DOI: 10.21917/ijivp.2011.0038

FUSION OF CRYPTOGRAPHIC WATERMARKING MEDICAL IMAGE SYSTEM WITH REVERSIBLE PROPERTY

P. Viswanathan[1] and P. Venkata Krishna[2]
[1]*School of Information Technology, VIT University, Tamil Nadu, India*
E-mail: pviswanathan@vit.ac.in
[2]*School of Computing Science and Engineering, VIT University, Tamil Nadu, India*
E-mail: pvenkatakrishna@vit.ac.in

Abstract
Large amount of medical information of patients to be maintained in online, hence more uploading is needed, which may reflects the problem in amount of time and privacy of information. This can be solved by watermarking which provide privacy and cryptography provides security. The proposed algorithm provides a single system of cryptographic watermarking method. Initially the patient information is encrypted using the symmetric key and then while hiding, the key will be extracted to retain the quality of the medical image after copyright extraction. During authentication the embedded information is extracted and decrypted. Further, the decrypted information is compared with the patient information. Finally, the extracted key is used to recover the medical image.The algorithm gives high payload capacity, less computational complexity, privacy of the patient and good reversible quality.

Keywords:
Encryption, Decryption, Invariants, Cryptography, Reversible Property, Embedding, Extraction, Watermarking, Fusion, Binary Data, Text Data, Variation

1. INTRODUCTION

Maintaining the medical information of a patient in today's world requires more storage and the information is very much needed for diagnosis [1]. Most of the time, the medical information will be given to the patient directly or sending it through email, which needs to be authenticated before giving/sending it to him. Many techniques are available for authentication and security of data [2] while dispatching the information of the patient such as enquiring the patient directly or mailing information using authorized email id. At times, the information may reach a wrong person or hackers may hack the information and can change it while in transaction which may result in false diagnose [3].

Nowadays, watermarking main purpose was to perform authentication and copyright protection. The watermarking based schemes are divided into fragile watermarking and semi fragile watermarking. Fragile watermarking means the watermarking is not detectable when any changes occur performed in the image. Semi fragile watermarking means the watermarking survive even after the legitimate distortion [4].

The medical image watermarking means hiding the patient report in their medical image for authentication and to maintain confidentiality [5]. The effectiveness of medical image watermarking which comes under the fragile watermarking lays in the storage compatibility and avoidance of redundant data. Since watermarking enables distortion, localisation and restoration, this may result in wrong diagnosis. The distorted medical image will be retained by reversing of original quality of the medical image [6] to avoid the problem.

The watermarking system must require imperceptible, statistically undetectable, resistant to lossy data and unambiguous. The good system must have good perceptually significant component against lossy and should resemble the image to protect any operation that is intentionally performed to damage the watermark resembles damage in image. The frequency domain of the image is viewed as a communication channel and watermarking as a signal that is transmitted through it. Attacks and unintentional signal distortion are treated as noise [7] shown in Fig.1.

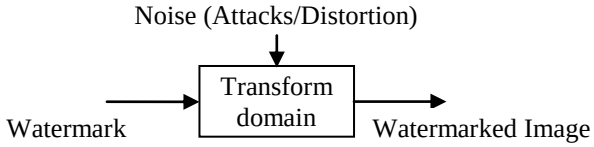

Fig.1. Transform Domain Watermarking

In information theoretic point of view, the reliable communication is achieved by Fig.2.

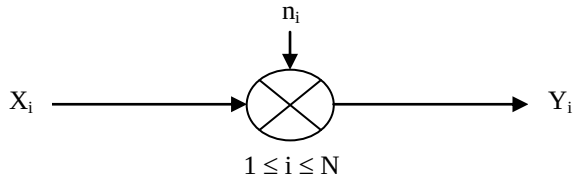

Fig.2. Spatial Domain Watermarking

where, X_i is the watermark vector of length N, n_i is the noise vector and Y_i is the watermark distorted by noise n.

In order to maintain the privacy of the information, symmetric key cryptographic system is used to secure the data [8]. In this, the private key is shared by sender and receiver to encrypt and decipher the data. The cryptographic system [9] efficiently maintains the confidential information in the fields such as forensic applications and defence.

In this paper, we introduce the cryptographic fusion watermarking medical image system with reversible property uses the symmetric cryptosystem before embedding focus on the privacy of the patient and patient report watermarked in the medical image focus on privacy and authentication of the patient and reversible property focus on retaining the original medical image. So everything provides well confidentiality of the patient information with less memory. The paper starts with the related works which contains some of the previous work done. Nextly, the proposed cryptographic watermarking system explains the

working concept of six modules; 1) Encryption 2) Hiding 3) Extracting 4) Decryption 5) Reversible and 6) Verification. At last the mathematical evaluation and performance evaluation of the proposed work is defined.

2. RELATED WORKS

Traditionally the watermarking system has been based on two methods namely spatial domain and frequency domain watermarking system. All these methods are exploited by interpreting noise with specific properties [10].

Some of watermarking methods in spatial domain such as Basic message coding in which embedding is performed by Eq.(1),

$$W(x, y) = I(x, y) + M \quad (1)$$

where W(x, y) is the watermarked Image, I(x, y) is the Input image and M is the message. The detector correlates the received image W(x, y) against each of the eight reference pattern, and uses the sign of each correlation to determine the most likely value for the corresponding bit. The Etrellis method is done by transforming the message into a bit code word. The Spread spectrum technique [11] is done by Eq.(2) and also by Eq.(3),

$$C = C + aW_i \quad (2)$$

$$C = C(e^{ax}{}_i) \quad (3)$$

where, C is the Coefficients to be altered and W is the water marked signal.

The watermarking methods based on frequency domain such as Discrete Fourier Transform which control the frequency of the host signal embed the watermark with the magnitude of its coefficients. The 2D DFT of an M x N image Eq.(4) and inverse Eq.(5),

$$F(U,V) = \frac{1}{MN}\sum_{M=0}^{M-1}\sum_{N=0}^{N-1} F(M,N)W_N^{kM}W_N^{lN} \quad (4)$$

The IDFT is given by,

$$F(M,N) = \frac{1}{MN}\sum_{M=0}^{M-1}\sum_{N=0}^{N-1} F(U,V)W_N^{-kM}W_N^{-lN} \quad (5)$$

where, $W_N = \exp\left\{\frac{-j2\pi}{N}\right\}$, $0 \le k,l \le N-1.$

Discrete cosine transform based watermarking [12] embed the watermark in low frequency, high frequency or Middle frequency components depend upon that the robustness, invisibility of the watermark varies. The embedding is performed by Eq.(6),

where,

$$C(0,0) = \sqrt{\frac{1}{N}} \qquad C(U,V) = \sqrt{\frac{1}{2N}}$$

$$1 \le x \le N-1, 1 \le y \le N-1$$

$$DCT(x,y) = \sum_{x=0}^{M-1}\sum_{y=0}^{N-1} C(U,V)\cos\left[\frac{\pi(2x+1)y}{2N}\right] \quad (6)$$

$$0 \le x \le N-1, 0 \le y \le N-1$$

Discrete wavelet transform which satisfies the Orthonormal property divide the image into high frequency and low frequency components and then hide the watermark in the component. It gives efficient reconstruction of the image [12] after extraction of watermarking.

The differential expansion based on frequency domain embedding algorithm with reversible property is closely related to our proposed work, but the major drawbacks in this technique is that the quality of the image will be radically corrupted due to under stream, over stream and round up error problem and also have less hiding capacity [13]. The robustness depends on the dimension of bit plane.

In order to secure the data, some work has been done using cryptographic system based on symmetric key system and asymmetric key system [14]. In our work, we used symmetric key system and it is already used in the data encryption system, advance encryption system, RC2 and RC4 etc [15].

3. CRYPTOGRAPHIC WATERMARKING FUSION SYSTEM

The medical image verification is the crucial course of action where the information of the patient must be maintained securely and certified without any distortion online [16].

We developed an encrypted data embedding process known as cryptographic fusion watermarking system is shown in Fig.3. Shows that the document of the patient is encrypted and then the cipher is embedded in the medical image using bit wise operation for authentication. Due to embedding, some of the details of the medical image may be corrupted, which can be recovered by using reversible property. It is used in medical image for fake safety and storage compatibility. Once authenticated the original image is retained by this model. The drawbacks of the system is, it only support the image of range 0 to 255 and due to watermarking the alteration is performed result in distortion in the medical image and if additive or removal of information in the medical image affects the watermarking.

In this paper, the fusion of cryptographic watermarking medical image system with reversible property consist of six modules; 1) Encryption, 2) Hiding, 3) Extracting, 4) Decryption, 5) Reversible and 6) Verification. At last the mathematical evaluation and performance evaluation of the proposed work is statistically evaluated.

3.1 ENCRYPTION

In this module, we introduce an encryption algorithm based on the private symmetric key cryptographic system, which is used to encrypt the patient information. The encryption algorithm converts the information into ASCII value and then it is converted to Binary data of 8 digit using equations (7), (8) and (9),

$$bin\_msg(k+j)=bitand(z,128) \quad (7)$$

$$z=bitshift(z,1) \quad (8)$$

$$bin\_msg(k+j)=bin\_msg(j+k)/128 \quad (9)$$

By using the key of four bit binary data the information will be changed into cipher using Eqs. (10), (11) and (12),

$$Qbin()=Rev(bin)/key \quad (10)$$

$$Rbin()=Rev(bin)\%key \quad (11)$$

$$Cbin\_msg()=Qbin() + Rbin() \quad (12)$$

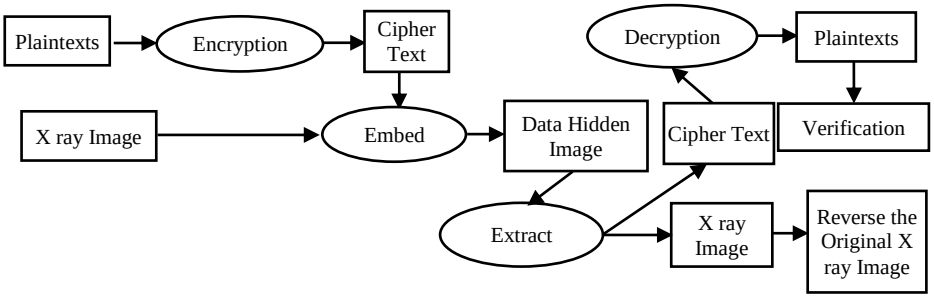

Fig.3. Cryptographic fusion watermarking system

where, Qbin() is the Quotient of binary digits and Rbin() is the Remainder of binary digits, '+' is concatenation, key with four binary digit , Rev() is reverse the binary digits and Cbin_msg() is the ciphered binary digits of the text.

3.2 EMBEDDING PROCESS

The transformed binary data called cipher has been taken as watermarking data which has to be hidden in the medical image. In this, the source image has 8 bit per pixel and the grey level is maintained in the intensity range between 0 and 255.

The course of action of this process is changing a particular bit of the medical image by the corresponding bit of the cipher. Then thecipher binary data is embedded in different location of the image with reversible property using equations (13), (14) and (15),

$$Image\ (m, k)=BitAND\ (Oimage(m, k),254) \quad (13)$$

$$If\ Oimage\ (m, k)!= Image(m, k);\ \ i=m, j=k \quad (14)$$

$$Hd\_img\ (m, k)=BitXOR\ (Image(m, k),Cbin\_msg\ (i)) \quad (15)$$

where, OImage () is the source image and Hd_img () represent the watermarked image. Thus the cipher binary data will be hidden in the medical image until the count moves to an end, where the number of characters will be considered as count.

3.3 EXTRACTION PROCESS

This process mainly focussed on certification and validation using watermarked image through embedding process. Here, we consider the source as the watermarked image and count as key for extracting the cipher text using Eq.(16),

$$Cbin\_msg\ (i)=BitAND\ (Hd\_img, 1) \quad (16)$$

3.4 DECRYPTION

This process mainly focussed on securing patient data through encryption process. The medical image of a particular patient will be guaranteed at this stage by converting the cipher data to plain data using Eq.(17) and Eq.(18).

$$Q1bin()=Qbin()\times key \quad (17)$$

$$Pbin()=Rev(Q1bin+Rbin) \quad (18)$$

where, Pbin() is the binary data of the plain text.

The obtained data will be further converted into ASCII value and then to character. The resultant data will be used for authentication and verification of the patient.

3.5 REVERSIBLE OPERATION

The reversible operation is used to remove the watermarking and get back the original medical image. Initially the embedded region of watermarked image will be converted to an intermediate image which will be processed using Eq.(19). The resultant image and the extracted key, which contains the (i, j)th position of the image where changes occur due to Eq.(11), will be processed further by Eq. (20) for reconstruction.

$$Image\ (m, k)=Hd\_img\ (m, k) \oplus Cbin\_msg() \quad (19)$$

$$OImage\ (m, k)=BitOR(Image\ (i, j),1) \quad (20)$$

3.6 AUTHENTICATION

In order to validate the ownership of the patient, multiple validations will be carried out. First, we check the count of characters and spaces in the notepad 'key' by comparing the decrypted data with the data which is present before extraction process. Next we check the deciphered data using the private key of 4 digit binary number. Finally, we compare the decrypted text with the patient information. If the text matches with the patient information then the medical image will be certified or else the image will be disqualified. Once validated, Eq.(20) and Eq.(21) will be used for reconstruction. Due to multiple validations the patient information will be maintained secure and private. If any one of the input is wrong, the patient is treated is a hacker.

4. MATHEMATICAL EVALUATION

The mathematical evaluation of the system is explained in this case study. We have taken the sample of image data as *105, 205, 100, 125, 224, 221, 123, 112* and the text data as 'a'. Initially the text data 'a' having the ASCII value of 97 is encrypted to the ASCII value of '179' by using the equations (11), (12) and (13) shown in Table.2. The conversion of all ASCII value to binary format is done by bitwise operation using equations (7), (8) and (9) shown in Table.1.

The sample cipher data 179 of the text data in binary format is embedded in the image using the equations (14), (15) and (16). The mathematical computation performed between the image and cipher data is shown in the Table.3. Due to embedding the original sample data is changed into *105, 205, 101, 125, 224, 221, 123, 113* which is called watermarked data.

The watermarked image data *105, 205, 101, 125, 224, 221, 123, 113* is taken as input for extraction and for reconstruction of image. The sample watermarked data is processed by the Eq.(17) such that embedded data will be comes out from the image which is used for authentication shown in Table.4. For reconstruction this extracted data is processed with the watermarked image using Eq.(20) and by using the index table and Eq.(21) the image is reconstructed is shown in Table.4.

The extracted binary data '10100011' is decrypted by using equations (18), (19) converted ASCII value of 179 to 97 represent the character 'a' as shown in Table.5. From this evaluation we can identify how the system is working with good reversible operation and the information of the patient is maintained confidentially.

Table.1. Binary Conversion

Bitand (179,128) = 128	*Bitshift (179,1) = 358*	*128/128* ***1***
Bitand (358,128) = 0	*Bitshift (358,1) = 716*	*0/128* ***0***
Bitand (716,128) = 128	*Bitshift (716,1) = 1432*	*128/128* ***1***
Bitand (1432,128) = 128	*Bitshift (1432,1) = 2864*	*128/128* ***1***
Bitand (2864,128) = 0	*Bitshift (2864,1) = 5728*	*0/128* ***0***
Bitand (5728,128) = 0	*Bitshift (5728,1)= 11456*	*0/128* ***0***
Bitand (11456,128)= 128	*Bitshift(11456,1) = 22912*	*128/128* ***1***
Bitand (22912,128) = 128		*128/128* ***1***

Table.2. Encryption

'a' = 01100001	*key = '1001'*
Reverse = 10110000	*Qbin = 10110000/1001 = 10011*
Rbin = 10110000%1001 = 101	*Cbin_msg = 101+10011* ***10110011 = 179***

Binary Conversion *Encrypted data = 179*

Data = '179' = 10110011

Image = 105,205,100,125,224,221,123,112

Table.3. Embedding

Original Image	***Bitand (image,254)***	***179***	***BitXOR (image,bin)***
105 '01101001'	***104*** *'01101000'*	***1***	*105 '01101001'*
205 '11001101'	***204*** *'11001100'*	***0***	*204 '11001100'*
100 '01100100'	*100 '01100100'*	*1*	*101 '01100101'*
125 '01111101'	***124*** *'01111100'*	***1***	*125 '01111101'*
224 '11100000'	*224 '11100000'*	*0*	*224 '11100000'*
221 '011011101'	***220*** *'01101110'*	***0***	*220 '11011100'*
123 ' 01111011'	***122*** *'01111010'*	*1*	*123 '01111011'*
112 '01110000'	*112 '01110000'*	*1*	*113 '01110001'*

Hidden Image = ***(105,205,101,125,224,221,123,113)***

Table.4. Extraction and Reconstruction

Original Image	***Embedded***	***Extraction BitAND (Image,1)***	***Reconstruction***	
			BitXOR (Img,B)	***BitOR (Img,1)***
105 '01101001'	*105 '01101001'*	***1***	***104***	***105***
205 '11001101'	*204 '11001100'*	***0***	***204***	***205***
100 '01100100'	*101 '01100101'*	***1***	*100*	*100*
125 '01111101'	*125 '01111101'*	***0***	***124***	***125***
224 '11100000'	*224 '11100000'*	***0***	*224*	*224*
221 '011011101'	*220 '11011100'*	***0***	***220***	***221***
123 ' 01111011'	*123 '01111011'*	***1***	***122***	***123***
112 '01110000'	*113 '01110001'*	***1***	*112*	*112*

Table.5. Decryption

Encrypted Data: 179' = 10110011	*key =1001*
*OIbin=10011*1001 = 10101011*	*Added 101 = 101 =10110000*
Right Shift = 01100001	*Plain text = 'a'*

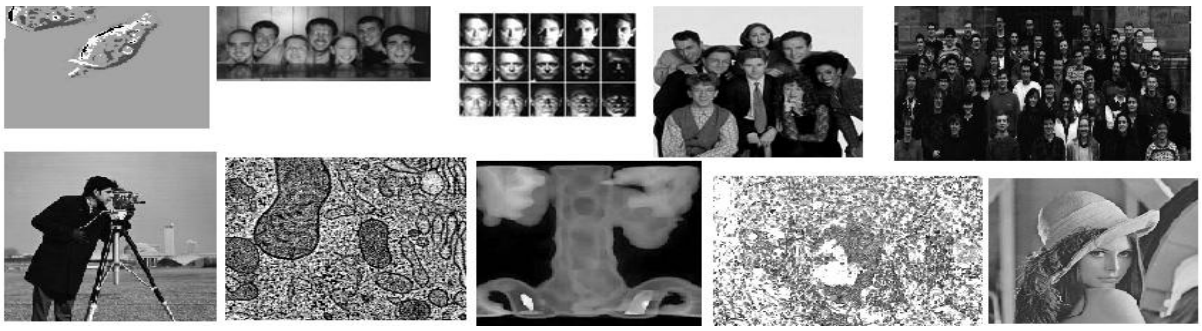

Fig.4. Input Tested Images

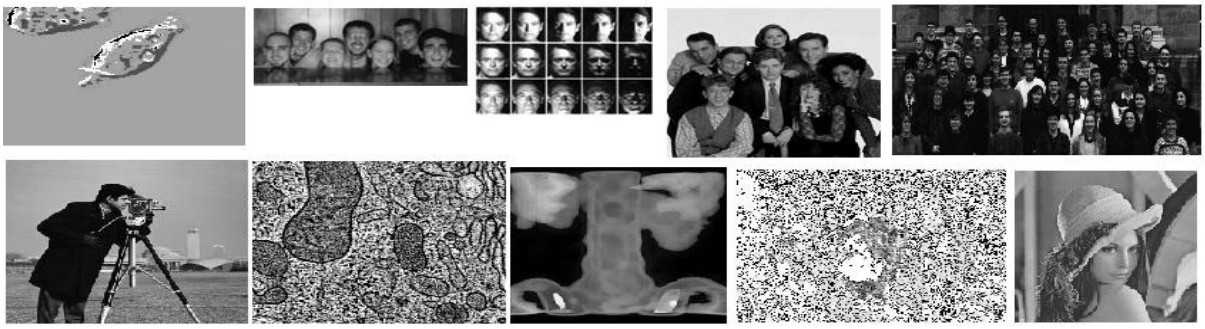

Fig.5. Watermarked Images

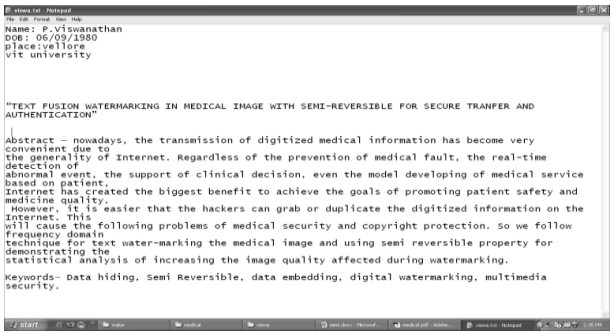

Fig.6. Plain & Decrypted Text

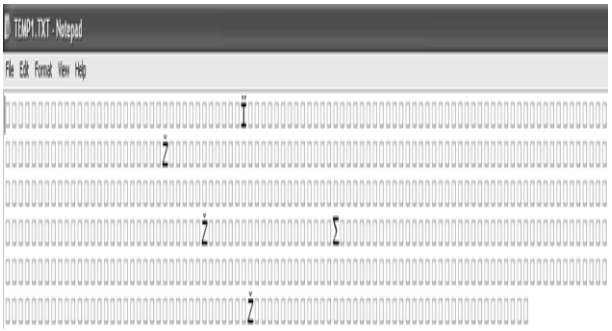

Fig.7. Encrypt & Embedded Text

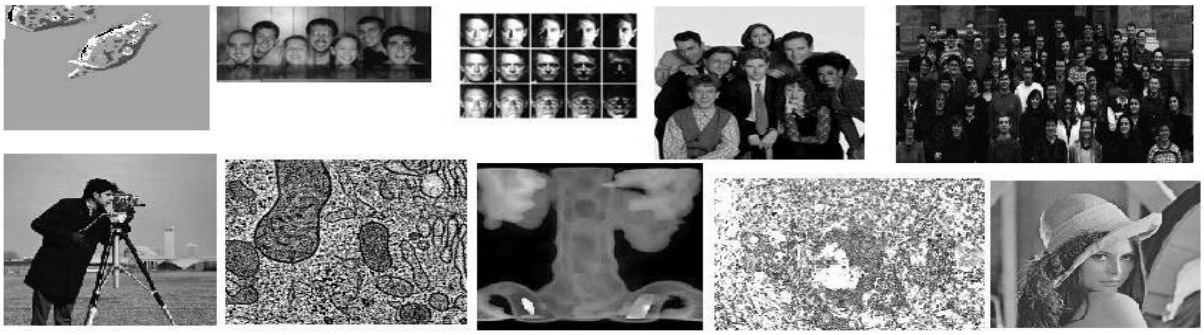

Fig.8. Reconstructed Images

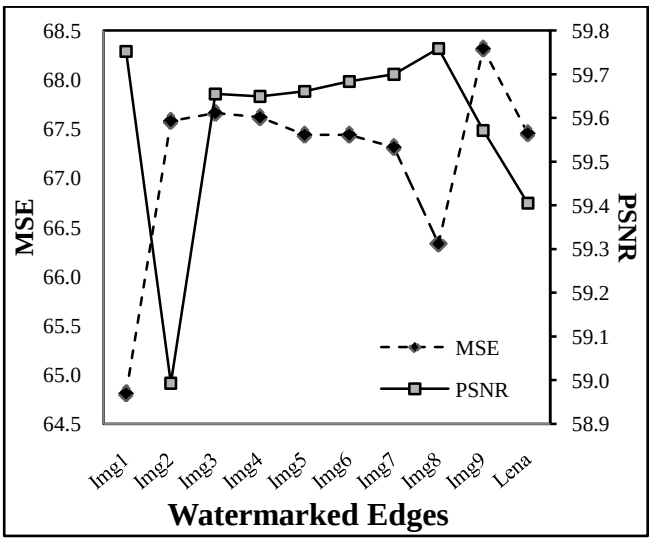

Fig.9. The MSE and PSNR for medical images

5. EXPERIMENTAL EVALUATION

We used the medical image of a patient of 0-255 grey level image and the details of the patient like, personal and diagnosed details which was entered in a notepad text file. The effectiveness of the cryptographic fusion watermarking system is demonstrated as follows. The text having the information of the patient in the notepad shown in Fig.6 and the original medical image shown in Fig.4 has been taken as source record. Initially, the text in the source record encrypted into cipher binary data shown in Fig.7 and then it was hidden into the medical image in the source record.

The image was authenticated using the extracted and decrypted cipher data from the watermarked image shown in Fig.5. Further, the obtained cipher data and watermarked data with the extracted key were processed to recover the original medical image shown in Fig.8. We validated the record using the notepad information and the information of the patient. Further the image contrast was improved by the frequency domain technique called DWT.

The image is further evaluated by Peak signal Noise ratio for the watermarked image using Eq.(21) and Mean square Error using Eq.(22) is shown in Fig.9, shows that due to embedding the quality of the image is affected. But for the evaluation of reconstructed image gives the Peak signal noise ratio infinity and Mean square error as 0. Hence the quality of the Image is maintained without any distortion.

$$MSE = \frac{1}{MN}\sum_{x=1}^{M}\sum_{y=1}^{N}[I(x,y) - I'(x,y)]^2 \quad (21)$$

$$PSNR = 20\mathrm{X}\log 10(\frac{255}{sqrt(MSE)}) \quad (22)$$

6. CONCLUSION

The Randomized cryptographic fusion watermarking system ensures security to the patient information since, the medical image watermarking is a semi fragile watermarking and hence if any hackers attack the image by filtering or adding noise to the image, the watermarking will be affected and it will not be used further for diagnose purpose. This system helps in keeping the information confidentially by encrypting and hiding the data randomly in different location in the medical image. This system also reduces the need of multiple documents which is needed to maintain the information that results in storage compatibility. The cost is minimal, since all the operations are performed using bitwise operations. Once the image is authenticated, this system provides good quality of the watermarked image and high-capacity applications for reversible data extraction. It protects medical images from distortion caused by data hiding.

In the proposed system the combination of cryptography and watermarking is used for medical image maintenance. We can further extend this system with the combination of cryptography based on Biometric data for personal authentication leads to more confidentiality.

REFERENCES

[1] Javier Pereira, Alfonso Castro, Dismer Ronda, Bernardino Arcay and Alejandro Pazos, "Development of a System for Access to and Exploitation of Medical Images", *Proceedings of the 15th IEEE Symposium on Computer-Based Medical Systems*, pp. 309-314, 2002.

[2] Jasni M. Zain and Abdul R.M. Fauzi, "Evaluation of Medical Image Watermarking with Tamper Detection and Recovery (AW-TDR)", *Proceedings of the 29th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, pp. 5661-5664, 2007.

[3] Chiou-Ting Hsu and Ja-Ling Wu, "Hidden digital watermarks in images", *IEEE Transactions on Image Processing*, Vol. 8, No. 1, pp. 58-68, 1999.

[4] Dom Osborne, Derek Rogers, Matthew Sorell, and Derek Abbott, "Multiple medical image ROI authentication using watermarking", *Proceedings of SPIE, Biomedical Applications of Micro- and Nanoengineering II*, Vol. 5651, pp. 221–231, 2005.

[5] Jessica Fridrich, Miroslav Goljan, and Rui Du, "Lossless data embedding new paradigm in digital watermarking", *EURASIP Journal on Applied Signal Processing—Special Issue on Emerging Applications of Multimedia Data Hiding*, Vol. 2002, No. 2, pp. 185-196, 2002.

[6] P. Viswanathan and P. Venkata Krishan, "Text fusion watermarking in Medical image with Semi-reversible for Secure transfer and Authentication", *International Conference on Advances in Recent Technologies in Communication and Computing*, pp. 585-589, 2009.

[7] Rajendra Acharya U, U.C. Niranjan, S.S. Iyengar, N. Kannathal and Lim Choo Min, "Simultaneous storage of patient information with medical images in the frequency domain", *Computer Methods and Programs in Biomedicine*, Vol. 76, No. 1, pp. 13-19, 2004.

[8] D. Jablon, "Strong Password Only Authenticated KeyExchange", *SIGCOMM Computer Communication Review*, Vol. 26, No. 5, pp. 5-26, 1996.

[9] S. Hebert, "A Brief History of Cryptography", an article available at http://cybercrimes.net/aindex.html.

[10] Ingemar Cox, Jeffrey Bloom and Matthew Miller, "*Digital Watermarking: Principles & Practice*", Morgan Kauffman Publishers, 2001.

[11] Malvar H.S and Florencio D.A.F, "Improved Spread Spectrum:A New Modulation Technique for Robust Watermarking", *IEEE Transactions on Signal Processing*, Vol. 51, No. 4, pp. 898-905, 2003,

[12] Farid Ahmed and Ira S. Moskowitz, "Correlation-based watermarking method for image authentication applications", *Optical Engineering*, Vol. 43, No. 08, pp. 1833–1838, 2004.

[13] J. Tian, "Reversible watermarking by difference expansion", *Proceedings of ACM Multimedia and Security Workshop: Authentication, Secrecy, and Steganalysis*, pp. 19–22, 2002.

[14] "Introduction to Public-Key Cryptography", an article available at developer. Netscape.com /docs/manuals/ security/pkin/contents.htm.

[15] William Stallings. "*Cryptography and Network Security-Principles and Practices*", Prentice-Hall, 2003.

[16] A. Ferreira *et. al*., "Integrity for electronic patient record reports", *Proceedings of 17th IEEE Symposium on Computer-Based Medical Systems*, pp. 4-9, 2004.