Digital Image Watermarking Techniques Using Artificial Intelligence

A Project Report submitted in fulfillment of the requirement for the award of the degree of

Master of Technology

in

Computer Science & Engineering

Under the Supervision of

Dr. Amit Kumar Singh

(Supervisor)

Dr. Pardeep Kumar

(Co-Supervisor)

By

Aditi Zear

Enrollment No: 142208

Jaypee University of Information Technology, Waknaghat, Solan, Himachal Pradesh-India 173234

Certificate

This is to certify that thesis report entitled **"Digital Image Watermarking Using Artificial Intelligence Techniques"**, submitted by **Aditi Zear** in fulfillment for the award of degree of Master of Technology in Computer Science & Engineering to Jaypee University of Information Technology, Waknaghat, Solan has been made under my supervision.

This work has not been submitted partially or fully to any other University or Institute for the award of this or any other degree or diploma.

Supervisor's Name - Dr. Amit Kumar Singh

Dated:

Signature

Co-Supervisor's Name - Dr. Pardeep Kumar

Dated:

Signature

Acknowledgement

I would like to take this opportunity to acknowledge all those who helped me during this report work. Compiling a year's work into this was an exhausting job, but writing this page of acknowledgement is a joyous task to cherish the memories of all those who helped me to enrich the newer experience of life.

At the very onset, I bow my head with reverence and dedicatedly accord my recondite and gratitude to "ALMIGHTY", the merciful and compassionate, whose grace, glory and blessings allowed me to complete this endeavor and without his encouragement and co-operation it would have never been possible for me to achieve this.

I owe my deep sense of respect and heart felt gratitude to my major supervisor ***Dr. Amit Kumar Singh, Assistant Professor, Computer Science and Engineering Department, Jaypee University of Information Technology*** for his meticulous and sagacious guidance, sympathetic encouragement, precise and constructive criticism and ever willing help throughout the course of this investigation as well as in the preparation of manuscript. I will always remain indebted to him for his unending guidance and untiring efforts in successful completion of this work. I consider myself fortunate to have worked under his able guidance.

I am highly obliged and grateful to co–supervisor, ***Dr. Pardeep Kumar, Assistant Professor, Computer Science and Engineering Department, Jaypee University of Information Technology*** for his valuable suggestion sand co-operation throughout my research work. I express my sincere and whole hearted thanks to him for rendering help and moral support.

I am thankful to office staff of the department for providing all the necessary and timely help. I am also thankful to respondents of my study for their co-operation who helped me to complete my study.

I wish to express my sincere thanks to all my friends for their support and guidance. There is paucity of words to express my heartiest thank to my friends ***Ms Kshitiza Vasudeva*** and ***Ms. Swati Sharma*** for their timely help, best wishes and cheerful company remained a morale booster and made things smother throughout the course of this study.

I owe my achievements to the unconditional love and support of my parents whose sacrifice I can never repay. They inspired me at every step of my life and encouraged me to never give up even in the face of overwhelming odds. I grope for words to express my deep feelings, love and affection to my younger brother.

Last but not least I would like to express my gratitude to all those who have helped, guided and supported me in one way or the other but have been inadvertently left out because all may not have been mentioned but none have been forgotten.

Needless to say, omissions are mine.

Name of the student- Aditi Zear

Dated:

Signature

Table of Content

List of Figures

List of Tables

List of Symbols

SN	Symbol	Description
1	I(m,n)	Cover Image
2	I'(m,n)	Watermarked Image
3	I_{max}	Maximum possible value of image pixel
4	W(i,j)	Original Watermark Image
5	W'(i,j)	Extracted Watermark Image
6.	X_k	current vector of weights and biases
7.	a_k	learning rate
8.	g_k	current gradient
9.	J	Jacobian matrix
10.	J^T	transpose of Jacobian matrix
11.	E	Vector of network errors.
12.	A_c	SVD decomposition of cover image.
13.	A_w	SVD decomposition of watermark image
14.	A_{wat}	SVD decomposition of watermarked image
15.	S_c	Singular matrix of cover image.
16.	S_w	Singular matrix of watermark image
17.	S_{wat}	Singular matrix of watermarked image
18.	S_w^*	Singular matrix of extracted watermark
19.	A(x,y)	DWT coefficients before embedding text watermark
20.	A'(x,y)	DWT coefficients after embedding text watermark
21.	Wbt	Text watermarking bits before embedding
22.	Wbt'	Extracted Text watermarking bits

List of Acronyms

Sr. no.	Acronym	Description
1	AI	Artificial Intelligence
2	DCT	Discrete Cosine Transform
3	DWT	Discrete Wavelet Transform
4	DFT	Discrete Fourier Transform
5	SVD	Singular Value Decomposition
6	GA	Genetic Algorithm
7	DE	Differential Evolution
8	PSO	Particle Swarm Optimizer
9	NN	Neural Network
10	FNN	Feed Forward Neural Network
11	BPNN	Back Propagation Neural Network
12	PSNR	Peak Signal To Noise Ratio
13	MSE	Mean Square Error
14	NC	Normalized Correlation
15	LM	Levenburg-Marquardt
16	EPR	Electronic Patient Record

Abstract

In the digital information age, digital documents such as text, image, audio, video and 3D computer graphics models can be easily copied, manipulated and distributed over the open channel. Recently, many innovative techniques have been widely used to protect the multimedia data transmission, storage, sharing and processing of digital contents. The main objectives behind attacks can be to alter, modify, or delete the digital contents to illegally claim ownership or preventing the information transfer to intended recipients. The digital watermarking techniques offer a valuable solution to these challenges/issues. The watermarking is a data hiding technique for inserting digital information, also known as watermark, into digital documents, which can be later extracted or detected for the purposes of identification and authentication in many applications. Robustness, imperceptibility, capacity, security and computational cost are the major benchmark parameters for general watermarking system**.** However, there exists some trade-off between these parameters of the watermark. Therefore, some optimization techniques are required to balance these benchmark parameters. In recent years, different artificial intelligent techniques are used as an optimization technique to offer the optimal balance between visual quality of the watermarked image and the robustness of the extracted watermark. The thesis is divided into six different chapters. Chapter wise description of the thesis report is described as follows:

Chapter 1 presents the basic concept of data hiding techniques, classification of watermarks, important characteristics and recent applications, Watermarking techniques in spatial and transform domain along with major benchmark performance parameters which include peak signal to noise ratio (PSNR), normalized correlation (NC), and bit error rate (BER) of the watermark algorithms. In addition, different Artificial Intelligence techniques such as Genetic Algorithm (GA), Particle Swarm Optimizer (PSO), Differential Evolution (DE), and Neural Networks (NN) are also introduced in this chapter.

Chapter 2 presents a brief review of various reported watermarking techniques and the performance of the techniques is compared in tabular form. Various Artificial intelligence techniques are used in different ways in combination with watermarking techniques to improve various performance factors are discussed in this chapter.

Chapter 3 presents a color image watermarking method using fusion of DWT and SVD instead of DWT or SVD applied individually. Further, the robustness of the extracted watermark is enhanced by using Back Propagation Neural Network (BPNN) training. The performance of the proposed method has been tested for different gain, size of watermark, different cover image modalities and known signal processing attacks. In addition, the proposed method offer better robustness performance than other reported techniques.

Further, a DWT, DCT, SVD and BPNN based multiple image watermarking method is presented for healthcare applications in **Chapter 4**. The performance of the proposed method has been tested for different gain, size of watermark, different cover image modalities and known signal processing attacks.

For identity authentication purpose in various applications, multiple watermarks in the form of image and text have been embedding in to the some multimedia object in **Chapter 5**. The proposed method using the fusion of DWT, DCT and SVD instead of DWT, DCT or SVD applied individually or the combination of DWT/DCT, DCT/SVD or DWT/SVD. The image watermark is scrambled by using Arnold transform before embedding into the cover which provides the extra level of security. Further, two different text watermarks in the form of symptom and signature are embedded into the cover object. Based on the robustness requirements, the more important watermark are embedded into the higher level DWT sub-bands and the less important watermarks are embedded into the lower level DWT sub-bands. The symptom watermarks is first compressed by arithmetic coding and the signature watermark is encoded by Hamming error correcting code before embedding into the cover media. The performance of the proposed method is evaluated for different gain factor, text watermark size and cover image modalities. Experimental results are provided to illustrate that the proposed method is able to withstand a known attacks. Hence, the proposed watermarking methods effectively solve various issues related health information management such as authentication, security, capacity, storage and bandwidth requirements.

Finally, findings of the thesis and future directions are presented in **Chapter 6**.

Chapter 1

Digital Image Watermarking: An Introduction

1.1 Introduction

From last few decades growth in technology of computers and computer networks provides quality of service and higher bandwidth for both wireless and wired networks. However the representation of media in digital form and evolution of internet also made easy to transmit digital media such as image, audio, video in an effortless way. These advancements also raised some security related issues for the protection of multimedia data and require some data hiding techniques. The goal of data hiding is not to restrict the access to host signal, but to ensure that the embedded data should be inviolate and recoverable. There are two techniques for data hiding: Steganography and Watermarking [1-2]. **Steganography** is defined as the technique of hiding communication, the hidden content is embedded in some cover media so that there will not be any eavesdropper's suspicion. **Watermarking** is one of the new methods that provide protection against various attacks, data authentication and security to digital media. It is the process of embedding secret information in the form of signal called watermark into digital media (i.e. image, audio and video) so that this secret information can detected and extracted out to check the real owner or identity of digital media. Watermarking is similar to steganography with additional requirement of robustness. In watermarking system watermark is embedded in such a way that it cannot be altered without making whole cover media meaningless [3-4]

1.2. Applications of Digital Watermarking

Digital watermarks are playing important role in various applications described below [3-4]:

1. **Copyright Protection:** Watermarking is used for the protection of copyrighted material over unsecure network. Networks like internet or peer-to-peer (p2p) networks have watermarking technologies to detect the copyrighted material from these networks.

2. **Content Archiving:** Watermarking can be used to add an identifier or serial number for archiving digital objects such as images, audio and video. Usually filenames are used as identifier for classifying digital objects which are fragile and can be easily changed. Therefore watermarks can be effectively used as identifier for classification and reduces tampering.
3. **Meta-data Insertion:** Watermarks can be used to insert metadata which is used to describe data. Images are used in search engines are labeled with their content. Photographs are used by journalists to insert story of their news. In medical application x-rays store patient information.
4. **Broadcast Monitoring:** It refers to the technique of checking whether the content that is broadcasted is same as the content that was expected to be broadcasted. Watermarking has major application in monitoring advertisement broadcasting.
5. **Tamper Detection:** Fragile watermarks are used to detect tampering and unauthorized access. It has important application in protecting sensitive data like satellite and medical images. Tamper detection is also used in court to prove whether the image is tampered or not.

1.3. Characteristics of Watermarking

The important characteristics of watermark are described below [3-4]:

1. **Robustness:** It is the ability in which watermark should survive from various signal processing, geometrical and malicious attacks.
2. **Imperceptibility:** The watermark should not be observed or seen by human and only be detected by watermark extraction process.
3. **Verifiability:** Watermark should provide full evidence of the owner of copyright protected digital data. It can be used for authentication and control illegal copying.
4. **Security:** The watermark should be secure so that any hacker cannot remove watermark without knowing the embedding algorithm and strength of watermark. This is usually achieved by security keys which can be either asymmetric keys or symmetric key.
5. **Computational cost:** Watermarking method should not be complex so that its computational cost remains less. If watermarking algorithms are very complex they require more computational cost.

6. **Capacity and data payload:** Capacity can be defined as maximum amount of information in the form of watermark that can be embedded in host image. Number of watermark bits in message is called data payload and number of times this data payload is repeated is called watermark capacity.

These characteristics are very important because based on them various watermarking techniques are classified. The performance of these watermarking techniques is evaluated based on important factors which are robustness and imperceptibility.

1.4. Performance Measures

The performance of digital image watermarking techniques is evaluated on the basis of some performance factors which are imperceptibility of watermarked image and robustness of extracted image and text watermark. Both of them are measured using PSNR and NC values [3-4].

1. **PSNR** determines the visual quality of the watermarked image. The PSNR (peak signal to noise ratio) is used to determine the degradation in the embedded image with respect to the host image. PSNR values between the original image (I(m,n)) and watermarked image ($I'(m,n)$) calculated by the formula as:

$$\mathrm{PSNR} = 10\log_{10}\left(\frac{(I_{max})^2}{\mathrm{MSE}}\right) \quad (1)$$

$$\mathrm{MSE} = \frac{1}{MN}\sum_{m=0}^{M-1}\sum_{n=0}^{N-1}[I(m,n) - I'(m,n)]^2 \quad (2)$$

2. **Normalized Correlation (NC)** is used to judge the robustness of the extracted watermark. The NC between the original watermark ($W(i,j)$) and extracted one ($W'(i,j)$) is defined by

$$\mathrm{NC} = \frac{\sum_i \sum_j W(i,j)W'(i,j)}{\sum_i \sum_j [W(i,j)]^2} \quad (3)$$

3. **Bit Error Rate (BER)** is used to evaluate the performance of text\string watermarks, where each string character is evaluated in the form of bits [5]. BER is defined as the ratio between number of incorrectly decoded bits and total number of bits.

$$\mathrm{BER} = \frac{(\text{Number of incorrectly decoded bits})}{(\text{Total no of bits})} \quad (4)$$

However, there exists a tradeoff between robustness and imperceptibility. Robustness is achieved when modifications made to host image by watermark are significantly large. It also affects the imperceptibility of the image because these modifications can be seen by human eyes. Therefore some optimization techniques are required to balance these performance factors.

Recently Artificial Intelligence techniques have been used to balance robustness and imperceptibility. Artificial intelligence techniques are used as an optimization technique to search optimal sub-bands and coefficients in transform domain to embed watermark with different scaling factors. Various AI techniques which can be used are Genetic Algorithm (GA), Particle Swarm Optimizer (PSO), Differential Evolution (DE), and Neural Networks (NN) [6-8]. GA, PSO and DE can be used to search the sub-bands, coefficients to find where to embed the watermark and then to find optimal scaling factors for different sub bands of an image. NN can be used in different ways. One way is to find the changeable threshold values of transform coefficients and another variation is they can be used to remove interference that affects watermarks [9-11].

1.5. Watermarking Techniques

The watermarking techniques can be classified on the basis of permanency, visibility, detection and domain. According to domain, watermarking techniques can be classified as spatial domain and transform domain techniques [12-13].

1.5.1. Spatial Domain Watermarking

It works by embedding watermark by modifying values of pixels. It is simple technique and requires less time and computational complexity. But this technique is less robust against attacks. Table 1.1 describes the comparison between some important spatial domain techniques. Various spatial domain techniques are [14-15]:

1. **Least significant bit (LSB):** It is commonly used spatial domain technique in which randomly pixels of cover image are selected and watermark is embedded in least significant bits. For e.g.

   Image: 10001000 10101001 11100011 11001100

   Watermark: 1 0 0 1

   Watermarked image: 1000100**1** 1010100**0** 1110001**0** 1100110**1**

2. **Predictive Coding Schemes:** This technique is more robust as compared to LSB. In this technique correlation between adjacent pixels is found. First set of pixels need to be embedded with watermark is taken and then difference between adjacent pixels is used to replace alternate pixels. At the receiver end cipher key is used for the retrieval of watermark.
3. **Correlation-Based Techniques**: In this technique a pseudo-random noise is added to an image and during decoding a correlation between two is found. If correlation value exceeds some threshold level watermark is found otherwise it is not. Let Iw represents watermarked image, pseudo-random noise W(x,y) can be added to cover image I using following equation:

   $$Iw(x,y) = I(x,y) + K*W(x,y) \quad (5)$$

   Here K is Gain factor. If we increase the value of K, the robustness of watermarked image increases but quality of image decreases.
4. **Patchwork Techniques:** This technique partitions image into two subsets. Some operation is then applied to these subsets in opposite direction. For example if one subset is decreased by factor x, the other subset should be increased by same amount.

Table 1.1: Comparison of Spatial Domain Watermarking Techniques

Considered Paremeters	LSB	Correlation Based	Patchwork Algorthm
Imperceptibility	High perceptual imperceptibility	Imperceptibility depends upon gain factor i.e. low gain factor results in high imperceptibility and vice versa.	Better imperceptibility
Robustness	Lacks robustness, vulnerable to noise, cropping, scaling etc	Like imperceptibility robustness also depends upon gain factor i.e. high gain factor results in more robustness	Robust against most type of attacks
Information Amount	Amount of information embedded depends on choosing the subset of image pixels	Amount of information embedded depends upon gain factor	Embed small amount of information

1.5.2. Transform Domain Watermarking

Spatial domain watermarking techniques are simple and easy to implement however they are not robust and also they do not allow further processing in order to increase the robustness of watermark. Transform domain techniques provide more robustness as compared to spatial domain techniques. In these techniques host image is converted into transform domain and then watermark is embedded in transform coefficients. To obtain watermarked image inverse transform is performed. Table 1.2 describes the comparison between some important transform domain techniques. Various transform domain techniques are [14-15]:

1. **Discrete Cosine Transform (DCT):** DCT of digital image provides frequency-space representation of an image by separating into different frequencies, low, high and middle frequency coefficients. Figure 1.1 shows the Discrete Cosine Region after applying DCT to image. The embedding of watermark data into middle frequency coefficients gives additional resistance to the lossy compression techniques, while avoiding significant modifications in cover image. DCT has also very good energy compaction property [16-18]. DCT coefficients for an input image (I) of size N×N are computed according to Eq. (1). D (i, j) is the DCT coefficient in row i and column j of the DCT matrix and I (x, y) is the intensity of the pixel in row x and column y of the image [13-15].

$$d(i,j) = \frac{1}{\sqrt{2N}} C(i)\, C(j) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} I(x,y) \cos\frac{(2x+1)i\pi}{2N} \cos\frac{(2y+1)i\pi}{2N} \quad (6)$$

$C(i), C(j) = \frac{1}{\sqrt{N}}$ for i, j = 0 and $C(i), C(j) = \sqrt{\frac{2}{N}}$ for i, j = 1,2,.....N-1

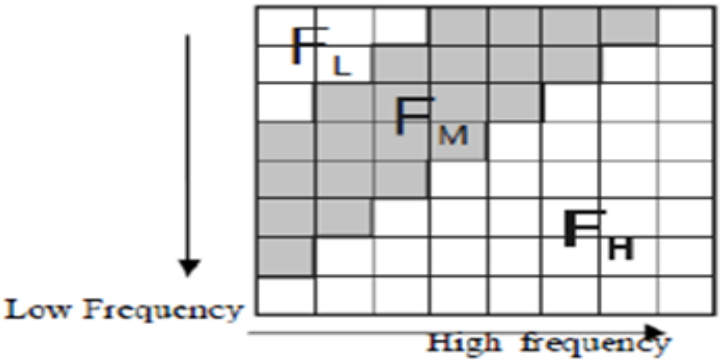


Figure 1.1: Discrete Cosine Transform Region [13-15]

2. **Discrete Wavelet Transform (DWT):** DWT of digital image provides multi-resolution representation of an image which helps in interpreting image information [19-20]. It transforms the two-dimensional digital image into four quadrants of different frequencies i.e. LL1, LH1, HL1, HH1 [21-22]. Figure 1.2 shows the two-level DWT decomposition of host image. The low frequency part LL1 can be split again into more quadrants of high and low frequencies i.e. LL2, LH2, HL2 and HH2. LL2 can be further decomposed into LL3, LH3, HL3 and HH3 until the signal is fully decomposed shown in Figure 2. The coefficients obtained by applying DWT to host image (H) are [13-15]:

$$H_{LL}^{I} = \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} g(x)\, g(y)\, H_{LL}^{I-1}(2u - x)(2v - y) \quad (7)$$

$$H_{LH}^{I} = \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} g(x)\, h(y)\, H_{LL}^{I-1}(2u - x)(2v - y) \quad (8)$$

$$H_{HL}^{I} = \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} h(x)\, g(y)\, H_{LL}^{I-1}(2u - x)(2v - y) \quad (9)$$

$$H_{HH}^{I} = \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} h(x)\, h(y)\, H_{LL}^{I-1}(2u - x)(2v - y) \quad (10)$$

Here u, v =1, 2, 3….. N-1, I is the level of DWT transform and h(n), g(n) are the impulse responses.

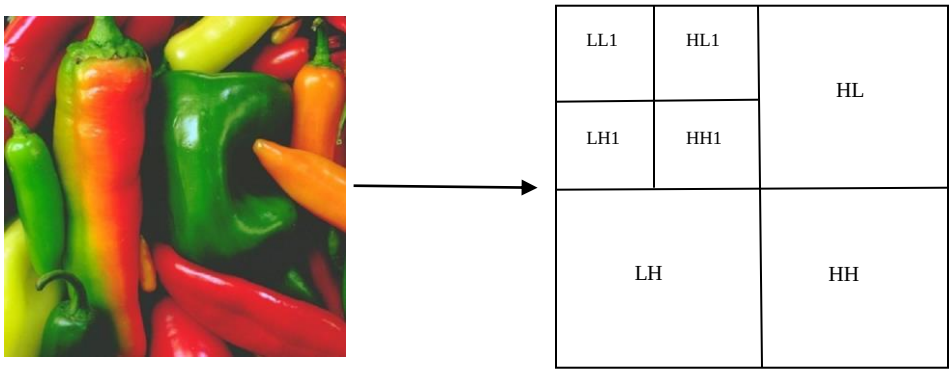


Figure 1.2: Two level DWT decomposition of host image [13-15]

Table 1.2: Comparison of Transform Domain Watermarking Techniques

Considered Parameters	DCT	DWT	DFT
Complexity	Computational cost and time is more as compared to spatial domain techniques	Computational cost and time is more as compared to DCT	Computational cost and time is more as compared to both DCT and DWT
Representation	Frequency space representation of image	Spatial and frequency representation of image	Phase and magnitude representation of image
Blocking Artefact	Present in higher compression ratios	Not present	Not present
Energy Compaction	Present because most of visually significant information is concentrated in few coefficients	Not present	Not present
Multi resolution property	Not present	Present i.e image can be shown from low to high resolution	Not present
Strongest components (for robustness)	Low frequency F_L band	Low frequency band (LL)	Central component (low frequency)
Resistance against Geometrical attacks	Not resistant	Not resistant	Resistant
Effect of change in transform coefficient	Affects entire image except it is implemented using block based approach	Affects image locally because of its property of spatial frequency locality	Full frame transform, affects entire image

3. **Singular Value Decomposition:** It decomposes matrix of host image into 3 rectangular matrices i.e. U, S and transpose (T) of V. SVD is very efficient in representing the intrinsic properties of an image. U and V are orthogonal square matrices in which columns are left and right singular vectors. S is diagonal matrix whose diagonal entries are singular values and in descending order [23-24]. These singular values represent the brightness of an image. The singular values are obtained by taking the square root of the eigen values of AA^T and A^TA. Let A is the square matrix then SVD can be represented as [24-25]:

$$A = USV^T \tag{11}$$

The relation between SVD and eigen values are given below:

$$AA^T = UDV^T(UDV^T)^T = UDV^T VDU^T = UD^2U^T \tag{12}$$

$$A^TA = (UDV^T)^TUDV^T = VDU^T UDV^T = VD^2V^T \tag{13}$$

Thus, U and V are calculated as the eigen vectors of AA^T and A^TA respectively. The square root of eigen values are the singular values along the diagonal of matrix D. If

the matrix A is real, then the singular values are always real number, and U and V are also real.

4. **Discrete Fourier Transform (DFT):** DFT provides robustness against various geometrical attacks like rotation, scaling, translation etc. DFT decomposes image into sine and cosine form. DFT magnitude and phase coefficients are modified while embedding watermark. DFT is translation invariant because any kind of spatial shifts affects the phase representation of an image and the magnitude representation remains unaffected [13-15].

1.6. Artificial Intelligence Techniques

AI techniques in digital image watermarking are basically used to remove the tradeoff between the two important performance factors i.e. robustness and imperceptibility of image. Some of these AI techniques are discussed below:

1.6.1. Back Propagation Neural Network

A typical neural network consists of an input layer, hidden layers and output layer. Number of nodes in input layer is determined by number of input and output variables. Each node is fully connected to its adjacent layers through links. Each link has weighting value to represent relational degree between two nodes. In BPNN output signal are compared with target and error is back propagated through output layer as shown in Figure 3.3. Before training network weights and biases have to be initialized [10-11]. Different algorithms for training BPNN are steepest descent method, adaptive learning rate, conjugate gradient, quasi-Newton and Levenburg-Marquardt (LM) algorithm. Gradient of performance function is used by all these algorithms to adjust weights to minimize the performance function. This gradient is determined using back propagation i.e. performing computations backward through network. The iteration of back propagation learning algorithm can be written as [26-27]:

$$X_{k+1} = X_k - a_k g_k \tag{12}$$

Here X_k is current vector of weights and biases, a_k is learning rate and g_k is current gradient. Like quasi-Newton algorithm, LM algorithm approach second order training speed without computing Hessian matrix. The Hessian matrix (H) can be approximated as [26]

$$H = J^T J \quad (13)$$

The gradient (g) can be calculated as

$$g = J^T e \quad (14)$$

Here J is the Jacobian matrix which contains first order derivative of network errors with respect to biases and weights. J^T is transpose of Jacobian matrix and e is vector of network errors.

The LM algorithm uses following Newton like update to approximate the Hessian matrix:

$$x_{k+1} = x_k - [J^T J + \mu I]^{-1} J^T e \quad (15)$$

here μ is a scalar which is used to determine whether gradient descent with smaller step size or Newton's method using Hessian matrix will be used. If μ = 0, it becomes Newton's method otherwise it becomes gradient descent with smaller step size [28-29].

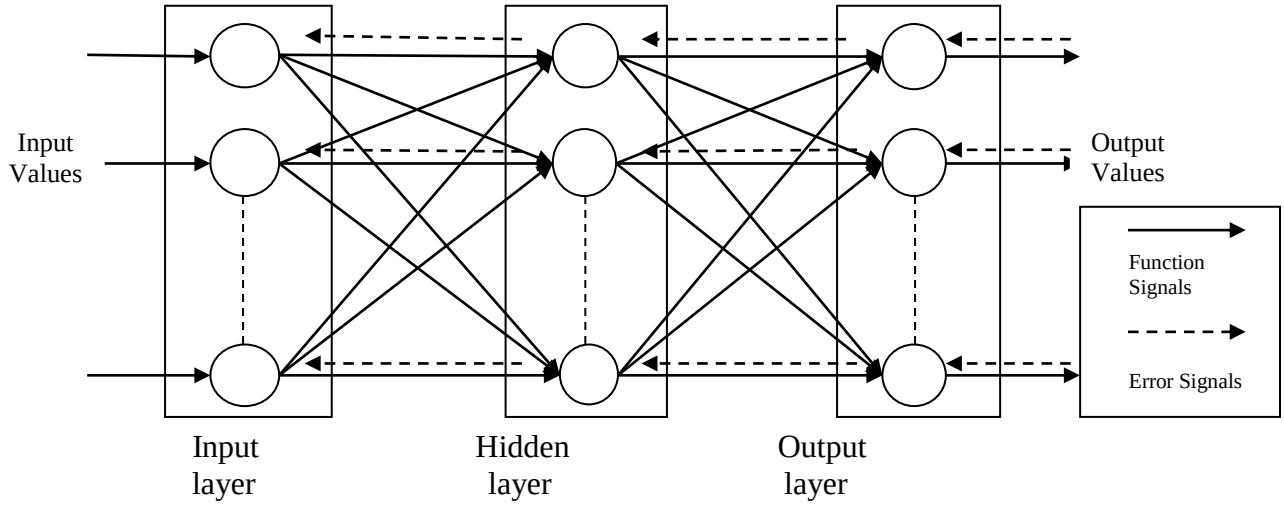


Figure 1.3: Back Propagation Neural Network

1.6.2. Genetic Algorithm

Genetic Algorithm (GA) is widely used as an optimization technique. It is a searching algorithm based on natural selection and genetics. GA uses population, which is composed of group of chromosomes to represent solution of system. Then fitness function is used to evaluate the fitness of each chromosome. Particular group of chromosomes is chosen to be parents and offspring are generated from these parents by using genetic operators which are crossover and mutation. Fitness of offspring is evaluated which decides whether selected offspring will replace current population or not. Operators of genetic algorithm are Initialization, Evaluation, Reproduction,

Crossover, and Mutation [6-8]. This GA cycle is repeated until some termination criteria for e.g. maximum number of generations, objective value below threshold [8].

1.6.3. Differential Evolution

Differential Evolution (DE) is optimization algorithm that can be used to minimize non-differentiable and non-linear continuous functions with real-valued parameters. It resembles the structure of evolutionary algorithm, but differs in generation of new candidate solutions and by its use of greedy selection scheme. It basically consists of three operators, Mutation, Crossover and selection. In mutation three distinct individuals from current population are selected to produce perturbed individual corresponding to target individual [8-9]. Crossover is performed on perturbed individual and target individual to generate trial individual. After that in selection process the fitness of trial individual is calculated and compared with the target individual. If trail individual is better than target individual it will be replaced for next generation otherwise it continues with target individual [9].

1.6.4. Particle Swarm Optimizer

It is an evolutionary scheme based on particles that perform. Like other evolutionary algorithms, a population of particles is randomly generated then by using iterative search optimum is found. Each particle is associated with velocity vector and position vector. Then based on position, velocity, and fitness criteria best position in swarm is found for each particle [7-8].

Chapter 2
Literature Survey

2.1 Review of Digital Image Watermarking using AI techniques

Artificial techniques have been used as optimization techniques in combination with various watermarking techniques in order to improve the performance of watermarking algorithms. Table 2.1 summarizes the performance of digital image watermarking using AI techniques. Review of image watermarking techniques using AI techniques is carried out and presented below:

Wei et al. [6] proposed a new approach for optimization in 8*8 DCT domains using genetic algorithm (GA) to improve the robustness and imperceptibility of image spread spectrum watermark algorithm. AC coefficients have been modified to embed spread spectrum watermark. These coefficients have been chose by GA in different bands to find best suitable AC coefficients for image with different characteristics. The experiment results show that the method is tested against signal processing attacks. The method is robust and achieved good image quality for different attacks. Nilchi et al [10]. presented a non-blind robust image watermarking technique based on DCT and Full Counter Propagation Neural Network (FCNN). FCNN has been used to simulate the perceptual characteristics of the original image. These perceptual features of the original image have been used to determine highest changeable threshold values of DCT coefficients and to embed watermark binary image. The watermarking algorithm has very good robustness to JPEG compression attacks as compared to other attacks. Aslantas et al. [7] introduced an optimal DWT-SVD based image watermarking technique using Particle Swarm Optimizer (PSO). In this scheme host image has been decomposed into sub bands and after that singular values of each sub band of host image have been modified by different scaling factors to embed watermark image. These modifications have been optimized using PSO to obtain highest robustness and transparency. Experimental results show that this scheme has given good results as compared to methods that use single scaling factor.

Lai et al. [30] introduced an image watermarking scheme using SVD and micro-genetic algorithm. The values of scaling factors has been obtained and optimized by means of micro-genetic algorithm to embed watermark. Watermark has been embedded by

modifying singular values of cover image by multiple scaling factors. The experimental results show that watermark is robust with highest NC value equal to 1. Aslantas et al. [8] proposed Intelligent Optimization Algorithms (IOA) namely Genetic Algorithm (GA), Differential Evolution (DE) and Particle Swarm Optimization (PSO) to improve performance of fragile watermarking based on DCT. In embedding process after modifying the least significant bits of transformation coefficients, these coefficients when transformed from frequency domain to spatial domain produces some round off errors. These errors have been corrected by intelligent optimization algorithms. Experimental results show that GA, DE and PSO have similar performance. Kumsawat et al. [31] proposed a blind digital image watermarking scheme in multi wavelet domain. In this scheme embedding method has been based on quantization index modulation technique. Genetic algorithm has been used as an optimization technique and used to search for optimal quantization steps to improve robustness of watermark and quality of watermarked image. Experimental results show that watermark is robust to common attacks such as median filtering, Gaussian filtering, image rotation etc.

Veysel Aslantas [9], presented a scheme for developing a robust image watermarking without losing the transparency using SVD watermarking method. The singular values of host image have been modified by multiple scaling factors. These modifications have been optimized using DE to achieve robustness and transparency. Experimental results obtained from this method show improvement in transparency and robustness for various signal processing attacks. This method has also been found superior over the use of constant scaling factor and even better than the results of using Genetic Algorithm. Poonam et al. [32] presented a method to improve robustness and imperceptibleness in watermarking. The singular values of 3^{rd} level DWT approximation matrix of original image has been embedded with the singular values of watermark. Genetic algorithm has been used as an optimization algorithm to optimize scaling factors with which watermark should be embedded in host image. Fitness function in this algorithm takes two values PSNR and correlation. Experimental results show that increase in scaling factors results in better performance in terms of robustness by keeping image quality to reasonable levels.

Lai et al. [33] introduced watermarking technique that uses SVD and GA. Singular values of cover image have been modified by multiple scaling factors to embed watermark. Genetic Algorithm has been used to search proper values to satisfy both imperceptibility and robustness requirements. Experimental results show that proposed scheme survived successfully after various signal processing attacks and also outperformed other similar works. Vafaei et al. [34] proposed a blind watermarking method in discrete wavelet transform domain based on neural networks. Artificial neural networks have been used to adjust the watermark strength. Binary image as watermark has been embedded repetitively into selected wavelet coefficients. Feed Forward Neural Networks satisfactorily maximize watermark strength using proper trainings by being adaptive based on knowledge of block features. Thus proposed method has high robustness and imperceptibility to different types of attacks such as cropping, filtering etc.

Chaudhary et al. [35] presented a new method for adaptive watermark strength optimization in DCT domain. Genetic Algorithm has been used to select DCT sub band and Particle Swarm Optimization (PSO) has been used as an optimization technique to intelligently select watermark strength. The proposed scheme shows better performance for imperceptibility and robustness tests. Ali et al. [36] proposed a technique using SVD and Differential Evolution in DCT domain. The original image has been partitioned into blocks and these blocks have been transformed into DCT domain. Then DCT coefficients of each block have been collected and a low-resolution approximation image has been constructed. SVD has been applied on this approximation image and its singular values have been modified with singular values of watermark. DE algorithm identifies best multiple scaling factors for embedding to achieve robustness without compromising quality of image. The watermark has been scrambled by Arnold Transform before embedding. Experiment results show that proposed technique yields strong robustness to geometrical and image processing attacks and imperceptibility is also promising.

Ali et al. [37] proposed an innovative watermarking scheme based on Differential Evolution and DWT-SVD transform domain. During embedding process host image has been transformed into sub bands of different frequencies by 3rd level DWT then watermarked image has been scaled down with multiple scaling factors and embedded in singular value matrix of LL and HH sub bands of host image to make watermark

invisible and robust. DE has been used to search these optimal scaling factors. To overcome false positive problem watermark has been embedded in lossless manner. Watermark has been used to generate secret key instead of embedding it to host image. Experimental results shows that this method not only guarantees imperceptibility but also provide strong robustness. Han et al. [38] proposed a new watermarking method based on host image analysis using SVD and Genetic Algorithm. This method has enhanced embedding capacity of watermark in order to embed more watermarks in host image and having same visual effect. Genetic algorithm has been used in embedding process to improve the image quality, security and robustness of watermarked image. Algorithm also satisfies an optimal compromise between robustness and image quality. Threshold T has been used to control embedding rate. Experiments ensured that this scheme has achieved imperceptibility and good robustness to general signal processing attacks.

Yen et al. [11] proposed a scheme to suppress the interference affecting watermarks. Watermarks have been embedded in host image using DCT technique. After that various common interferences such as salt-and-pepper noise, Gaussian noise, clipping and rotation have been used to destroy the watermarked image. Back Propagation Neural Network algorithm when combined with DCT watermarking scheme has been used to suppress these interferences that affect watermarks. The simulation results demonstrate the effectiveness of this technique in restoring watermarked image. Hu et.al [39] proposed a color image blind watermarking algorithm based on BPNN and wavelet significant tree. Using Ycbcr color image model, wavelet significant tree can be found by decomposing luminance component with wavelet. After that correlativity among the nodes of wavelet significant tree has been defined by non-linear relationship found using trained Back Propagation Neural Network (BPNN). Based on this relationship, watermark has been embedded into wavelet significant trees. During extraction the watermark the watermark has been extracted without original image. Experimental results demonstrate that this scheme has good transparency and robustness as compared to some other algorithms.

Mohananthin et al. [40] introduced DWT based digital image watermarking techniques using BPNN and human visual system (HVS). BPNN has been used to embed the watermark in DWT domain, to reduce errors and to improve the rate of learning. Trained

neural networks can also recover the watermark from watermarked images. Experimental results show that the algorithm has excellent imperceptibility in terms of PSNR (peak signal to noise ratio). Nasir et al. [41] proposed a wavelet based blind color image watermarking algorithm for copyright protection. Multiple watermark bits have been embedded into luminance component and blue component of cover image. Image normalization scheme has been used in this algorithm to reduce synchronization errors because of geometrical attacks. Experimental results show that the proposed watermarking scheme has good imperceptibility and robust against common signal processing attacks and some geometrical attacks.

Saini et al. [42] proposed a hybrid watermarking embedding and extraction scheme based on DWT and SVD. The basic algorithm consists of three main steps. In the first step watermark has been embedded into original image using DWT-SVD and then various attacks have been applied on watermarked image. Finally watermark has been extracted using BPNN, which has been used to establish relationship among singular values of original image, attacked image and extracted watermarked image. Experimental results show that proposed algorithm produces acceptable MSE (mean square error values) and good robustness in case of various kinds of attacks. Chun et al. [43] proposed a digital image watermarking scheme for multimedia copyright protection based on DCT and Artificial Neural Network (ANN). ANN has been used to model Human Visual System (HVS). The watermarking strength for DCT coefficients have been decided using ANN based image adaptive method. Experimental results show that without any visual degradation this method has increased robustness of watermark by increasing watermark strength. The method has also good adaptability.

Yang et al. [44] proposed a watermarking scheme for color images based on DWT and Neural networks. Three exactly same watermarks and some different expanded bit streams which are generated from three channels of color image have been adaptively embedded into low frequency sub bands. Because of adaptive learning capabilities of neural network, these expanded bit streams have been used to train BPNN to represent relationship between neighboring wavelet coefficients. Based on this training, three watermark results have been extracted and voted to decide final watermark. Experimental

results show that the proposed scheme is robust against various kinds of attacks. This scheme has also good performance in terms of imperceptibility and JPEG compression.

Ramamurthy et al. [45] compared two novel approaches to embed watermark into host image using quantization based on BPNN and Dynamic Fuzzy Interference System (DFIS). The cover image has been decomposed into 3-levels using quantization and DWT. The bitmap has been selected as watermark. The BPNN has been implemented to embed and extract the watermark in one method. DFIS has been used to generate the watermark weighing function to embed and extract the watermark in other method. Experimental results demonstrate that proposed watermarking algorithms are imperceptible and robust to various attacks such as JPEG compression, salt & peppers noise, median filtering, rotation etc. BPNN algorithm provides better NCC (Normalized Cross Correlation) for median filtering attack as compared to DFIS model. Soliman et al. [46] presented a secure patient medical images and authentication scheme to enhance the confidentiality, integrity and security of medical images transmitted through internet. This paper proposed a watermarking scheme by invoking PSO technique in Quantization Index Modulation and SVD has been used in conjunction with DWT. PSO has been used to get basic quantization steps which have been varied to achieve suitable location for images having different frequency characteristics. Experimental results demonstrate that this method has improved the quality watermarked image and also increased the robustness of watermark against various attacks.

Mingzhi et al. [47] proposed a DWT and DCT based watermarking scheme to protect copyright of digital image. During embedding cover image has been decomposed using two-level DWT and then HL2 sub-band has been chosen and divided into 4×4 blocks to perform DCT on each block. Watermark bit has been embedded by predefined pattern-0 or pattern-1 into middle band coefficients of DCT. After that inverse DCT and inverse DWT has been applied to obtain the watermarked image. Different attacks have been then applied to watermarked image. During extraction process correlation between middle band coefficients of block DCT and predefined pattern (Pattern-0 and Pattern-1) has been calculated) to decide whether embedded bit was either 0 or 1. Genetic algorithm has been used to optimize parameters such as PSNR and NCC for embedding and

extraction. Experimental results show that proposed algorithm is robust against various kinds of attacks.

Table 2.1: Digital Image Watermarking Using Artificial Intelligence Techniques

S.no	Author's name	Techniques Used	Watermark/ Cover Image	Results (Highest values)
1	Wei et al. [6]	DCT, Genetic Algorithm (GA)	Watermark of size 2048 bits Gold hill image (256*256)	PSNR = 51db Similarity value = 8.5
2	Nilchi et al. [10]	DCT, Full Counter Propagation Neural network (FCNN)	Watermark: binary image (64*64) Barbara gray image (512*512)	PSNR =46.15db Similarity percentage value =99.92%
3	Aslantas et al. [7]	DWT-SVD, Particle Swarm Optimizer (PSO)	Watermark: gray level image (256*256) Lena Image (512*512)	NC = 0.9997
4	Lai et al. [30]	SVD, micro-Genetic Algorithm (GA)	Watermark: binary image (32*32) Lena image (256*256)	NC = 1
5	Aslantas et al. [8]	DCT, Genetic algorithm (GA), Differential Evolution (DE), Particle Swarm Optimizer (PSO), Clonal Selection Algorithm (CSA)	Watermark: binary image (64*64) Lena, Baboon, F-16 and Peppers image (256*256)	PSNR = 56.2858db NC = 1
6	Kumsawat et al. [31]	Multiwavelet domain Genetic Algorithm (GA)	Watermark of size 512 bits Lena, Baboon, Gold hill and Peppers gray level image (512*512)	PSNR = 46.70db NC = 1
7	VeyselAslantas [9]	SVD Differential evolution (DE)	Watermark: grey level image (32*32) Lena image (256*256)	PSNR = 38.023db NC = 1
8	Poonam et al. [32]	DWT Genetic Algorithm (GA)	Watermark: original watermark image (64*64) Original dog image (512*512)	PSNR = 47.9997db NC = 0.9702
9	Lai et al. [33]	SVD Genetic Algorithm (GA)	Watermark: binary image (32*32) Lena Image (512*512)	Proposed scheme survive after attacks and outperforms other similar works.
10	Vafaei et al. [34]	DWT Feed Forward Neural Network (FFNN)	Watermark: binary image 32*32 Lena, Baboon, Airplane, Barbara gray scale images (512*512)	PSNR = 48.25db NC = 1
11	Chaudhary et al. [35]	DCT Particle Swarm Optimizer (PSO)	Lena, boat, baboon, couple images (512*512)	PSNR = 48.10db NC = 0.99
12	Ali et al. [36]	DCT-SVD Arnold Transform Differential evolution (DE)	Watermark: gray scale image (64*64) Airplane, baboon image (512*512)	PSNR = 36.3848db NC = 0.9998
13	Ali et al. [37]	DWT-SVD Differential evolution (DE)	Watermark: binary image (64*64) Couple image (512*512)	PSNR = 35.2357db
14	Han et al. [38]	SVD Genetic Algorithm (GA)	Lena, Baboon, Barbara, Peppers, Bird, Cameraman, Gold hilland Airplane (256*256)	PSNR = 45.82db NC = 1
15	Yen et al. [11]	DCT, Back Propagation Neural Network (BPNN)	Watermark : original image (32*32) Lena image (256*256)	NC = 1

Basant et al. [48] proposed secure spread-spectrum based watermarking algorithms for embedding sensitive medical information such as doctor signature and hospital logo into radiological image for identity authentication purposes. In this method, different watermark messages are hidden in the same transform coefficients of the cover image using PN code. Performance of the method has been analyzed by varying the gain factor, sub band decomposition levels, size of watermarks, wavelet filters and medical image modalities. Simulation results show that the proposed method achieved higher security and robustness against JPEG attacks. Giakoumaki et al. [49] proposed a wavelet based multiple watermarking schemes to address various health information management issues such as protection of sensitive data, data authentication, image archieving and retrieval. The scheme allows definition of a region of interest (ROI) and information present there in aims at integrity control. The robustness of method is enhanced by using repetitive embedding of BCH encoded watermarks. Experimental results demonstrate that this algorithm is efficient in terms of imperceptibility, robustness and integrity control capability

Chapter: 3
Robust Watermarking Technique using Single Image Watermark

Abstract

In this chapter, an algorithm for digital watermarking based on discrete wavelet transforms (DWT) and singular value decomposition (SVD) has been proposed. In the embedding process, the host color image is decomposed into third-level DWT. Low frequency band (LL3) is transformed by SVD. The watermark image is also transformed by SVD. The S vector of watermark information is embedded in the S component of the host image. Watermarked image is generated by inverse SVD on modified S vector and original U, V vectors followed by inverse DWT. Watermark is extracted using an extraction algorithm. In order to enhance the robustness performance of the image watermark, Back Propagation Neural Network (BPNN) is applied to the extracted watermark to reduce the effects of different noise applied on the watermarked image. Results are obtained by varying the gain factor and size of the cover and watermark image, Experimental results are provided to illustrate that the proposed method is able to withstand a variety of signal processing attacks and has been found to be giving superior performance for robustness and imperceptibility compared to existing methods suggested by other authors.

3.1. Introduction

Nowadays growth in technology such as computers and computer network offers widespread use of multimedia contents such as digital image, audio and video. This growth has also made easy duplication and distribution of this multimedia data. Therefore, protection of multimedia content has become essential and difficult job. Digital watermarking is one of the new, popular and efficient techniques for multimedia data protection. In this scheme, a document called watermark is embedded into the digital data to protect it from unauthorized use in various social applications such as copy protection, tamper detection, broadcast monitoring, content archiving, fingerprinting, healthcare, cyber watermarking and content authentication [1-5]. In addition, digital

watermarks are also used to protect state driver licenses by providing covert and machine readable layer of security to fight against various issues such as digital counterfeiting, fraud, identity theft etc. [50]

Yang et al. [44] proposed a color image watermarking method based on DWT and BPNN. In the embedding process, three identical watermarks of size 40×30 have been adaptively embedded into the low frequency sub-bands generated from three channels (R, G & B) for a color image of size 512×512 respectively. The experimental results have been shown that the proposed scheme is robust against various kinds of signal processing attacks. Yen et al. [11] proposed a digital watermarking scheme based on DCT and BPNN. In the embedding process, DCT has been applied on the cover image of size 256×256 and the watermark of size 32×32 is embedded into the mid frequency region. Further, the embedded image contains the DCT coefficients were converted back to the spatial domain by using the inverse DCT. The simulation results indicated that the method is found to be robust for different attacks.

A digital image watermarking based on discrete wavelet transform (DWT) and singular value decomposition (SVD) using BPNN has been proposed. Color images are considered as cover/host and watermark. In the embedding process, the host color image is decomposed into third-level DWT. Low frequency band (LL3) is transformed by SVD. The watermark image is also transformed by SVD. The S vector of watermark information is embedded in the S component of the host image. Watermarked image is generated by inverse SVD on modified S vector and original U, V vectors followed by inverse DWT. Watermark is extracted using an extraction algorithm. In order to enhance the robustness performance of the image watermark, Back Propagation Neural Network (BPNN) is applied to the extracted watermark to reduce the effects of different noise applied on the watermarked image. The embedding and extraction process of proposed algorithm are described below:

3.2. Embedding algorithm for image watermark

The embedding process is described in Figure 3.1(a). Watermark image is embedded into cover image using following steps: -

1. Apply third-level DWT transform on cover image to decompose it into corresponding sub bands.

2. Select LL3 sub band and apply SVD on Red (R), Green (G) and Blue (B) components of cover image to partition it into three matrices U, S and V.

   $A_{ci} = U_{ci}S_{ci}V_{ci}^{T}$ i = R, G & B (1)

3. Apply SVD on Red (R), Green (G) and Blue (B) components of watermark image to obtain its corresponding matrices similar to step 2.

   $A_{wi} = U_{wi}S_{wi}V_{wi}^{T}$ i = R, G & B (2)

4. Modify the singular values of different color components LL3 sub band of cover image with the singular values of different components of watermark image. Here k is defined as the scaling factor with which watermark image is embedded into host image.

   $S_{wati}=S_{ci}+k*S_{wi}$ (3)

5. Obtain modified LL3* sub band using following equations.

   $A_{wati} = U_{ci} * S_{wati} * V_{ci}^{T}$ (4)

6. These arrays (A_{watr}, A_{watg}, A_{watb}) are concatenated in three dimension to obtain modified $LL3^{*}$ sub-band.
7. Change LL3 sub band of cover image with the modified $LL3^{*}$ sub band at third level and apply Inverse Discrete Wavelet Transform (IDWT) to get watermarked image A_{wat}.
8. Apply attacks and noise to the watermarked image to check the robustness of the proposed algorithm.

3.3. Extraction algorithm for image watermark

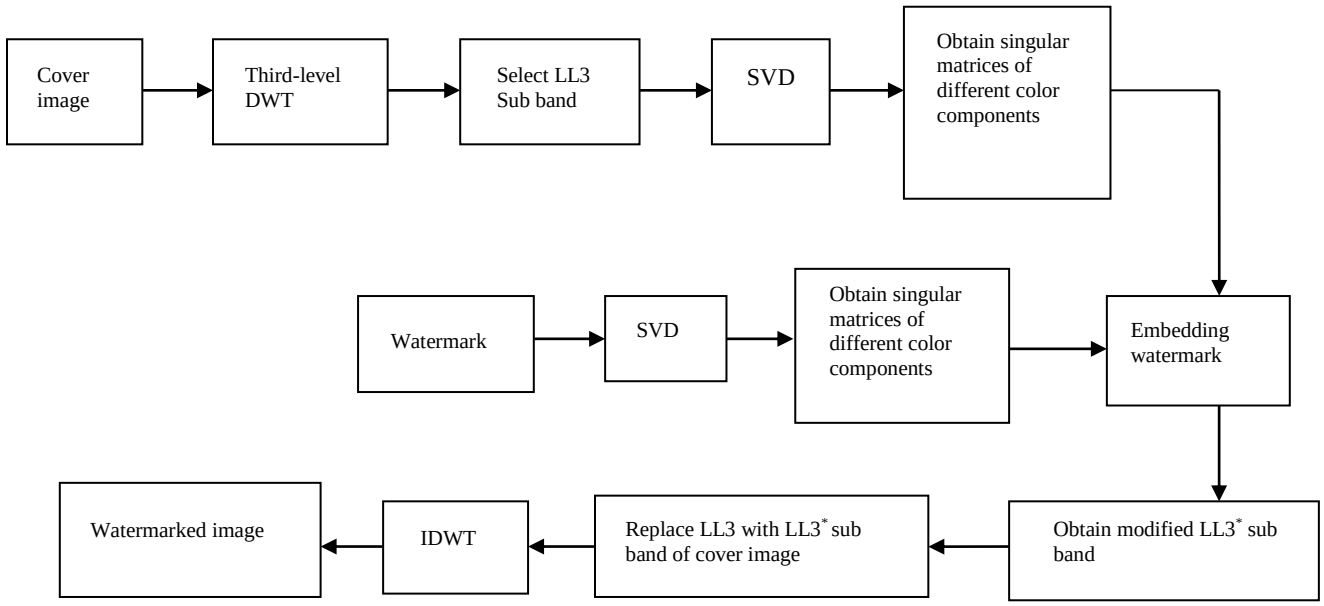
The extraction process is described in Figure 3.1(b). Watermark image is extracted from watermarked image using following steps: -

1. Apply third-level DWT transform on cover image to decompose it into corresponding sub bands.
2. Select LL3 sub-band and apply SVD on Red (R), Green (G) and Blue (B) components of cover image to partition it into three matrices U, S and V.

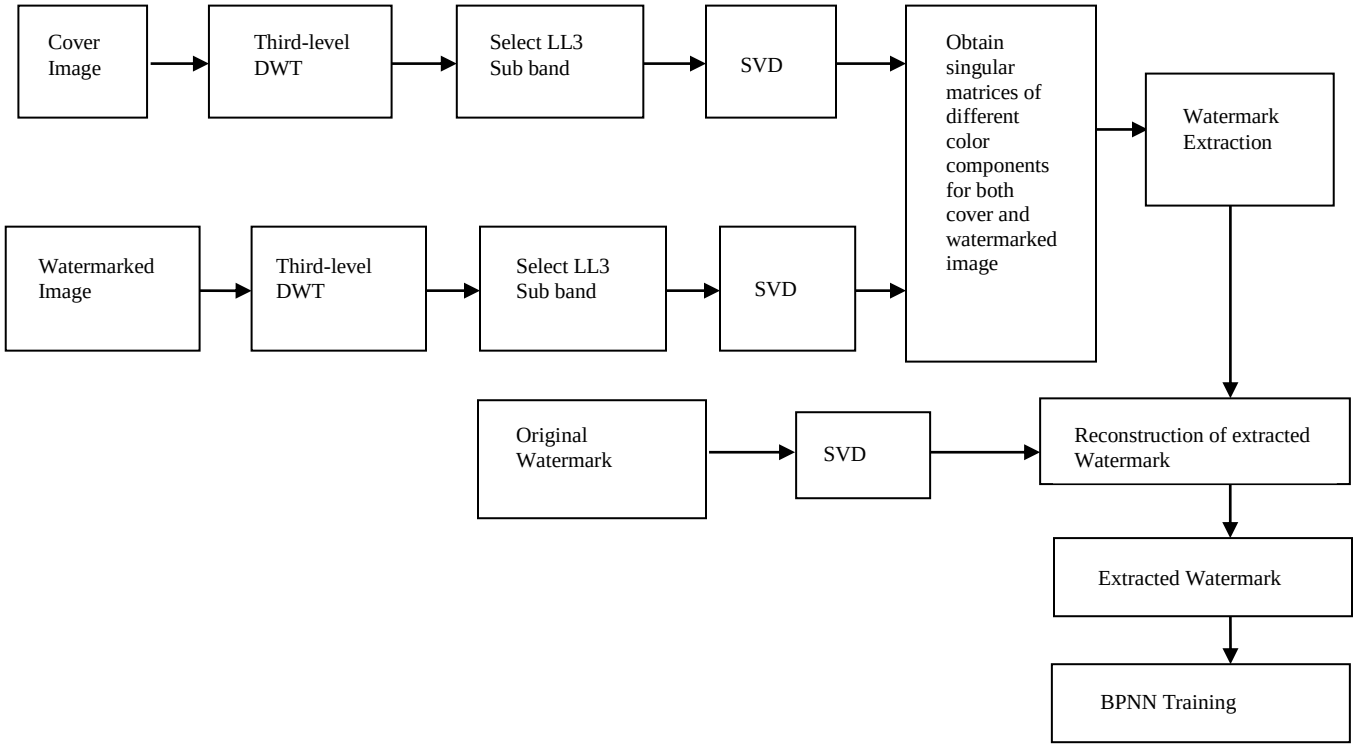
   $A_{ci} = U_{ci}S_{ci}V_{ci}^{T}$ i = R, G & B (5)

3. Apply SVD on Red (R), Green (G) and Blue (B) components of watermark image to obtain its corresponding matrices similar to step 2.

   $A_{wi}=U_{wi}S_{wi}V_{wi}^{T}$ (6)



(a)



(b)

Figure 3.1: (a) Watermark embedding and (b) Watermark extraction Process

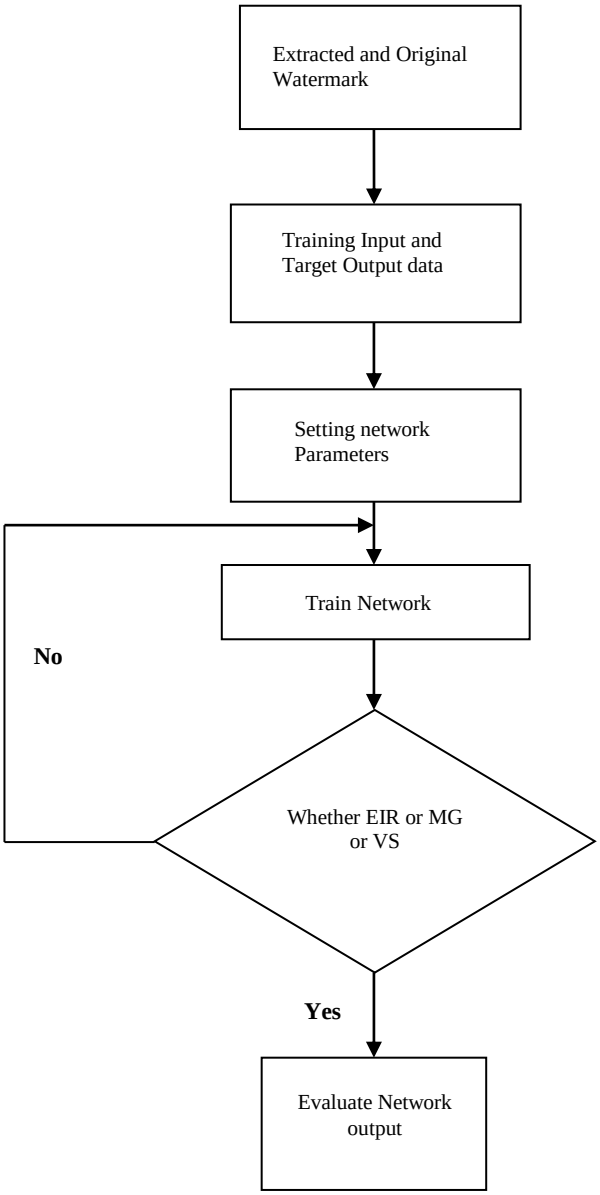


Figure 3.2: BPNN Training Process

4. Apply step 1 and step 2 to watermarked image to obtain its corresponding SVD Matrices for LL3 sub band.

$$A_{wati}=U_{wati}S_{wati}V_{wati}^{T} \quad (7)$$

5. Obtain singular values of watermark image from the singular values of LL3 sub band of watermarked image and cover image by using following equations:

$$S_{wi}^{*}=(S_{wati}-S_{ci})/k \quad (8)$$

6. Obtain extracted watermark using this equation:

$A_{ewi}=U_{wi}* S_{wi}^{*} * V_{wi}^{T}$ (9)

These arrays (A_{ewr}, A_{ewg}, A_{ewb}) are concatenated in three dimension to obtain extracted watermark image A_{ew}.

7. BPNN is then applied to extracted watermark to remove noise and interferences in order to improve its robustness. Figure 3.2 shows the BPNN training process.

3.4. Experimental Results and Analysis

We describe the performance of the combined DWT-SVD watermarking algorithm using BPNN. The color Peppers image of size 512×512 as cover image and the logo image of size 64×64 is consider as watermark image. Also, Back Propagation Neural Network (BPNN) is applied to the extracted watermark to achieve the better robustness performance of the proposed method against different signal processing attacks. Strength of watermark is varied by varying the gain factor in the watermarking algorithm. For testing the robustness and quality of the watermarked image of the proposed scheme MATLAB is used. Also, evaluate the quality of watermarked image by the parameter PSNR and robustness of the proposed algorithm by NC. Figure 3.3 (a), Figure 3.3(b) and Figure 3.3(c) shows the cover Pepper image, watermark logo image and watermarked images respectively.

Figure 3.3: (a) Cover image (b) Watermark image and (c) Watermarked image

Figure 3.4 :Extracted logo watermark (a) without and (b) with BPNN training

Figure 3.4(a) and Figure 3.4(b) shows the extracted watermark without and with using the BPNN training respectively. The PSNR and NC performance of the proposed method is shown in Table 3.1 to Table 3.3. Table 3.4 shows the NC performance of the proposed method is better than the existing methods. Figure 3.5 to Figure 3.8 shows the graphical representation of Table 3.1 to Table 3.4 respectively.

In Table 3.1, the PSNR and NC performance of the proposed method has been evaluated without any noise attack. Without using the BPNN, the maximum PSNR value is 36.26 dB where the NC value is 0.19 at gain factor = 0.01. However, the NC value has been obtained as 0.82 with BPNN at the same gain. With BPNN, the maximum NC value is 0.98 at gain factor = 0.1. However, the NC value has been obtained as 0.9 without using BPNN at the same gain. Hence, the NC performance of the proposed method has been improved up to 76.82% with BPNN. We found that larger the gain factor, stronger the robustness and smaller the gain factor, better the image quality. Table 3.2 shows the effect of cover image, proposed algorithm was tested for other images like Earth, Fruits, Sky, Medical and Lena images. With BPNN, the highest NC value have been obtained with Earth image at gain = 0.1. However, the highest NC value has been obtained with the same cover image without using the BPNN. Here, the ratio of the size of the cover and watermark image is very important. Hence, the NC performance of the proposed method has been improved up to 20.62% with BPNN.

Table 3.1: PSNR and NC values at different gain factors for Peppers and Logo1

SN	Gain Factor	Without using BPNN		With BPNN	Improvement in NC values (%)
		PSNR	NC	NC	
1	0.01	36.26	0.19	0.82	76.82
2	0.05	35.83	0.88	0.97	9.28
3	0.1	34.78	0.9	0.98	8.16

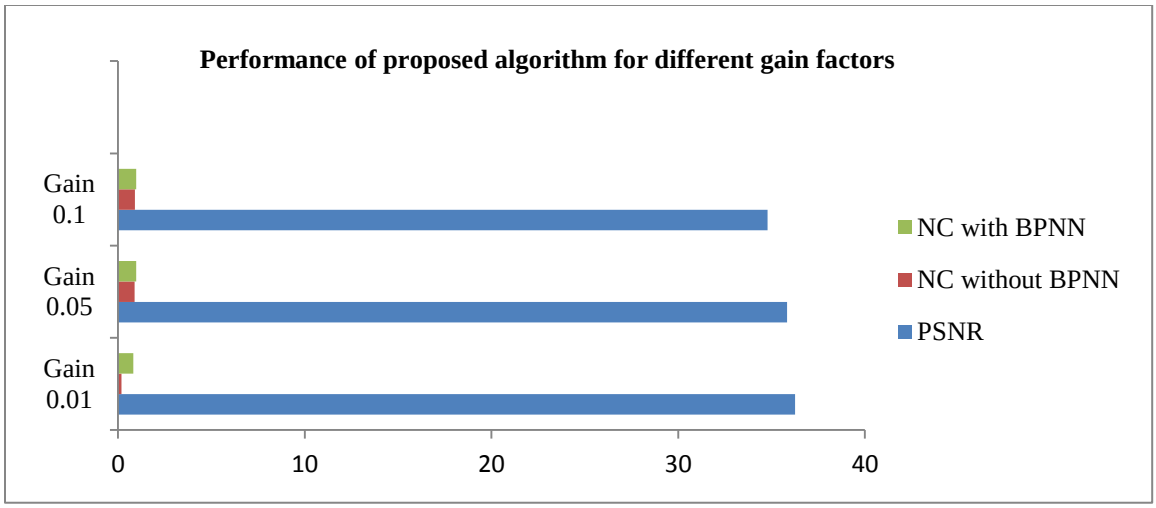


Figure 3.5: PSNR and NC values at different gain factors for Peppers and Logo1

Table 3.2: NC and PSNR performance for different size of cover and watermark image at gain 0.1

S N	Cover image	Watermark image	Cover image size	Watermark image size	PSNR (dB)	NC	NC (using BPNN)	Improvements in NC Values (%)
1.	Peppers	Logo_1	512*512	64*64	34.78	0.90	0.98	8.16
2.	Earth	Logo_2	1024*1024	128*128	32.31	0.98	0.99	1.01
3.	Fruits	Logo_3	256*256	32*32	30.41	0.85	0.96	11.46
4.	Sky	Logo_4	128*128	16*16	34.35	0.80	0.94	14.89
5	Medical	Tumor	512*512	64*64	37.88	0.77	0.97	20.62
5.	Lena	Logo_5	64*64	8*8	26.98	0.81	0.90	10

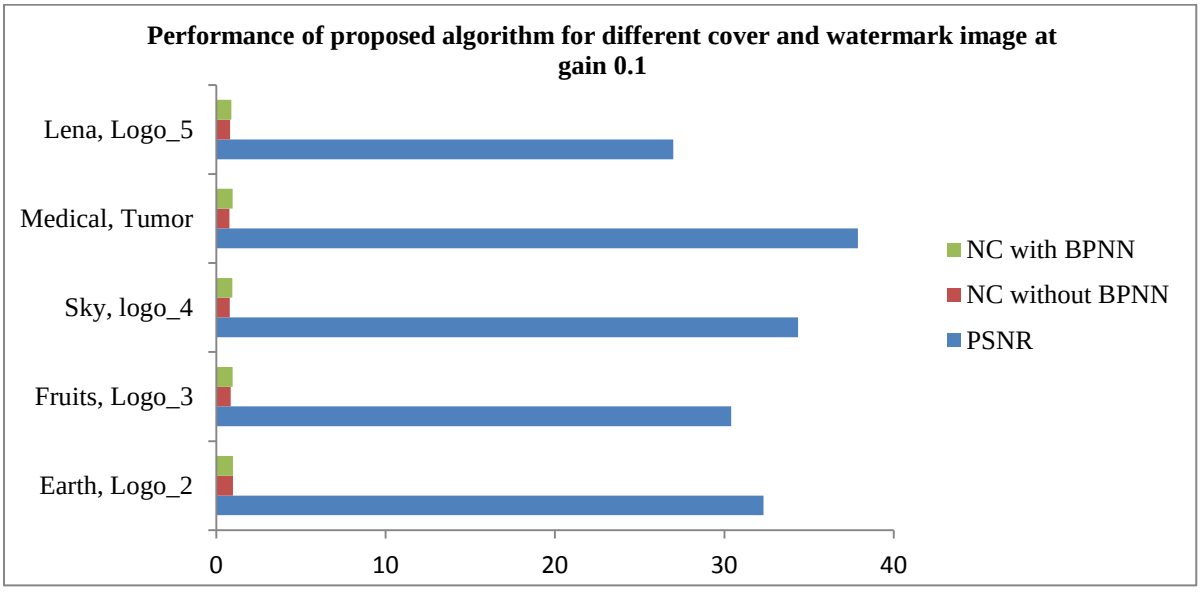


Figure 3.6: NC and PSNR performance for different size of cover and watermark image at gain 0.1

Table 3.3 shows the performance of the proposed method against different attacks. All the considered attacks are applied to watermarked image created from cover Peppers image and logo image at gain factor = 0.1. Without BPNN, the highest NC value has been obtained against JPEG compression (QF = 60). It is 0.87. However, the lowest NC is 0.46 against Rotation attacks. With BPNN, all the NC values are above 0.8 for different attacks. The highest NC value has been obtained against JPEG compression (QF = 60). It is 0.96. However, the lowest NC is 0.81 against Rotation attacks. Hence, the NC performance of the proposed method has been improved up to 43.21% with BPNN. Table 3.4 provides the performance comparison with the existing methods. In this Table, the maximum NC value with proposed method has been obtained as 0.9634 against 0.4861 and 0.9634 and obtained by the existing method proposed by Jagadeesh et al. [51] and Li et al. [52] respectively. Overall, the proposed method is better to that of the existing methods.

Table 3.3: NC and PSNR performance for different attacks at gain 0.1

SN	**Attack**	**NC(using DWT, SVD)**	**NC(using DWT, SVD, BPNN)**	**Improvements in NC Values (%)**
1.	JPEG 10	0.76	0.89	14.61
2.	JPEG 30	0.85	0.96	11.46
3.	JPEG 60	0.87	0.96	9.38
4.	Salt &Peppers (density = 0.05)	0.67	0.85	21.18
5.	Salt &Peppers (density = 0.2)	0.62	0.84	26.19
6.	Salt &Peppers (density = 0.3)	0.61	0.84	27.38
7.	Gaussian(Mean=0,Variance=1)	0.63	0.85	25.88
8.	Gaussian(Mean=0.2,Variance= 1.2)	0.78	0.83	6.02
9.	Rotation	0.46	0.81	43.21
10.	Crop	0.64	0.82	21.95
11.	Resize	0.59	0.84	29.76

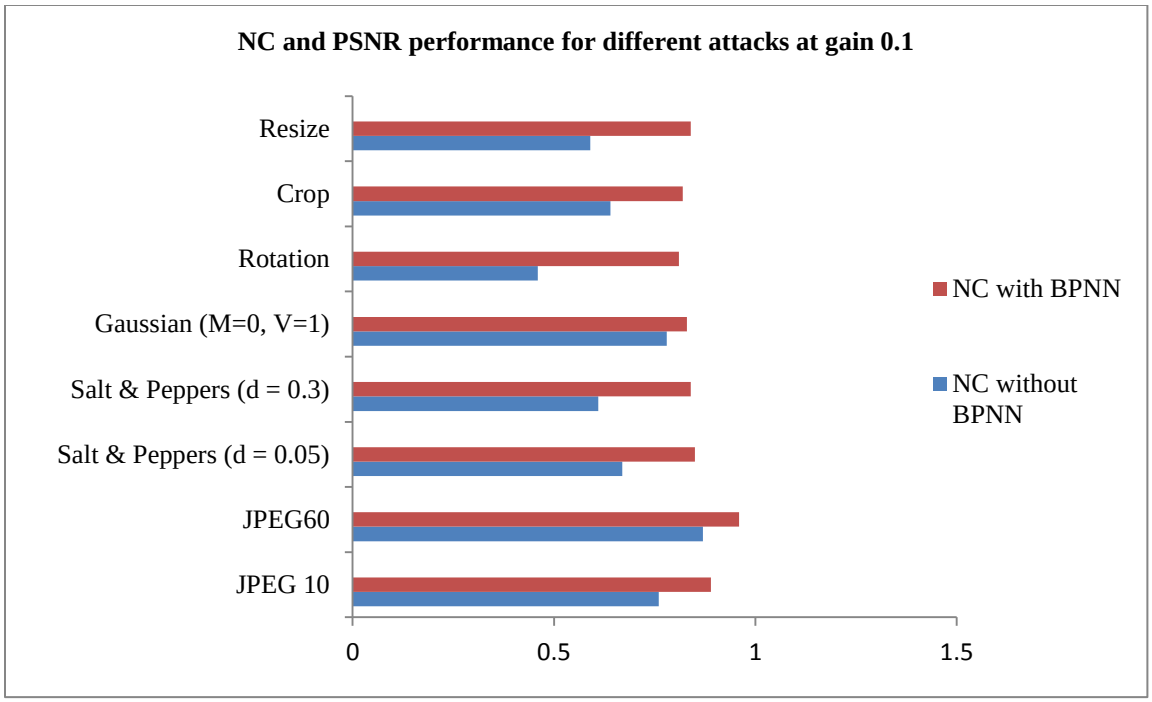


Figure 3.7: NC and PSNR performance for different attacks at gain 0.1

Table 3.4: The comparison results under NC value

Types of Attack	**Jagadeesh et al. [51]**	**Li et al. [52]**	**Proposed Method**
	NC Values	NC Values	NC Values
JPEG Compression (QF=100)	0.9304	0.4832	0.9599
Cropping	0.6547	0.3223	0.822
Resize (512-400-512)	0.4484	0.3541	0.8439
Salt & Pepper Noise(0.001)	0.9634	0.4861	0.9634

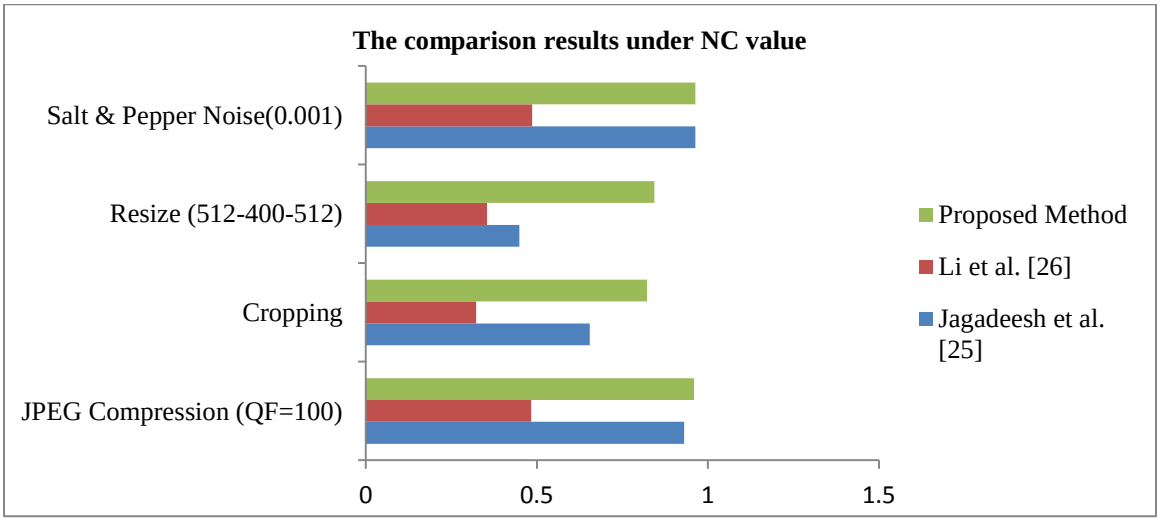


Figure 3.8: The comparison results under NC value

3.5. Conclusion

The proposed color image watermarking scheme is based on DWT, SVD and BPNN To improve the robustness performance of the proposed method, Back Propagation Neural Network (BPNN) is applied to the extracted watermark which gives the higher Normalized Correlation (NC) values compared to without using the BPNN. However the robustness performance of RGB color image model is low because of the high correlation among the R, G and B color components. The performance of the proposed algorithm can be improved by using other color image models such as YIQ, Ycbcr, HVS etc.

Chapter: 4
Robust Watermarking Technique using Multiple Image Watermarks

Abstract

In this chapter, an algorithm for multiple digital watermarking based on discrete wavelet transforms (DWT), discrete cosine transform (DCT) and singular value decomposition (SVD) has been proposed for healthcare applications such as teleophthalmology, telemedicine, tele-diagnosis and tele-consultancy services. Multiple watermarks are used in this algorithm to reduce the consequences of medical identity thefts. In the embedding process, the cover medical image is decomposed into third-level DWT. Low frequency bands (LH2 and LL3) are transformed by DCT and then SVD is applied to DCT coefficients. Two watermarks in form of images are also transformed by DCT and then SVD. The singular values of the watermark information are embedded in the singular value of the cover medical image. Watermarks are extracted using an extraction algorithm. In order to enhance the robustness performance of the image watermarks, Back Propagation Neural Network (BPNN) is applied to the extracted watermarks to reduce the effects of different noise applied on the watermarked image. Results are obtained by varying the gain factor and the different cover image modalities. Experimental results are provided to illustrate that the proposed method is able to withstand a variety of signal processing attacks and has been found to be giving excellent performance for robustness and imperceptibility.

4.1. Introduction

Recently, there is growth in medical field due to development of healthcare applications. However, the most important issues in this area are protecting the sharing and transmission of patient information via internet. Digital image watermarking plays an important role in various health information management issues such as protection of sensitive data, data authentication, image archieving and retrieval etc [53-55].

Basant et al. [48] proposed secure spread-spectrum based watermarking algorithms for embedding sensitive medical information such as doctor signature and hospital logo into radiological image for identity authentication purposes. In this method, different

watermark messages are hidden in the same transform coefficients of the cover image using PN code. Performance of the method has been analyzed by varying the gain factor, sub band decomposition levels, size of watermarks, wavelet filters and medical image modalities. Simulation results show that the proposed method achieved higher security and robustness against JPEG attacks. Giakoumaki et al. [49] proposed a wavelet based multiple watermarking schemes to address various health information management issues such as protection of sensitive data, data authentication, image archieving and retrieval. The scheme allows definition of a region of interest (ROI) and information present there in aims at integrity control. The robustness of method is enhanced by using repetitive embedding of BCH encoded watermarks. Experimental results demonstrate that this algorithm is efficient in terms of imperceptibility, robustness and integrity control capability.

Medical image watermarking has various applications such as:

- Embedding of data in medical images save so much storage space and bandwidth requirement for the transmission of medical images in telemedicine applications.
- It helps in maintaining the confidentiality of patient especially if disease is clandestine in nature.
- Sometimes tampering in medical data may even cost a life because of wrong diagnosis. People will not try to tamper the patient data if it is hidden in medical images.
- Medical image watermarking also helps in reducing medical identity thefts which are the serious security concern reported in various survey.

This algorithm for multiple digital watermarking based on discrete wavelet transform (DWT), discrete cosine transform (DCT) and singular value decomposition (SVD) has been proposed for healthcare applications such as teleophthalmology, telemedicine, tele-diagnosis and tele-consultancy services. In the embedding process, the cover medical image is decomposed into third-level DWT. Low frequency bands (LH2 and LL3) are transformed by DCT and then SVD is applied to DCT coefficients. Two watermarks in form of images are also transformed by DCT and then SVD. The singular values of the watermark information are embedded in the singular value of the cover medical image. Watermarks are extracted using an extraction algorithm. In order to enhance the

robustness performance of the image watermarks, Back Propagation Neural Network (BPNN) is applied to the extracted watermarks to reduce the effects of different noise applied on the watermarked image.

4.2. Embedding algorithm for image watermarks

The embedding process is described in Figure 4.1(a). Image watermarks are embedded into cover image using following steps: -

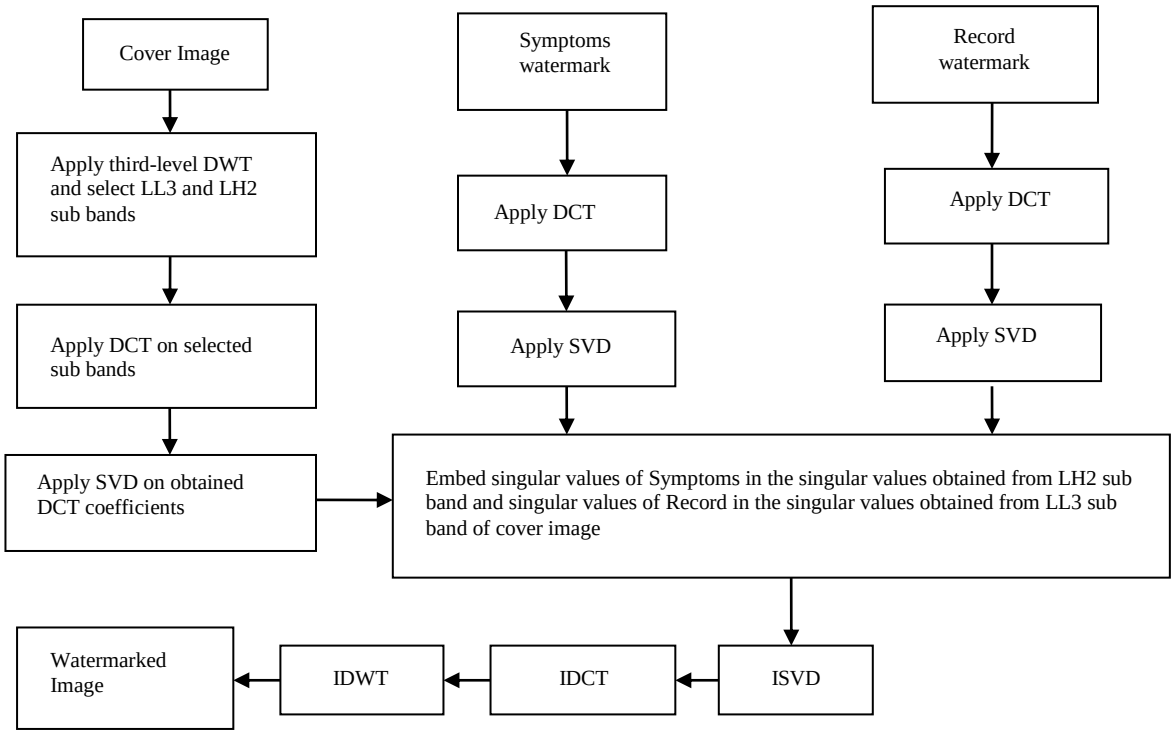
1. Apply third-level DWT transform on cover image to decompose it into corresponding sub bands and select LH2 and LL3 sub-bands.
2. Apply DCT to the selected sub-bands and then apply SVD to transformed DCT coefficients to obtain their corresponding three matrices U, S and V.

   $A_{ci} = U_{ci}S_{ci}V_{ci}^{T}$ i = LH2 &LL3 sub-bands (1)
3. Apply DCT on watermark images (Symptoms and Record) and then apply SVD to DCT coefficients to obtain their corresponding matrices similar to step 2.

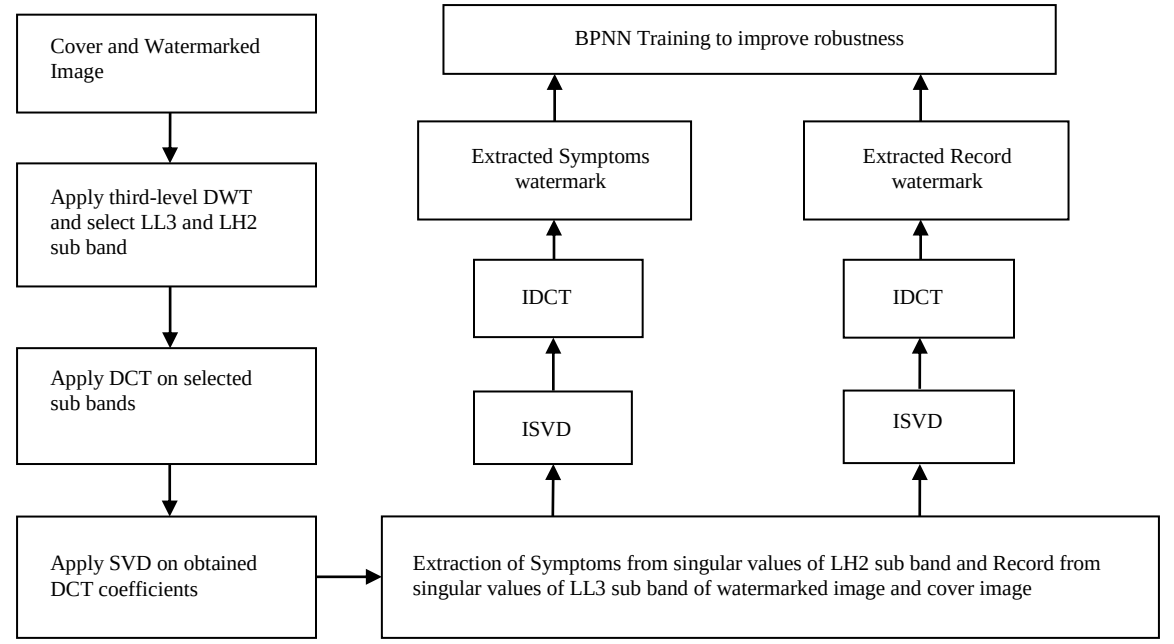
   $A_{wi} = U_{wj}S_{wj}V_{wj}^{T}$ j =Symptoms & Record (2)
4. Modify the singular values of LH2 sub band of cover image with the singular values of Symptoms and singular values of LL3 sub band of cover image with the singular values of Record. Here k is defined as the scaling factor with which watermark images are embedded into host image.

   $S_{wati} = S_{ci} + k*S_{wj}$ (3)
5. Obtain modified DCT coefficients by applying Inverse Singular Value Decomposition (ISVD) using following equations.

   $A_{wati} = U_{ci} * S_{wati} * V_{ci}^{T}$ (4)
6. Obtain modified $LH2^{*}$ and $LL3^{*}$ sub bands by applying Inverse Discrete Cosine Transform (IDCT) to modified DCT coefficients
7. Change LH2 and LL3 sub bands of cover image with the modified $LH2^{*}$ and $LL3^{*}$ sub band and apply Inverse Discrete Wavelet Transform (IDWT) to get watermarked image A_{wat}.
8. Apply attacks and noise to the watermarked image to check the robustness of the proposed algorithm.



(a)



(b)

Figure 4.1: (a) Watermark embedding and (b) Watermark extraction Process

4.3. Extraction algorithm for image watermarks

The extraction process is described in Figure 4.1(b). Watermark image is extracted from watermarked image using following steps: -

1. Apply third-level DWT transform on cover image to decompose it into corresponding sub bands and select LH2 and LL3 sub-bands.
2. Apply DCT to the selected sub-bands and then apply SVD to transformed DCT coefficients to obtain their corresponding three matrices U, S and V.

   $A_{ci} = U_{ci}S_{ci}V_{ci}^{T}$ i = LH2 &LL3 sub-bands (5)
3. Apply DCT on watermark images (Symptoms and Record) and then apply SVD to DCT coefficients to obtain their corresponding matrices similar to step 2.

   $A_{wj} = U_{wj}S_{wj}V_{wj}^{T}$ j = Symptoms & Record (6)
4. Apply step 1, step 2 to watermarked image to obtain its corresponding SVD Matrices for LH2 and LL3 sub bands.

   $A_{wati}=U_{wati}S_{wati}V_{wati}^{T}$ (7)
5. Obtain singular values of Symptoms and Record from the singular values of LH2 and LL3 sub band of watermarked image and cover image respectively by using following equation:

   $S_{wj}^{*} = (S_{wati} - S_{ci})/k$ (8)
6. Obtain extracted watermarks by applying inverse Singular Value Decomposition (ISVD) using equation (9) and then inverse Discrete Cosine Transform (IDCT).

   $A_{ewj}=U_{wj} * S_{wj}^{*} * V_{wj}^{T}$ (9)
7. BPNN is then applied to extracted watermarks to remove noise and interferences to improve their robustness. BPNN process has been described in chapter 3 in Figure 3.2.

4.4. Experimental Results and Analysis

The performance of the combined DWT-DCT-SVD watermarking algorithm has been evaluated in terms of quality of the watermarked image (PSNR) and robustness of the watermarked image (NC) using BPNN. The gray-scale medical C/CLump image of size 512×512 as cover image, the Symptoms image of size 128×128 and the Record image of size 64×64 is considered as image watermarks. Also, Back Propagation Neural Network (BPNN) is applied to the extracted watermarks to achieve the better

robustness performance of the proposed method against different signal processing attacks. Strength of watermarks is varied by varying the gain factor in the watermarking algorithm. For testing the robustness of two watermarks and quality of the watermarked medical image of the proposed scheme MATLAB is used. Also, evaluate the quality of watermarked image by the parameter PSNR and robustness of the proposed algorithm by NC. Figure 4.3(a)-Figure 4.3(d) shows the cover C/CLump image, Symptoms image, Record image and watermarked images respectively. Figure 4.4(a) and Figure 4.4(b) shows the extracted watermarks without using the BPNN training respectively. Figure 4.5(a) and Figure 4.5(b) shows the extracted watermarks with using the BPNN training respectively. The PSNR and NC performance of the proposed method is shown in Table 4.1 to Table 4.3. Figure 4.5 to Figure 4.10 shows the graphical representation of Table 4.1 to Table 4.3 respectively

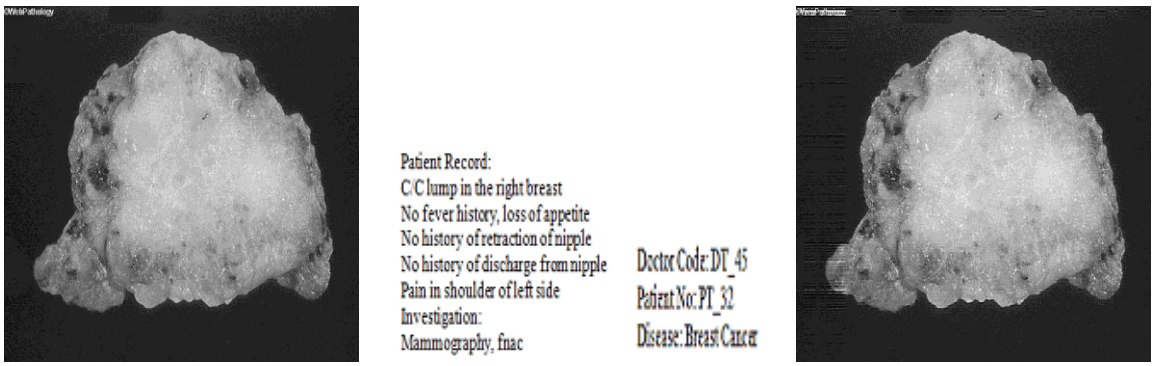


Figure 4.2: (a) C/CLump Cover image (b) Symptoms image (c) Record image and (d) Watermarked image

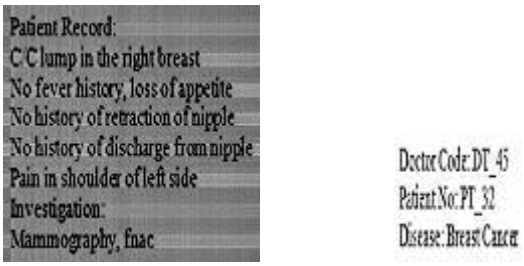


Figure 4.3: Without using BPNN(a) Extracted Symptoms image (b) Extracted Record image

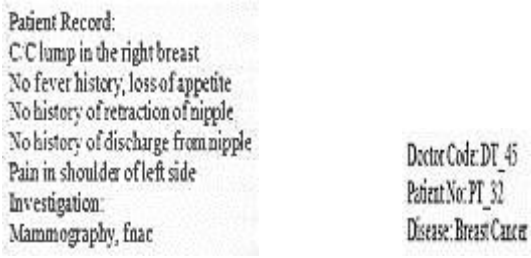


Figure 4.4: With using BPNN(a) Extracted Symptoms image (b) Extracted Record image

In Table 4.1, the PSNR and NC performance of the proposed method has been evaluated without any noise attack. Without using the BPNN, the maximum PSNR value is 41.36 dB where the NC value is 0.9427 and 0.8641 for Symptoms image and Record image respectively at gain factor = 0.01. With BPNN, the maximum NC value is 0.9814 at gain factor = 0.04 for Symptoms image and for Record image maximum NC is 0.9948 at gain factor = 0.18. However, for the same gain factors the NC values have been obtained as 0.9679 and 0.9934 for Symptoms and Record watermark image respectively without using BPNN. We found that larger the gain factor, stronger the robustness and smaller the gain factor, better the image quality. Record image requires more robustness, therefore gain factor = 0.18 is used for Table 4.2 and Table 4.3. Table 4.2 shows the effect of cover image, proposed algorithm was tested for other images like Ultrasound, Mammography, CT-scan, MRI and Lena images. With BPNN, the highest NC values have been obtained with Lena image at gain = 0.18 are 0.9916 for symptoms image and 0.9934 for Record image. However, the highest NC values for both watermarks have been obtained with the same cover image without using the BPNN. Here, the ratio of the size of the cover and watermark image is very important.

Table 4.1: PSNR and NC performance of the proposed method at different gain

SN	Gain factor	Without BPNN			With BPNN	
		PSNR	NC (Symptoms)	NC (Record)	NC (Symptoms)	NC (Record)
1	0.01	41.36	0.9427	0.8641	0.9812	0.9065
2	0.02	40.72	0.9660	0.9743	0.9802	0.9771
3	0.03	39.02	0.9676	0.9862	0.9806	0.9878
4	0.04	37.99	0.9679	0.9892	0.9814	0.9907
5	0.05	36.94	0.9675	0.9913	0.9808	0.9920
6	0.08	34.46	0.9625	0.9925	0.9791	0.9935
7	0.1	33.08	0.9572	0.9930	0.9663	0.9943
8	0.12	31.96	0.9508	0.9933	0.9642	0.9942
9	0.15	30.59	0.9391	0.9936	0.9699	0.9944
10	0.18	29.46	0.9285	0.9934	0.9662	0.9948
11	2.0	28.78	0.9220	0.9935	0.9639	0.9942

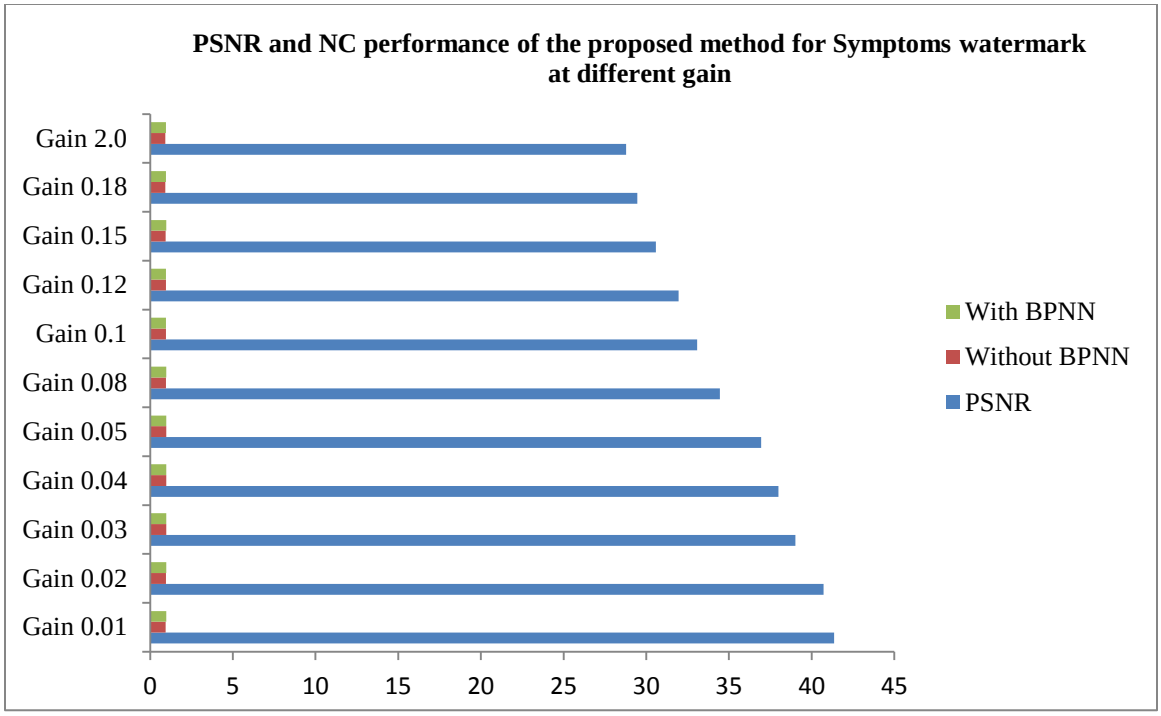


Figure 4.5: PSNR and NC performance of proposed method for Symptoms watermark at different gain

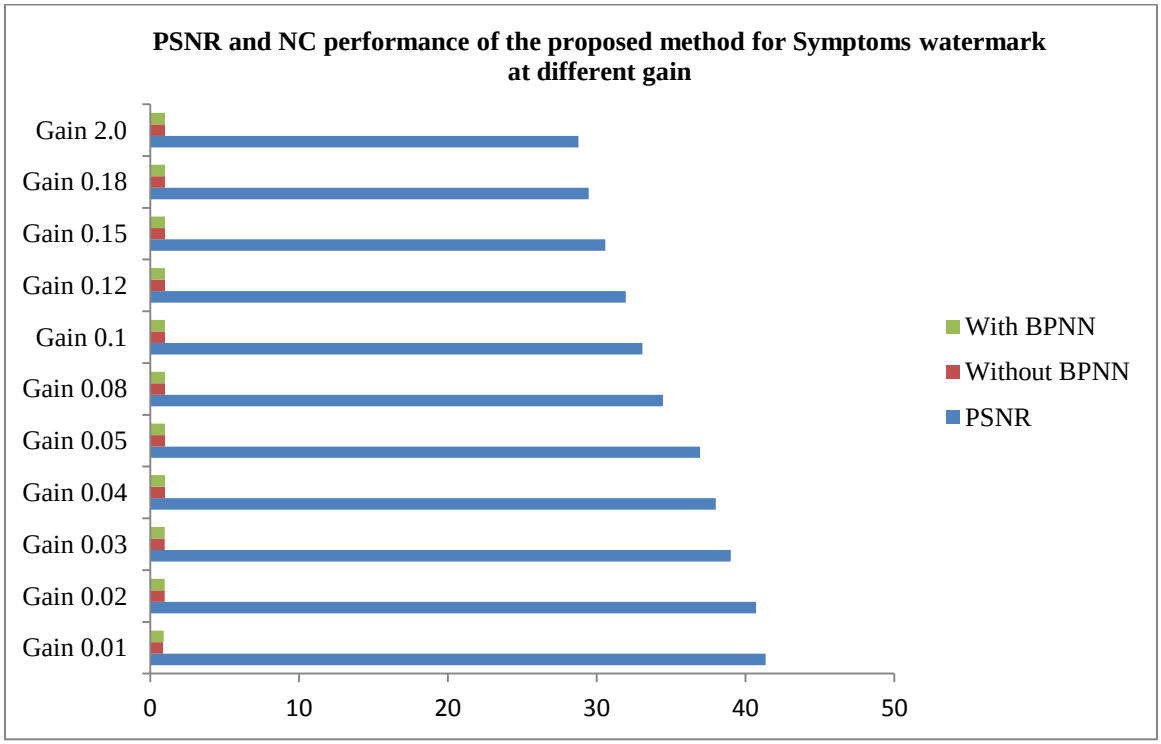


Figure 4.6: PSNR and NC performance of the proposed method for Record watermark at different gain

Table 4.2: NC and PSNR performance for different cover images at gain 0.18 for Symptoms and Record

SN	Cover Image	Without using BPNN			With BPNN	
		PSNR	NC (Symptoms)	NC (Record)	NC (Symptoms)	NC (Record)
1	Ultrasound	29.26	0.9612	0.9347	0.9734	0.9397
2	Mammography	30.99	0.9034	0.9918	0.9585	0.9926
3	CT-scan	28.08	0.9831	0.9709	0.9880	0.9782
4	MRI	28.93	0.9594	0.9827	0.9768	0.9904
5	Lena	27.35	0.9889	0.9927	0.9916	0.9934

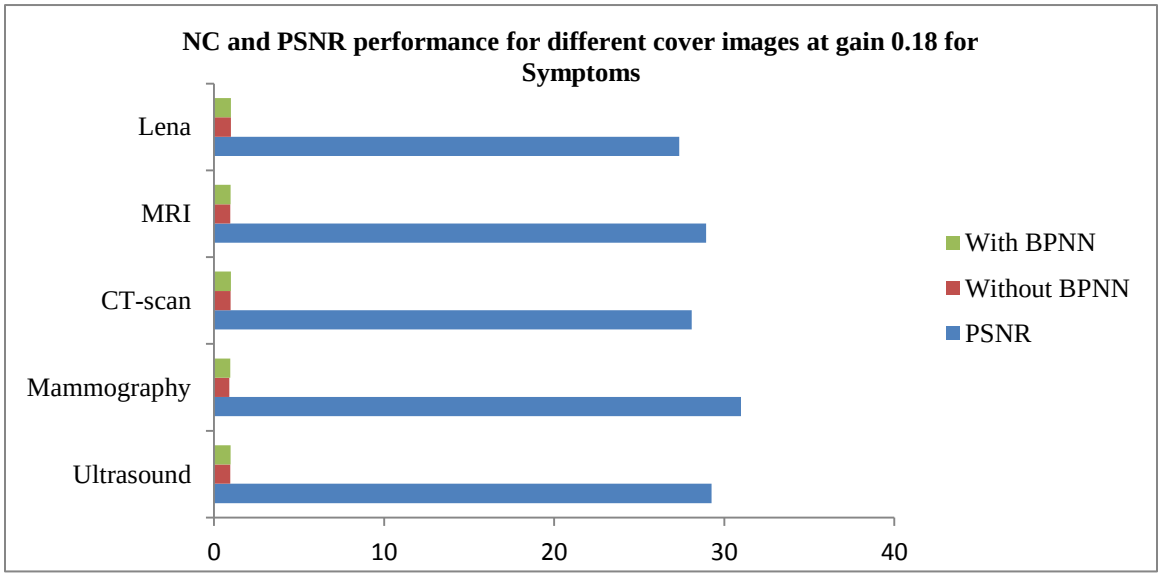


Figure 4.7: NC and PSNR performance for different cover images at gain 0.18 for Symptoms

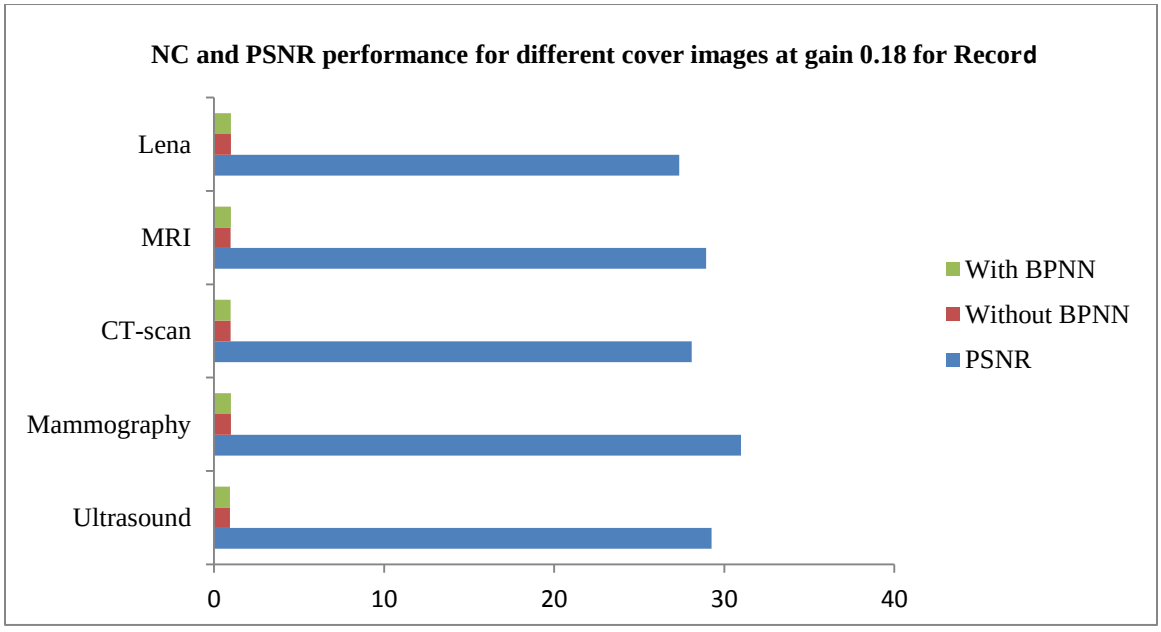


Figure 4.8: NC and PSNR performance for different cover images at gain 0.18 for Record

Table 4.3 shows the performance of the proposed method against different attacks. All the considered attacks are applied to watermarked image created from cover C/CLump image and Symptoms image and Record image at gain factor = 0.18. Without BPNN, the highest NC value has been obtained against low pass filtering for symptoms image and for symptoms image highest NC obtained against JPEG 100. These values are 0.9329 and 0.9934 for Symptoms image and Record image respectively. However, the lowest NC is 0.5798 against Rotation for Symptoms image and the lowest NC is 0.6596 against Salt & Peppers noise (density = 0.05) for Record image. With BPNN, all the NC values are above 0.9 for maximum attacks. The highest NC value has been obtained for Symptoms is 0.9661 against JPEG compression (QF = 100). However, the lowest NC is 0.7348 against Average Filtering. Similarly with BPNN, the highest NC value has been obtained for Record is 0.9939 against JPEG compression (QF = 100). However, the lowest NC is 0.8531 against Gaussian (Mean=0.01, Variance=0.02).

Table 4.3: NC performance of the proposed method for different attacks at gain = 0.18

SN	Attacks	Without using BPNN		With BPNN	
		NC (Symptoms)	NC (Record)	NC (Symptoms)	NC (Record)
1	JPEG 10	0.9197	0.9682	0.9611	0.9907
2	JPEG 30	0.9282	0.9908	0.9654	0.9913
3	JPEG 60	0.9085	0.9928	0.9599	0.9934
4	JPEG 70	0.9179	0.9932	0.9631	0.9936
5	JPEG 100	0.9283	0.9934	0.9661	0.9939
6	Salt & Peppers (density = 0.02)	0.7397	0.9220	0.8967	0.9367
7	Salt & Peppers (density = 0.01)	0.8301	0.9651	0.9292	0.9684
8	Salt & Peppers (density = 0.001)	0.9217	0.9923	0.9636	0.9935
9	Salt & Peppers (density = 0.05)	0.6287	0.6596	0.8405	0.8942
10	Gaussian (Mean=0, Variance =0.01)	0.6818	0.9411	0.8765	0.9417
11	Gaussian (Mean=0.01,Variance=0.02)	0.5953	0.8178	0.8239	0.8531
12	Gaussian (Mean=0, Variance =0.001)	0.8939	0.9901	0.9515	0.9908
13	Median Filtering	0.8457	0.9833	0.8657	0.9861
14	Crop (5%)	0.8977	0.9404	0.9406	0.9545
15	Rotation (5˚)	0.5798	0.7843	0.7912	0.9806
16	Resize	0.9206	0.9825	0.9626	0.9879
17	Average filtering	0.6709	0.9809	0.7348	0.9863
18	Low pass filtering	0.9329	0.9933	0.9660	0.9940
19	Gamma Correction	0.9249	0.9200	0.9650	0.9668
20	JPEG + Salt & Peppers	0.8208	0.9683	0.9273	0.9705
21	JPEG + Gaussian	0.6835	0.9256	0.8796	0.9288

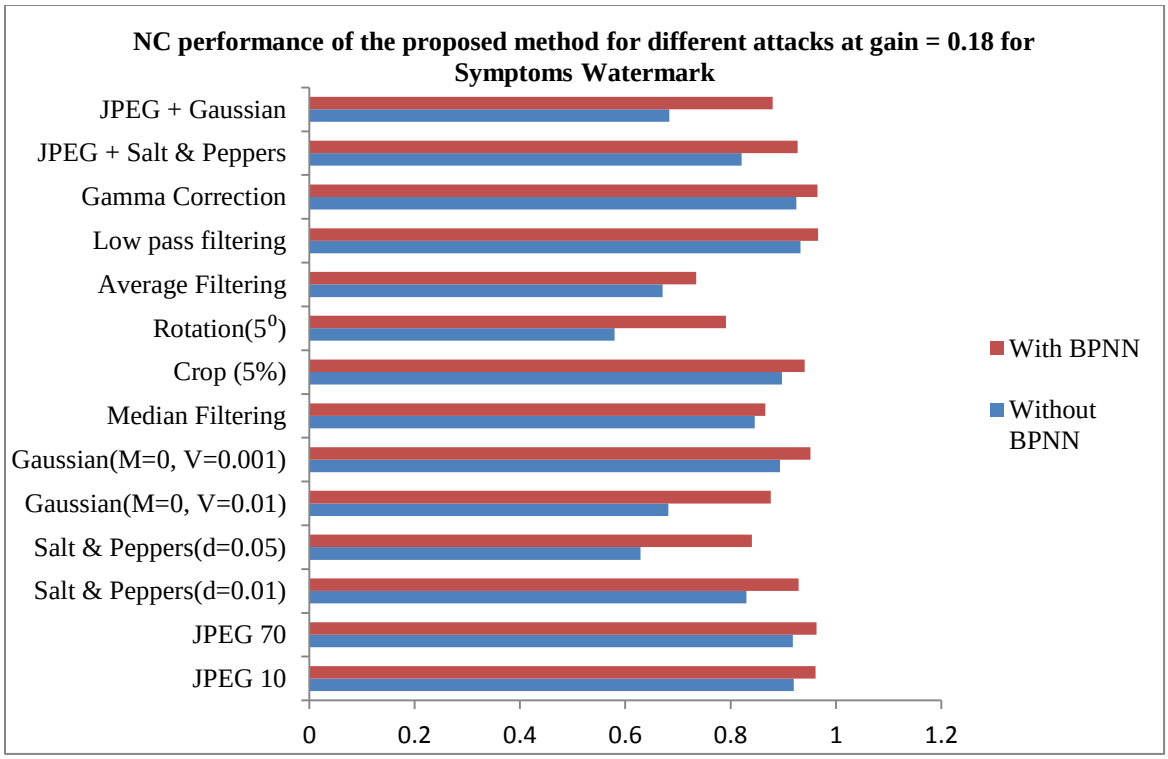


Figure 4.9: NC performance of proposed method for different attacks at gain = 0.18 for Symptoms watermark

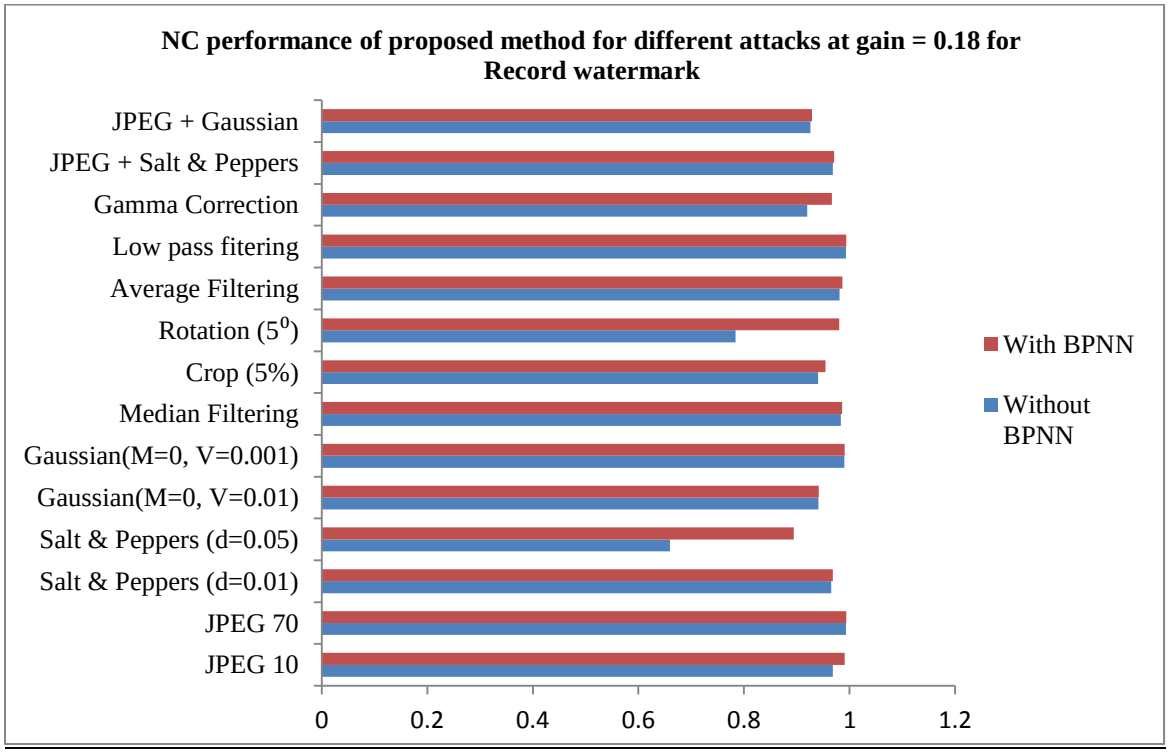


Figure 4.10: NC performance of proposed method for different attacks at gain = 0.18 for Record watermark

4.5. Conclusion

The main contribution of multiple images watermarking scheme based on DWT, DCT and SVD using BPNN is identified as follows:

- The fusion of DWT, DCT and SVD offer better performance in terms of imperceptibility, robustness and capacity as compared to DWT, DCT and SVD applied individually.
- Embedding of the multiple watermarks within the cover image helps in reducing the consequences of patient identity thefts. In addition, it also conserves transmission bandwidth and storage space requirements.
- BPNN effectively improves the robustness performance and provides high NC values as compared to without using BPNN.

The proposed method may have increased the computational complexity to some extent which needs to be investigated separately.

Chapter: 5

Robust and Secure EPR Data using Multiple Text and Image Watermarks

Abstract

In this chapter, an algorithm for multiple watermarking based on discrete wavelet transforms (DWT), discrete cosine transform (DCT) and singular value decomposition (SVD) has been proposed for healthcare applications. For identity authentication purpose, the proposed method uses three watermarks in the form of medical Lump image watermark, the doctor signature/identification code and diagnostic information of the patient as the text watermarks. In the embedding process, the cover medical image is decomposed into third-level DWT. Low-high frequency band (LH1) of the first level DWT is transformed by DCT and then SVD is applied to DCT coefficients. The image watermark is also transformed by DCT and SVD. The singular values of the watermark image information are embedded in the singular value of the cover medical image. Two different text watermarks are embedded at the second (LH2) and third level (LL3) DWT sub-band of the cover. In order to improve the robustness performance of the image watermark, Back Propagation Neural Network (BPNN) is applied to the extracted watermark to reduce the noise effects on the watermarked image. In addition, the security of the image watermark is enhanced by using Arnold transform before embedding into the cover. Further, the symptom and signature text watermarks are also encoded by lossless arithmetic compression technique and Hamming error correction code respectively. The compressed and encoded text watermark is then embedded into the cover image. Experimental results are obtained by varying the gain factor, different sizes of text watermarks and the different cover image modalities. The results are provided to illustrate that the proposed method is able to withstand a different of signal processing attacks and has been found to be giving excellent performance for robustness, imperceptibility, capacity and security simultaneously. Therefore the proposed method may find potential application in prevention of patient identity theft in healthcare applications.

5.1. Introduction

The continuous developments in Information and Communication technologies (ICTs) and multimedia technology offers widespread use of multimedia contents such as images, audio and video. All these technological advancements introduced a progressive change in various health care facilities such as information management, Hospital Information System (HIS) and medical imaging. Telemedicine is defined as use of ICTs in order to provide healthcare services when practicing doctors, patients and researchers are present in different geographical locations. Although such transmission and distribution of Electronic Patient Record (EPR) raises various security related issues such as reliability, integrity, security, authenticity and confidentiality [55-57]. Various applications of medical image watermarking are listed in chapter 4.

Mousavi et al. [58] have presented an automatic method for segmenting ROI part from the original image. The method is better than others techniques in this domain in terms of robustness. For ROI detection, several image processing tools have been used like morphological operation, low pass filtering, thresholding and labeling. ROI part remains unchanged even after the attacks like Gaussian, Median, Wiener and Sharpening filters. To increase the comparative results after attacks by uniquely producing ROI vertices, "Window size correction" has been proposed for the algorithm. Results prove that the proposed algorithm is very accurate in obtaining ROI part and robust as compared to other algorithms. Solanki et al. [59] have given a reliable watermarking methodology for medical images. The main task was to improve the security of the hidden information and make it more reliable. Image is enhanced after loading and then subtraction, thresholding is applied to divide ROI/RONI and to find high intensity areas. The proposed algorithm uses RSA and DWT for providing two-way security by encrypting the watermark and then applying DWT. The experimental results evaluate the algorithm as secure and robust.

This algorithm for multiple digital watermarking based on discrete wavelet transforms (DWT), discrete cosine transform (DCT) and singular value decomposition (SVD) has been proposed for healthcare applications such as teleophthalmology, telemedicine, tele-diagnosis and tele-consultancy services. Multiple image and text watermarks are used in

this algorithm for authentication, indexing and archieving medical information and to reduce the consequences of medical identity thefts.

Embedding process consists of decomposing cover medical image into third-level DWT. Low frequency LH1 band is transformed by DCT and then SVD is applied to DCT coefficients. Image watermark (Lump) is scrambled using Arnold Transform in order to provide security to sensitive information and after that it is transformed using DCT and then SVD. The singular values of the watermark information are embedded in the singular value of the cover medical image. Low frequency bands (LH2 and LL3) are used to embed text watermarks. Doctor's identification code (Signature text watermark) requires more robustness therefore it is embedded in the higher level LL3 sub band. Hamming encoder algorithm is applied to Signature watermark before embedding in order to increase its robustness. Information related to patient's symptoms and diagnoses reports (Symptoms text watermark) are embedded in LH2 sub band. Arithmetic coding is applied before embedding symptoms watermark to increase the capacity of our watermarking algorithm. Watermarks are extracted using an extraction algorithm. In order to enhance the robustness performance of the image watermark, Back Propagation Neural Network (BPNN) is applied to the extracted watermarks to reduce the effects of different noise applied on the watermarked image.

5.2. Allocation of Medical Watermarks

The proposed multilevel watermarking of medical images embeds multiple text and image watermarks into medical cover image. Table 5.1 shows the allocation of image and text watermarks according to robustness and capacity requirements at different DWT sub-bands.

Table 5.1: Allocation of different watermarks according to robustness and capacity criteria at different sub band

SN	Medical watermark	DWT sub band	Purpose of Embedding
1	Signature	LL3	Contains Doctor's Identification code for the purpose of Authentication
2	Symptoms	LH2	Contains Patient's history and diagnostic reports related information for the purpose of preventing addition storage, transmission requirements and in order to increase capacity
3	Lump	LH1	Contains reference image watermark for the purpose of data integrity control

5.3. Embedding algorithm for image watermark

The embedding process is described in Figure 5.1 (a). Watermark image is embedded into cover image using following steps: -

1. Apply third-level DWT transform on cover image to decompose it into corresponding sub bands and select LH1 sub-band.
2. Apply DCT to the selected sub-band and then apply SVD to transformed DCT coefficients to obtain corresponding three matrices U, S and V.

   $A_c = U_c S_c V_c^T$ (1)
3. Encrypt the watermark image (Lump) using Arnold Transform
4. Apply DCT on encrypted watermark image (Lump) and then apply SVD to DCT coefficients to obtain corresponding matrices similar to step 2.

   $A_w = U_w S_w V_w^T$ (2)
5. Modify the singular values of LH1 sub band of cover image with the singular values of Lump. Here k is defined as the scaling factor with which watermark images are embedded into host image.

   $S_{wat} = S_c + k*S_w$ (3)
6. Obtain modified DCT coefficients by applying Inverse Singular Value Decomposition (ISVD) using following equations.

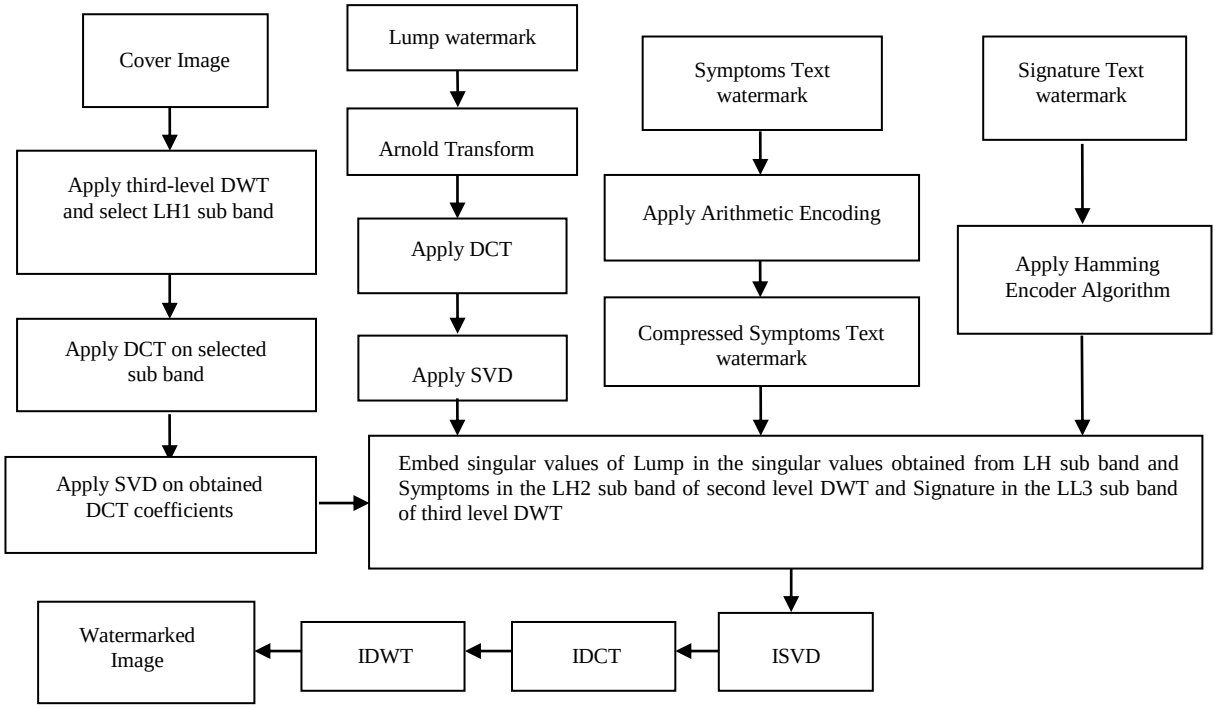
   $A_{wat} = U_c * S_{wat} * V_c^T$ (4)
7. Obtain modified $LH1^*$ sub band by applying Inverse Discrete Cosine Transform (IDCT) to modified DCT coefficients

8. Change LH1 sub band of cover image with the modified $LH1^*$ sub band and apply Inverse Discrete Wavelet Transform (IDWT) to get watermarked image.
9. Apply attacks and noise to the watermarked image to check the robustness of the proposed algorithm.

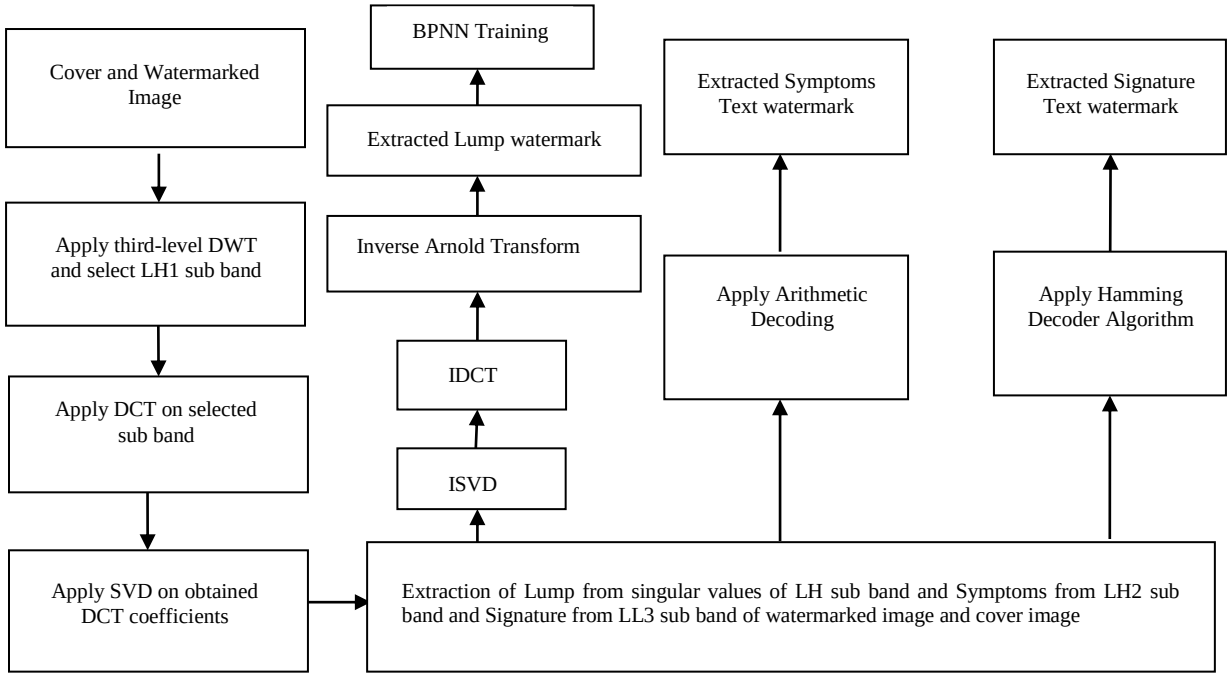
5.4. Extraction algorithm for image watermark

The extraction process is described in Figure 5.1(b). Watermark image is extracted from watermarked image using following steps:

1. Apply third-level DWT transform on cover image to decompose it into corresponding sub bands and select LH1 sub band.
2. Apply DCT to the selected sub-band and then apply SVD to transformed DCT coefficients to obtain their corresponding three matrices U, S and V.
   $A_c = U_c S_c V_c^T$ (5)
3. Apply DCT on watermark image (Lump) and then apply SVD to DCT coefficients to obtain their corresponding matrices similar to step 2.
   $A_w = U_w S_w V_w^T$ (6)
4. Apply step 1, step 2 to watermarked image to obtain its corresponding SVD Matrices for LH1 sub band.
   $A_{wat} = U_{wat} S_{wat} V_{wat}^T$ (7)
5. Obtain singular values of Lump from the singular values of LH1 sub band of watermarked image and cover image respectively by using following equation:
   $S_w^* = (S_{wat} - S_c)/k$ (8)
6. Obtain extracted watermark by applying inverse Singular Value Decomposition (ISVD) using equation (9) and then inverse Discrete Cosine Transform (IDCT).
   $A_{ew} = U_w * S_w^* * V_w^T$ (9)
7. Decrypt the extracted watermark by applying inverse Arnold Transform to obtain final extracted Lump image watermark
8. BPNN is then applied to extracted watermarks to remove noise and interferences in order to improve their robustness. BPNN training process has been described in chapter 3 in figure 3.2.



(a)



(b)

Figure 5.1: (a) Watermark embedding and (b) Watermark extraction Process

5.5. Embedding algorithm for Text watermark

The embedding process is described in Figure 5.1(a). Figure 5.3(a)-Figure 5.3(b) shows Signature and Symptoms watermarks. Text watermarks (Signature and Symptoms) are embedded into cover image using following steps: -

1. Apply third-level DWT transform on cover image to decompose it into corresponding sub bands and select LH2 and LL3 sub bands.
2. Convert the Signature text watermark into binary bits.
3. Apply Hamming Encoder algorithm to binary bits of Signature text watermark and replace (0,1) by (-1,1) in the watermarking bits.
4. Apply Arithmetic Encoding to Symptoms text watermark and replace (0,1) by (-1,1) in the watermarking bits similar to step3.
5. Embed the text watermarking bits obtained from Symptoms watermark to LH2 sub band of cover image and watermarking bits obtained from Signature watermark to LL3 sub band of cover image using equation (10).

   $A_i'(x,y) = A_i(x,y)(1 + k * Wbt_i)$ i = Signature and Symptoms watermarks (10)

   $A_i'(x,y)$ and A(x,y) are DWT coefficients before and after embedding process, Wbt is text watermarking bits and k is the gain factor .
6. Change LH2 and LL3 sub bands of cover image with the modified $LH2^*$ and $LL3^*$ sub band and apply Inverse Discrete Wavelet Transform (IDWT) to get watermarked image.

5.6. Extraction algorithm for text watermark

The extraction process is described in Figure 5.1(b). Text watermarks (Signature and Symptoms) are extracted from watermarked image using following steps: -

1. Apply third-level DWT transform on cover image to decompose it into corresponding sub bands and select LH2 and LL3 sub bands.
2. Apply third-level DWT transform on watermarked image to decompose it into corresponding sub bands and select $LH2^*$ and $LL3^*$ sub bands.
3. Extract watermark bits of Signature text watermark form LL3 sub band of cover image and $LL3^*$ sub band of watermarked image and Symptoms text watermark form LH2 sub band of cover image and $LH2^*$ sub band of watermarked image using equation (11).

$Wbt_i' = \frac{A_i'(x,y) - A_i(x,y)}{k * A_i(x,y)}$ i=extracted Symptoms and Signature watermarks (11)

$f'(x,y)$ and f(x,y) are DWT coefficients of cover and watermarked image respectively, Wbt' is extracted text watermarking bits and k is the gain factor .

4. Apply Arithmetic Decoding process to obtained watermark bits of Symptoms watermark and convert watermark bits into text to obtain Symptoms text watermark.
5. Apply Hamming Decoder algorithm to obtained watermark bits of Signature watermark and convert watermark bits into text to obtain Signature text watermark.

5.7. Experimental Results and Analysis

The performance of the combined DWT-DCT-SVD watermarking algorithm has been evaluated in terms of quality of the watermarked image (PSNR), Bit Error Rate (BER) of text watermarks and robustness of the watermarked image (NC) using BPNN. The gray-scale medical C/CLump image of size 512×512 as cover image, the Lump image of size 256×256 is considered as image watermark. Signature watermark of size 12 characters and Symptoms watermark of size 190 characters are considered as text watermarks. Back Propagation Neural Network (BPNN) is applied to the extracted image watermark to achieve the better robustness performance of the proposed method against different signal processing attacks. Strength of watermarks is varied by varying the gain factor in the watermarking algorithm. For testing the robustness of three watermarks and quality of the watermarked medical image of the proposed scheme MATLAB is used. Figure 5.3(a)-Figure 5.3(c) shows the cover CT-scan image, Lump watermark image and watermarked images respectively. Figure 5.4 shows the Signature and Symptoms text watermarks. Figure 5.5(a) and Figure 5.5(b) shows the extracted watermarks with and without using the BPNN training respectively. The PSNR, BER and NC performance of the proposed method is shown in Table 5.2 to Table 5.6. Figure 5.5 shows the graphical representation of Table 5.2 and Figure 5.6 to Figure 5.8 shows the graphical representation of Table 5.4 to Table 5.6 respectively

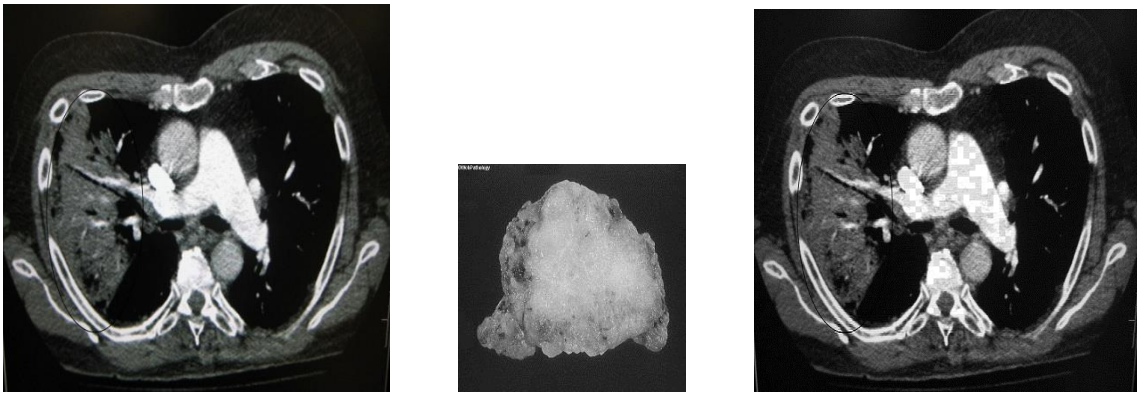


Figure 5.2: (a) CTscan Cover image (b) Lump image (c) Watermarked image

Doctor's Signature/ID: BXBPS4999S1
Diagnostic Information
Hospital Code: JUITWAKNAGHAT
Patient No: 200_Ward_ABC
Symptoms: c/c Lump in right barest_No fever history_Pain in right shoulder_No history of retraction and discharge from Hospital_Other reports_MammographNo 1568_FNAC39_B+_SOLAN

Figure 5.3 :Text watermarks, Signature and Symptoms

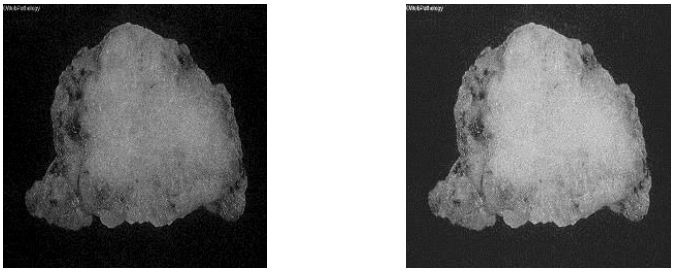


Figure 5.4 :Extracted Lump watermark (a) without and (b) with BPNN training

In Table 5.2, the PSNR and NC performance of the proposed method has been evaluated without any noise attack. Without using the BPNN, the maximum PSNR value is 43.88 dB where the NC value is 0.9344 for Lump image and at gain factor = 0.01. With BPNN, the maximum NC value is 0.9888 at gain factor = 0.08 for Lump image. However, for the same gain factors the NC values has been obtained as 0.9861 for Lump watermark image without using BPNN. We found that larger the gain factor, stronger the robustness and smaller the gain factor, better the image quality. BER of signature text watermark is 0 for

all gain factors. BER of Symptoms text watermark is 0.2174 and 0.1087 for gain factors 0.01 and 0.02 respectively. However for other gain factors the BER is 0 for Symptoms watermark. The NC of Lump image is maximum at gain factor 0.08 and also the BER of both watermarks is 0 at same gain factor, therefore gain factor = 0.08 is used for Table5.4-Table5.6. The Signature watermark contains Doctor's identification code hence it has been kept fixed for other tests. Table 5.3 shows the effect of symptoms watermark, proposed algorithm is tested for different size of Symptoms watermark at different gain factors. The maximum PSNR is obtained at gain factor 0.01 is 43.95, however the NC value obtained at this gain factor without using BPNN is 0.9363 for 50 characters of Symptoms watermark. With BPNN, the maximum NC obtained is 0.9889 at gain factor 0.05 for 50 characters of Symptoms watermark. The BER rate of signature watermark is 0 for all gain factors. The Symptoms watermark shows some BER at some gain factors for different character's size.

Table 5.2: PSNR, NC and BER performance of the proposed method at different gain

SN	Gain Factor	PSNR	BER (Text Watermark)		NC	
			Signature	Symptoms	Without BPNN	With BPNN
1	0.01	43.88	0	0.2174	0.9344	0.9547
2	0.02	41.22	0	0.1087	0.9764	0.9844
3	0.05	36.53	0	0	0.9846	0.9889
4	0.08	33.59	0	0	0.9861	0.9888
5	0.1	32.09	0	0	0.9852	0.9875
6	0.12	30.85	0	0	0.9853	0.9872
7	0.15	29.33	0	0	0.9849	0.9864
8	0.2	27.29	0	0	0.9851	0.9866

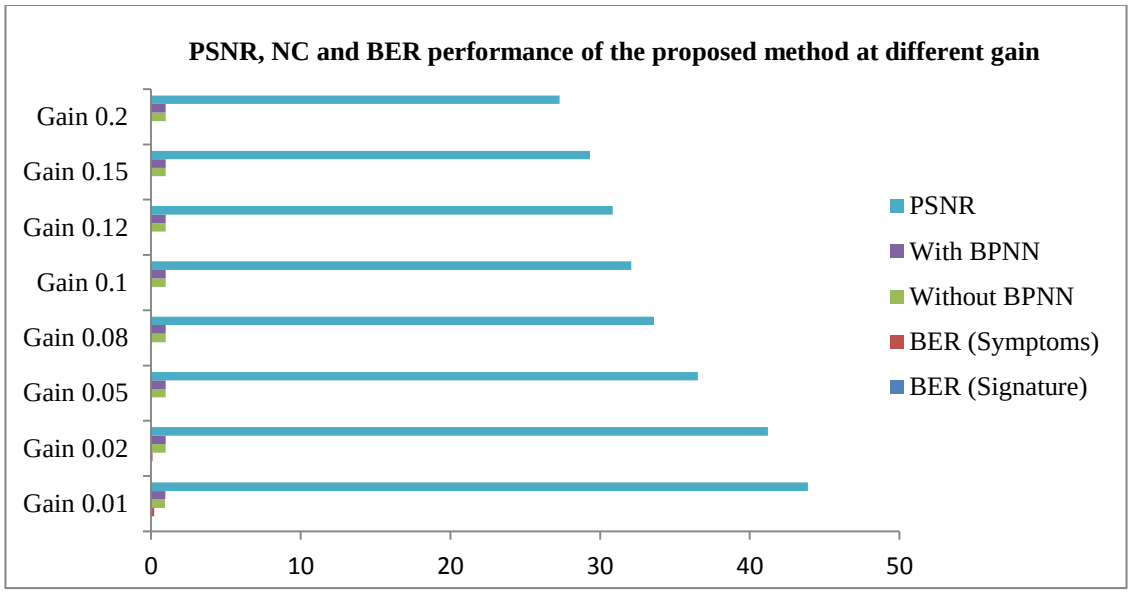


Figure 5.5: PSNR, NC and BER performance of the proposed method at different gain

Table 5.4 shows the effect of cover image, proposed algorithm was tested for other images like Ultrasound, Mammography, Brain, MRI, Mandrill and Lena. With BPNN, the highest NC values have been obtained with MRI image at gain = 0.08 is 0.9888 for Lump image. However, the highest NC value for Lump watermark has been obtained with the same cover image without using the BPNN. Here, the ratio of the size of the cover and watermark image is very important. The BER of Signature text watermark is 0 for all cover images. The symptoms watermark shows BER 0.1087 and 0.4348 for Mammography and Ultrasound cover images respectively

Table5.3: PSNR, NC and BER performance for different no of characters in Symptoms watermark at different gain

SN	Number of characters	Gain Factor	PSNR	BER		NC	
				Signature	Symptoms	Without BPNN	With BPNN
1	50	0.01	43.95	0	0.4202	0.9363	0.9563
		0.05	36.54	0	0	0.9846	0.9889
		0.1	32.12	0	0.4202	0.9853	0.9875
2	100	0.01	43.93	0	0.2110	0.9378	0.9573
		0.05	36.52	0	0	0.9846	0.9888
		0.1	32.10	0	0.2110	0.9851	0.9874
3	150	0.01	43.92	0	0	0.9356	0.9556
		0.05	36.51	0	0	0.9845	0.9887
		0.1	32.11	0	0	0.9854	0.9877
4	200	0.01	43.89	0	0.1370	0.9339	0.9541
		0.05	36.52	0	0	0.9847	0.9888
		0.1	32.09	0	0	0.9853	0.9877

Table 5.4: PSNR, NC and BER performance for different cover images at gain 0.08

SN	Cover Image	PSNR	BER (Text Watermark)		NC	
			Signature	Symptoms	Without BPNN	With BPNN
1	Brain	33.55	0	0	0.9745	0.9825
2	Mammography	32.94	0	0.1087	0.9474	0.9638
3	Ultrasound	34.34	0	0.4348	0.9642	0.9770
4	Lena	32.93	0	0	0.9795	0.9855
5	MRI	34.33	0	0	0.9869	0.9888
6	Mandrill	31.54	0	0	0.9845	0.9849

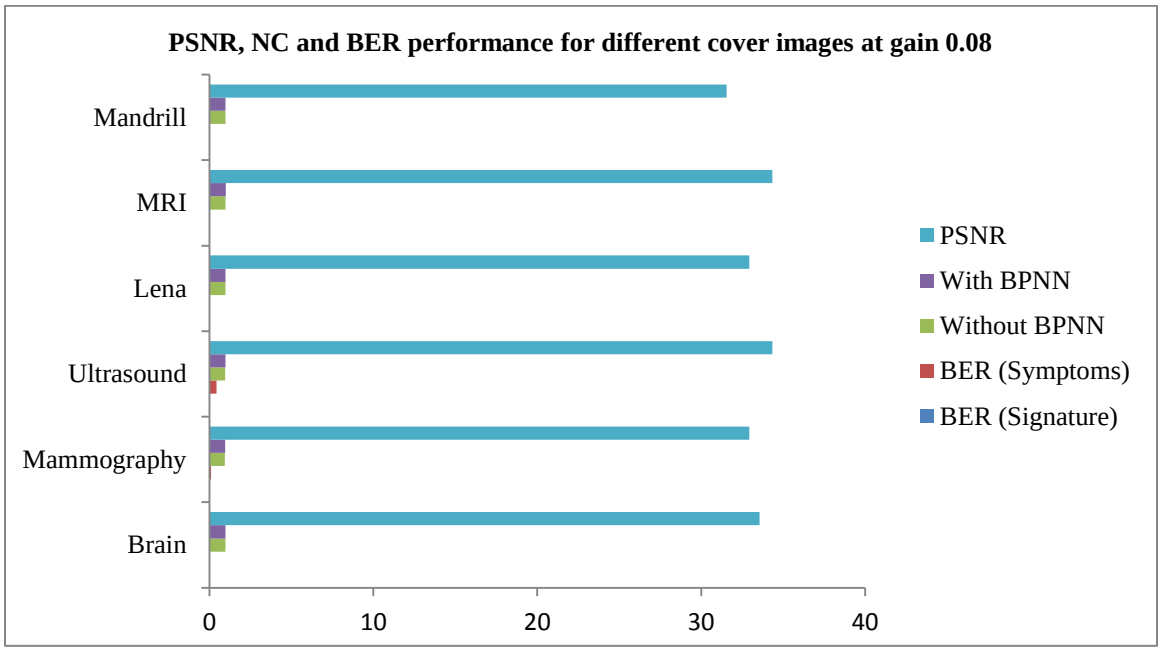


Figure 5.6: PSNR, NC and BER performance for different cover images at gain 0.08

In Table 5.5, the performance of proposed algorithm is tested for different Text watermark size at gain 0.08. Similar to Table 5.3 size of Signature watermark is fixed and the size of Symptoms watermark is varied to different characters. From the results it is clear that, there is not any significant change in PSNR, BER and NC values by changing the size of characters of Symptoms watermark.

Table5.5: PSNR and NC and BER performance for different text watermark size at gain 0.08

SN	Text Watermark size (in characters)		PSNR	BER		NC	
	Signature	Symptoms		Signature	Symptoms	Without BPNN	With BPNN
1	12	10	33.62	0	0	0.9860	0.9886
2	12	20	33.62	0	0	0.9861	0.9887
3	12	50	33.60	0	0	0.9860	0.9887
4	12	75	33.60	0	0	0.9862	0.9888
5	12	100	33.59	0	0	0.9861	0.9889
6	12	150	33.61	0	0	0.9861	0.9886
7	12	200	33.61	0	0	0.9861	0.9887

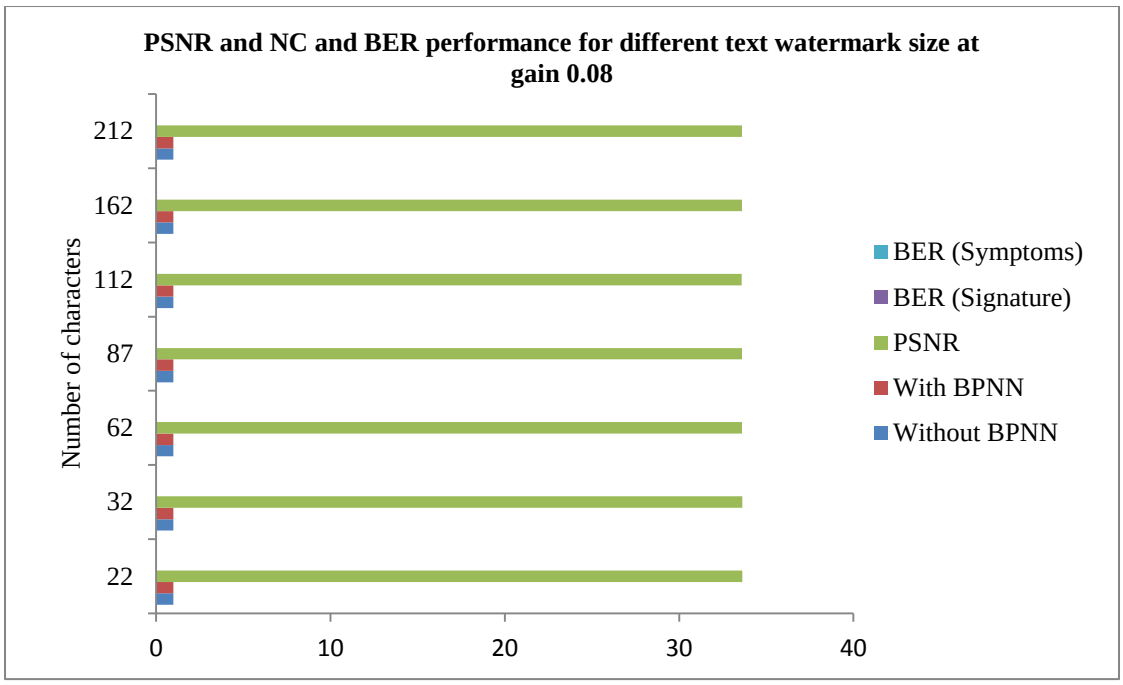


Figure 5.7: PSNR and NC and BER performance for different text watermark size at gain 0.08

Table 5.6 shows the performance of the proposed method against different attacks. All the considered attacks are applied to watermarked image created from cover CT-scan image and Lump watermark image, Signature text watermark and Symptoms text watermark at gain factor = 0.08. Without BPNN, the highest NC value has been obtained is 0.9852 against Gaussian low pass filtering for Lump image. However, the lowest NC is 0.0025 against median filtering for Lump image. With BPNN, the highest NC value has been obtained for Lump is 0.9889 for Gaussian low pass filtering. However, the lowest NC is 0.0123 against Median filtering. The highest BER of Symptoms watermark is 47.619 for Crop attack. The highest BER of Signature watermark is 0.4474 for Crop attack, however for maximum attacks the BER is 0.

Table 5.6: BER and NC performance of the proposed method for different attacks at gain = 0.08

SN	Attacks	BER		NC	
		Signature	Symptoms	Without BPNN	With BPNN
1	JPEG 10	0	0.1087	0.2081	0.3120
2	JPEG 30	0	0	0.9733	0.9803
3	JPEG 60	0	0	0.9679	0.9703
4	JPEG 80	0	0	0.9812	0.9871
5	JPEG 100	0	0	0.9860	0.9886
6	Salt & Peppers (density = 0.02)	0	0.2031	0.6926	0.7013
7	Salt & Peppers (density = 0.01)	0	0	0.7569	0.7747
8	Salt & Peppers (density = 0.001)	0	0	0.9604	0.9658
9	Gaussian(Mean=0.01,Variance=0.002)	0	0.2174	0.8365	0.8748
10	Gaussian (Mean=0, Variance =0.001)	0	0	0.9307	0.9466
11	Gaussian (Mean=0.01,Variance =0.0005)	0	0	0.9741	0.9761
12	Average filtering	0	0.1087	0.9824	0.9869
13	Low pass filtering	0	0.1087	0.9852	0.9889
14	Median filtering	0	0.2237	0.0025	0.0123
15	Speckle (Variance=0.02)	0.1119	28.57	0.8286	0.8673
16	Speckle (Variance=0.01)	0.1119	10.7143	0.9024	0.9286
17	Speckle (Variance=0.005)	0	0	0.9860	0.9886
18	Rotation (2˚)	0.3356	2.3810	0.4022	0.4442
19	Crop (6.25%)	0.4474	47.619	0.8691	0.9059
20	Resize (512-410-512)	0	0.3356	0.9177	0.9377
21	JPEG80 + Gaussian(M=0.01,V=0.002)	0	0.1119	0.8135	0.8558
22	JPEG80 + Salt & Peppers (d = 0.002)	0	0	0.9074	0.9312
23	Gaussian(M=0.01,V=0.002)+ Speckle (V=0.005)	0	0.2237	0.7901	0.8276
24	Salt & Peppers(d = 0.002) + Speckle (V=0.005)	0.2237	1.1905	0.7947	0.8328
25	JPEG80+ Speckle (V=0.005)	0	0.2237	0.9585	0.9645

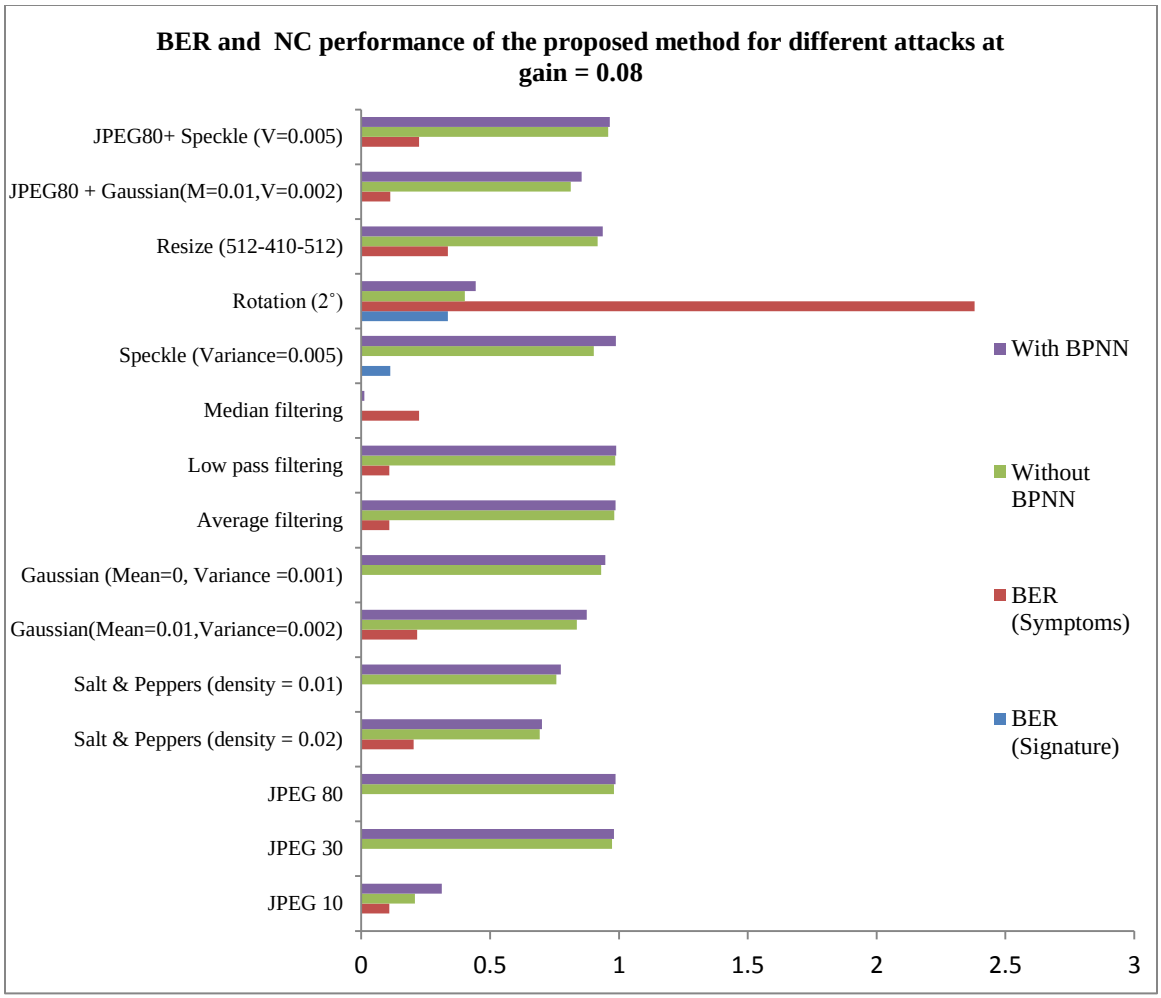


Figure 5.8: BER and NC performance of the proposed method for different attacks at gain = 0.08

5.8. Conclusion

The main contribution of proposed hybrid image-watermarking technique based on DWT, DCT and SVD using BPNN is identified as follows:

- The fusion of DWT, DCT and SVD offer better performance in terms of imperceptibility, robustness and capacity as compared to DWT, DCT and SVD applied individually.
- Embedding of the multiple watermarks within the cover image helps in reducing the consequences of patient identity thefts. In addition, embedding patient's detail in medical images conserves transmission bandwidth and storage space requirements.

- To improve the robustness performance of the proposed method, Back Propagation Neural Network (BPNN) is applied to the extracted watermark which gives the higher Normalized Correlation (NC) values compared to without using the BPNN.
- Security and confidentiality are provided by scrambling the Lump watermark using Arnold Transform before embedding
- Applying Arithmetic Coding to Symptoms watermark before embedding improves its capacity. In addition to this it also helps in reducing tradeoff between capacity, imperceptibility and robustness requirement of watermark.
- Signature watermark is embedded for authentication purpose and to increase its robustness, Hamming error correcting code is applied to it before embedding.

Therefore, the proposed algorithm effectively solves various issues related health information management such as Authentication, Security, Capacity, Storage and Bandwidth requirements. However, it may have increased the computational complexity to some extent which needs to be investigated separately.

Chapter 6
Conclusion and Future Directions

This thesis describes some techniques of digital image watermarking methods that offer higher robustness. The suggested methods of digital image watermarking with reported findings can be potentially useful for bandwidth efficient secure digital documents dissemination over the open channel.

Chapter 1 presents the basic concept of data hiding techniques, classification of watermarks, important characteristics and recent applications, Watermarking techniques in spatial and transform domain along with major benchmark performance parameters of the watermark algorithms. In addition, different Artificial Intelligence techniques are also introduced in this chapter.

Chapter 2 presents a brief review of various reported watermarking techniques and the performance of the techniques is compared in tabular form. Various Artificial intelligence techniques are used in different ways in combination with watermarking techniques to improve various performance factors are discussed in this chapter. Through literature survey it was noticed that the protection of digital documents is the prime concern when such information is transmitted over open channels.

Chapter 3 presents a color image watermarking method using fusion of DWT and SVD instead of DWT or SVD applied individually. Further, the robustness of the extracted watermark is enhanced by using Back Propagation Neural Network (BPNN) training. The performance of the proposed method has been tested for different gain, size of watermark, different cover image modalities and known signal processing attacks. In addition, the proposed method offer better robustness performance than other reported techniques. Referring table 3.1 it is evident that the BPNN based proposed method offered up to 76% enhancement in NC values over the method without using the BPNN. Moreover, Table 3.3 shows the performance of the proposed method for different attacks. In this table, the NC values have been obtained in the range from 0.81 to 0.96 for rotation and JPEG attacks respectively. Referring Table 3.4 it is established that the proposed method offer better robustness performance than the other reported techniques.

Further, a DWT, DCT, SVD and BPNN based multiple image watermarking method is presented for healthcare applications in **Chapter 4**. The performance of the proposed method has been tested for different gain, size of watermark, different cover image modalities and known signal processing attacks. Referring Table 4.1 to Table 4.3 it established that the performance of the proposed method is evaluated with and without using the BPNN. From these tables it is evident that the BPNN based method offer better performance than without using BPNN.

For identity authentication purpose in various applications, multiple watermarks in the form of image and text have been embedding in to the same multimedia object in **Chapter 5**. The performance of the proposed method is evaluated for different gain factor, text watermark size and cover image modalities. Experimental results are provided to illustrate that the proposed method is able to withstand a known attacks. Referring Table 5.2 to Table 5.6 the performance of the proposed method is evaluated. Table 5.5 show the PSNR, BER and NC performance of the proposed method is evaluated for different size (up to 200 characters) of Symptoms watermark. However, the size of signature watermark is considered as 12 characters. Table 5.6 show the NC performance of the proposed technique is evaluated for different attacks. Referring this Table it is evident that the NC performance is obtained in the range from 0.0123 to 0.9889 using BPNN. However, NC performance is obtained in the range from 0.0025 to 0.9860 without using BPNN. Further, the BER performance of signature watermark is obtained in the range from 0 to 0.4474. However, The BER performance of Symptoms watermark is obtained in the range from 0 to 47.61.

The performance of proposed methods highly depends on embedding and extraction process, gain factors, noise variations and size of watermarks. The obtained experimental results can be gainfully utilized for achieving robust and secure digital image watermarking for bandwidth efficient transmission of digital information over open channels. The proposed techniques have improved the robustness of the watermarks and the quality of the watermarked image, which are the prime objectives of the research. However, it may have increased the computational complexity to some extent which needs to be investigated separately. Also, it may be desirable to investigate the performance of the watermarking methods that use some new transform, machine learning techniques, biometrics, different color space model, video watermarking etc.

Research Publications

1. Aditi Zear, Amit Kumar Singh and Pardeep Kumar, "Digital Image Watermarking Techniques using Artificial Intelligence: New Trends in Information Security" In Proc. of 'First International Conference on Computer and Electronics Engineering (ICCEE)', Hyderabad, India. Tata McGraw-hill publishers, pp. 6-12, 2016.
2. Aditi Zear, Amit Kumar Singh and Pardeep Kumar (**Accepted**), "Robust Watermarking Technique using Back Propagation Neural Network: A Security Protection Mechanism for Social Applications", A Special Issue on Recent Trends in Security of Mobile Cloud Computing and the Internet of Things, International Journal of Information and Computer Security, Inderscience (**Scopus index**).
3. Aditi Zear, Amit Kumar Singh and Pardeep Kumar, "A Proposed Secure Multiple Watermarking Technique based on DWT, DCT and SVD for Application in Medicine", Multimedia Tool and Applications, Springer (SCI Index, IF = 1.346) (**Under review**)
4. Aditi Zear, Amit Kumar Singh and Pardeep Kumar Multiple Watermarking for Healthcare Applications, Journal of Intelligent Systems, Degruter (Scopus index) (**Under review**)

References

1. W. Bender, D. Gruhl, N. Morimoto and A. Lu, “Techniques for data hiding”. IBM Systems Journal, Vol. 35, No 3.4, pp. 313-336, 1996.
2. Provos, Niels, and Peter Honeyman, "Hide and seek: An introduction to steganography." Security & Privacy, IEEE, Vol. 1, No. 3, pp. 32-44, 2003.
3. A. Cheddad, J. Condell, K. Curran and P. McKevitt, “Digital Image Steganography: Survey and Analyses of Current Methods”. Signal Processing, Elsevier, Vol. 90, No. 3, pp. 727-752, 2010.
4. P. Singh and R S Chadha, “A Survey of Digital Watermarking Techniques, Applications and Attacks”. International Journal of Engineering and Innovative Technology (IJEIT), Vol. 2, No. 9, pp. 165-175, 2013.
5. Amit Kumar Singh, Mayank Dave, and Anand Mohan, “Multilevel Encrypted Text Watermarking on Medical Images Using Spread-Spectrum in DWT Domain”. Wireless Personal Communications, pp.1-18, 2015.
6. W. Zhicheng, L. Hao, Dai Jufeng and W. Sashuang, “Image watermarking based on Genetic algorithm”. IEEE International Conference on Multimedia and Expo, ICME, pp. 1117-1120, 2006.
7. V. Aslantas, A. L. Dogan and Serkan Ozturk, “DWT-SVD based image watermarking using Particle Swarm Optimizer”. IEEE International Conference on Multimedia and Expo, ICME, pp. 241-244, 2008.
8. V. Aslantas, S. Ozer and S. Ozturk, “Improving the performance of DCT-based fragile watermarking using intelligent optimization algorithms”. Optics Communications, Elsevier, Vol. 282, No. 14, pp. 2806–2817, 2009.
9. V. Aslantas, “An optimal robust digital image watermarking based on SVD using differential evolution algorithm”. Optics Communications, Elsevier, Vol. 282, No. 5, pp. 769–777, 2009.
10. N. Nilchi Ahmad R and T. Ayoub, “A new robust digital image watermarking technique based on the discrete cosine transformation and neural network”. IEEE International Symposium on Biometrics and Security Technologies, ISBAST, pp. 1-7, 2008.
11. C-T Yen and Y-J Huang, “Frequency domain digital watermark recognition using image code sequences with a back-propagation neural network”. Multimedia Tools and Applications, Springer, pp. 1-11, 2015.

12. T. S Tagare and S. Kuri, “Digital Image Watermarking -An Overview”. International Journal of Computer Science Information Engineering Technologies, Vol. 1, No. 3, pp. 2277-4408. 2015.
13. R. Singh, “Digital Image Watermarking: An Overview”. International Journal of Research (IJR), Vol. 2, Issue 05, pp. 1087-1094, 2015.
14. V. M. Potdar, S. Han and E. Chang,"A survey of digital image watermarking techniques." 3rd IEEE International Conference on Industrial Informatics (INDIN), pp. 709-716, 2005.
15. P. Parashar and R. K. Singh, “A Survey: Digital Image Watermarking Techniques”. International Journal of Signal Processing, Image Processing and Pattern Recognition Vol. 7, No. 6, pp. 111-124, 2014.
16. N. Ahmidi. and Reza Safabakhsh, “A Novel DCT-based Approach for Secure Color Image Watermarking”. International Conference on Information Technology: Coding and Computing, IEEE, pp. 709-713, 2004.
17. Han Baoru, and Jingbing Li. "Medical Image Watermarking in Sub-block Three-dimensional Discrete Cosine Transform Domain." International Journal Bioautomation, Vol. 20, No. 1, pp. 69-78 2016.
18. Kumar Arvind, Pragya Agarwal, and Ankur Choudhary. "A Digital Image Watermarking Technique Using Cascading of DCT and Biorthogonal Wavelet Transform." International Conference on Recent Cognizance in Wireless Communication & Image Processing, Springer, pp. 21-29, 2016.
19. M. Barni and F Bartolini, “Improved Wavelet-Based Watermarking Through Pixel-Wise Masking”. IEEE Transactions On Image Processing, Vol. 10, No. 5, pp. 783-791, 2001.
20. Ganic Emir, and Ahmet M. Eskicioglu. "Robust DWT-SVD domain image watermarking: embedding data in all frequencies." Workshop on Multimedia and Security, ACM, pp. 166-174, 2004.
21. Nikita Kashyap and G. R. Sinha (2012), "Image watermarking using 3-level discrete wavelet transform (DWT)". International Journal of Modern Education and Computer Science Vol. 4, No. 3 pp. 50-56.
22. Nagpal Sujata, Shashi Bhushan, and Manish Mahajan. "An Enhanced Digital Image Watermarking Scheme for Medical Images using Neural Network, DWT and RSA." International Journal of Modern Education and Computer Science (IJMECS), Vol. 8, No. 4, pp. 46-56 2016.

23. Jeong, Jaehun. "PSO Optimized Multipurpose Image Watermarking Using SVD and Chaotic Sequence." 10th International Conference on Bio-Inspired Computing--Theories and Applications, BIC-TA, Springer, Vol. 562, p. 1, 2016.
24. Mallick, Ajay Kumar, and Sushila Maheshkar. "Digital Image Watermarking Scheme Based on Visual Cryptography and SVD." 4th International Conference on Frontiers in Intelligent Computing: Theory and Applications (FICTA), Springer, pp. 589-598, 2016.
25. Nandi Sarthak, and V. Santhi, "DWT–SVD-Based Watermarking Scheme Using Optimization Technique." Artificial Intelligence and Evolutionary Computations in Engineering Systems, Springer, pp. 69-77, 2016.
26. Martin T. Hagan, and Mohammad B. Menhaj, "Training feed forward networks with the Marquardt algorithm". IEEE Transactions on Neural Networks, pp. 989-993, 1994.
27. T. P. Vogl, J. K. Mangis, A. K. Zigler, W. T. Zink and D. L. Alkon, "Accelerating the convergence of the back-propagation method." Biological cybernetics, Vol. 59, No. 4-5, pp. 257-263, 1998.
28. R. A. Jacobs, "Increased Rates of Convergence through Learning Rate Adaptation". Neural Networks, Vol. 1, No. 4, pp. 295-308, 1988.
29. D.E Rumelhart, G.E. Hinton, R.J. Williams (1986), "Learning internal representations by error propagation". Parallel Data Processing, M.I.T. Press, Cambridge, Vol.1, Chapter 8, pp. 318-362, 1986.
30. C-C Lai, H-C Huang and C-C Tsai, "Image watermarking scheme using singular value decomposition and micro-genetic algorithm". International conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), IEEE, pp. 469-472, 2008.
31. P. Kumsawat, K. Attakitmongcol and A. Srikaew, "An Optimal Robust Digital Image Watermarking Based on Genetic Algorithms in Multiwavelet Domain". WSEAS Transactions On Signal Processing, Vol. 5, No. 1, pp. 42-51, 2009.
32. Poonam, S. Kundu, S. Kumar and K. Chander, "Efficient Genetic Algorithm based Image Watermarking using DWT-SVD Techniques". International Conference on Computing Sciences (ICCS), IEEE, pp. 82-87, 2012.
33. Lai. Chih-Chin, Chih-Hsiang Yeh, Chung-Hung Ko, and Chin-Yuan Chiang. "Image watermarking scheme using Genetic algorithm." Sixth International Conference on Genetic and Evolutionary Computing (ICGEC), IEEE, pp. 476-479, 2012.

34. M. Vafaei, H. Mahdavi-Nasab and H. Pourghassem, “A New Robust Blind Watermarking Method Based on Neural Networks in Wavelet Transform Domain”. World Applied Sciences Journal, Vol. 22, pp. 1572-1580, 2013.
35. A. Chaudhry, B. Sikandar, M. Ishtiaq, A. Jaffar, J. Y. Kim, M Ishtiaq and T. A. Tuan, Genetic Swarm Based Robust Image Watermarking. 7th International Conference on Ubiquitous Information Management and Communication, ACM, p. 6, 2013.
36. M. Ali, C. Wook Ahn and M. Pant (2014), "A robust image watermarking technique using SVD and differential evolution in DCT domain." Optik-International Journal for Light and Electron Optics, Vol. 125, No. 1, pp. 428-434, 2014.
37. Musrrat Ali, Chang WookAhn and Patrick Siarry, “Differential evolution algorithm for the selection of optimal scaling factors in image watermarking”. Engineering Applications of Artificial Intelligence, Vol. 31, No. 31, pp. 15–26, 2014.
38. J. Han, X. Zhao and C. Qiu, “A digital image watermarking method based on host image analysis and genetic algorithm”. Journal of Ambient Intelligence and Humanized Computing, pp. 1-9, 2015.
39. Hu Xuelong, Xu Lian, Lin Chen, and Yongai Zheng. "Robust blind watermark algorithm of color image based on neural network." International Conference on Neural Networks and Signal Processing, IEEE, pp. 430-433, 2008.
40. N. Mohananthini and G. Yamuna. "Watermarking for images using wavelet domain in Back-Propagation neural network”. International Conference on Advances in Engineering, Science and Management (ICAESM), IEEE, pp. 100-105, 2012.
41. I.A Nasir and A. Abdurrman. "A Robust Color Image Watermarking Scheme Based on Image Normalization." Proceeding of the World Congress on Engineering, Vol. 3, pp. 3-5. 2013.
42. Hemraj Saini "Efficient hybrid watermarking approach by using SVD, DWT, and Back Propagation Neural Network." International Advance Computing Conference (IACC), IEEE, pp. 985-990, 2014.
43. Mei Shi-Chun, Li Ren-Hou, Dang Hong-Mei, and Wang Yun-Kuan. "Decision of image watermarking strength based on artificial neural-networks”. 9th International Conference on Neural Information Processing, ICONIP, IEEE, pp. 2430-2434, 2002.
44. Qun-ting Yang, Tie-gang Gao, and Li Fan. "A novel robust watermarking scheme based on neural network” International Conference on Intelligent Computing and Integrated Systems (ICISS), IEEE, pp. 71-75, 2010.

45. Nallagarla Ramamurthy, and Dr S. Varadarajan. "Robust Digital Image Watermarking Scheme with Neural Network and Fuzzy Logic Approach."International Journal of Emerging Technology, Advanced Engineering, Vol. 2, No. 9, pp. 555-562, 2012.
46. Mona M Soliman, Aboul Ella Hassanien, Neveen I. Ghali, and Hoda M. Onsi. "An adaptive watermarking approach for medical imaging using swarm intelligent." International Journal of Smart Home, Vol. 6, No. 1, pp. 37-50 , 2012.
47. Cheng Mingzhi, Li Yan, Zhou Yajian, and Lei Min. "A combined DWT and DCT watermarking scheme optimized using genetic algorithm." Journal of Multimedia, Vol. 8, No. 3, pp. 299-305, 2013.
48. Kumar, B., Singh, H. V., Singh, S. P., & Mohan, A., "Secure spread-spectrum watermarking for telemedicine applications". Journal of Information Security, Vol. 2, No. 2, pp. 91–98, 2011.
49. Giakoumaki, A., Pavlopoulos, S., & Koutsouris, D., "A medical image watermarking scheme based on wavelet transform". 25th Annual International Conference of IEEE-EMBS, San Francisco, pp. 1541–1544, 2004.
50. http://www.digitalwatermarkingalliance.org/faqs.asp
51. B. Jagadeesh, P. Rajesh Kumar, and P. Chenna Reddy, "Robust Digital Image Watermarking Scheme in Discrete Wavelet Transform domain using Support Vector Machines". International Journal of Computer Applications, Vol. 73, No. 14, pp. 1-7, 2013.
52. Chun-hua Li, Ling He-fei, Lu Zheng-ding, "Semi-fragile watermarking based on SVM for image authentication". International Conference on Multimedia and Expo, IEEE, Beijing, China, pp. 1255–1258, 2007.
53. Micheal Agbaje, Oludele Awodele, and Chibueze Ogbonna, "Applications of Digital Watermarking to Cyber Security (Cyber Watermarking)". Proceedings of Informing Science & IT Education Conference (InSITE), pp. 1-1, 2015.
54. Amit Kumar Singh, Mayank Dave and Anand Mohan, "Hybrid Technique for Robust and Imperceptible Multiple Watermarking using Medical Images", Journal of Multimedia Tools and Applications: An International Journal, Springer, pp. 1-21, 2015.
55. M. Terry, "Medical Identity Theft and Telemedicine Security". Telemedicine and e-Health, Vol. 15, No. 10, pp. 1-5, 2009.
56. Dan Bowman, http://www.fiercehealthit.com/story/researchers-use-digital-watermarks-protect-medical-images, 2012
57. Michael Ollove, www.usatoday.com/story/.../stateline-identity-thefts-medical.../5279351,2009.

58. Mousavi, Seyed Mojtaba, Alireza Naghsh, and S. A. R. Abu-Bakar. "A heuristic automatic and robust ROI detection method for medical image watermarking." Journal of digital imaging, Springer, Vol. 28, No. 4, pp. 417-427, 2015.
59. Solanki, Neha, and Sanjay K. Malik. "ROI based medical image watermarking with zero distortion and enhanced security." International Journal of Modern Education and Computer Science, Vol. 6, No. 10, pp. 40-48, 2014.