AN ENCRYPTION AIDED WATERMARKING ALGORITHM FOR SECURE AUTHENTICATION OF MEDICAL IMAGES

K.Anusudha

Department of Electronics Engineering, Pondicherry University, Pondicherry - 605014, (India)

ABSTRACT

Modern healthcare systems are based on managing diagnostic information of patients through E-health. E-health refers to the Internet enabled healthcare applications involving transacting personal health records or information and other internet based services including e-Pharmacy etc. This paper introduces a hybrid digital watermarking scheme for copyright protection and authentication of medical images. The proposed method is based on Discrete WaveletTransform (DWT) and Singular Value Decomposition (SVD). In this method, two watermark images are hided in the HL and LHsub bands of the cover image after two level decomposition using Haar wavelet by modifying the singular values with thesingular values of the watermark images. Advanced Encryption Standard (AES) is deployed for increasing the level of security of the watermarked medical image. The simulation results demonstrates the capability of the proposed scheme to securely make available security attributes in both frequency and encrypted domain while minimizing image distortion.

Keywords: *Advanced Encryption Standard,Discrete Wavelet Transformation, Singular Value Decomposition,Watermarking.*

1. Introduction

Processing and handling medical information by computers and sharing them over high speed network infrastructure have become a common practice since wide deployment of low cost computing and networking hardware[1]. In the last decade, uses of advanced electronic and digital equipment in healthcare services has been found to increase many folds. Physicians diagnose based on the electronic and digital data [2]. Exchange of medical images between hospitals located in different geographical locations is also on the rise. But unfortunately, this exchange of medical images through insecure open networks -Internet adds top potential risk of espionage provides of changes to occur in medical images and consequently creates a threat of undesirable outcome because little important information contained in the image gets lost or corrupted. Large image databases have been handled in hospitals both for clinical and research purposes. These image databases need to be protected against malicious attacks and made more beneficial by annotating early-diagnosis related information. For this purpose, authentication of the medical images such as X-ray, MRI, Ultrasound, etc can be performed through watermarking, whereby an invisible watermark (secret message) related to the host image is inserted in the host image itself[3]. The secret message can not only make authentication of the host image, but could also be helpful in embedding extra/auxiliary information related to the host image. Secret embedding of the watermark signal, no matter how much invisible it may be, can cause degradation to the resultant image quality. Therefore, reversible watermarking is applied to overcome this drawback by applying a mechanism that can provide the exact original image after the watermark has been successfully extracted [4]. Traditional approaches such as cryptography can also perform this reversibility operation but the basic shortcoming is the

loss of semantic information of the host image, i.e., after encryption the image may not be visible/understandable, which is not the case in watermarking.

The paper aims to develop medical image authentication systems which can not only authenticate medical images but would also be able to secretly communicate auxiliary information.Security of medical information imposes three mandatory characteristics: 1.Confidentiality, 2. Reliability and 3.Non repudiation [5]:

1. Confidentiality means that only the entitled persons have access to the information and that information is not made available or disclosed to unauthorized individuals, entities or processes.

2. Reliability which has two aspects; Integrity means the information has not been modified or destroyed by non-authorized person, and authentication is the proof that the information belongs indeed to the correct patient and is issued from the correct source.

3. Non repudiation is the guarantee that neither of the parties involved will be able to deny having sent or received the message.

Researchers proposed watermarking techniques and reported findings in the literature survey both integrity and confidentiality requirements (Wang et al.,2000; Zhou et al,2001;Chao et al,2002;Giakoumaki et al,2003;Shieh et al,2004; Piva et al,2005;Xuan et al,2006;

Wang et al[6] proposed to embed secret messages in the moderately significant bit of the cover image. A genetic algorithm is developed to find an optimal substitution matrix for the embedding of the secret messages. They also proposed to use a local pixel adjustment process (LPAP) to improve the image quality of the stego image. As the local pixel adjustment process modifies the LSBs, the technique cannot be applied to data hiding schemes based on simple LSB substitution. Zhou et al [7] presented a method that attaches digital signature and EPR into the medical image. Their method uses LSB replacing technique to embed the signature.Chao et al [8] proposed a secure data hiding technique based on the bipolar multiple base conversion to allow a variety of EPR data to be hidden within the same mark image.Giakoumaki et al [9] presented a wavelet based multiple watermarking approach.Their method addresses confidentiality protection and data authentication problems by using three separate watermarks.

Shieh et al [10] a genetic algorithm (GA) based watermarking scheme is presented.GA is used to locate the optimal frequency bands for watermark embedding.Piva et al [11] a simple and secure self recovery authentication technique is presented which hides an image digest in subbands of Discrete Wavelet Transform. Xuan et al [12] have presented histogram shifting based reversible watermarking techniques .In this work, a part of the histogram of high frequency wavelet co-efficients shifted towards right by one point and then watermark is embedded by using the histogram zero point.

2. Digital Watermarking

Digital watermarking is a process whereby arbitrary information is encoded into an image in such a way that the additional payload is imperceptible to image observers.Image watermarking has been proposed as a suitable tool to identify the source,creator, owner, distributor, or authorized consumer of a document or an image .It can also be used to detect a document or an imagethat has been illegally distributed or modified. Encryption, used in cryptography, is aprocess of obscuring information to make it unreadable to observers without specifickeys or knowledge. This technology is sometimes referred to as data scrambling. Watermarking complemented by encryption can serve a large number of purposesincluding copyright protection, broadcast monitoring, and data authentication.

2.1Elements of a watermarking system

Awatermarking system is much like a communication system consisting of three main elements: a transmitter, a communication channel, and a receiver.The embedding of the to-be-hidden information within the host signal plays the role of data transmission; any processing applied to the host data after information concealment, along with the interaction between the concealed data and the host data itself, represents the transmission through a communication channel; the recovery of the hidden information from the host data acts the part of the receiver.

2.2 Embedding

In watermark embedding, or watermark casting, an embedding function $\mathcal{E}$takes the host asset A, the watermark signal w, and, possibly, a key K,and generates the watermarked assetA_w *:*

$$\mathcal{E}(A, w, K) = A_w \qquad (1)$$

2.3Concealment

The main concern of the embedding part of any data hiding system is to make the hidden data imperceptible. This task can be achieved either implicitly, by properly choosing the set of host features and the embedding rule, or explicitly, by introducing a concealment step after watermark embedding. The properties of the human senses must be carefully studied, since imperceptibility ultimately relies on the imperfections of such senses. Thereby, still image and video watermarking will rely on the characteristics of the Human Visual System (HVS), whereas audio watermarking will exploit the properties of the Human Auditory System (HAS).

2.4 Watermark impairments

After embedding, the marked asset A_w, enters the channel, i.e. it undergoes a series of manipulations. Manipulations may explicitly aim at removing the watermark from A_w , or may pursue a completely different goal, such as data compression, asset enhancement or editing. The output of the channel is denoted by the symbol A'_w.

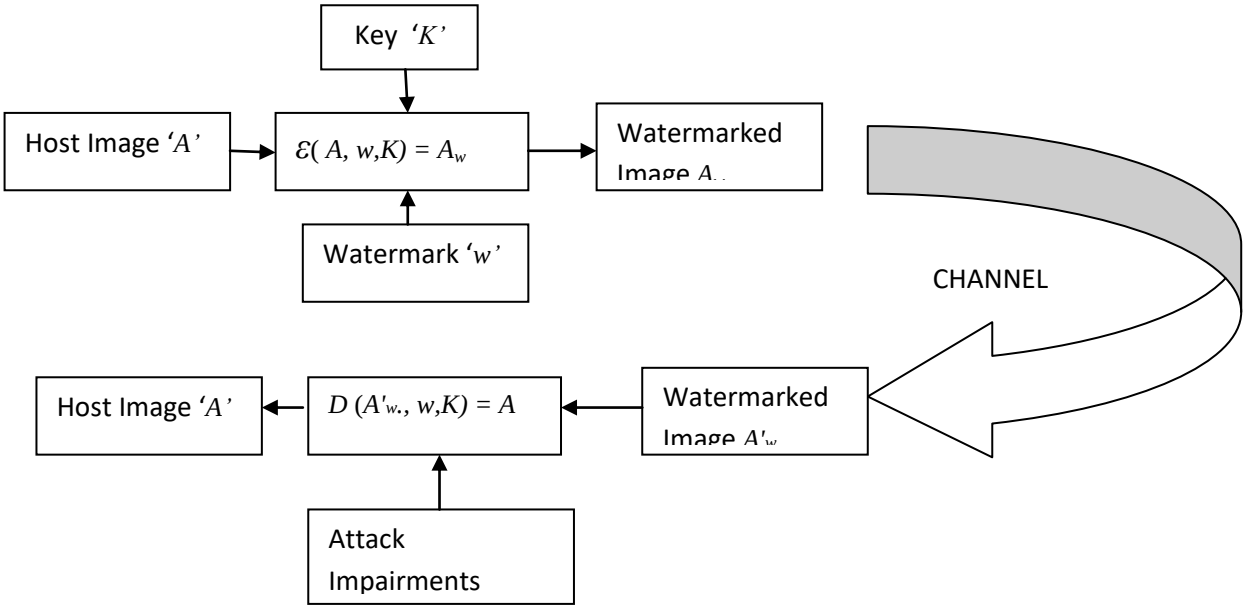


Fig 1. Digital Watermarking system

2.5 Watermark Detection

The receiver part of watermarking scheme can assume two different forms namely blind and non-blind scheme.The distinction between readable and detectable watermarking can be further highlighted by considering the different form assumed by the decoding/detection function D characterizing the system. In blind,

detectablewatermarking, the detector P is a three- argument function accepting asinput a digital asset *A*, a watermark code b, and a secret key *K* (the secret key is an optional argument which may be present or not). As an output *D* decides whether *A* contains b or not, that is

$$D(A,b,K) = 1/0 \quad (2)$$

3. Discrete Wavelet Transform

The DWT divides an image into four parts namely a lower resolution approximation component (LL) as well as horizontal (HL), vertical (LH) and diagonal (HH) detail components. The LL sub band is obtained after low-pass filtering both the rowsand columns and contains a rough description of the image. The HH sub-band is high-pass filtered in both directions and have the high-frequency components along the diagonals. The HL and LH sub bandsare the results of low-pass filtering on one direction and high-pass filtering in the other direction. After the image is processed by the wavelet transform, most of the information contained in the host image is concentrated into the LL image. LH sub band contains mostly the vertical detail information which corresponds to horizontal edges. HL band represents the horizontal detail information from the vertical edges. The process can be repeated to obtain multiple scale wavelet decomposition [13]. Fig. 2 shows the DWT decomposition.

Fig.2. DWT decomposition

4.Singular Value Decomposition (SVD)

Singular value decomposition (SVD) is a general linear algebra technique for a variety of applications including solving most linear least-squares problems, computing pseudo-inverse of a matrix and multivariate analysis[15]. Let A be a general real matrix of order m x n and its SVD is the factorization:

$$A = PQR^T \quad (3)$$

Where P and R are orthogonal (unitary) matrices and Q = diag ($\lambda_1, \lambda_2, \ldots, \lambda_r$), where λ_i, i = 1 to r is the singular values of the matrix A with r = min (m, n) and it satisfies $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_r$.The first r columns of P and R are the left and right singular vectors of A respectively. There are many advantages to use SVD in digital image processing. Firstly, the SVD transformation can be applied to an image with arbitrary sizes. It can be a square or a rectangle. Secondly, singular values of the digital image are less affected if general image processing is performed. Lastly singular values contain intrinsic algebraic properties of an image. T

5. Advanced Encryption Scheme (AES)

Rijndael is a block cipher developed by Joan Daemen and Vincent Rijmen. The algorithm is flexible in supporting any combination of data and key size of 128, 192, and 256 bits. However, AES merely allows a 128 bit data length that can be divided into four basic operation blocks. These blocks operate on array of bytes

and organized as a 4×4 matrix that is called the state. For full encryption, the data is passed through Nr rounds (Nr = 10, 12, 14) .These rounds are governed by the following transformations:

1. Subbyte Transformation: Is a non linear byte Substitution, using a substation table (s-box), which is constructed by multiplicative inverse and Affine Transformation.
2. Shift rows transformation: Is a simple byte transposition, the bytes in the last three rows of the state are cyclically shifted; the offset of the left shift varies from one to three bytes.
3. Mix columns transformation: Is equivalent to a matrix multiplication of columns of the states. Each column vector is multiplied by a fixed matrix. It should be noted that the bytes are treated as polynomials rather than numbers.
4. Add round key transformation: Is a simple XOR between the working state and the round key. This transformation is its own inverse.
5. Expansion key: With AES encryption, the secret key is known to both the sender and the receiver. The AES algorithm remains secure, the key cannot be determined by any known means, even if an eavesdropper knows the plaintext and the cipher text.

6.Proposed Schemes

6.1 Discrete Wavelet Transform Based Watermarking

In the proposed technique the watermark is embedded in the wavelet domain. The DWT (Discrete Wavelet Transform) separates an image into a lower resolution approximation image (LL) as well as horizontal (HL), vertical (LH) and diagonal (HH) detail components. The process can then be repeated to compute multiple "scale" wavelet decomposition. The methods used are as given below:

6.1.1Watermark Embedding

The embedding technique is based on addition of third level DWT decomposed host image and first level decomposed watermark image. The corresponding sub bands of the host image are replaced with the watermark imageto obtain the watermarked image..The reason for different levels of decomposition is to substitute the change in the dimension of the two. embedded into the cover image based on the equation shown below.

$$I_{w,m,n} = DWT(h) + DWT(w) \qquad (4)$$

Where 'h' denotes the coefficients of the transformed host image, 'w' denotes the coefficient of the watermark to be embedded in the host image.Fig 3.depicts the embedding block.

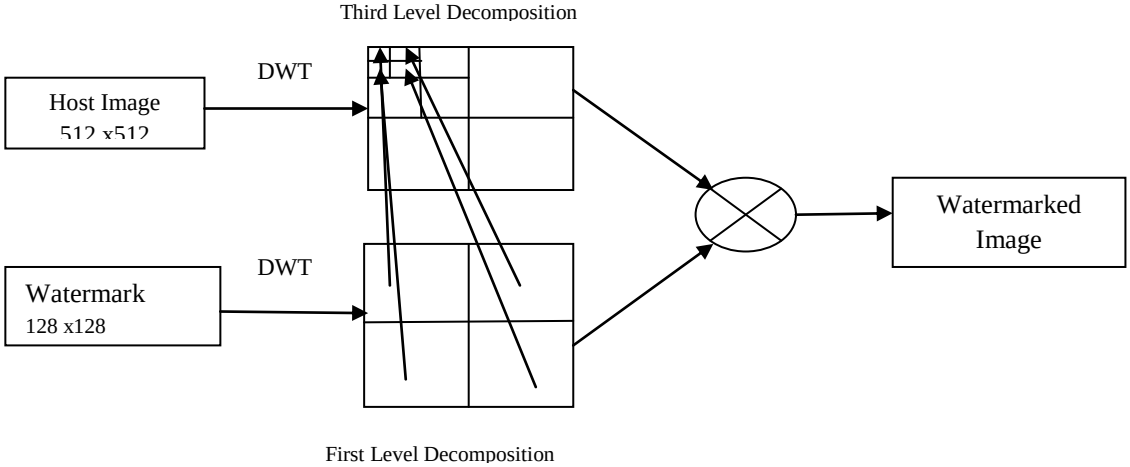


Fig 3.Scheme I Embedding block: Discrete wavelet transformed Watermarking

6.1.2 Watermark Detection

To retrieve the watermark the same level of decompositions are done at the receiver end. Subtraction of the corresponding co-effficients retrieves the original host image.. This method can be easily extended to a multiple watermarks.

6.2.Combined Discrete Wavelet Transform and Singular Value Decomposition Watermarking

The second proposed scheme is based on DWT SVD technique. DWT is very suitable to identify the areas in the host image where a watermark can be embedded effectively. In general most of the image energy is concentrated at the lower frequency sub-bands LL and therefore embedding watermarks in these sub bands may degrade the image significantly. Embedding in the low frequency sub-bands, however, could increase robustness significantly. On the other hand, the high frequency sub-bands HH includes the edges and textures of the image and the human eye is not generally sensitive to changes in such sub-bands. This allows the watermark to be embedded without being perceived by the human eye. Hence to achieve acceptable robustness and imperceptibility watermark images are embedded only on the HL and LH bands of the host image by modifying the singular values of the host image.

6.2.1Algorithm – Embedding the Watermark

Apply 3-level Haar wavelet transform on the host image A.

Step 1: Perform SVD to HL and LH sub bands of the host image.

$$A^k = P^k Q^k R^{kT}, \qquad k=1, 2$$

Where '*k* ' represents one of two sub bands.

Step 2:Apply first level Haar wavelet transform to the watermark images.

Step 3:Perform SVD to HL, LH sub bands of watermark image 1 and watermark image 2 respectively.

$$W^k = P_W^k Q_W^k R_W^{kT}$$

Step 4:Modify the singular values in HL and LH sub bands of the host image with the singular values in HL and LH sub bands of the watermark image 1and watermark image 2 respectively.

$Q_{WM}^k = Q^k + \alpha Q_W^k$

Step 5: Obtain the modified DWT coefficients.

$$A^{*k} = P^k Q_{WM}^k R^{kT}$$

Step 6:Apply inverse DWT using two sets of modified DWT coefficients and two sets of non-modified DWT coefficients to obtain the watermarked imageA_{WM}.

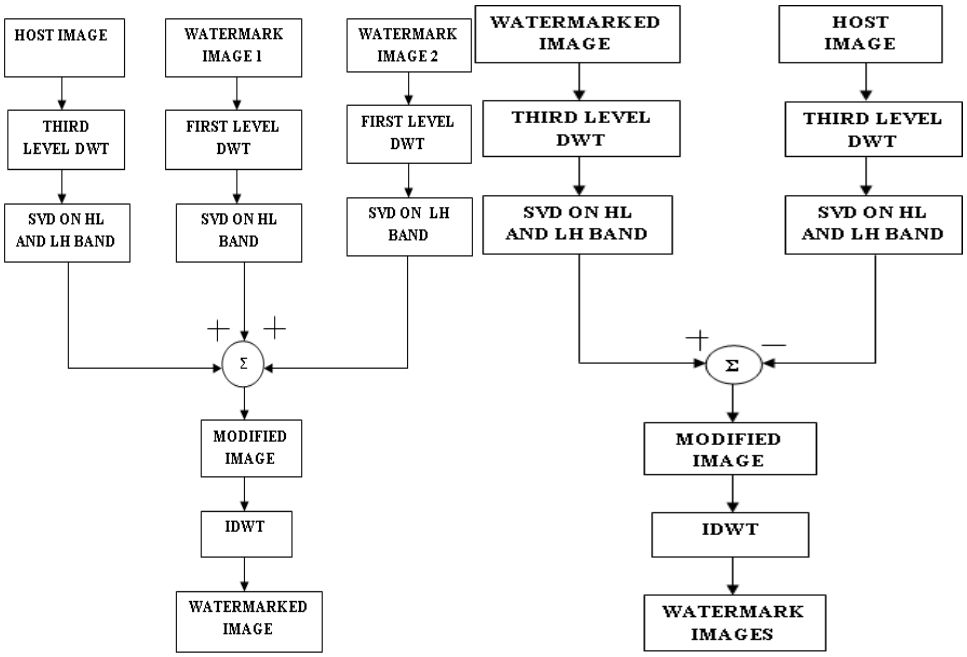


Fig 4. Scheme II: Embedding BlockFig 5. Scheme II: Extraction Block

6.2.2 Algorithm – Extracting the Watermark

Step 1:Perform 3-level Haar wavelet transform on the watermarked image A^{*}_{WM}.

Step 2:Perform SVD to the HL and LH sub bands of the watermarked image

$A^{*k}_{WM}=P^{*k}Q^{*k}_{WM}R^{*kT}$, k =1, 2 Where k represents one of two sub bands..

Step 3:The singular values of watermark images can be extracted as $Q^{*k}_{W}=(Q^{*k}_{WM}-Q^{k})/\alpha$

Step 4:The watermark images can be obtained as

$$W^{*k}=P^{k}_{W}Q^{*k}_{W}R^{kT}_{W}$$

In the proposed model the host image is decomposed by three levels DWT and applying SVD to HL, LH bands. The two watermark images undergoes single level DWT and applying SVD to the HL, LH bands of the watermark image 1 and watermark image 2 respectively. An important property of SVD-based watermarking is that the largest of the modified singular values change very little for most types of attacks. Here watermark image embed only a part (HL, LH) of the host image which will improve the imperceptibility and robustness.

6.3Discrete wavelet Transform and SVD Technique with Advanced Encryption Scheme

The third scheme is proposed to combine advanced encryption scheme with the DWT-SVD watermarking technique. The main objective of the proposed scheme is to increase the level of security to the watermarked medical data transmitted over open channel.

7. Simulation and Analysis

7.1 Results of the proposed scheme

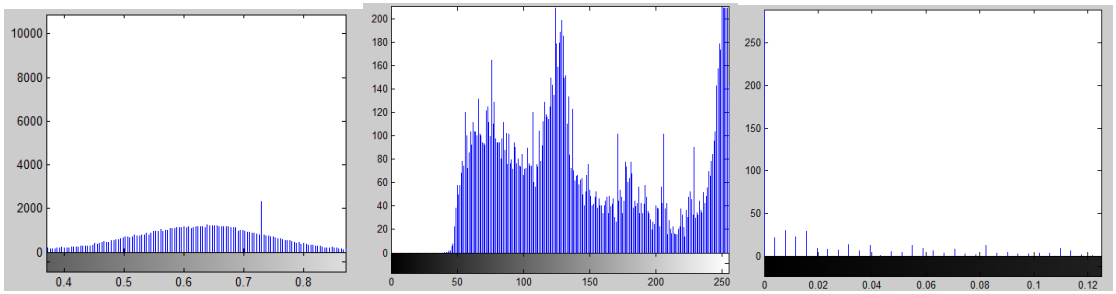
The images taken for the analysis of the three proposed schemes are a host image of dimension 512x512 pixels and the watermarks of dimension 128x128 pixels. The simulation results of the proposed first scheme Discrete wavelet transformed scheme watermarks the host image with one watermark only by means of a random key generation. The simulation resultis shown in Fig 6.

(a) (b) (c)

Fig 6 (a) The Host image 512x512 (b) Watermark image 128x128(c) Watermarked image

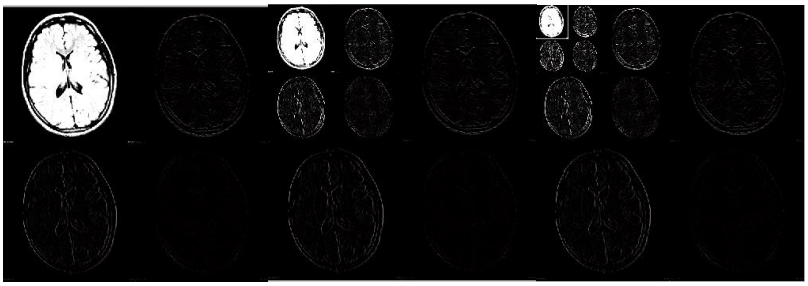
(a) (b) (c)

Fig 7. (a) Host image (b) Watermark I (c) Watermark II



(a) (b) (c)

Fig 8. Histogram of (a) Host image (b)Watermark I (c) Watermark II



(a) (b) (c)

Fig 9.Discrete wavelet transformed host image (a) First level (b) Second level (c) Third level

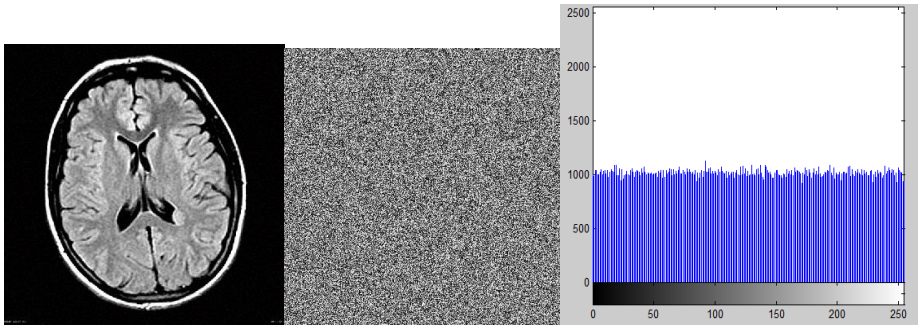


Fig 10.Watermarked ImageFig 11. AES encrypted Watermarked host imageFig 12.Histogram of the Watermarked image

Fig 6-9 shows the simulated output of the second scheme namely the Combined Discrete Wavelet Transform and Singular Value Decomposition Watermarking and Fig 10. Shows the AES encrypted watermarked host image and Fig 11.shows the histogram of the encrypted image.

7.2 Performance analysis

The performance evolution of the watermarking approach is analysed against various attacks. The Peak-Signal-To-Noise is defined as:

$$PSNR = \frac{10log_{10}(255)^2}{MSE} \quad (5)$$

Where 'MSE' is the mean squared error between the original and distorted image and is defined as follows:

$$MSE = \frac{1}{mn}\sum_{i,j=0}^{m-1,n-1}[I(i,j) - K(i,j)] \quad (6)$$

Where m, n gives the size of the image and $I(i,j), k(i,j)$ are the pixel values at location (i,j) of the original and distorted image respectively However, robustness is measured by the normalized correlation coefficient (NC) whose peak value is one and calculated by formula:

$$NC = \frac{\sum_i \sum_j W(i,j) * W'(i,j)}{\sqrt{\sum_i \sum_j W(i,j)^2}\sqrt{\sum_i \sum_j W(i,j)^2}} \quad (7)$$

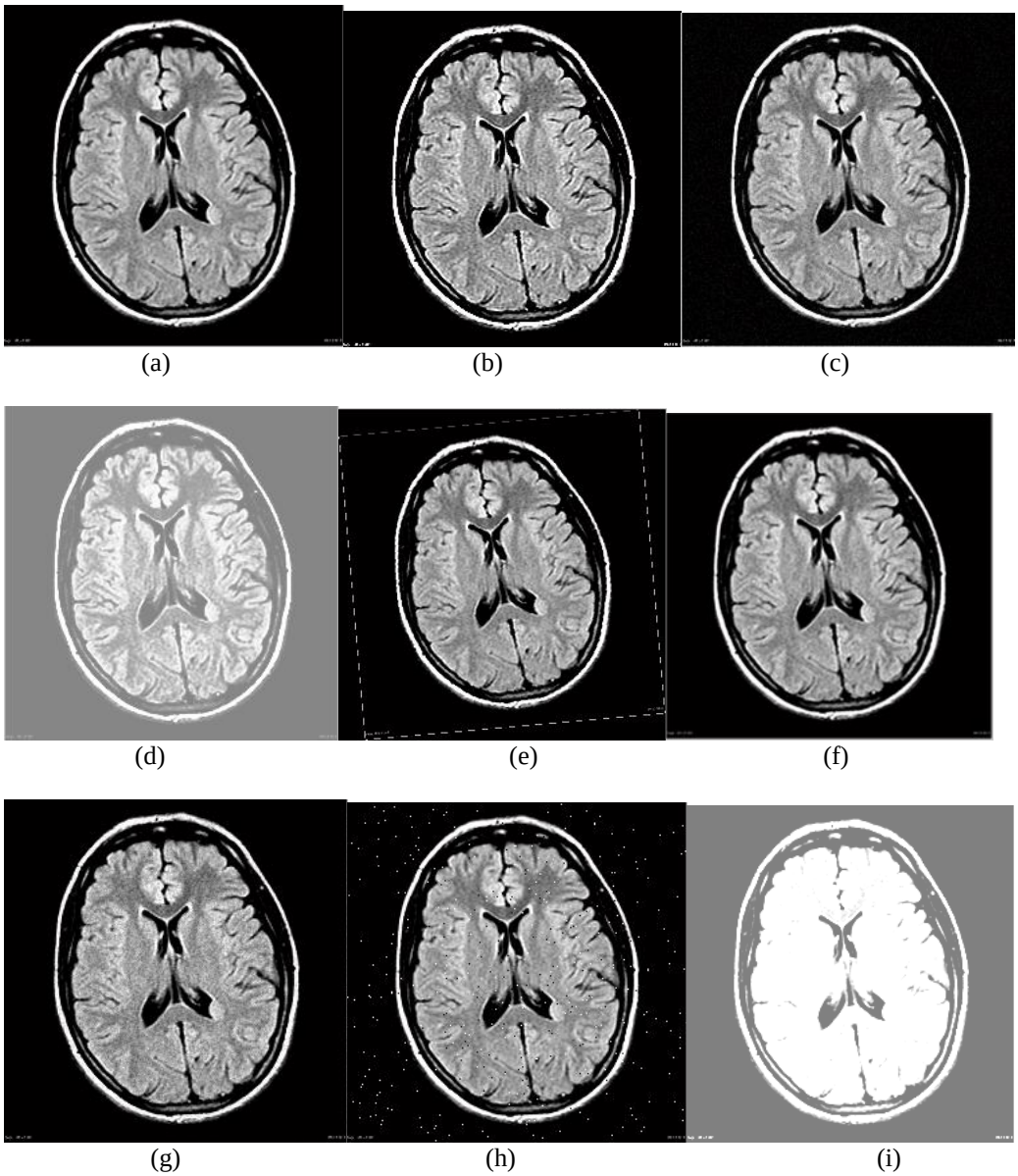
The Number of pixel change per rate gives the changes happening to the pixels of the watermarked image to tat of the host image.

$$\frac{\sum D(i,j)}{W \times H} \times 100\ \% \quad (8)$$

The unified average changing intensity is calculates using :

$$\frac{1}{W \times H}\left[\sum_{i,j}\frac{C_1(i,j)-C_2(i,j)}{2^L-1}\right] \quad (9)$$

The robustness of the proposed techniques are checked by exposing the watermarked image to various types of removal and geometric attacks.Removal attacks aim at removing the watermark signal fromthe watermarked image, without attempting to break the securityof the watermarking algorithm. This type of watermark attack doesnot attempt to find out the encryption techniques used or how thewatermark has been embedded. It results in a damaged watermarkedimage, hence a damaged watermark signal, where no simplepost processing can recover the watermark signal from theattacked data. Included in this category are noising, histogramequalisation, blur, and sharpen attacks.



(a) (b) (c)

(d) (e) (f)

(g) (h) (i)

Fig 13.Noise attacked watermarked Images a) Gaussain Blur b) Sharpening c) Gaussian Noise d) Histogram Equalisation e)Rotation f)Rescaling g)Speckle Noise h)Salt and pepper i) Contrast stretching

Geometry attacks are rather different from removal attacks. Instead of aiming to remove or severely damage the watermark signal, this type of attack intends to distort it. Examples of geometric attacks include rotation, scaling, translation, shearing, etc. It is, however, still theoretically possible for the detector to recover the original watermark if the detail of the geometric attack can be established and a countermeasure applied. The process of correctingthis type of attack is often referred to as 'synchronisation;however, the complexity of the required synchronisation process might be prohibitively expensive and slow.

Table I Performance comparison of the proposed watermarking schemes

Type of Attack	Scheme I – DWT			Scheme II – DWT- SVD			Scheme III – DWT- SVD-AES		
	PSNR (dB)	NPCR	UACI	PSNR (dB)	NPCR	UACI	PSNR (dB)	NPCR	UACI
Without attack	38.43	0.89	0.38	48.76	0.96	0.46	54.65	1.00	0.50
Gaussian Blur	36.45	0.67	0.26	47.45	0.86	0.38	53.35	0.88	0.44
Sharpening	37.68	0.78	0.31	47.89	0.89	0.42	54.01	0.98	0.49
Gaussian Noise	36.21	0.61	0.22	44.56	0.58	0.19	53.14	0.86	0.40
Histogram Equalisation	37.21	0.73	0.29	45.78	0.64	0.26	52.34	0.76	0.37
Rotation	34.45	0.46	0.10	45.89	0.68	0.29	52.56	0.79	0.39
Rescaling	35.67	0.58	0.21	46.23	0.75	0.32	51.12	0.69	0.33
Speckle Noise	33.78	0.38	0.08	44.56	0.58	0.19	52.10	0.75	0.37
Salt and pepper	36.56	0.65	0.24	41.34	0.32	0.12	53.57	0.89	0.46
Contrast Stretching	37.65	0.76	0.30	44.58	0.58	0.19	53.25	0.87	0.43

Table I shows the performance of the various proposed watermarking schemes when subjected to various attacks. The robustness of the proposed schemes are measured on various parameters such as Peak signal to noise ratio, Number of pixel change per rate (NPCR) and Unified average changing Intensity (UACI) .The NPCR for a good watermarking technique is expected to have a value 1 and UACI with a value 0.5. From the

table it is observed that among the three proposed schemes, the third scheme gives better parametric values when exposed to various attacks such as Gaussian blur, Sharpening, Gaussian noise, Histogram Equalisation,Rotation,Rescaling,Speckle noise, Salt and pepper noise and Contrast stretching

8. Conclusion

The contribution of the paper is to introduce three different digital watermarking schemes applicable for medical Images. The analyses were carried out in MATLAB software.The three schemes are framed in such a way that level of security increases as the methodology of watermarking technique utilizes both encryption and watermarking technique. From the performance it is observed that the first scheme is less robust against various attacks as it uses only one watermark. The second scheme is a dual watermarking technique which embeds the watermark in HL and LH band using SVD technique. The proposed scheme gives a better performance when compared to scheme I but the watermarked data can be subjected to various geometric attacks. The third scheme uses Advanced encryption technique to encrypt the watermarked data. The performance of the proposed scheme is shown is observed to be robust to various attack on comparison to the proposed technique.

References

[1] K. Youngberry, Telemedicine Research, Journal of Telemedicine and Telecare, Vol. 10, No. 2, pp. 121-123, 2004.

[2] S. Tachakra, X. H. Wang, R. S. Istepanian, Y. H. Song, Mobile e-health: The Unwired Evaluation of Telemedicine, Telemedicine Journal of e-health, Vol. 9, No. 3, pp. 247-257, 2003.

[3] M. D. Swanson, M. Koayashi, A. H. Tew_k, Multimedia Data Embedding and Watermarking Technologies, IEEE transaction on Information Technology in biomedicine, Vol. 86, pp. 1064-1087, 1998.

[4] Chang, C.C., Tai, W.L., Lin, C.C.,.A reversible data hiding scheme based on side match vector quantization, IEEE Transactions on Circuits Systems Video Technology 16 (10), 1301–1308,2000.

[5] H. Berghel, L. O, Gorman, Protecting ownership rights through digital watermarking", IEEE Computational Magazine. 29 (7) 101–103,1996.

[6] Wang, R. Z., Lin, C. F., & Lin, J. C. , Image hiding by optimal LSB substitution and genetic algorithm, Pattern Recognition, 34(3), 671–683,2001.

[7] Zkou, X.Q., Huang, H.K. and Lou, S.L., Authenticity and integrity of digital mammography images. IEEE Transactions on Medical Imaging, **20**(8), pp. 784-791, 2001.

[8] Chao, H.M., Hsu, C.M. and Miaou, S.G.,A data-hiding technique with authentication, integration, and confidentiality for electronic patients records, IEEE Transactions Information Technology in Biomedicine, **6**, pp. 46-53, 2002.

[9] Giakoumaki, D. Rogers, J. Mazumdar, R. Coutts, D. Abbott, An Overview of Wavelets for Image Processing for Wireless Applications", Proceedings of SPIE: Smart Structures, Devices and Systems, University of Melbourne, Australia, Vol. 4935, pp.427-435, 2003.

[10] C. Shieh, H. Huang, F. Wang, J. Pan, Genetic watermarking based on transform domain techniques, Pattern Recogn. 37, 555–565,2004.

[11] Piva, A. Bouridane, M. Ibrahim, S. Boussakta, Digital image watermarking using balanced multiwavelets, IEEE Trans. Signal Process. 54 (4), 1519–1536,2006.

[12] Xuan, Lee, Y. K. & Chen, L. H. , High capacity image steganographic model". In IEEE proceedings of vision, image, and signal processing Vol. 147, pp. 288–294,2004.

[13] P. Shah, P. Choudhari, S. Sivaraman, Adaptive wavelet packet based audio steganography using data history, in: Proceedings of the 2008 IEEE Region 10and the 3rd International Conference on Industrial and Information Systems, pp. 1–5,2008.

[14] Zhou, X.Q., Huang, H.K. & Lou, S.L. , Authenticity and integrity of digital mammography images, IEEE Transactions on Medical Imaging, vol. 20, no. 8, pp. 784-791,2001.

[15] G. Bhatnagar, B. Raman, K. Swaminathan, DWT-SVD based dual watermarking scheme, Applications of Digital Information and Web Technologies, First International Conference on the ICADIWT 2008, pp. 526–531.

[15] J. Zain, M. Clarke, Issues in Watermarking Medical Images, SETIT 2005, 3rdInternational Conference: Science of Electronic, Technologies of Information and Telecommunications, 2005.

[16] A. Nikolaidis, I. Pitas, Region-based image watermarking, Image ProcessingIEEE Transactions on 10 (11) , 1726–1740,2001.

[17] S. Voloshynovskiy, S. Pereira, T. Pun, J.J. Eggers, J.K. Su,Attacks on digitalwatermarks: classification, estimation based attacks, and benchmarks,Communications Magazine, IEEE 39 (8) 118–126,2001

[18] P. N. Tao, and Eskicioglu, A robust multiple watermarking scheme in theDiscrete Wavelet Transform domain, Internet Multimedia Management System Conference 5601133-144 ,2004.

[19] V. Licks, R. Jordan, Geometric attacks on image watermarking systems,Multimedia, IEEE 12 (3) 68–78,2005

[20] J.K. Joseph, Ruanaidh, P. Thierry, Rotation, scale and translation invariant spreadspectrum digital image watermarking, Signal Process. 66 (3), 303–317,1998..