Image Watermark Embedded Using Dwt, Neural Network and RSA

Sujata Nagpal[1], Dr. Shashi Bhushan[2], Dr. Manish Mahajan[3]

[1]Research Scholar, Department of Information Technology, Chandigarh Engineering College Landran, Mohali, India, E-mail: *nagpalsujata@gmail.com*

[2]Head, Computer Science Engineering Department, Chandigarh Engineering College, Landran India, E-mail: *shashibhushan6@gmail.com*

[3]Head Computer Science Engineering Department, CGC-College of Engineering, Landran, Mohali India, E-mail: *cgccoe.hodcse@gmail.com*

Abstract: The image watermarking is the procedure of hiding a digital picture inside another image for the copyright protection. Watermarking must has to be done in such a way that the original pixel arrangement of the cover image does not get distorted. A lot of previous work has been done in the contrast of effective and secure watermarking. In this paper, we have proposed a novel technique by utilizing DWT, Neural Network and RSA encryption for improving security in watermarking which is enhanced in our proposed model. The results are evaluated utilizing parameters PSNR (Peak Signal to Noise Ratio) and MSE (Mean Squared Error). The whole simulation has been taken place in MATLAB environment.

Keywords: Discrete Wavelet Transform; RSA; Neural Network; Encryption

I. INTRODUCTION

The quick improvement of advanced media gives an awesome comfort to receiving, utilizing, adjusting the data [1]. The advancement in computer network communications creates data transmission generally basic and brisk at the same time, there can likewise be risks of attacks in the computerized media that is being transmitted [2]. There has been an unprecedented development of methods for copyright protection of diverse sorts of information, particularly interactive media data since the 1990s. This has got to be vital as a result of the straightforwardness in advanced duplicating and dispersal. Computerized duplicates can be made like the first flag and later be reused or even controlled. Detectable characteristics of proprietorship or credibility have been utilized for quite a long time as a part of the type of stamps, seals, signatures [3]. Be that as it may, with the present circumstance of information control advances, impalpable computerized imprints are needed [4].

Cryptography [5] is one among the arrangements that were recommended then yet as a rule, particular and expensive equipment is likewise included. There is additionally an expanding requirement for programming and now and again, equipment that takes into consideration security of proprietorship rights. Another issue with cryptography is that, once the information is unscrambled, it will never again be secure [6].

Digital watermarks have been as of late proposed for the verification and copyright protection of audio, video and still pictures [7]. In such applications, the watermark is installed inside of a video frame, cover image, or audio sequence such that resulting modification to the watermarked picture can be distinguished with high likelihood [8]. An advanced watermark is an obvious or imperceptible

recognizable proof code that is for all time inserted in the information and stays exhibit inside of the information even after any decoding procedure [9]. As it were, a computerized watermark is a recognizing bit of data that is held fast to the information that it is proposed to ensure which implies that it ought to be hard to extract or expel the watermark from the watermarked item. The information may be audio, picture or video. On the off chance that the information is replicated, then the data is additionally conveyed in the duplicate [10, 11]. A specific sign may convey a few unique watermarks in the meantime. Since watermarking can be connected to different sorts of information, the intangibility imperative will take distinctive structures, contingent upon the properties of the recipient [12]. Notwithstanding indistinctness, there are some alluring qualities that a watermark ought to have, for example robustness. The watermark ought to be resistible to standard controls which may be purposeful or unexpected and it ought to be factually irremovable.

Digital watermarking could probably be of two categories:

a) Visible watermarking and
b) Invisible watermarking [13].

In visible watermarking, the data is noticeable in the picture or feature. The data may be content or a logo which recognizes the proprietor of the media. In invisible watermarking, data is added as computerized information to picture, audio or video, yet can't be seen [14]. The concealed data can be recognized to some degree.

The idea of computerized watermarking is gotten from steganography [18]. Both steganography and watermarking depict systems that are utilized to keep data by implanting it into the cover information. The systems utilized for steganography are normally not robust against alteration of the information. Computerized watermarking then again ought to be strong against endeavors to uproot the concealed information. A mainstream use of watermarking is verification of proprietorship.

II. IMAGE WATERMARKING

Watermarking a picture is one of the digital data that can be watermarked. A modest procedure might flip the last bit of information representing every single pixel in each photograph [19]. Therefore, the picture will utmost likely not be conspicuously dissimilar as of the unique picture since altering any of blue's, red, or green, smallest significant bit will not impact the picture all that ample. This is applying a watermark in the direction of a spatial domain [20]. There's another method of enhancing a watermark by way of adding it to a frequency domain. For instance, an individual may possibly create a picture which goes by various alterations similar to Fast Fourier Transform in advance on applying some watermark, and then prepare a transposed transformation to acquire the actual picture.

Image watermarking is characterized as the incognito implanting of information into advanced pictures. Despite the fact that watermarking conceals data in any of the advanced Medias, computerized images are the most prevalent as bearer because of their recurrence use on the web. Since the extent of the picture record is immense, it can hide extensive measure of data [21]. HVS (Human Visual System) can't separate the typical image and the image with shrouded information. What's more with that advanced images incorporates substantial measure of abundance bits, pictures transformed into the most popular cover articles for watermarking. Subsequently this exploration uses image as cover file.

In image watermarking the information is hidden exclusively in images, so that outsiders can decrypt information easily [22]. Watermarking helps lot in the field of secret communication. Information embedded in one image is sent from sender side to receiver side in such a process, that it not distinguishable whether image contains important information or not. The files that needed to be sent from sender side can be text, image, and audio [23].Watermark Embedding Technique/algorithm should be imperceptible i.e. embedding watermark should not affect the quality of image. Peak Signal to Noise Ratio (PSNR) and Mean Squared Error (MSE) is calculated between the original image and the corresponding watermarked image to measure of the quality of a watermarked image.

III. 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 methodology of proposed work is given as:

A. Methodology

There are three panels given in the main GUI that are:

1. Training panel

Step 1: First of all, upload base image for training.
Step 2: DWT training applied. The discrete wavelet transform is an awfully valuable means for signal investigation and image processing, principally in multi-resolution demonstration. It can crumble signal into different components in the frequency sphere. The method goes in this manner: A low pass filter in addition to a high pass filter is selected, in such a way that they exactly halve the frequency range between themselves. This particular type of filter pair is entitled as Analysis Filter pair. Initially, low pass filter is implemented for every single row of information, in that way attaining the low frequency components of the row. Now, high pass filter is implemented for similar row of information, as well as correspondingly high pass constituents are disjointed, and then positioned next to the low pass components. This process is implemented for altogether rows.
Step 3: Then apply neural network for training. When performing classification analysis with a set of current information, one communal method, entitled holdout authentication, is to splitting the information inside a larger information group (often 80 percent) for training the neural network and a smaller data set (20 percent) for analyzing the system. Training means discovering the neural network weights and biases that minimize some error value.

2. Testing panel

Step 4: Then go to test panel and upload the test image/cover image from data base
Step 5: Then upload the image to be watermarked.
Step 6: Then apply RSA encryption. RSA stands for Rivest, Shamir, in addition to Adelman, one more names on the designer. RSA can be used pertaining to key alternate along with digital camera signatures and also the encryption associated with tiny blocks associated with files. Currently, RSA is generally utilized to encrypt your procedure key useful for secret key encryption (message integrity) or perhaps your message's hash value (digital signature).
Step 7: Then embed using Neural Network. Neural networks are those networks that are the collection of simple elements which function parallel. A neural network could train to accomplish a

particular operator by regulating values of the weights between elements. Network operator is determined via connections in the middle of elements. There are several activation functions that are used to produce relevant output.
Testing the NN is similar to the training process. After training, the NN is ready for testing using a test dataset. This specific dataset is minor than training dataset to certify that network might detect intrusions it was trained to detect. Likewise test dataset is completed once to conclude performance rate. This specific rate is consists of a distinct detection rate as well as failure rate. The detection rate is how well the network correctly identifies as normal or intrusion. The failure rate is the percentage of misidentified.

3. Extraction panel

Step 8: Upload image.
Step 9: Extract using Neural Network.
Step 10: Evaluate parameters using Neural Network.

B. Flowchart

Fig. 1 represents the flowchart for the proposed method.

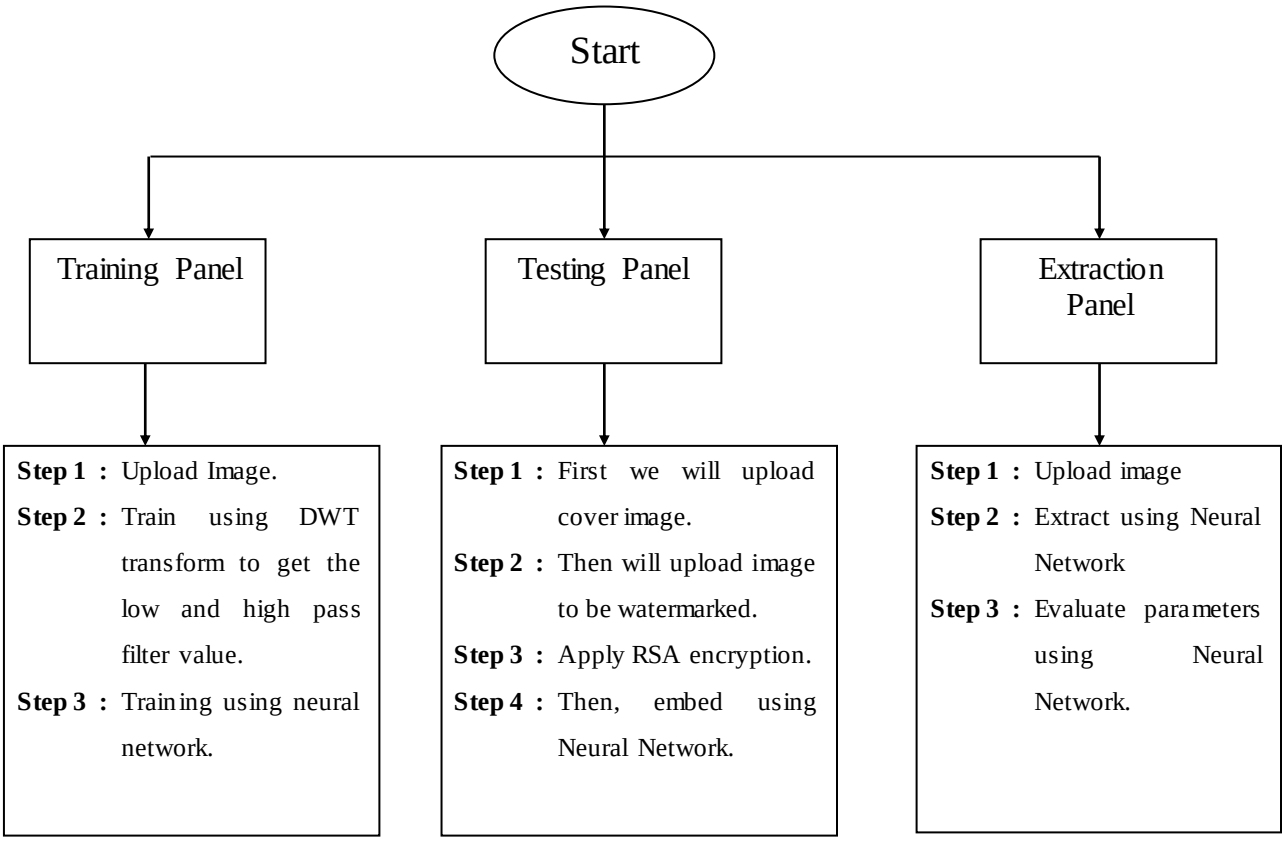

Fig. 1: Flowchart for proposed method

IV. COMPARISON OF RESULTS

A. *Results and Discussion*

The proposed algorithm is implemented in MATLAB. Football image is selected as a cover image. The size of cover image is 512×512. Barbara image is selected as a watermark and the size of watermark is 64×64. In table 1, PSNR and MSE are calculated to measure the performance of the proposed algorithm.

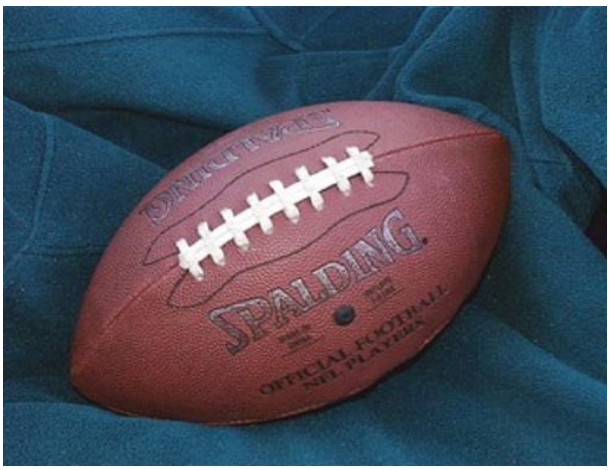

Fig. 2: Cover Image

Fig. 3: Watermark Image

Table 1: PSNR and MSE values with various attacks

Sr. No.	*Type of Attack*	*MSE*	*PSNR*
1.	Watermarked Image	0.3071	54.4358
2.	Salt & Pepper Noise	0.4781	52.6841
3.	Gaussian Noise	0.4180	53.2927
4.	Speckle Noise	0.4781	52.6841
5.	Localvar Noise	0.5973	51.1997
6.	Rotation	0.6496	50.5874
7.	Median Filtering	0.5567	51.6431

Fig. 4 and Fig 5 show the graphical representation of MSE and PSNR values with different attacks. The result of MSE with different attacks lies between 0 and 0.7. The results are better with lower MSE value. The result of PSNR with different attacks lies between 50 and 55. Quality of the image is better with higher PSNR values.

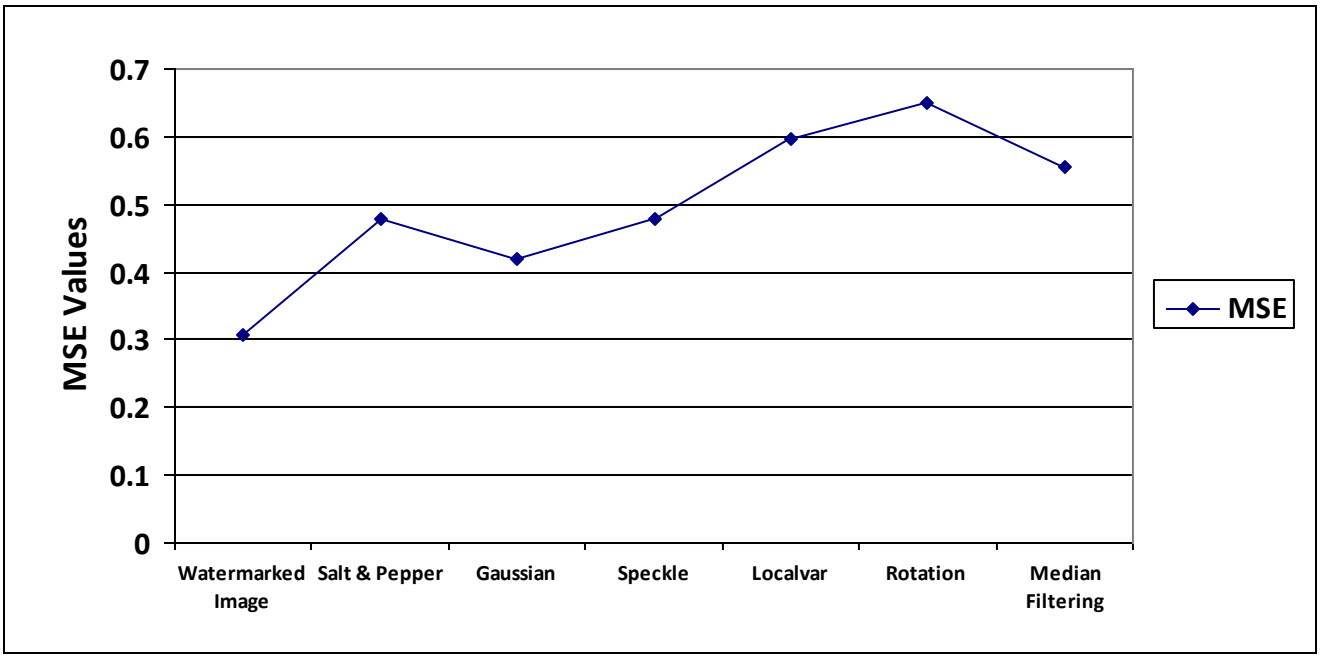

Fig. 4: Graph of MSE values

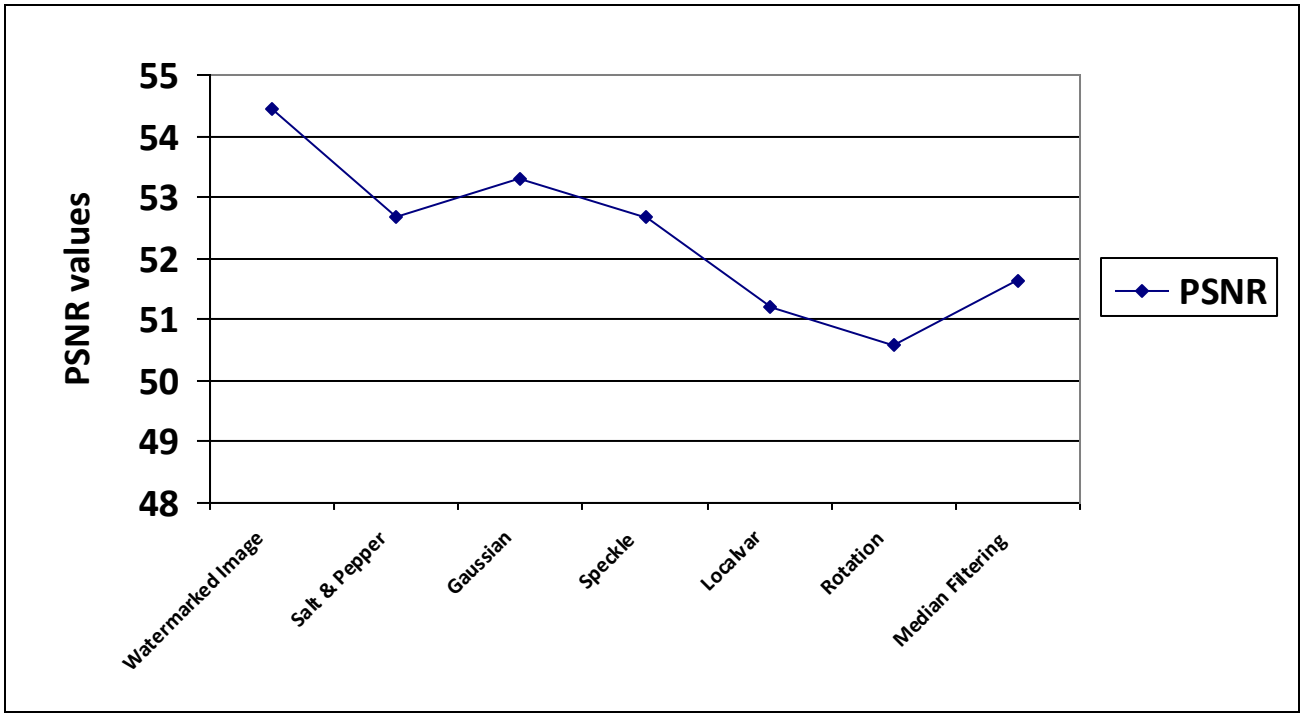

Fig. 5: Graph of PSNR values

The performance of the proposed method is compared with the existing method by using two parameters i.e. MSE and PSNR as shown in table 2[16]. Office_4 image of size 512×512 is chosen as a cover image and Barbara image of size 64×64 is chosen as a watermark.

Table 2: Comparison of existing and proposed scheme

Sr. No.	*Type of Attack*	*MSE(Existing)*	*MSE(Proposed)*	*PSNR(Existing)*	*PSNR(Proposed)*
1.	Watermarked Image	0.9202	0.2631	42.2396	55.1358
2.	Salt & Pepper Noise	0.6455	0.4091	50.1625	53.4134
3.	Median Filtering	0.4468	0.7110	49.6735	50.4502
4.	Rotation	0.6324	0.4126	50.2536	52.8717

Fig. 6 shows the comparison of MSE values of the existing and proposed method. It is observed that MSE values of the proposed method are lesser than the existing method. Lesser the value of MSE better will be the results.

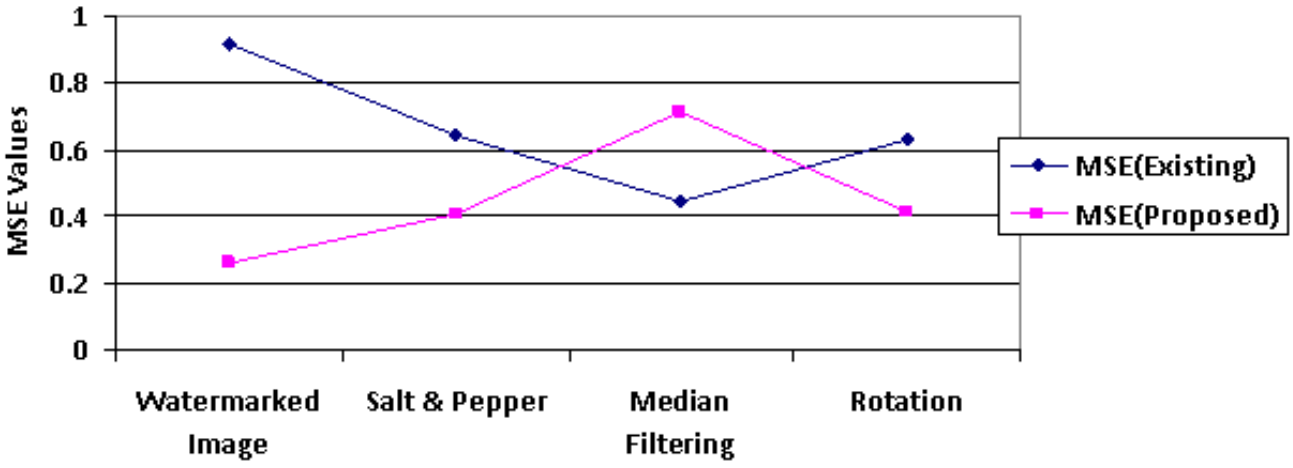

Fig. 6: Comparison of MSE values

Fig. 7 shows the comparison of PSNR values of the existing and proposed method. It is observed that PSNR values of the proposed method are higher than the existing method. Higher the value of PSNR better will be the results.

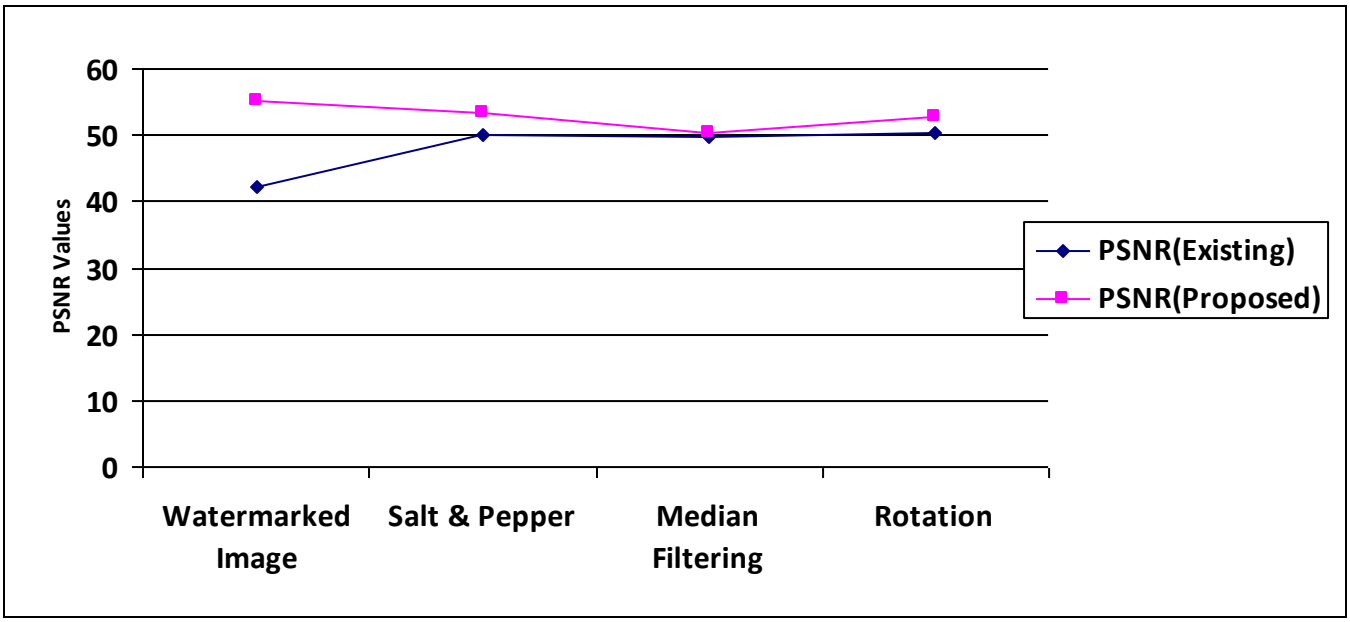

Fig. 7: Comparison of PSNR values

V. CONCLUSION AND FUTURE SCOPE

In the proposed work, we have used hybridization of dwt and neural network for training the images initially. Later we used RSA encryption for encrypting data in the image and then embed it by utilizing technique that is Neural Network. Once testing phase is completed then we have successfully extracted the data from image. By again applying neural network and evaluate their results on the basis of given parameters such as PSNR and MSE. The results obtained shows that we have enhanced results as compared to previous systems utilized. In future we can use hybridization of various algorithms to obtain optimized and much better results.

VI. REFERENCES

[1] R.G. Van Schyndel, A. Z. Tirkel, and C. F. Osborne. (1994). A Digital Watermark. Proc. IEEE 1st International Conference on Image Processing (ICIP 94), Austin TX, vol. 2, Nov. 1994, pp. 86-90, doi: 10.1109/ICIP.1994.413536.

[2] R. liu and T. tan. (2002). An SVD-Based Watermarking Scheme for protecting rightful ownership. vol. 4(1).

[3] S. Kimpan, A. Lasakul and S. Chitwong. (2004). Variable Block Size Based Adaptive Watermarking in Spatial Domain. Proc. IEEE Symp. on Communications and Information Technology (ISCIT 04), vol. 1, Oct. 2004, pp. 374-377, doi: 10.1109/ISCIT.2004.1412871.

[4] Vidyasagar M. Potdar, Song Han and Elizabeth Chang. (2005). A Survey of Digital Image Watermarking Techniques. 3rd IEEE International Conference on Industrial Informatics (ICII 05), Aug. 2005, pp. 709-716, doi: 10.1109/INDIN.2005.1560462.

[5] B. Verma, S. Jain, D.P. Agarwal and A. Phadikar. (2006). A New Color Image Watermarking Scheme. Infocomp Journal of Computer Science, vol. 5, pp. 37-42.

[6] Ruth Buse Dili, Elijah Mwangi. (2007). An Image Watermarking Method Based on the Singular Value Decomposition and the Wavelet Transform. Institute of Electrical and Electronics Engineers(IEEE 07), Sept. 2007, pp. 1-5, doi: 10.1109/AFRCON.2007.4401580.

[7] B.Chandra Mohan, S. Srinivas Kumar. (2008). A Robust Image Watermarking Scheme using Singular Value Decomposition. Journal of Multimedia, vol. 3, pp. 7-15.

[8] Ben Wang, Jinkou Ding, Qiaoyan Wen, Xin Liao and Cuixiang Liu. (2009). An Image Watermarking Algorithm Based On DWT, DCT And SVD. Proc. IEEE IC-NIDC 09, Beijing, Nov. 2009, pp.1034-1038, doi: 10.1109/ICNIDC.2009.5360866.

[9] Chih-Chin Lai and Cheng-Chih Tsai. (2010). Digital Image Watermarking Using Discrete Wavelet Transform and Singular Value Decomposition. IEEE Transactions on Instrumentation and Measurement, Nov. 2010, vol. 59(11), pp. 3060-3063, doi: 10.1109/TIM.2010.2066770.

[10] A. Rajani and Dr. T. Ramashri. (2011). Image Watermarking Algorithm Using DCT, SVD and Edge Detection Technique. International Journal of Engineering Research and Applications(IJERA 11), vol. 1(4), pp. 1828-1834.

[11] Zhen Li, Kim-Hui Yap and Bai-Ying Lei. (2011). A New Blind Robust Image Watermarking Scheme in SVD-DCT Composite Domain. 18th IEEE International Conference on Image Processing(ICIP 11), Brussels, Sept. 2011, pp. 2757-2760. doi:10.1109/ICIP.2011.6116241.

[12] Praful Saxena, Shanon Garg and Arpita Srivastava. (2012). DWT-SVD Semi-Blind Image Watermarking Using High Frequency Band. 2nd International Conference on Computer Science and Information Technology (ICCSIT 12), April 2012, pp. 138-142.

[13] Puneet Kr Sharma and Rajni. (2012). Analysis of Image Watermarking Using Least Significant Bit Algorithm. International Journal of Information Sciences and Techniques (IJIST 12), vol. 2(4), July 2012, pp. 95-101.

[14] Shaikh Rakhshan Anjum and Priyanka Verma. (2012). Performance Evaluation of DWT based Image Watermarking using Error Correcting Codes. International Journal of Advanced Computer Research (IJACR 12), vol. 2(7), Dec. 2012, pp. 151-156.

[15] S. Poongodi and B. Kalaavathi. (2012). Comparative Study of Various Transformations in Robust Watermarking Algorithms. International Journal of Computer Applications, vol. 58(11), pp. 36-42.

[16] Nallagarla Ramamurthy and Dr. S. Varadarajan. (2012). Robust Digital Image Watermarking Scheme with Neural Network and Fuzzy Logic Approach. International Journal of Emerging Technology and Advanced Engineering, vol. 2(9), pp. 555-562.

[17] Ramamurthy Nallagarla and S. Varadarajan. (2012). The Robust Digital Image Watermarking Scheme with Back Propagation Neural Network in DWT Domain. International Conference on Modelling Optimization and Computing, Procedia Engineering, vol. 38, pp. 3769-3778, doi:10.1016/j.proeng.2012.06.432.

[18] Bhupendra Ram. (2013). Digital Image Watermarking Technique Using Discrete Wavelet Transform and Discrete Cosine Transform. International Journal of Advancements in Research & Technology(IJART 13), vol. 2(4), April 2013, pp. 19-27.

[19] Ramandeep Kaur and Sonika Jindal. (2013). Semi-Blind Image Watermarking Using High Frequency Band Based on DWT-SVD. International Conference on Emerging Trends in Engineering and Technology (ICETET 13), Nagpur, Dec. 2013, pp. 19-24, doi: 10.1109/ICETET.2013.5.

[20] Neha Solanki and Sanjay K. Malik. (2014). ROI Based Medical Image Watermarking with Zero Distortion and Enhanced Security. International Journal of Modern Education and Computer Science(IJMECS 14), Oct. 2014, pp. 40-48.

[21] Yu Changhui, Gao Shangbin, Feng Wanli. (2014). Digital Watermarking Technology based on DCT and Neural Net. 7th International Conference on Intelligent Computation Technology and Automation (ICICTA), Changsha, Oct. 2014, pp. 202-205, doi: 10.1109/ICICTA.2014.56.

[22] Rashedul Islam and Jong-Myon Kim. (2014). Reliable RGB Color Image Watermarking using DWT and SVD. 3rd International Conference on Informatics, Electronics and Vision(ICIEV 14), Dhaka, May 2014, pp. 1-4, doi: 10.1109/ICIEV.2014.6850815.

[23] Krishna Rao Kakkirala and Srinivasa Rao Chalamala. (2014). Block Based Robust Blind Image Watermarking Using Discrete Wavelet Transform. International Colloquium on Signal Processing & its Applications(CSPA 14), Kuala Lumpur, March 2014, pp. 58-61, doi: 10.1109/CSPA.2014.6805720.

