Biological and Applied Sciences

Vol.59: e16161070, January-December 2016
http://dx.doi.org/10.1590/1678-4324-2016161070
ISSN 1678-4324 Online Edition

BRAZILIAN ARCHIVES OF
BIOLOGY AND TECHNOLOGY

AN INTERNATIONAL JOURNAL

An Efficient Watermarking Scheme for Medical Data Security With the Aid of Neural Network

K.Kalaivani [1]*.
[1] *Department of Electronics and Instrumentation Engineering, Easwari Engineering College, India.*

ABSTRACT

Digital watermarking has emerged as major technique for ensuring security for various types of data like medical data, digital copyright protection, transaction tracing and so on. With the advancement in digital data distribution over the network there has been increase in the need for protection of such data from unauthorized copying or usages. Watermarking helps in providing the security to some extent. Robustness against any sort of unauthenticated attack is the major requirement of watermarking. In this paper we proposed an efficient watermarking technique for medical data security with the aid of neural network. Usage of neural network is generally used to create and control watermarking strength automatically. This method provides better watermarked data which can be highly secured to unauthorized usage. It is observed that the proposed method provides better security for the multimedia data when compared with other data security methods.

Key words: Digital Watermarking, Medical data security, HVS Model, Discrete Wavelet Transform, Neural network.

*Author for correspondence: kalaivanieec12345eie@gmail.com

INTRODUCTION

The rapid development of computer networks and increased use of multimedia data via the Internet have resulted in fast and convenient exchange of digital information. With the ease of editing and perfect reproduction, the protection of ownership of digital audio, image and video materials become an important concern [1]. Increase in distribution of multimedia content over wired/wireless network is due to the applications like video on demand, video telephony, online photo sharing etc. Since the emerging wired and wireless IP networks are open networks, they are vulnerable to eavesdropping. Thus, confidentiality is especially important for secure multimedia distribution over IP based networks [2]. Because of the convenience and speed of the internet, multimedia data can easily be transmitted, duplicated, and reproduced by pirates. Moreover, with the continual expansion of digital multimedia and the internet, the problem of ownership protection of digital information is increasingly important. Techniques are needed to prevent copying, forgery and unauthorized distribution of images and video [3]. As many advanced tools are readily available to duplicate and modify those data in the Internet easily, security is the major concern, which requires some mechanisms to protect digital multimedia data [4]. The information security technology has two main branches which are commonly used such as cryptography and information hiding. Information hiding is divided into steganography and watermarking [5].

Watermarking refers to the process of adding a hidden structure, called a watermark, into a multimedia data that carries either, the information about the owner of the cover or, the recipient of the original data object. Watermark applications include broadcast monitoring, copy control, transaction tracing, and copyright protection. Robustness, invisibility and security are the three most important properties that need to be satisfied for such applications [6].When watermarking is done by digital means we refer to digital watermarking [7].The digital watermarking is a new developed former technology of information security. There have been many applications for digital watermarking in many fields such as digital images, video, audio and so on. For vector geo-spatial data there were a few studies on the digital watermarking [8]. Image watermarking, video watermarking and audio watermarking are enlisted as categories of Digital watermarking in accordance to the range of application [9]. An important aspect of any Watermarking scheme is its robustness against attacks. The notion of robustness is intuitively clear. Robustness is the capacity of tolerance of attacks on the watermarked data. A watermark is robust if it cannot be impaired after rendering the attack on the data. Based on robustness, watermarking scheme can be divided into fragile, semi-fragile and robust [10]. Some of the applications where digital watermarking can be effectively utilized are Digital copyright protection, Transaction tracing and fingerprinting, Digital content management, Digital content authentication and verification, Lyric sync services [11].

The rest of the paper is organized as follows: Section 2 explains some of the recent researches related to our method. Section 3 explains our proposed methodology that involves HSV, Neural network and watermark embedding. In section 4 the results of the proposed method is discussed. The overall performance of our proposed method is analyzed in Section 5. Section 6 is the concluding remarks of the method.

RELATED WORK

A handful of researches have been done in the field of data security for obtaining the efficient protection of data. Watermarking is a common method used for data protection. Some of the recent researches are mentioned below.

B.Chandra Mohan and S. Srinivas Kumar. [12] have proposed a robust image watermarking scheme for multimedia copyright protection. Here, host image was partitioned into four sub images. Watermark image such as 'logo' was embedded in the two of these sub images, in both D and U components of Singular Value Decomposition of two sub images. Watermark image was embedded in the D component. A copy of the watermark was embedded in the columns of U matrix using comparison of the coefficients of U matrix with respect to the watermark image. If extraction of watermark from D matrix was not complete, there was a fair amount of probability that it could be extracted from U matrix.

Jobin Abraham and Dr.Varghese Paul. [13] have proposed a method for watermarking gray scale images in spatial domain by modifying the least significant bits of the pixels in the image. Data to be embedded is integrated in the image selectively on a subset of pixels using a rule that replaces the LSB's of the image with the watermark signal bits. The method was successful in generating marked copies of the original image with high PSNR value and good visual qualities suitable for distribution via any media or publishing in Internet.

With the rapid development of e-commerce and internet technology, the applications of multimedia products were widely spread. Meanwhile the issue on the security of the copyright has been receiving more and more attention recently. D.Mathivadhani*et al.* [14] have proposed new digital watermarking algorithm. This algorithm uses images and different types of noise were also added. The PSNR for each image was used to measure the efficacy of the algorithm. This objective measure was also used to determine the influence of the better type of noise.The results support the concept that the simpler wavelet transforms and add noise to a signal.

Kaur *et al.* [15] have proposed a DCT based watermarking scheme which provides higher resistance to image processing attacks such as JPEG compression, noise, rotation, translation etc. The watermark was embedded in the mid frequency band of the DCT blocks carrying low frequency components and the high frequency sub band components remain unused. Watermark was inserted by adjusting the DCT coefficients of the image and by using the private key. Watermark could then be extracted using the same private key without resorting to the original image. Performance analysis shows that the watermark was robust.

Pranab Kumar Dhar and Jong-Myon Kim [16] have proposed a watermarking scheme based on Fast Fourier Transformation (FFT) for copyright protection of digital audio. In this watermarking scheme, the original audio was segmented into non-overlapping frames. Watermarks were embedded into the selected prominent peaks of the magnitude spectrum of each frame. Informal listening reveals excellent imperceptibility of the embedded watermark. Simulation results suggest that the imperceptible watermarks embedded with the proposed method were highly robust against various kinds of attacks such as noise addition, cropping, re-sampling, re-quantization, MP3 compression, and low pass filtering.

Reddy *et al.* [17] have proposed a Wavelet based watermarking scheme that hides the mobile signals and messages in the transmission. The proposed method uses the successive even and odd values of a neighborhood to insert the authenticated signals or digital watermark (DW). The digital watermark information was not inserted in the adjacent column and row position of a neighborhood. The proposed method resolves the ambiguity between successive even odd gray values using

LSB method. Hence the method was simpler but difficult to break, which was an essential parameter for any mobile signals and messages.

Image Watermarking has become an important data authentication technique nowadays for images. Watermarking has been accepted as a complementary technology to multimedia encryption, providing some additional level of protection of intellectual property rights.Jahnvi Sen *et al.* [18] have proposed a watermark digital images without distorting the vital regions that are of interest to the customer. Hence, the value of the image was preserved. At the same time, the ownership of the digital image could be proven whenever required on the production of the key by the legal owner, thereby, keeping a check on illegal copying of the copyrighted image.

PROPOSED METHODOLOGY FOR MEDICAL DATA SECURITY USING WATERMARKING

The Medical data security has become a major requirement to avoidunauthorized usage of the data. A means to provide proper data security is yet to be developed. Moreover, medical data security is a major concern considering the fact that various confidential data are transferred through the internet. Watermarking proved to be an efficient method for providing the data security. The major intention this paper is to design an efficient watermarking technique to provide data security with the aid of neural network. The proposed technique makes use of human visual system for providing better invisibility to the watermark data. The first step in the proposed method is watermark embedding. Here the input data is splitted into different blocks and for each block multiwavelet transform is applied. The next process is the application of data to the neural network. The various inputs to the neural network are texture sensitivity, frequency sensitivity, luminance sensitivity and entropy sensitivity. The neural networks are used to create and control watermarking strength automatically. Next inverse transformation is used to obtain watermarked data. The proposed method is explained below in detail.

Human Visual System Model (HVS)

The basic requirement of the watermarking is its robustness against any sort of unauthorized attacks as well as its efficiency. By utilizing the human visual system model in the watermarking process the above requirement can be obtained. Usually human visual system provides the facility that there will be no noticeable difference to the image data even when all the pixel value of images is changed by a certain amount. In human visual system, the sensitivity of the eye to different spatial frequencies is determined by the frequency sensitivity. The threshold of the noise is detected with the help of the luminance sensitivity for a constant background. Whenever the luminance of background changes the corresponding frequency is adjusted.The various sensitivity factors of HVS model are explained below.

➢ Frequency Sensitivity:

The frequency sensitivity forms the basic factor for the Human visual system model. However the low frequency coefficient and the high frequency coefficient of the matrix cannot be used for watermark embedding because at the low frequency coefficient the watermark may change and watermark embedding in high frequency coefficient may remove the watermark from the image after compression. Hence the medium frequencies are used for watermark embedding. The medium frequency provides better watermark embedding which cannot be removed while image compression.

➢ Luminance Sensitivity:

The luminance sensitivity measures the brightness of an image. Generally brightness helps in identifying the noise in the image background. The luminance sensitivity is expressed as *Ls* and it is calculated using the expression,

$$Ls = \left(\frac{K_{DC,n}}{K_{DC}'} \right)^{\gamma} \qquad (1)$$

Where $K_{DC,n}$ is the DC coefficient of *nth* block of the discrete wavelet transform and K_{DC}' is the mean value of all the DC coefficients of the image and γ is a constant value to control the degree of luminance sensitivity.

- Texture Sensitivity:

The texture sensitivity of an image can be calculated by quantizing the values of the image using quantization table. The value obtained has to be rounded off to its nearest integer. The formula for calculating texture sensitivity is shown below,

$$Ts = \sum_{a,b=1}^{N} Rnd\left[\frac{K_n(a,b)}{Q(a,b)} \right] \qquad (2)$$

Where (*a*,*b*) represents the point in the *nth* block and *Rnd*[ ] represents the rounded value of result.

- Entropy sensitivity:

The amount of information in an image is represented by the entropy value and it plays a major role in classification of the image block. The entropy sensitivity is calculated using the expression given below,

$$Es = \sum_{a,b=1}^{N} K_n(a,b) \bullet \log \frac{1}{K_n(a,b)} \qquad (3)$$

Using these formulas we can calculate the entropy sensitivity. These sensitivity values are used as the input to the neural network. The next section explains about the neural network technique for watermarking.

Neural Network Application in Watermarking

Generally the neural networks are trained such that the input has to deliver a specified output. The neural network has greater compatibility with the human visual system. The Back propagation Neural Network is employed in the proposed method with Levenberg-Marquardt algorithm for training. In a neural network there are three layers namely input layer, hidden layer and output layer. The major reason behind the usage of the neural network is to provide an output with maximum watermarking strength. The figure 1 given below shows the general back propagation neural network architecture with the input layer, hidden layer and the output layer.

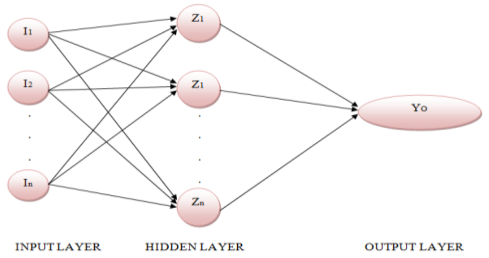

Figure 1: General Back propagation Neural Network Architecture.

The application of Levenberg-Marquardt to neural network training provides lots of possibility for an improved training process.This algorithm has been shown to be the fastest and easiest method for training the back propagation neural networks. It also has an efficient implementation in MATLAB software, since the solution of the matrix equation is a built-in function, so its attributes become even more pronounced in a MATLAB environment. The feature components are the frequency, luminance, texture and entropy sensitivity values. These sensitivity values are fed as the input to the input layer of the neural network. These are then fed to the hidden layer using the activation function and then to the output layer. During these training in neural network using Levenberg Marquardt algorithm, an image 'I' is divided into (m x n) blocks of pixels. Each block is then scanned to form an input vector G(x) of size (m x n) .It is assumed that the hidden layer of the layer network consists of N neurons and it is characterized by an appropriately selected weight matrix ‘ω’. The entire blocks of the original image is passed through the hidden layer to obtain the hidden signals H(x), which represent encoded input image blocks G(x). The learning process is repeated a number of time until the errors in the outputs are reduced. The neural network thus creates an invisible watermarking with maximum power. Hence neural network can be utilized for generating watermarking with more efficient and powerful against authentication.

Watermark Embedding

Watermark embedding is the process of embedding the watermark to an image for providing security from unauthorized usage. In watermark embedding the first step is to apply the DWT to the input image. The technique is used to decompose the color spaces into different frequency bands using the filters. The watermark size determines the selection of the frequency bands in the corresponding color space of the image. This will provide additional resistance to the image. The watermarking is encoded continuously on the image from beginning to last coefficients of the medium frequency band which can provide maximum robustness against the distortion. After this decomposition of the image into blocks the next step is to choose the size of the watermark (NxN) where the value of N varies based on the number frequency bands utilized.

In order to maintain the robustness of the image against the various distortions which the image can undergo, we use an insertion force without affecting the basic requirement like robustness and invisibility. This force depends on the characteristics of the zones of insertion and must be lower than a visual threshold of perceptibility. Neural network applied to digital watermark embedded process simulates human visual characteristic to determine the maximum watermark embedded intensity as the frequency selected for the process is the mid frequency. The embedding process steps are at first the input image is decomposed into color channels. Then to these decomposed image channel DWT is applied to decompose it into number of frequency bands. The size of the watermark determines the number of color spaces and the frequency bands for embedded watermarking. The flow diagram of watermark embedding is shown in figure 2

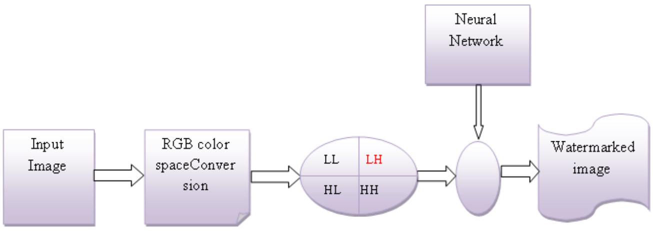

Figure 2: Watermark Embedding

The output expression for the embedded image is given as in the eqn (4),

$$E_{a,b,n} = C_{a,b,n}\left(1+\omega_{a,b,n} WM_{a,b,n}\right) \qquad (4)$$

where $E_{a,b,n}$ is the embedded output of position (a,b) of the *n*th block of the image, $C_{a,b,n}$ is the DWT coefficient of position (a,b) of the *n*th block of the image, $\omega_{a,b,n}$ is the adaptive weight of the watermark at position (a,b) of the *n*th block of the image and $WM_{a,b,n}$ is the watermark at position (a,b) of the *n*th block of the image.

Watermark Extraction

The watermark which is embedded in the image can be extracted by applying the inverse process for the embedded technique. In watermark extraction, the first step is to convert the watermarked image into colorspaces.Then apply DWT to decompose the corresponding color space of the image in which the watermark is embedded. Next by using the same process as used in watermarking the weights are computed from the original image. The flow diagram for the watermark extraction process is as shown in figure 3.

As shown in figure 3, the watermarked image is then used as the input for the watermark extraction process. The inverse procedure used for the watermark embedding in used for the extraction process. The watermarked image in then applied for the color space decomposition where the color spaces are separated from the watermarked image. After the RGB color space conversion of the watermarked image, DWT is applied to decompose the respective color space of the cover image at different bands in which watermark is hidden. Using this process the image can be extracted. The above process is repeated for each of the band where the watermark image is embedded. Thus we obtain the original input image applied for the watermark embedding process without any variation in the quality as well as the features. The expression for the watermark extraction is as given in eqn (5),

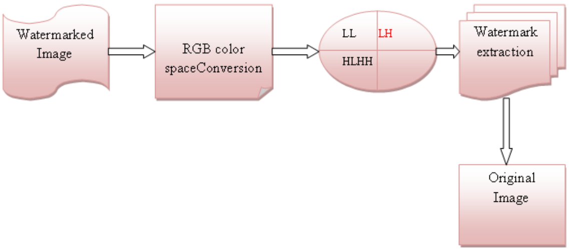

Figure3: Watermark Extraction

$$WM_C = \left(C_{a,b,n} - C^*_{a,b,n}\right) / \left(\omega_{a,b,n} \bullet C_{a,b,n}\right) \qquad (5)$$

Where $C^{*}_{a,b,n}$ is the DWT coefficient of the corrupted image at position *(a,b)*, WM_{C} is the corrupted watermark and $\omega_{a,b,n}$ is the adaptive weight of the watermark at position (a,b) of the *n*th block of the image. Using this expression the watermark in the image can be extracted from the watermarked image.

RESULTSAND DISCUSSION

The proposed method for data security of the medical data using watermarking was implemented in the working platform of MATLAB . The Watermarking is embedded in the input images and the upcoming result of the proposed work has been shown in figure 4.

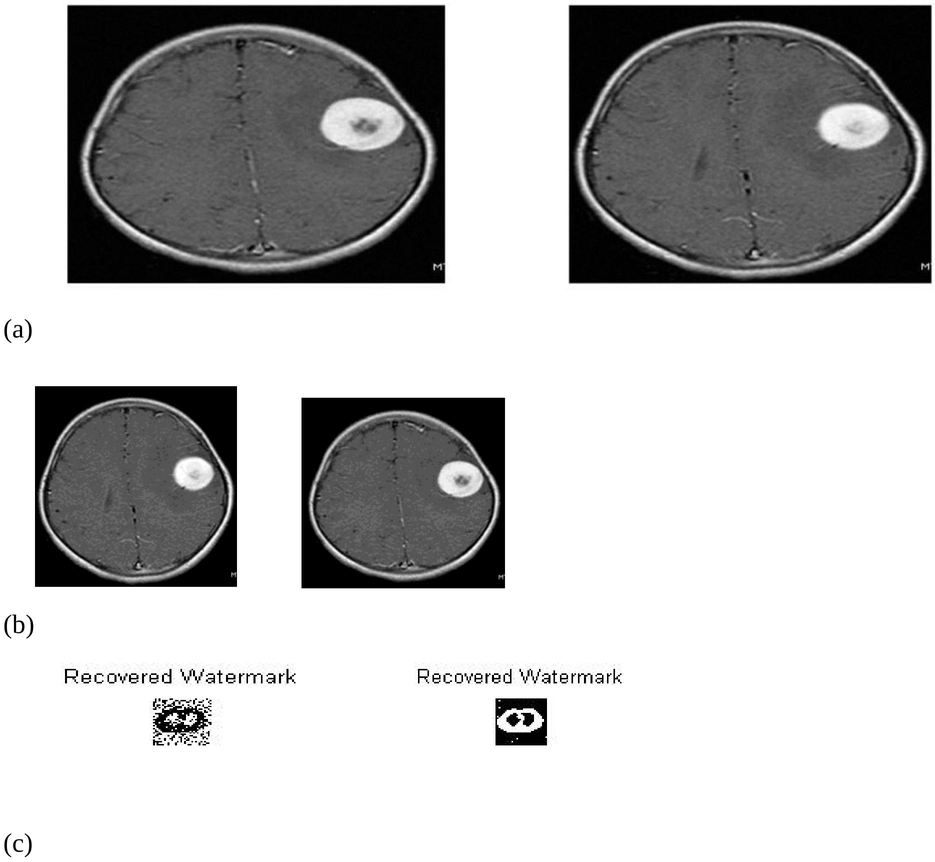

Figure 4. (a) Original medical images of human brain, (b) Watermarked image, (c) Recovered Watermark.

The figure4(a) shows the medical image for brain (an1 and an2) in which the proposed watermarking technique is applied. The DWT is applied for these images, trained with the neural network method and then proposed watermarking technique is applied to get the watermarked image as shown in figure4 (b) for the corresponding images.Figure 4 (c) shows the recovered watermark images from the watermarked image. The result shows that the proposed watermarking process proved to be more stable and can be utilized for high secure data to ensure authorized usage.

The same procedure is repeated for the lung images (N1 and N2) as shown in figure 5.

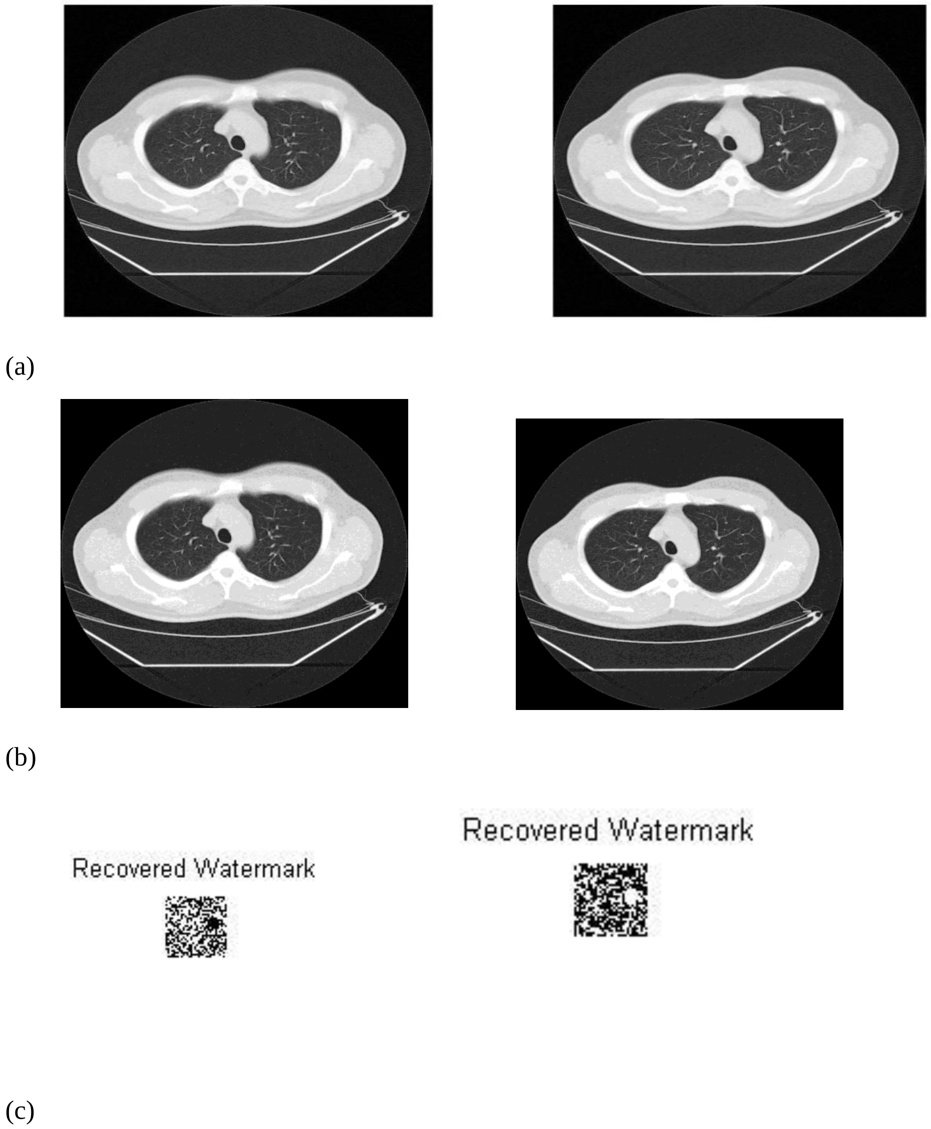

Figure 5: (a) Original medical image of human lungs (N1 and N2), (b) Watermarked image, (c) Recovered Watermark.

Figure5 shows the second set of images of human lungs (N1 and N2) where the proposed method of the watermarked images is applied. The figure5(a) shows the medical images for human lungs (N1 and N2). The DWT is applied for these images, trained with the neural network method and then proposed watermarking technique is applied to get the watermarked image as shown in figure5 (b) for the corresponding images. Figure5 (c) shows the recovered watermark images from the watermarked image. The result shows that the proposed watermark process proved to be more stable and can be utilized for high secure data to provide unauthorized usage.

PERFORMANCE ANALYSIS

The table 1 shows the NC (normalized correlation) and the PSNR value for the watermarked images for the two medical images examined.

Table 1: Normalized correlation (NC) and PSNR value for the medical images**.**

Medical images	Normalized correlation (NC)	PSNR
an1	0.9842	35.3143
an2	0.7498	33.3925
N1	0.8577	34.08
N2	0.8278	34.083

PSNR values for the watermarked images are calculated for each input image using the formula,

$$PSNR = 10\log_{10}\frac{D^2}{S_E} \quad (6)$$

where 'D 'is the maximum variations in input images and 'S_E 'is the mean square error of the watermarked images which is calculated using the expression given below,

$$S_E = \frac{1}{PQ}\sum_{a=0}^{P-1}\sum_{b=0}^{Q-1}\left(g(a,b) - g'(a,b)\right)^2 \quad (7)$$

where P x Q is the size of the image, $g(a,b)$ is the pixel intensity of the original image and $g'(a,b)$is the pixel intensity of the watermarked image.Using the formula the mean square error value is calculated.

The PSNR values of proposed method is then compared with existing method like ROI based watermarking using LSB technique [19] and it is estimated that proposed method proved to deliver better PSNR values.The comparison is shown in Table 2.

In Table 2,the PSNR value of the proposed method is compared with the existing methodto prove the performance of proposed method. As shown in the Table 2, the PSNR value of the proposed method proved to be better when compared with the existing method .

The Figure 6 shown which represents the graphical view of the PSNR value for both the existing and the proposed method based on the values given in the Table 2. The graph illustrates that the PSNR value is improved in proposed method.

Table 2 : Comparison of Proposed method with Existing Method

Watermarked images	**PSNR Proposed Method**	**Existing Method**
an1	35.3143	24.08
an2	33.3925	24.07
N1	34.08	24.77
N2	34.083	24.79

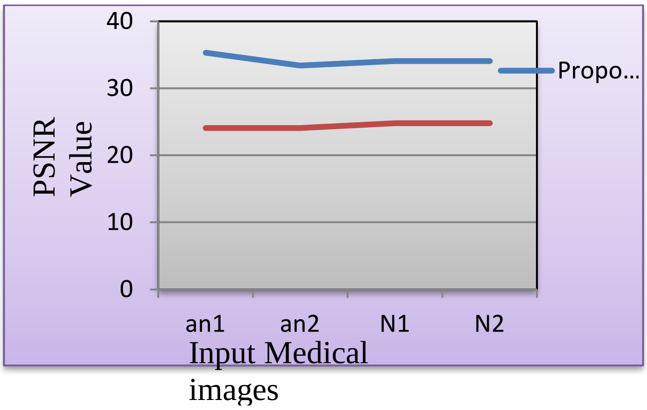

Figure 6 : Graphical representation of PSNR value for proposed and existing methods.

CONCLUSION

In this paper, a new method of watermarking for medical data security with the aid of neural network is described. Here the neural network is employed with the Levenberg-Marquardtalgorithminorder to improve the control of watermarking strength and also for improving the performance of conventional watermarking technique. Simulation result indicates the proposed method proves to be more efficient when compared to the previous methods used for data security. The watermark extraction provided in the proposed method proved to provide the image which does not vary from its original image. The result shows that the proposed watermark process proved to be more stable and can be utilized for high security to the data to assure authorized usage.

REFERENCES

Yongdong Wu and Hweehua Pang, “A Lightweight Buyer-Seller Watermarking Protocol", Journal of Advances in Multimedia, Vol.2008, No. 2, Jan 2008.

Nidhi S Kulkarni, Balasubramanian Raman, and IndraGupta,"Selective Encryption Of Multimedia Images", In.Proc.of National Systems Conference, NSC,Dec 2008.

Chi-Hung Fan, Hui-Yu Huang And Wen-Hsing Hsu ,"A Robust Watermarking Technique Resistant JPEG Compression", Journal Of Information Science And Engineering,Vol.27,pp.163-180,2011.

V.Santhi and Dr.ArunkumarThangavelu ,"DWT-SVD Combined Full Band Robust Watermarking Technique for Color Images in YUV Color Space", International Journal of Computer Theory and Engineering, Vol. 1, No. 4,pp.424-429, Oct 2009.

K. VenkataRamana, Dr.B.RaveendraBabu and Sri Ch.RatnaBabu, "A Randomized Secure Data Hiding Algorithm Using File Hybridization for Information Security", International Journal on Computer Science and Engineering,Vol. 3, No. 5,pp.1878-1889, May 2011.

Emad E. Abdallah, A. Ben Hamza and Prabir Bhattacharya," Video watermarking using wavelet transform and tensor algebra", Journal of Signal Image and Video Processing ,Vol.4,No. 2, pp. 233-245,2010.

EmanuilRednicAnd Andrei Toma,"Security Management in a Multimedia System", Journal of Applied Quantitative Methods, Vol.4, No.2, pp.237-247, 2009.

Chang-Qing Zhu, Cheng-Song Yang And Qi-Sheng Wang, "A Watermarking Algorithm For Vector Geo-Spatial Data Based On Integer Wavelet Transform",In.proc.of the International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences, Vol. 37,Beijing, 2008.

A.Umaamaheshvari and K.Thanushkodi ,"High Performance and Effective Watermarking Scheme for Medical Images", European Journal of Scientific Research, Vol.67, No.2, pp.283-293, 2012.

Dr. Swati Sherekar, Dr.V.M.Thakare and Dr. Sanjeev Jain ,"Attacks and Countermeasures on Digital Watermarks: Classification, Implications, Benchmarks", International Journal Of Computer Science And Applications Vol. 4, No. 2, Jun-Jul 2011.

Hebah H.O. Nasereddin, "Digital Watermarking A Technology Overview", International Journal of Research and Reviews in Applied Sciences, Vol.6, No.1, pp.89-93, Jan 2011.

B.Chandra Mohan and S. Srinivas Kumar ,"A Robust Image Watermarking Scheme using Singular Value Decomposition", Journal Of Multimedia, Vol. 3, No. 1,pp.7-15, May 2008.

Jobin Abraham and Dr.VarghesePaul,"Watermarking Grayscale Images using Text for Copyright Protection", International Journal of Computer Applications, Vol.31,No.9,pp.0975–8887, Oct 2011.

D.Mathivadhani and Dr.C.Meena ,"Performance Evaluation of Key for Watermarking Using 2-D Wavelet Transformations", International Journal of Engineering Science and Technology,Vol.3 No. 3,pp.1959-1966, Mar 2011.

Blossom Kaur, Amandeep Kaur and Jasdeep Singh ,"Steganographic Approach For Hiding Image In Dct Domain", International Journal of Advances in Engineering & Technology, Vol. 1,No.3,pp.72-78,Jul 2011.

Pranab Kumar Dhar and Jong-Myon Kim, "Digital Watermarking Scheme Based on Fast Fourier Transformation for Audio Copyright Protection", International Journal of Security and Its Applications, Vol. 5, No. 2, Apr 2011.

Dr.B.Eswara Reddy, P.Harini, S.MaruthuPerumal& Dr.V.VijayaKumar,"A New Wavelet Based Digital Watermarking Method for Authenticated Mobile Signals", International Journal of Image Processing (IJIP), Vol.5, No.1, 2011.

Jahnvi Sen ,A.M. Sen and K. Hemachandran ,"An Algorithm For Digital Watermarking Of Still Images For Copyright Protection", Indian Journal of Computer Science and Engineering,Vol.3, No.1,pp.46-52, Feb-Mar 2012.

A Lavanya and V Natarajan,"Enhancing security of DICOM images during storage and transmission in distributed environment", Indian Academy of Sciences, Vol. 36, pp.515–523, 2011.

Received: February 03, 2016;
Accepted: July 14, 2016