International Journal of Bio-Science and Bio-Technology
Vol.7, No.6 (2015), pp.55-64
http://dx.doi.org/10.14257/ijbsbt.2015.7.6.07

Medical Image Watermarking Schemes against Salt and Pepper Noise Attack

Mr. Venugopal Reddy CH[1] and Dr. Siddaiah.P[2]

[1]Research Scholar, Dept of ECE, University College of Engineering and Technology, Acharya Nagarjuna University, Guntur, A.P, India
[2]Professor and Principal, University College of Engineering and Technology, Acharya Nagarjuna University, Guntur, A.P, India
[1]venugopalreddy.sai@gmail.com, [2]siddaiah_p@yahoo.com

Abstract

In this paper, we 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 GA is used while 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 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 salt & pepper noise attack.

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

1. Introduction

In the recent years, medical images are produced from a wide variety of digital imaging equipments, such as computed tomography (CT), magnetic resonance imaging (MRI), computed radiography (CR) and so forth. With the increasing use of internet and appearance of new system such as picture archiving and communication systems (PACS), the usability of digital form of medical images has been increased [1]. Images in digital imaging equipments can be printed on films or papers. Moreover, in these equipments images with patient data in DICOM format can be stored on different types of storage media such as CD or DVD [2]. DICOM is a standard file format for transmission and storage of digital medical images in health care centers [3]. Header in DICOM image format stores patient's information such as patient identification number, name, sex, and age [4]. Insurance companies, hospitals and patients may want to change this data for various reasons. Therefore, protecting medical images against this threat is necessary. Watermarking can be used as a solution. Digital image watermarking means placing a hidden data (patients information) within the body of an image without changing image size or format. After embedding the data, watermarked medical image can still conform to the DICOM format [5].

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. The Water mark is proposed to be implemented using a Hybrid Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) approach. This

ISSN: 2233-7849 IJBSBT

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.

2. 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.

2.1 Discrete Wavelet Transforms (DWT)

In two-dimensional DWT, each level of decomposition produces four bands of data denoted by LL, HL, LH, and HH [6]. The LL sub-band can further be decomposed to obtain another level of decomposition. This process is continued until the desired number of levels determined by the application is reached In DWT-based watermarking; the DWT coefficients are modified to embed the watermark data. Because of the conflict between robustness and transparency, the modification at a given level is usually made in HL, LH, and HH sub-bands [7, 8].

2.2 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].

2.3 Singular Value Decomposition (SVD)

SVD is one of the most useful tools of linear algebra with several applications in image compression, and other signal processing fields[12].Every real matrix A can be decomposed into a product of 3 matrices $A = USV^T$, where U and V are orthogonal matrices, $U^TU = I$, $V^TV = I$, and $S = \text{diag}(\lambda 1, \lambda 2, ...)$[12,13]. The diagonal entries of S are called the singular values of A, the columns of U are called the left singular vectors of A, and the columns of V are called the right singular vectors of A. This decomposition is known as the *Singular Value Decomposition (SVD)* of A, and can be written as

$$A = \lambda 1 U1 V1^T + \lambda 2 U2 V2^T + \ldots + \lambda r\, Ur Vr^T,$$

Where r is the rank of matrix A. It is important to note that each singular value specifies the luminance of an image layer while the corresponding pair of singular vectors specifies the geometry of the image [14]. In SVD-based watermarking, several approaches are possible. A common approach is to apply SVD to the whole cover image, and modify all the singular values to embed the watermark data. An important property of SVD-based watermarking is that the largest of the modified singular values change very little for most types of attacks [15].

2.4 Encryption Algorithms

Ron Rivest, Adi Shamir, and Leonard Adleman (RSA) Algorithm. RSA is an asymmetric key encryption algorithm [16]. Over 1000 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 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.1. Key Expansion, 2. Initial Round, 3. Nine Rounds, 4. Final Round. Initial round has only added round key operation. Each round has the following steps, a. Substitute Bytes, b. Shift Rows. Mix columns. Add Round Key. In the final round steps a, b, and d are performed, excluding step: c. 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].

3. Genetic Algorithm Optimization (GA)

The core components of the GA [19, 20] are 1) Fitness Value, 2) Selection, 3) Crossover,4) Mutation.1)Fitness Function: A Measurement of how well the chromosome fit the search space.2)Selection: Selection is based on the survival-of-the-fittest mechanism. Chromosome are selected based on the fitness value.3)Cross Over: The Chromosome with the higher fitness values generate more offspring.4)Mutation: After Crossover , the strings are subjected to mutation. Mutation of a bit involves flipping it changing 0 to 1 and vice versa with a small probability. The three GA operators, selection, crossover, and mutation, are applied to the chromosomes repeatedly to determine the best solution over successive generations [21, 22].

In this work Genetic Algorithm (GA) 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 2. The selection is based on 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.

4. 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 Equation (1).

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

The Peak Signal to Noise Ratio (PSNR) is used to find the deviation of watermarked and attacked image from the original image. Equation (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 Equation (3). MaxBits gives 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 Equation (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' represent the original and extracted watermark, respectively.

Structural Similarity Index (SSIM) index is a method for measuring the similarity between embedded and extracted watermark images. The SSIM is measured between two windows X and Y of common size N*N on image using Eq. (5).

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \quad (5)$$

5. 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.,Ai=$UiSiViT$ where Ai=HL

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

Step 5: Modify the singular value of Ai by embedding singular value of W such that , Siw= Si+α×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., $Siw=U\_SiwS\_SiwV\_Si$ 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., $LL,,HL,and\ HH$).

Step 3: Apply SVD to HL sub band i.e., $w=UiwSiwViwT$, Where $Aiw=HL$ Compute $Sw*=(Siw-Si)/\alpha$, 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., $W*=Uw\times S\_Sw*\times VwT$.

6. 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. The watermark embedding process is optimized using Genetic Algorithm (GA) and the results presented below are the best of the twenty trial runs.

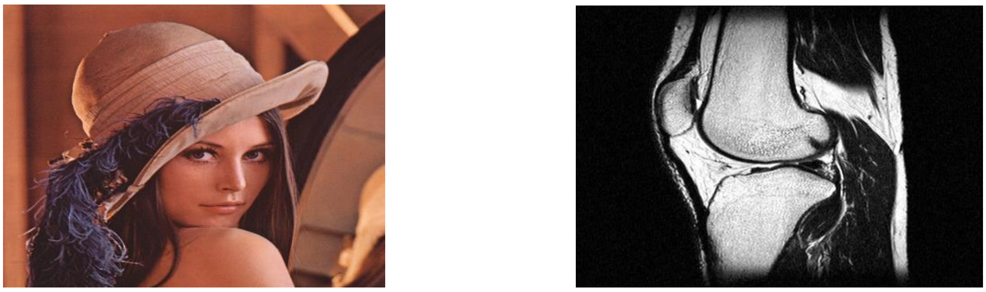


Figure 2. Images: a) Natural Image (Lena) b)Watermark Image (MRI Knee

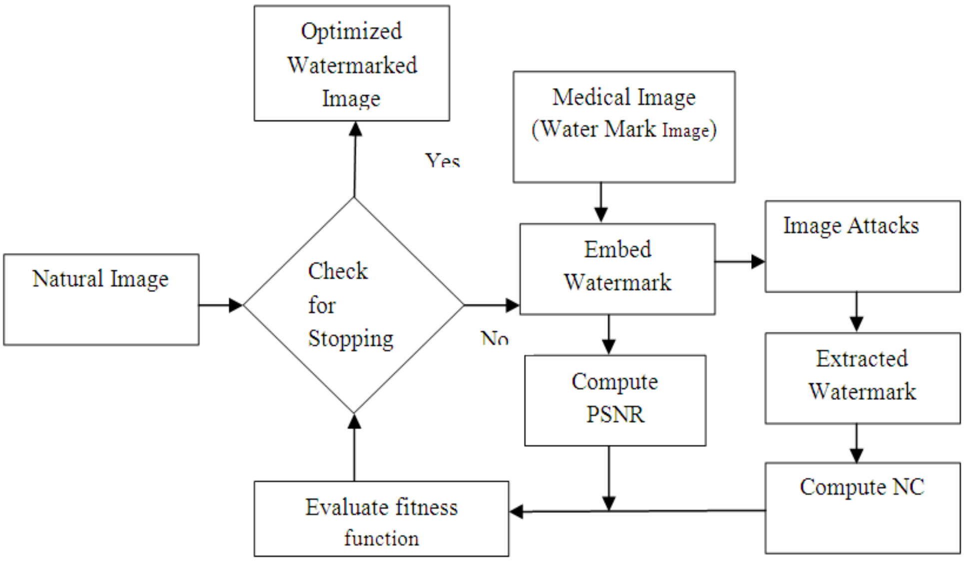


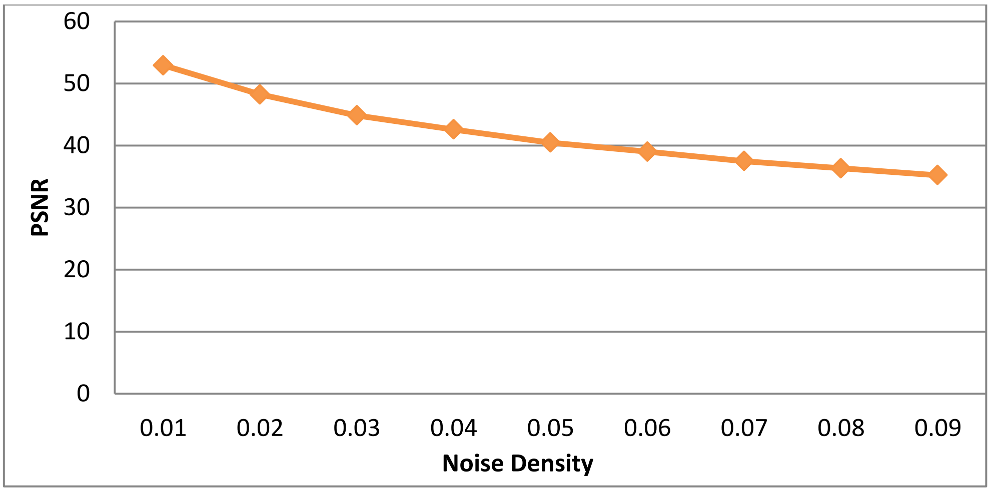
Figure 1. Block Diagram of Optimization of Watermarking using GA

6.1. Performance Analysis of Watermarking for Different Densities of Salt & Pepper Noise Attacks Using DWT and LWT Approaches

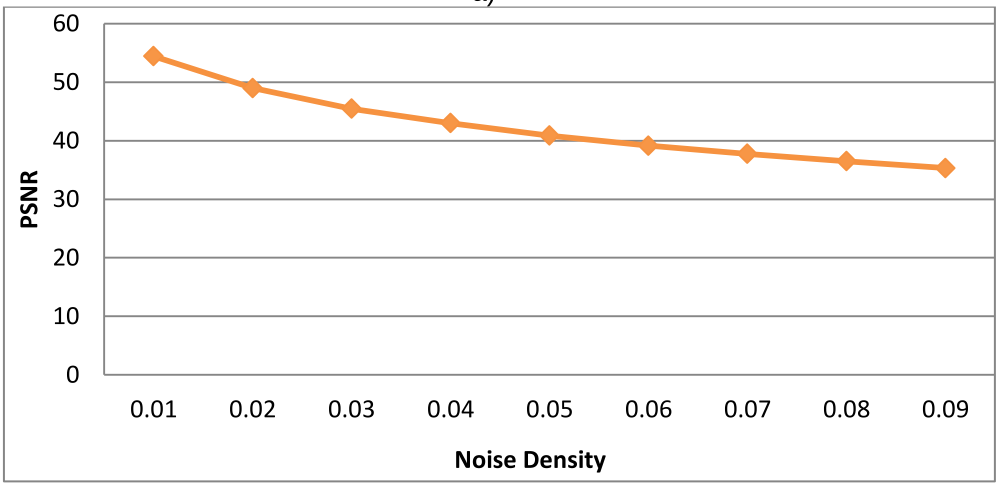
Table 1 presents the degradation in PSNR performance for different densities of salt & pepper noises. This analysis is done for the DWT and LWT schemes.

Table 1. Reduction in PSNR with the Increase of Salt and Pepper Noise Density for DWT &LWT

Density of Salt and Pepper Noise	PSNR(db)		NC		SSIM-RSA		SSIM-AES	
	DWT	LWT	DWT	LWT	DWT	LWT	DWT	LWT
0.01	52.93	54.4205	0.991902	0.976371	0.998883	0.999169	0.999059	0.999345
0.02	48.2185	48.9979	0.991079	0.975561	0.998883	0.999169	0.999059	0.999345
0.03	44.8524	45.4575	0.991365	0.974931	0.998835	0.999169	0.999011	0.999345
0.04	42.5775	42.9952	0.989278	0.974909	0.998923	0.99917	0.999099	0.999346
0.05	40.4804	40.8588	0.995223	0.975387	0.998676	0.99917	0.998852	0.999346
0.06	38.9974	39.1446	0.988584	0.974185	0.99883	0.999138	0.999006	0.999315
0.07	37.4954	37.7365	0.986428	0.973335	0.998923	0.999138	0.999099	0.999315
0.08	36.3283	36.4796	0.987293	0.973072	0.99883	0.999138	0.999006	0.999315
0.09	35.2229	35.3054	0.985274	0.97792	0.998923	0.999088	0.999099	0.999264
1.0	11.6759	11.7015	0.916056	0.917444	0.998923	0.99914	0.999099	0.999316

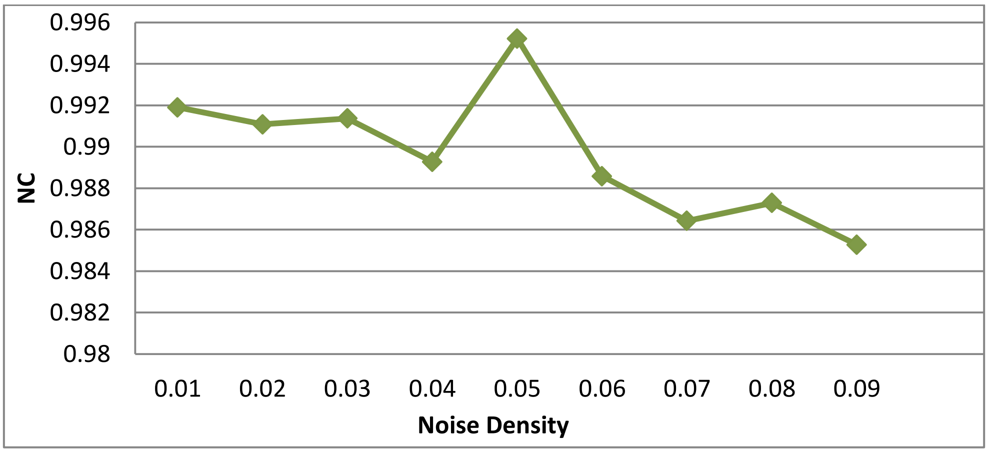


a)

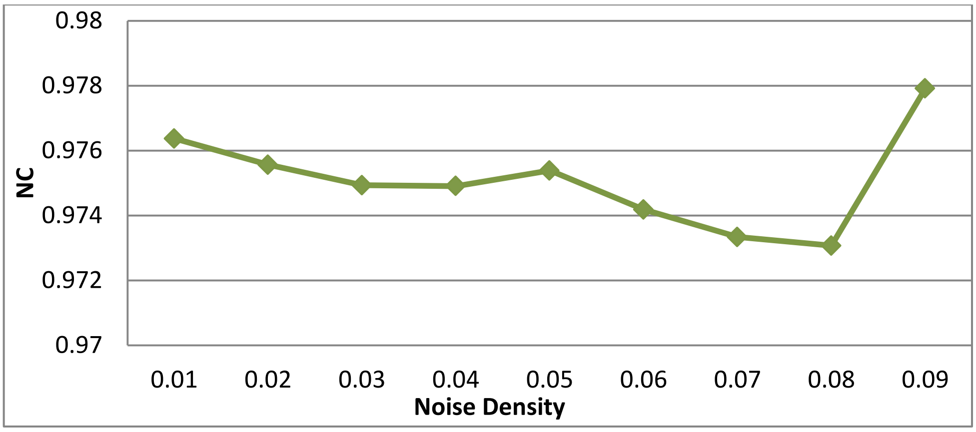


b)

Figure 3. Reduction in PSNR with the Increase of Salt and Pepper Noise Density: a) for DWT, b) for LWT

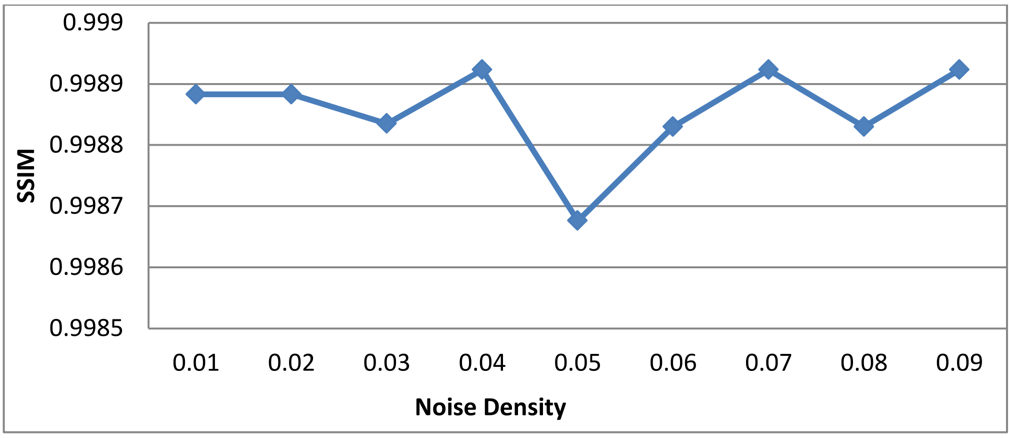


a)

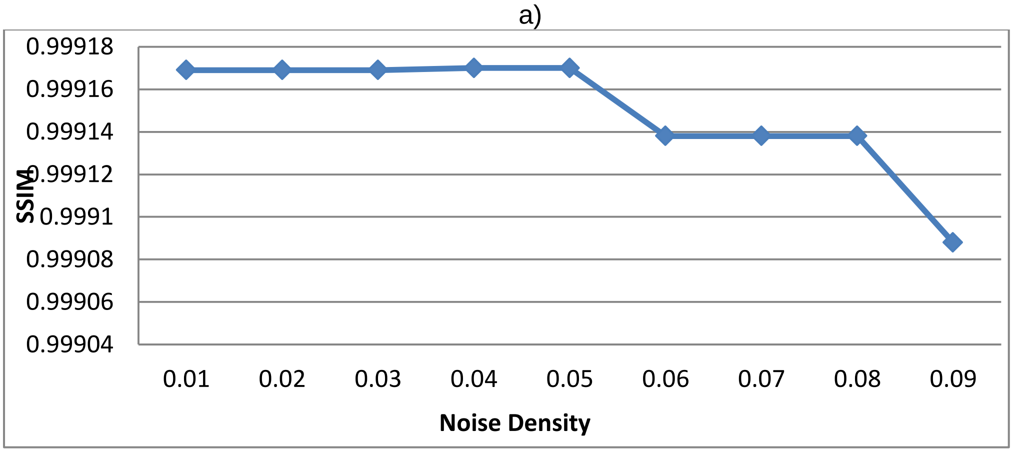


b)

Figure 4. NC Variation with Increase of Salt and Pepper Noise Density: a) for DWT, b) for LWT



a)



b)

Figure 5. SSIM Variation with the Increase of Salt and Pepper Noise Density: a) for DWT, b) for LWT

Figure 2.a) & b) provide the visual representation of how the PSNR value changes when there is increase in noise density. It can be observed as the noise density increased there is a rapid degradation in PSNR value for both DWT and LWT schemes.

The watermarked images were subject to salt and pepper noise attacks with various noise density ranges, which indicate the percentage of gray levels added into the image.

The results from the Table 1 prove that the images are more resilient to salt and pepper noise attacks for low density ranges.

7. Conclusions

In this paper, a medical image watermarking algorithm based on SVD-DWT-LWT using GA was proposed. The cover image was decomposed to 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 demonstrate that as the noise density increased there is a rapid degradation in PSNR value for both DWT and LWT schemes. But, the proposed algorithm maintains almost all high NC, SSIM values for the variation of noise density of salt and pepper noise attack for both DWT and LWT schemes.

References

[1] D. Anand and U. C. Niranjan, "Watermarking medical images with patient information", Proc. 20th Annual Int. Conf. of IEEE engineering in medicine and biology, vol. 20, no. 2, **(1998)**.
[2] C. S. Lu and H. Y. M. Liao, "Multipurpose watermarking for image authentication and protection", IEEE Trans. Image Processing, vol. 10, no. 10, **(2001)**, pp. 1579-1592.
[3] G. Coatrieux, C. Quantin, J. Montagner, M. Fassa, F. A. Allaert and C. Roux, "Watermarking medical images with anonymous patient identification to verify authenticity", Journal of Studies in Health Technology and Informatics, vol. 136, **(2008)**, pp. 667-672.
[4] J. M. Zain, A. R. Fauzi and A. Aziz, "Clinical evaluation of watermarked medical images", Proc. 28th IEEE EMBS Annual International Conference, New York City, USA, **(2006)**, pp. 5459-5462.
[5] X. Guo and T. Zhuang, "A lossless watermarking scheme for enhancing security of medical data in PACS", Proc. SPIE Medical Imaging: PACS and Integrated Medical Information Systems: Design and Evaluation, CA, United States, vol. 5033, **(2003)**, pp. 350-359.
[6] N. M. Makbol and B. E. Khoo, "Robust blind image watermarking scheme based on Redundant Discrete Wavelet Transform and Singular Value Decomposition", Int. J. Electron. Commun. (AEÜ), **(2012)**, http://dx. doi. org/10. 1016/j. aeue. 2012. 06. 008.
[7] A. A-H. Abu-Errub and Aymen, "Performance Optimization of Discrete Wavelets Transform Based Image Watermarking Using Genetic Algorithms", Journal of Computer Science, **(2008)**, pp. 834-841.
[8] S. Dandapat, J. Xu, O. Chutatape and S. M. Krishnan, "Wavelet transform domain data embedding in a medical image", Proc. 26th Annual Int. Conference of the IEEE EMBS, **(2004)**, pp. 1-5.
[9] W. H. Chang, Y. S. Lee, W. S. Peng and C. Y. Lee, "A line-based, memory efficient and programmable architecture for 2D DWT using lifting scheme", IEEE Int. Symposium on Circuits and Systems, Sydney, Australia, **(2001)**, pp. 330-333.
[10] Daubechies and W. Sweldens, "Factoring wavelet transforms into lifting schemes", The Journal of Fourier Analysis and Applications , vol. 4, **(1998)**, pp. 247-269.
[11] W. Sweldens, "The lifting scheme: a custom-design construction of biorthogonal wavelets", Applied and Computational Harmonic Analysis, vol. 3, no. 15, **(2000)**, pp. 186.
[12] D. Kahaner, C. Moler and S. Nash, "Numerical methods and software", Prentice-Hall, Inc., Upper Saddle River, NJ, **(1989)**.
[13] R. Liu and T. Tan, "An SVD-based watermarking scheme for protecting rightful ownership", IEEE Trans. Multimedia, vol. 4, no. 1, **(2002)**, pp. 121 -128.
[14] V. Aslantas, L. A. Dog, Abreven and S. Ozturk, "DWT-SVD based image watermarking using particle swarm optimizer", Proc. IEEE Int. Conf. Multimedia Expo, **(2008)**, pp. 241-244.
[15] Q. Li, C. Yuan and Y.-Z. Zhong "Adaptive DWT-SVD domain image watermarking using human visual model", Proc. 9th Int. Conf. Adv. Commun. Technol., **(2007)**, pp. 1947 -1951.
[16] R. L. Rivest, A. Shamir and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", Communications of the ACM, vol. 21, no. 2, **(1978)**, pp. 120-126.
[17] W. Stallings, "Cryptography and Network Security: Principles and Practice", 5th Edition, Prentice Hall, **(2010)**.
[18] "Federal Information Processing Standards Publication 197", Advanced Encryption Standard (AES), **(2001)** November 26.
[19] S. Thede, "An introduction to genetic algorithms", Journal of Computing Sciences in Colleges, vol. 20, Issue 1, **(2004)** October, pp. 115-123.
[20] D. E. Goldberg, "Genetic Algorithm in Search , Optimization & machine Learning", Addison-Weseley, **(1989)**.
[21] M. Srinivas and L. M. Patnaik, "Genetic Algorithm : A Survey", IEEE, **(1994)**.

[22] B. Jagadeesh, S. S. Kumar and K. R. Rajeswari, "A Genetic Algorithm based oblivious image watermarking scheme using Singular Value Decomposition", IEEE International Conference on Networks and Communications, **(2009)**, pp. 224-229.
[23] J. J. Grefenstette, "Optimization of Control Parameters for Genetic Algorithms", IEEE Transactions on Systems, Man and Cybernetics, vol. 16, no. 1, **(1986)**, pp. 122-128.
[24] C.-S. Shieh, H.-C. Huang, F.-H. Wang and J.-S. Pan, "Genetic watermarking based on transform domain techniques", Pattern Recognition, vol. 37, no. 3, **(2004)**, pp. 555-565.

Authors

Venugopal Reddy, Professor in the department of ECE, Nalanda Institute of Engineering & Technology, Guntur, affiliated to JNTU Kakinada, A.P. Has more than 15 years of teaching experience. He got his B. Tech (ECE) from K.S.R.M. Engg College, Kadapa, A. P, affiliated to S.V University, Tirupathi, A. P. M.E (Commn.Sys) from Dr. M. G. R Engg 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 No. of research publications in his credit. His research interests are in the areas of Image Processing, Signal Processing and Communications.

P. Siddaiah, Professor and Principal, University College of Engineering and Technology, Acharya Nagarjuna University, Guntur, A. P, India. He obtained his B.Tech degree in Electronics and Communication Engineering 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 & ISRO. He has published several papers in National and International Journals and Conferences. He is a life member of FIETE, IE, and MISTE.

