STM JOURNALS

Journal of Artificial Intelligence Research & Advances
ISSN: 2395-6720(online)
Volume 2, Issue 3
www.stmjournals.com

Analysis of Image Watermarking Techniques against Various Noise Attacks for Medical Images using Genetic Algorithm (GA)

Reddy V*, Siddaiah P
[1]Department of ECE, University College of Engineering and Technology,
Acharya Nagarjuna University, Guntur, Andhra Pradesh, India

Abstract

In this paper, we have presented a dual secure digital image watermarking algorithm based on discrete wavelet transforms (DWT), lifting wavelet transforms (LWT) and singular value decomposition (SVD) using genetic algorithm (GA) for medical images. The natural image is chosen as cover image and is decomposed up to three levels using discrete wavelet transform. The medical image is chosen as a watermark. The genetic algorithm is used to embed and extract the watermark. The encryption is proposed to be effected using RSA and AES encryption algorithms. A graphical user interface (GUI) which enables the user to have an ease of operation in loading the image, watermark it, encrypt it and also retrieve the original image whenever necessary is also designed and presented in this paper. Peak signal to noise ratio (PSNR) and normalized correlation coefficient (NC) are computed to measure the image quality of the proposed technique. Experimental results show that the proposed watermarking technique has good imperceptibility and robustness against to image processing attacks such as sharpening, smoothening, motion blur, salt and pepper noise, gaussian noise, speckle noise and poisson noise.

Keywords: *DWT, LWT, SVD, GA, RSA and AES*

****Author for Correspondence*** E-mail: venugopalreddy.sai@gmail.com

INTRODUCTION

Telemedicine combines medical information system with information technology that includes use of computers to receive, store and distribute medical information over long distances. Currently, telemedicine applications in tele-consulting, tele-diagnosis, tele-surgery and remote medical education plays a vital role in the evolution of the healthcare domain [1]. The transmission, storage and sharing of electronic medical data through the networks have many purposes such as diagnosis, finding new drugs and for scientific research. Exchange of medical image between hospitals located in different geographical locations is a common practice.

Hence, the healthcare industry demands secure, robust and more information hiding techniques promising strict secured authentication and communication through internet or mobile phones. So, it is necessary to develop the new techniques to improve the security of medical images. The security of the medical images is purely based on the following things such as (i) Confidentiality (ii) Integrity (iii) Authentication [1–3]. Confidentiality is the protection of data from unauthorized disclosure. It means that only the entitled users have access to the information [1]. Integrity is the assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion or replay) [4]. Authentication is the assurance that the communicating entity is the one that it claims to be, a proof that the information belongs indeed to correct patient [5].

To provide the above security to the contents embedded into the image and also to the image, now-a-days we have used watermarking technique.

In this work, we have implemented a dual security approach for maintaining the data integrity of the medical images. Watermarking and encryption of watermarked image is

proposed (Figure 1). The watermark is proposed to be implemented using a hybrid discrete wavelet transform (DWT) and singular value decomposition (SVD) approach. This watermarking procedure is optimized using genetic algorithm (GA) where GA is used to find the optimum value of parameters used in the watermarking scheme to obtain the trade-off between imperceptibility and robustness. A measure is achieved by comparing the PSNR and NC values and optimizing the final watermark accordingly. A RSA algorithm is implemented to encrypt the image. The performance of the watermarking approach and encryption is validated by the performance measure like PSNR, NC, SSIM and CV.

METHODOLOGIES

This work aims at exploiting the features of discrete wavelet transforms (DWT), lifting wavelet transforms (LWT) and singular value decomposition (SVD) to provide a robust and imperceptible watermark. Similarly, RSA and AES algorithms are used for encrypting the watermarked images to provide an extra layer of security. This section dwells on these concepts and methods used in this research work.

A. Discrete Wavelet Transforms (DWT)

Images are usually non-stationary two-dimensional signals and wavelet transform is effective in such case. The discrete wavelet transform (DWT) generates a matrix which is used for image processing since it captures both frequency and location information. Discrete wavelet transformation (DWT) when applied on image, it decompose image into four frequency sub-bands (LL, HL, LH, HH) where, LL refers to low pass band and other three sub-bands corresponds to horizontal (HL), vertical (LH) and diagonal (HH) high pass bands [6, 7]. Figure 4 shows two-level DWT decomposition of image. In general, the watermark can be inserted into low frequency sub-bands (LL) because it increases the robustness of watermark but at the same time it may degrade the image significantly. High frequency bands (HH) contains edges and textures and changes that are caused due to watermark data inserted in such band cannot be noticed by human eye [8].

B. Lifting Wavelet Transforms (LWT)

Lifting wavelets come under the category of second generation wavelets that have distinctive advantages over traditional first generation wavelets [9]. The lifting wavelets trim down the computing time and memory requirements as they adopt an in position realization of wavelet transform. Unlike traditional wavelets, the computations for lifting wavelets are performed in integer domain rather than real domain. More over the inverse process in lifting wavelets is ruination of the processes performed during the forward transformation. Lifting designs perfect reconstruction filter banks by beginning from the basic nature of the wavelet transform. Wavelet transforms build sparse representations by exploiting the correlation inherent in most real world data [10, 11].

C. Singular Value Decomposition (SVD)

The singular value decomposition (SVD) based watermarking technique is to find the SVD of the cover image or each block of the cover image, and then modify the singular values to embed the watermark. There are two main properties to employ SVD method in digital watermarking scheme [12, 13]: Firstly, the singular values of an image have very good stability, that is, when a small perturbation is added to an image, its singular values does not change significantly. Secondly, the singular values represent intrinsic algebraic image properties.

In general, the watermark can be scaled by a scaling factor which is used to control the strength of the watermark. It is found that the scaling factor is set to be constant in some SVD-based studies. However, many argued that considering a single and constant scaling factor may not be applicable [14]. The larger the *SF*, the more the distortion of the quality of the host image (transparency) and the stronger the robustness. On the other hand, the smaller the scali8ng factor, the better the image quality and the weaker the robustness [15]. SVD decomposes an M x N real matrix A into a product of three matrices $^{A=US}V^T$, where U and V^T are M x N and N x N orthogonal matrices, respectively. S is an N x N diagonal matrix. The elements of S are only nonzero on the diagonal and are called the *SV*s of A.

D. Encryption Algorithms

Ron Rivest, Adi Shamir, and Leonard Adleman (RSA) Algorithm. RSA is an asymmetric key encryption algorithm [16]. Over thousands bits long numbers are used. Therefore, it can avoid attacks like brute force, man-in-middle and so on. RSA algorithm involves the following steps: (a) Key (private, public) generation. (b) Encryption is performed using receiver's public key. c) At the receiver's side decryption is performed using the receiver's private key [16].

Advanced Encryption Standard (AES) was published by NIST (National Institute of Standards and Technology) in 2001 [17]. It has 128,192, or 256 bits variable key length. AES encryption is fast and flexible in block ciphers and can be implemented on various platforms. AES (specifies a cryptographic algorithm that can be used to protect the electronic data. AES algorithm is a symmetric block cipher, which can encrypt and decrypt the information. In this work 8 rounds and 256 bit key lengths are used. AES Encryption includes the following steps: as key expansion, initial round, nine rounds, and final round. Initial round has only added round key operation. Each round has the following steps as: substitute bytes, shift rows and mix columns. Now, add round key. In the final round steps a, b, d is performed excluding the step, AES decryption part. A 10 set of reverse rounds are performed to transform encrypted image into the watermarked images using the same encryption key [18].

GENETIC ALGORITHM OPTIMIZATION (GA)

The core components of the Genetic Algorithm [19, 20] are as under:

1) Fitness Value
2) Selection
3) Crossover
4) Mutation

Fitness Function: A Measurement of how well the chromosome fit the search space.

Selection: Selection is based on the survival-of-the-fittest mechanism. Chromosomes are selected based on the fitness value.

Cross Over: The Chromosome with the higher fitness values generate more offspring.

Mutation: After crossover, the strings are subjected to mutation. Mutation of a bit involves flipping it changing from 0 to 1 and vice versa with a small probability. The three genetic algorithms; operators, selection, crossover, and mutation are applied to the chromosomes repeatedly to determine the best solution over successive generations [21–23]. In this work, genetic algorithm function available in the Matlab optimization tool box is used in the proposed work. The population size is fixed at 20. The elite count used is fixed at 10 % of the population which is 2. The selection is based on the ranking. The cross over fraction is fixed at 0.2 and the adaptive feasible mutation function is used. The migration of the population is fixed as forward with a forward fraction of 0.2. The maximum number of generations is fixed at 100.

PROBLEM FORMULATION FOR MULTI -OBJECTIVE OPTIMIZATION

In this work, the type of wavelet in a particular wavelet family of discrete wavelet transform (DWT) and the scaling factor used in singular value decomposition (SVD) are using the multi-objective optimization function. The fitness function used for this multi-objective optimization is given by eqn (1).

Min {f = (100-PSNR) + (1-NC) + (1-SSIM) + MSE} (1)

The peak signal to noise ratio (PSNR) is used to find the deviation of watermarked and attacked image from the original image. Eqn (2) represents the PSNR. In this equation mean squared error (MSE) for two M * N monochrome images *f* and *z* and it is given by eqn (3). Max-Bits give the maximum possible pixel value (255) of the image.

$$PSNR = 10X \log_{10} \frac{MaxBits^2}{MSE} \quad (2)$$

$$MSE = \frac{1}{MxN} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} ((f(x,y) - z(x,y))^2 \quad (3)$$

Normalized coefficient (NC) gives a measure of the robustness of watermarking. After extracting the watermark, the normalized correlation coefficient (NC) is computed between the original watermark and the extracted watermark using eqn (4). This is used to judge the existence of the watermark and to measure the correctness of the extracted watermark.

$$NC=\frac{\sum_{i}^{j} w(i,j)w'(i,j)}{\sqrt{\sum_{i}^{j} w(i,j)^2 \sum_{i}^{j} w'(i,j)^2}} \quad (4)$$

Where, w and w' represents the original and extracted watermark, respectively.

PROPOSED ALGORITHM

The water marking is proposed to be implemented using a hybrid approach which encompasses discrete wavelet transforms (DWT), lifting wavelet transforms (LWT) and singular value decomposition (SVD) techniques. The resultant of multi-objective optimization in form type of wavelet in a particular wavelet family of discrete wavelet transform (DWT) and the scaling factor used in singular value decomposition (SVD) is used in the process of embedding and extracting the watermark. In this algorithm, Medical image is taken as the watermark and it is embedded in each block of the Natural image (cover image) by altering the wavelet coefficients of selected DWT sub bands. The steps involved in this process are described below.

a) **Watermark Embedding and Encryption**

Step 1: Obtain the medical image to be embedded and the input natural.

Step 2: Perform DWT by using the optimized selection of wavelet obtained through optimization approach on the natural image to decompose it into four non-overlapping sub-bands: LL, HL, LH, and HH.

Step 3: Apply SVD to HL sub-band i.e.,= $UiSiViT$ where, $Ai= HL$

Step 4: Apply SVD to the watermark i.e.,= $UwSwVwT$ where, $W= Watermark$

Step 5: Modify the singular value of Ai by embedding singular value of W such that , $Siw= Si+\alpha \times Sw$,where Siw is modified singular matrix of Ai and α denotes the scaling factor, is used to control the strength of watermark signal the value of which is optimized through Genetic Algorithm(GA) using the multi objective function.

Step 6: Then apply SVD to this modified singular matrix Siw i.e., $Siw=U\_SiwS\_SiwV\_$ and obtain the modified DWT coefficients, i.e., $Aiw=Ui \times S\_Siw \times ViT$.

Step 7: Obtain the watermarked image Aw by applying inverse DWT using one modified and other non modified DWT coefficients.

Step 8: Then, encrypt the watermarked image with RSA or AES algorithms in the time domain.

b) **Decryption and Watermark Extraction**

Step 1: Decrypt the encrypted image to obtain the watermarked image.

Step 2: Apply the chosen DWT to decompose the watermarked image Aw in to four sub bands (i.e., LL,).

Step 3: Apply SVD to HL sub band i.e., = $UiwSiwViwT$, Where $Aiw=HL$.

Compute $w*= (Siw-Si)/\alpha$, where $Sw*$ singular matrix of extracted watermark

Step 4: Apply SVD to $Sw*$ i.e., $Sw*= U\_Sw*S\_Sw*V\_Sw*T$

Step 5: Now, compute extracted watermark $W*$ i.e., $W*= Uw \times S\_Sw* \times VwT$.

RESULTS AND DISCUSSION

The natural image, *Lena* is taken as a representative image for analysis and the MRI Knee image is considered to be the watermark (Figure 2). The watermark embedding process is optimized using genetic algorithm and the results presented below are the best of the twenty trial runs. The below tabular column specifies performance of different types of wavelets families and the scalar function as optimized by the proposed approach.

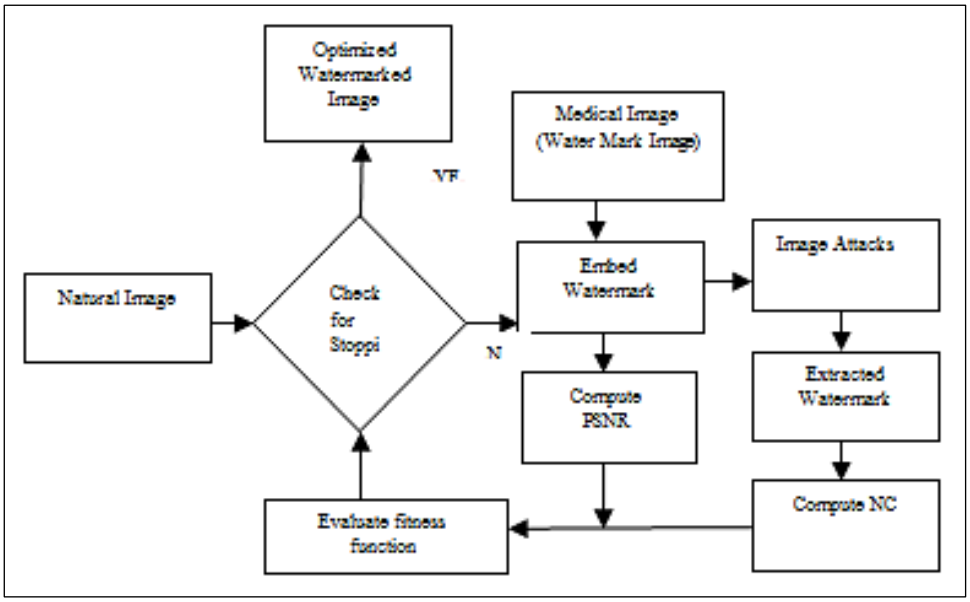


Fig. 1: *Block Diagram of Optimization of Watermarking using GA.*

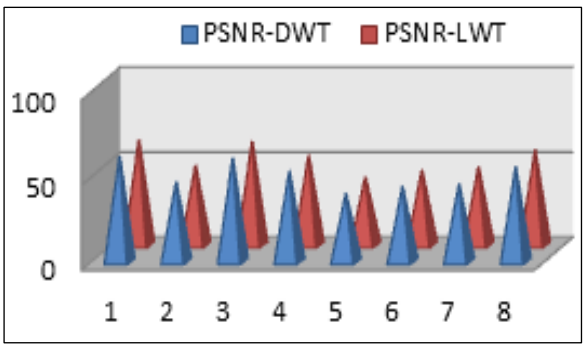
Fig. 2: *(a) Natural Image (Lena), (b) Watermark Image (MRI Knee).*

A. Performance Analysis of Water Marking for Different Noise Attacks Using DWT and LWT Approaches.

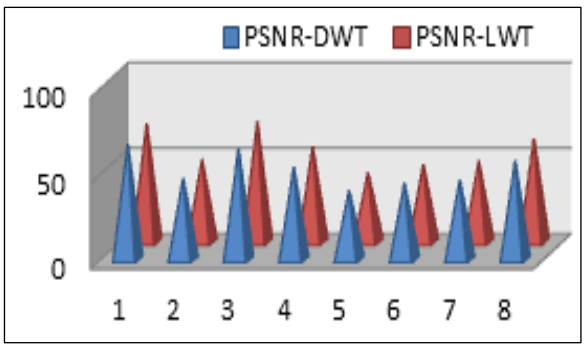
The below (Table 1) provides the implications of different noise attacks on the robustness and imperceptibility for both DWT and LWT schemes. The attacks considered are sharpening, smoothening, motion blur, salt and pepper noise, gaussian noise, speckle noise and poisson noise. It can be observed that the salt and pepper noise results in high degradation of PSNR values when compared to other attacks across different wavelet families. Similarly, the degradation in NC values is higher when the watermark is attacked with motion blur. Speckle noise comes best to motion blur when degrading the performance of NC.

Table I: *Comparison in Performance of Watermarking for Different Noise Attacks between DWT and LWT.*

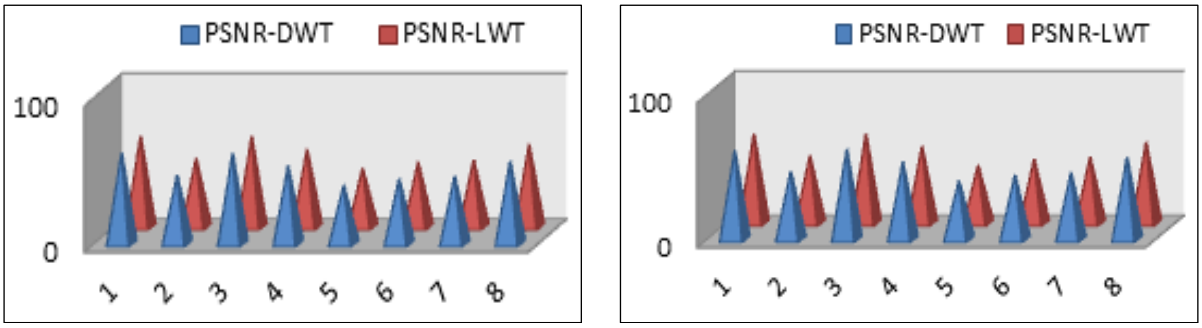
DWT	Attack	PSNR (db)		NC	
		DWT	LWT	DWT	LWT
Haar	No Attack	62.36	62.36	0.995769	0.995769
	Sharpening	47.24	47.24	1	1
	Smoothening	61.57	61.57	0.996084	0.996084
	Motion Blurr	53.65	53.44	0.9716	0.974207
	Salt and Pepper Noise	40.48	40.42	0.994597	0.993887
	Gaussian Noise	44.67	44.69	0.992693	0.992304
	Speckle Noise	46.23	46.35	0.986926	0.984243
	Poisson	56.29	56.59	0.996481	0.99398
Daubechies	No Attack	62.99	62.53	0.992564	0.994752
	Sharpening	47.39	48.15	1	0.991768
	Smoothening	62.81	65.29	0.989782	0.978318
	MotionBlurr	53.95	55.09	0.967783	0.952594
	Salt and Pepper Noise	40.48	40.84	0.99479	0.973889
	Gaussian Noise	44.79	45.23	0.989773	0.975359
	Speckle Noise	46.49	47.22	0.981821	0.966765
	Poisson	56.35	58.81	0.995885	0.975324
Symlets	No Attack	62.64	62.64	0.994439	0.994439
	Sharpening	47.28	47.31	1	1
	Smoothening	61.86	62.30	0.994702	0.992475
	Motion Blurr	53.72	53.72	0.970815	0.970815
	Salt and Pepper Noise	40.55	40.49	0.99083	0.990525
	Gaussian Noise	44.72	44.71	0.991929	0.99167
	Speckle Noise	46.29	46.37	0.985746	0.983928
	Poisson	56.66	56.70	0.993374	0.993172
Bior Splines	No Attack	61.53	62.96	0.99983	0.992739
	Sharpening	47.29	47.27	1	1
	Smoothening	62.00	62.72	0.993975	0.990362
	Motion Blurr	53.92	53.92	0.968281	0.968281
	Salt and Pepper Noise	40.52	40.46	0.990341	0.995948
	Gaussian Noise	44.68	44.67	0.992841	0.993033
	Speckle Noise	46.49	46.49	0.981936	0.981647
	Poisson	56.31	56.49	0.996272	0.994702



a) For Haar Wavelet

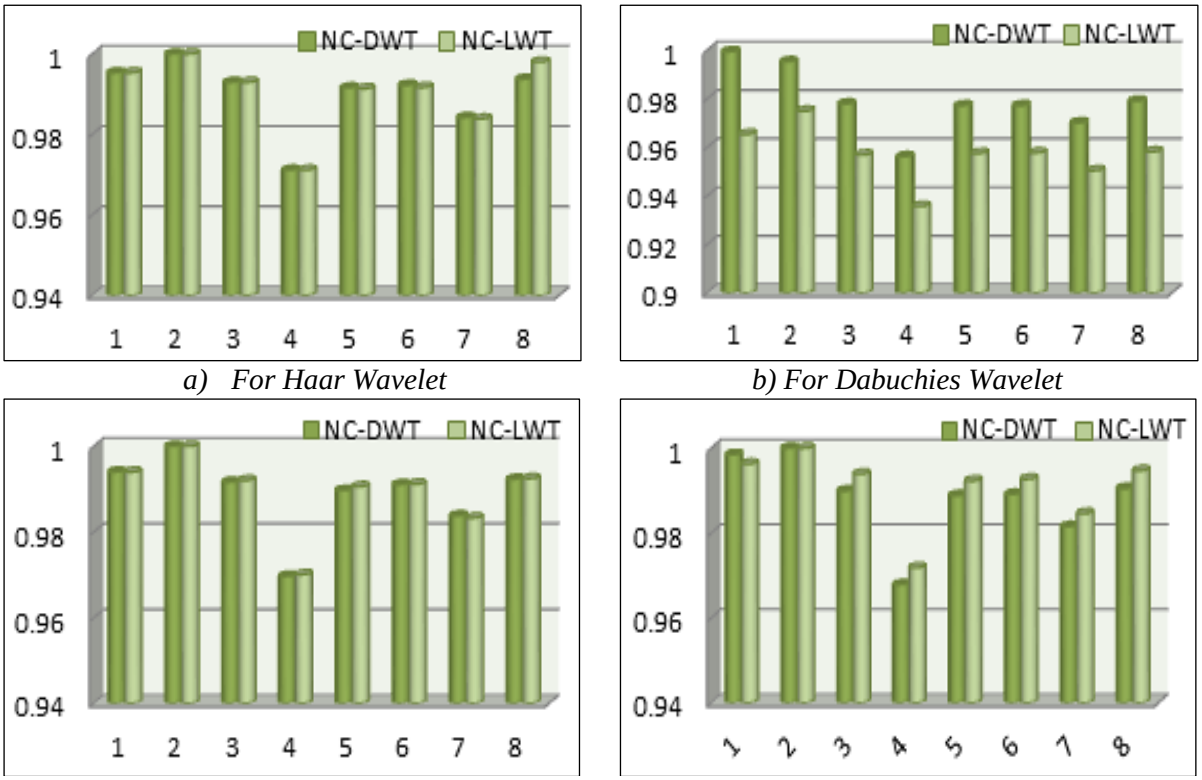


b) For Dabuchies Wavelet



c) For Symlets Wavelet *d) For Biorsplines Wavelet*

Fig. 3: *Plot of Degradation in Performance of PSNR for No attack, Sharpening, Smoothening, Motion Blurr, Salt and Pepper Noise, Gaussian Noise, Speckle Noise, Poisson Noise Attacks.*



a) For Haar Wavelet *b) For Dabuchies Wavelet*

c) For Symlets Wavelet *d) For Biorsplines Wavelet*

Fig. 4: *Plot of Degradation in Performance of NC for No Attack, Sharpening, Smoothening, Motion Blurr, Salt and Pepper Noise, Gaussian Noise, Speckle Noise, Poisson Noise Attacks.*

The attacks considered to represent in the above (Figures 3, 4) are s follows:

1. No attack
2. Sharpening
3. Smoothening
4. Motion blurr
5. Salt pepper noise
6. Gaussian noise
7. Speckle noise
8. Poisson noise and blue color bars for DWT and pink color bars for LWT schemes.

CONCLUSIONS

In this paper, a medical image watermarking algorithm based on SVD-DWT-LWT using GA was proposed. The cover image was decomposed to a required level in wavelet domain. The wavelet coefficients were embedded by changing the values of appropriately selected sub-band coefficients in DWT domain using GA optimization. Experimental results show that the values of PSNR of the watermarked images in the proposed method are always greater than 40 db and it can represent acceptable

robustness against image processing attacks such as sharpening, smoothening, motion blur, salt and pepper noise, gaussian noise, speckle noise and poisson noise. Algorithm is robust to sharpening, smoothening, motion blur, salt and pepper noise, gaussian noise, speckle noise and poisson noise attacks. But, it can be observed that the salt and pepper noise results in high degradation of PSNR values when compared to other attacks across different wavelet families. Similarly, the degradation in NC values is higher when the watermark is attacked with motion blur. Speckle noise comes best to motion blur when degrading the performance of NC.

REFERENCES

1. Coatrieux et al. Relevance of watermarking in medical imaging. *Proceedings of IEEE EMBS International Conference on Information Technology Applications in Biomedicine*. 2000; 250–255p.
2. Coatrieux et al. A review of image watermarking applications in healthcare. *Proceedings of 28th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*. 2006; 4691–4694p.
3. Chao et al. A data-hiding technique with authentication, integration, and confidentiality for electronic patient records. *IEEE Trans. Inf. Technol. Biomed*. 2002; 6(1): 46–53p.
4. Jennett et al. Telemedicine and security. Confidentiality, integrity, and availability: A Canadian perspective. *Studies in Health Technology and Informatics*. 1996; 29: 286–298p.
5. Coatrieux et al. Strict integrity control of biomedical images. *Proc. SPIE Security and Watermarking of Multimedia Contents III*. SPIE 2001; 43(14): 229–240p.
6. Al-Haj A. Combined DWT-DCT Digital Image Watermarking. *Journal of Computer Science*. 2007; 3(9): 740–746p.
7. Aymen et al. Performance Optimization of Discrete Wavelets Transform Based Image Watermarking Using Genetic Algorithms. *Journal of Computer Science*. 2008; 834–841p.
8. Nikolaidis A and Pitas I. Asymptotically optimal detection for additive watermarking in the DCT and DWT domains. *IEEE Trans. Image Process.* 2003; 12(5): 563–571p.
9. Lee et al. A line-based, memory efficient and programmable architecture for 2D DWT using lifting scheme. *IEEE Int. Symposium on Circuits and Systems*, Sydney, Australia, 2001; 330–333p.
10. Daubechies and Sweldens W. Factoring wavelet transforms into lifting schemes. The Journal of Fourier Analysis and Applications. 1998; (4): 247–269p.
11. Sweldens W. The lifting scheme: a custom-design construction of biorthogonal wavelets. *Applied and Computational Harmonic Analysis.* 1996; 3(15): 186–2000p.
12. Kahaner D, Moler C, Nash S et al. *Numerical methods and software.* Prentice-Hall, Inc., Upper Saddle River, NJ, 1989.
13. Chang C, Tsai P, Lin C et al. SVD-based digital image watermarking scheme. Pattern Recognition Letters. 15 Jul 2005; 26(10): 1577–1586p.
14. Aslantas V. A singular-value Decomposition-Based Image Watermarking Using Genetic Algorithm. *International Journal of Electronics and Communications.* 2007; 62: 386–393p.
15. Tsai et al. Image Watermarking Scheme Using Singular Value Decomposition and Micro-genetic Algorithm. In: *Proceedings of International Conference on Intelligent Information Hiding and Multimedia Signal Processing.* 2008; 469–472p.
16. Rivest RL, Shamir A, Adleman L et al. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*. 1978; 21(2): 120–126p.
17. Stallings W. *Cryptography and Network Security: Principles and Practice*. 5th Edn, Prentice Hall, 2010.
18. Federal Information Processing Standards Publication 1997, Advanced Encryption Standard (AES), Nov 26, 2001.
19. Thede S. An Introduction to Genetic Algorithms. *Journal of Computing Sciences in Colleges*. Oct 2004; 20(1): 115–123p.

20. Goldberg DE. Genetic Algorithm in Search, Optimization and machine Learning. Addison-Weseley, 1989.
21. Srinivas M and Patnaik LM. Genetic Algorithm: A Survey. IEEE, 1994.
22. Kumsawat P, Attakitmongcol K and Srikaew A et al. A New Approach for Optimization in Image Watermarking by Using Genetic Algorithms. *J. IEEE Transactions on Signal Processing*. 2005; 53, 4707–4719p.
23. Grefenstette JJ. Optimization of Control Parameters for Genetic Algorithms. *IEEE Transactions on Systems, Man and Cybernetics*. 1986; 16(1): 122–128p.

Authors bibliographies

CH. Venugopal Reddy is working as Professor in the department of ECE, Nalanda Institute of Engineering and Technology, Guntur, affiliated to JNTU Kakinada, A.P. It has more than 15 years of teaching experience. He got his B.Tech (ECE) from K.S.R.M. Engineering College, Kadapa, A.P, affiliated to S.V University, Tirupathi, A.P. M.E (Commn. Sys) from Dr. M.G.R Engineering College, Chennai, T.N affiliated to Anna University, Chennai. He is presently pursuing Ph.D in the area of digital image water marking, Acharya Nagarjuna University, Guntur. He has a good numbers of research publications in his credit. His research interests are in the areas of image processing, signal processing and communications.

Dr. P. Siddaiah obtained B.Tech degree in Electronics and Comm. Engg. from JNTUA college of Engineering in 1988. He received his M.Tech degree from SV University, Tirupathi. He did his PhD program in JNTU, Hyderabad. He is the chief Investigator for several outstanding projects sponsored by Defense organizations and AICTE, UGC and ISRO. He is currently working as a Principal, University College of Engineering and Technology, Acharya Nagarjuna University, Guntur, A.P, India. He has taught a wide variety of courses for UG and PG students and guided several projects. Several members successfully completed their PhD under his guidance. He has published several papers in national and international journals and conferences. He is a life member of FIETE, IE and MISTE.

Cite this Article
Reddy and Siddaiah. Analysis of Image Watermarking Techniques against Various Noise Attacks for Medical Images using Genetic Algorithm(GA). *Journal of Artificial Intelligence Research and Advances*. 2015; 2(3): 36–44p.