to assess organs in the belly and pelvis, among other things. This approach employs radio waves and a magnetic field to allow for a more detailed examination of the body's organs and tissues. It can be used to look for spinal injuries, aberrant tissues, and blood vessels, among other things. CT scans are identical to X-rays, except they use several X-rays projected from various angles to create a 3-D image of various organs. All diagnoses are based on the collected medical picture, thus medical photos should be taken care of to validate the identity. Watermarking is utilized in this industry to address the safety and convenience concerns of patients.

Distortions and Noise

Images are susceptible to a variety of sounds. Any deterioration in an image's signal is referred to as noise. It occurs when an image is sent from one location to another and is disrupted by external factors. For image transmission, many devices such as network cables, satellites, and so on can be employed. Various types of noise, like Poisson, Gaussian, Salt, Pepper, and others, might arise during communication. Gaussian noise can be induced in digital photographs during acquisition or transmission. In terms of temperament, this noise is additive. Each pixel in the noised picture is the result of adding the original pixel and a random value. The sort of noise in which the PDF is equivalent to the normal distribution is known as Gaussian noise. The Gaussian distribution noise is another name for it. This sort of noise is caused by modified Gaussian distribution values.

High temperature, electrical circuit noise, and sensor noise are all factors of Gaussian noise. Shot noise is another name for Poisson noise. It's a type of electronic noise that a Poisson growth can shape. Diverse pixels in the image are subjected to independent noise levels in this noise. Impulse noise is another name for salt and pepper noise. Black and white spots are strewn across the image's pixels with this technique. This sort of noise is created by pointing and sudden changes in the visual signal. A morphological filter or median filter was an excellent noise control strategy for this kind of noise. When the image's original pixel values

are amplified by some random values, speckle noise is formed. The bright and dark spots in the image represent patterns of destructive and constructive interference. Speckle noise was the result of these patterns. The Zero-mean Gaussian white noise with intensity-dependent variance factors is known as Localvar noise. This can be expressed in MATLAB as follows:

K = imnoise(O,'localvar',B)

It inserts local variance B zero-mean Gaussian white noise into the image. B was an array of the same length as O. In today's world, the most prevalent attack in a picture is a rotation strike. The image is spun in numerous directions, including 180 degrees, 360 degrees, and 90 degrees.

Neural network

A Neural Network was a sophisticated tool that can represent both simple and complicated input and output interactions. The advancement of technology paves the way for the creation of artificial systems capable of performing complicated tasks formerly handled by human brains. In the following aspects, NNs mimic the human brain: Learning methods can be used to provide knowledge to NN. The strength of inter-neuron links, known as weights, is where NN knowledge is saved.

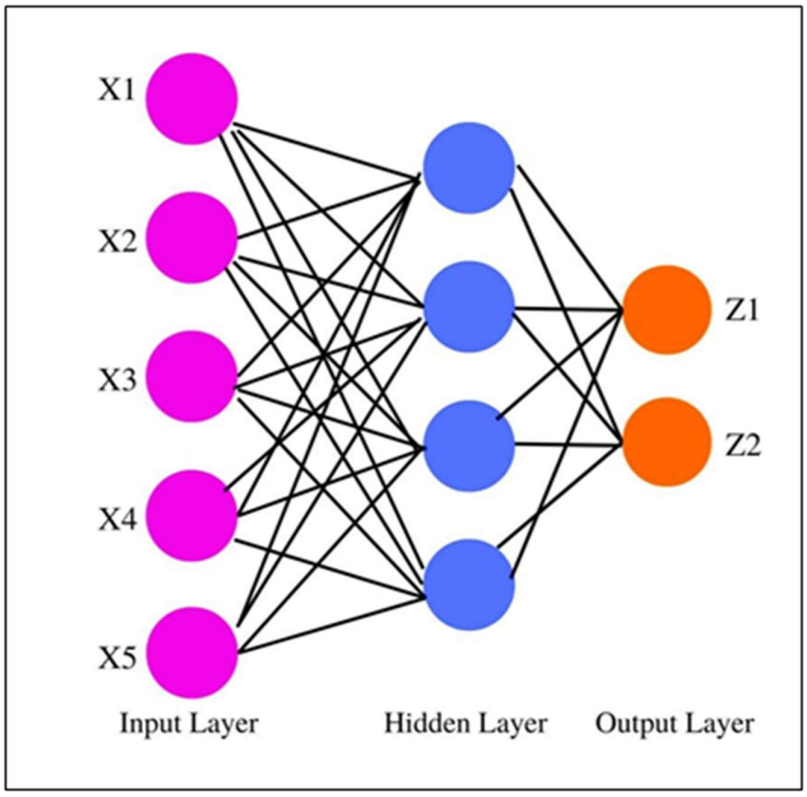


Fig. 3. neural network structure

The basic perceptron can only solve issues that are linearly independent or separable. Humans can learn a little about the way the net loss is moving by taking the partial derivative of the network error function concerning each load. In reality, if we subtract the negative of this derivative from the mass, the error will reduce until it hits a local minimum. This makes logical because a positive derivative indicates that the mistake is increasing as the weight increases. If the derivative was negative, the logical thing to do is to add a negative number to the weight, and vice versa. This approach is known as the learning algorithm because it obtains partial derivatives and applies them to each of the levels, leading from the output nodes to hidden unit weights, then from the hidden units to input data weights. Backpropagation modeling with enough hidden units was shown to estimate any non-linear function to arbitrary precision. Backpropagation learning neural networks are an excellent contender for signal forecasting and system simulation because of this.

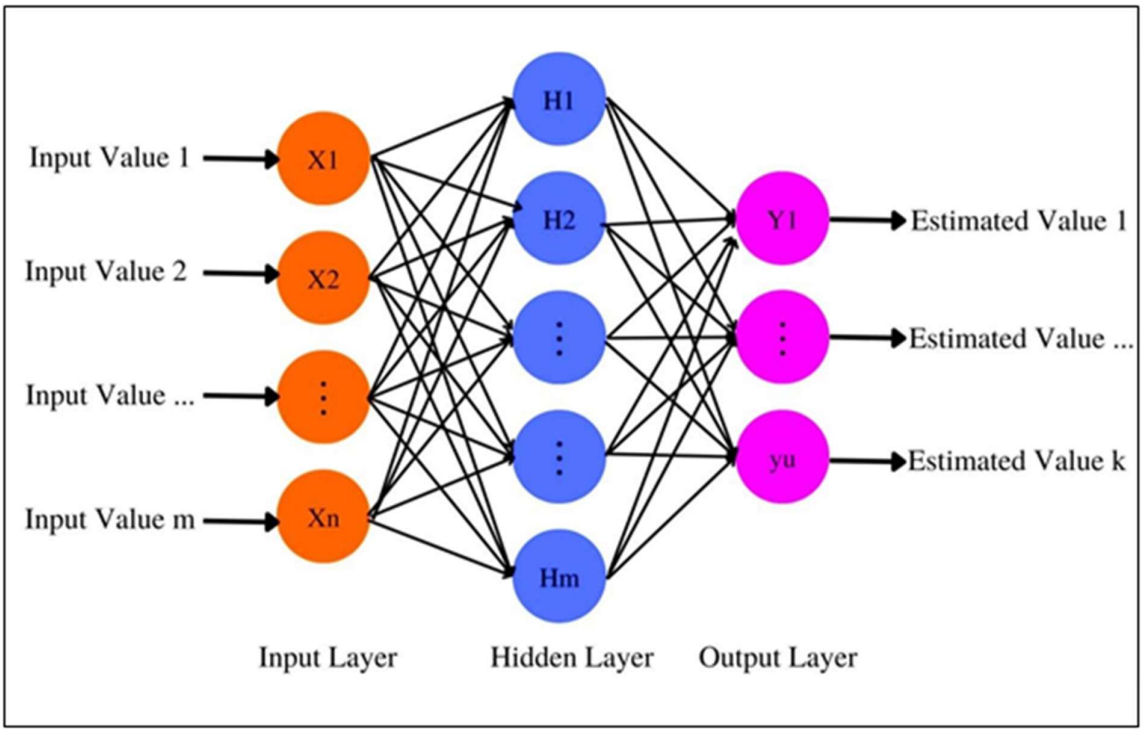


Fig. 4. Neural Network with Back Propagation

3. Result and Discussion

The suggested algorithm's experimental outcomes are analyzed in this section. The robustness and imperceptibility of the suggested method are assessed using various parameters, and various assaults are used to test its resilience.

MATLAB 7.10.0 is used to implement the proposed method (R2010a). Six grayscale and six colorful medical photos with a size of 512512 are used to evaluate the suggested approach. The watermark has a grayscale watermark with a size of 6464 pixels. MSE, PSNR, BCR, BER, and NCC are used to evaluate the proposed scheme's performance. These metrics are used to assess the watermarked image's accuracy. To test the resilience of the watermarked image, various attacks are used. The grey scale watermarked healthcare images and the watermarked healthcare images with varied attacks are shown in Table 1. To test the robustness and imperceptibility of the suggested approach, several parameters are assessed for watermarked images and watermarked images with varied attacks. Table 2 depicts colored watermarked healthcare photos as well as watermarked healthcare images with various attacks.

Table 1. Gray scale healthcare image outcomes in an experiment.

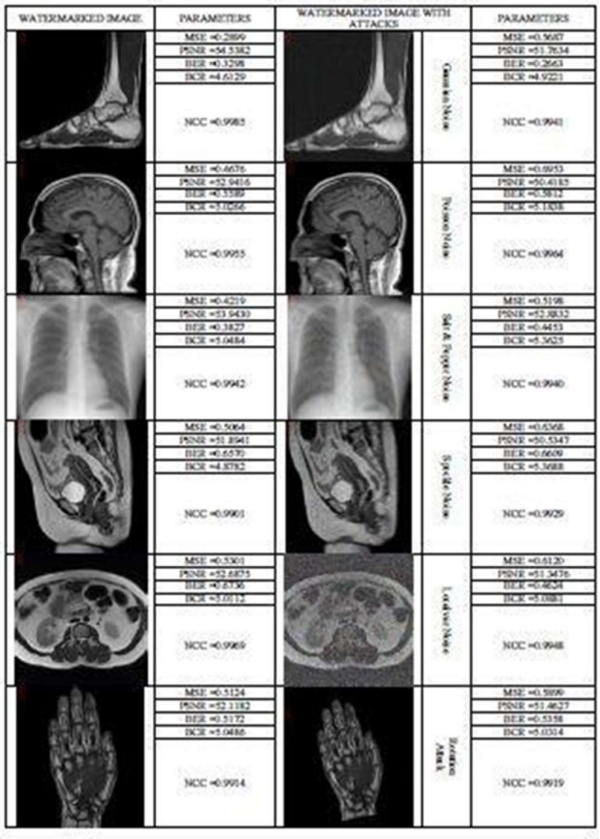
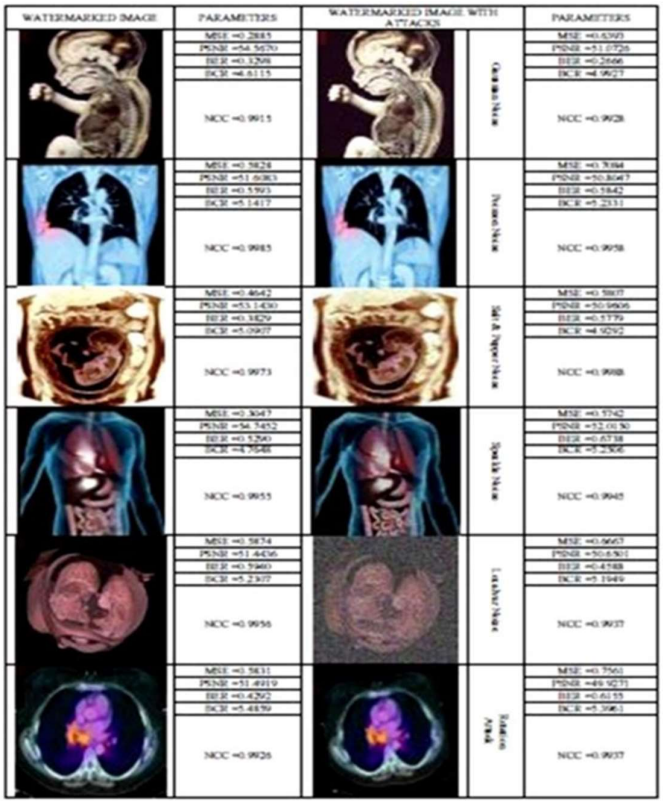


Table 2. Colored healthcare image outcomes in an experiment.



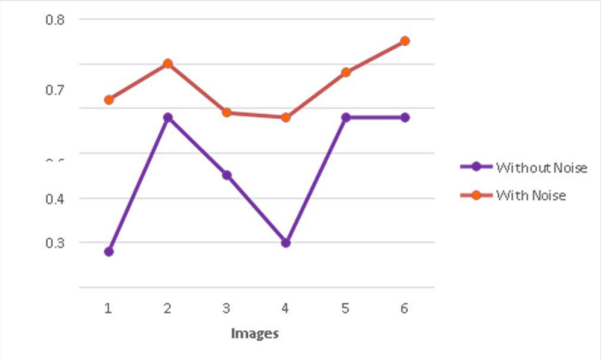


Fig.5. MSE values Graph

Figure 5 shows MSE values for various colored medical pictures. The watermarked photos are subjected to various attacks to determine their robustness. Poisson Noise, Gaussian Noise, Speckle Noise, Salt and Pepper Noise, Rotation Impact, and Localvar Noise are some of the attacks. The MSE values for all watermarked pictures are between 0.3 and 0.7, and the MSE values for all watermarked photos with multiple threats are between 0.6 and 0.9, as shown in the graph above.

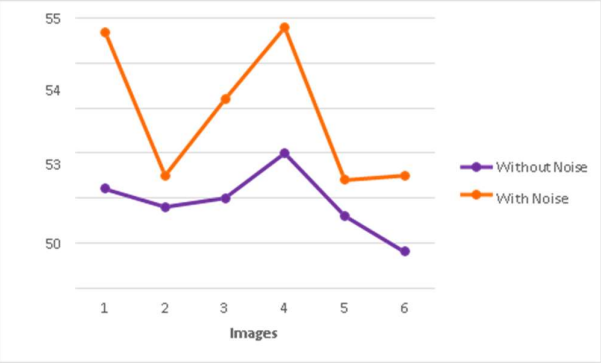


Fig.6. PSNR values Graph

Table 3 compares the proposed scheme with the existing one. MSE with a lower value produces better results. This demonstrates that the proposed system is imperceptible and robust.

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

Figure 6 shows PSNR values for various colored medical pictures. To demonstrate the resilience of the proposed approach, several assaults are used on watermarked photos. Poisson Noise, Gaussian Noise, Speckle Noise, Salt and Pepper Noise, Rotation impact, and Localvar Noise are some of the attacks available. Table 4 compares the proposed scheme with the

existing one. PSNR values for all watermarked photos are between 50 and 54, and PSNR values for all watermarked pictures with various threats are between 51 and 55, as seen

in the graph above. PSNR with a higher value yields better results. This demonstrates that the proposed system is imperceptible and robust.

Table 4. Comparison of results

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

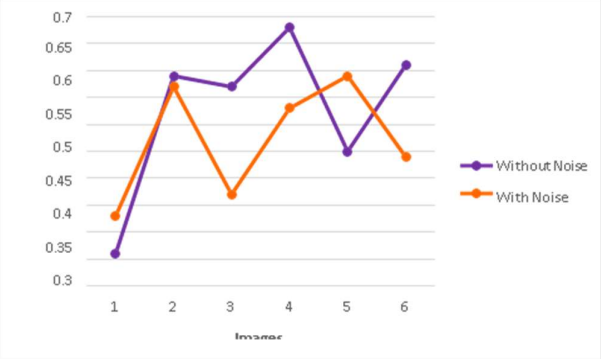


Fig.7. BER values Graph

Figure 7 shows the BER values for various colored healthcare images. The imperceptibility of the suggested method is assessed using parameters from watermarked photos, and the robustness of the approach is assessed using various assaults on these watermarked pictures. The BER values for all photos are between 0.4 and 0.8, as seen in the graph above, and a lower BER value yields better outcomes. This demonstrates that the proposed system is imperceptible and robust.

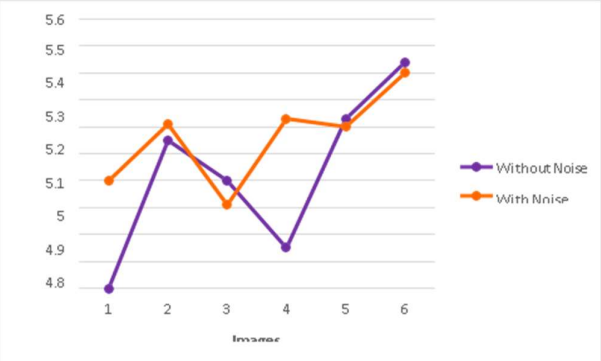


Fig.8. BCR values Graph

Figure 8 shows BCR values for various colored medical pictures. To test the durability of the proposed approach, several assaults are used on the watermarked photos. This robustness means that data may be delivered safely even if it is subjected to a variety of threats. Using various attacks, the implanted watermark may not be effectively changed. Table 5 compares the proposed scheme with the existing one. An embedded watermark is also crucial so that the

image's informational component does not become distorted. The ranges of BCR for watermarked photos and watermarked pictures with varied threats are between 5.4 and 6.5, as seen in the graph above, and a higher BCR value yields better outcomes. This demonstrates that the proposed system is imperceptible and robust.

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

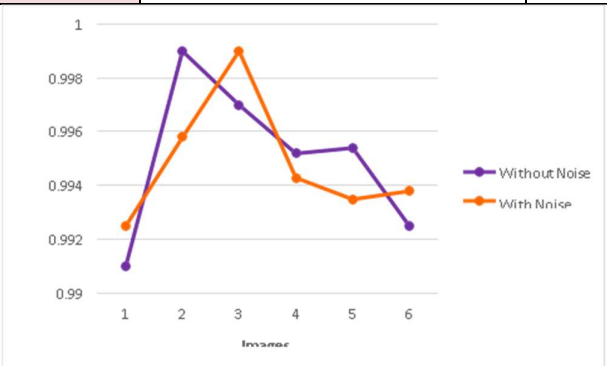


Fig.9. NCC values graph

Figure 9 shows the NCC values for various colored medical imagery. The levels of NCC for all photos are near 1, as can be seen in the graph above, and a greater value of NCC yields better outcomes. This demonstrates the robustness of the suggested method.

4. Conclusion

The higher and lower pass filter values are obtained using DWT in this study. The photos are then trained using a Neural Network. To make the watermark safer, the RSA technique was employed to encrypt it. After that, a Neural Network is used to embed and remove the watermark. Five variables are used to evaluate the results: MSE, NCC, PSNR, BER, and BCR.

Reference

1. Sultan, Kiran, et al. "Reversible and fragile watermarking for medical images." Computational and mathematical methods in medicine 2018 (2018).
2. Shehab, Abdulaziz, et al. "Secure and robust fragile watermarking scheme for medical images." IEEE access 6 (2018): 10269-10278.
3. Bharati, Subrato, et al. "Analysis of DWT, DCT, BFO & PBFO algorithm for the purpose of medical image watermarking." 2018 International Conference on Innovation in Engineering and Technology (ICIET). IEEE, 2018.
4. Assini, Imane, et al. "A robust hybrid watermarking technique for securing medical image." Int. J. Intell. Eng. Syst 11.3 (2018): 169-176.

5. Lakshmi, C., et al. "Encryption and watermark-treated medical image against hacking disease—An immune convention in spatial and frequency domains." Computer Methods and Programs in Biomedicine 159 (2018): 11-21.
6. Swaraja, K. "Medical image region based watermarking for secured telemedicine." Multimedia Tools and Applications 77.21 (2018): 28249-28280.

7. Goléa, Nour El-Houda, and Kamal Eddine Melkemi. "ROI-based fragile watermarking for medical image tamper detection." International Journal of High Performance Computing and Networking 13.2 (2019): 199-210.
8. Wu, Xiaoqi, et al. "Contourlet-DCT based multiple robust watermarkings for medical images." Multimedia Tools and Applications 78.7 (2019): 8463-8480.
9. Favorskaya, Margarita, Eugenia Savchina, and Konstantin Gusev. "Feature-based synchronization correction for multilevel watermarking of medical images." Procedia Computer Science 159 (2019): 1267-1276.
10. Dai, Qianning, et al. "SWT-DCT-based robust watermarking for medical image." Innovation in medicine and healthcare systems, and multimedia. Springer, Singapore, 2019. 93-103.
11. Su, Guo-Dong, Chin-Chen Chang, and Chia-Chen Lin. "Effective self-recovery and tampering localization fragile watermarking for medical images." IEEE Access 8 (2020): 160840-160857.
12. Thakur, Sriti, et al. "Chaotic based secure watermarking approach for medical images." Multimedia Tools and Applications 79.7 (2020): 4263-4276.
13. Soni, Mukesh, and Dileep Kumar. "Wavelet based digital watermarking scheme for medical images." 2020 12th International Conference on Computational Intelligence and Communication Networks (CICN). IEEE, 2020.
14. Anand, Ashima, and Amit Kumar Singh. "An improved DWT-SVD domain watermarking for medical information security." Computer Communications 152 (2020): 72-80.
15. Novamizanti, Ledya, Ida Wahidah, and N. P. D. P. Wardana. "A Robust Medical Images Watermarking Using FDCuT-DCT-SVD." Int. J. Intell. Eng. Syst 13.6 (2020): 266-278.