ISSN 2321 -9017
Volume 3, No.4, June - July 2015
International Journal of Bio-Medical Informatics and e-Health
Available Online at http://www.warse.org/IJBMIeH/static/pdf/file/ijbmieh01342015.pdf

Improving the security of images transmission

Asmaa Sabet Anwar[1,4], Kareem Kamal A.Ghany[2,4], Hesham El.Mahdy[3]
[1] Faculty of Computers and Information, Cairo University, Egypt,
asmaa.sabet91@yahoo.com
[2] Faculty of Computers and Information, Beni-Suef University,
kareem.ict@gmail.com
[3] Faculty of Computers and Information, Cairo University, Egypt,
ehesham@cu.edu.eg,ehesham@fci-cu.edu.eg
[4]ISI Research Lab www.isirlab.net

ABSTRACT

The security of images transferred via internet is very important issue. The proposed system tries to satisfy all requirements of security to ensure that any medical image related to any patient do not allow to be accessed via any unauthorized person. We can use an encryption scheme for encrypt medical image. Only the authorized person can decrypt this medical image and can obtain the original image. The ownership of these medical images is very important to improve. We can identify the ownership of any medical image by using watermark related to the owner of this medical image. We used name of the patient and serial number. Capture the ear image of the owner then extract features from ear after that encrypt those features then used it as watermark. The size of the medical image is very effective point in transmitting via internet. Because of this the proposed system used mix of compression techniques applied on medical image before sending via internet. Run time is very important in any system and complexity is very important aspect in computer science. To reduce run time and complexity of the proposed system, we can use DWT to separates an image into approximation image LL, HL LH and HH.

Key words: Security of image, RSA, AES, LZW, BCH, watermark, medical images.

1. INTRODUCTION

Sharing images via internet is very important and wide nowadays especially medical images. Medical Image Sharing is a term for the electronic exchange of medical images between hospitals, physicians and patients. In past the process of exchange information between hospital and patients is done using traditional methods such as a CD or DVD or patients carry it with themselves, but now technology allows to share these images using the internet [1] .Because of the previous reason we need to apply security of electronic medical information, or patient health information that is digitally stored [2]. Physicians sometimes need to access this information to be able to make the best decisions about patient health. Patients must have the right to control the process about their health information sharing.
Security is very important in public media like internet and we have a lot of challenges in this track. Internet used to transfer important medical image related to patient like lab test results, medications, allergies, and other information, they are increasingly being stored and viewed on computers [3]. The responsibility of protecting patient's information from the harm attacks depend on physicians, they must ensure privacy and confidentiality of the patient information [4]. The purpose of this research is to secure any type of images especially medical images. This refers to maintaining the integrity of electronic medical information, ensuring availability to that information, authentication of that information to ensure that authorize people only can access the information. We should ensure images transmission success with reducing the storage cost and the transmission time, but without affecting the quality.

2. RELATED WORK

Security techniques become more complex as the speed of computers increases. Most of researcher focus on improve existing technique or provide new technique to improve the security of images.

Ahmed Mahmood et al in [3] tried to improve security of medical image by divide the medical image into two regions Region of interest (ROI) and Region of background (ROB). ROI include most important part of the image. ROB include the less important part of the image. In their algorithm, they tried to secure image by applying encryption technique in ROI and embed watermark in ROB. They used Chinese remainder theorem (CRT) to encrypt the medical image but CRT method did not show good performance to secure the medical images and this is related to characteristics of the medical images. The watermarked data is the user-name of the person that requested for the medical images and a serial number between the two parties to achieve authenticity and avoid any forgery one. Their encryption technique did not show good values and use weak watermark values like name which can be predicted.
Gonzalo Alvarez et al in [4] tried to improve encryption technique that used in [5] to produce more secure system but in their research did not put in their mind ownership of the image and data integrity.
Bibhudendra Acharya et al in [6] suggested efficient method of encryption of image. Proposed Adv-Hill algorithm is more secure to brute force attacks as compared to original Hill cipher algorithm.

Chin-Chen Chang et al in [7] their proposed system uses fast encryption algorithm for image cryptosystems. Their method depends on vector quantization (VQ). Their schema applied compression techniques which have a base table for encoding/decoding but did not use watermarks to identify ownership and confidentiality.

V.Chandra et al in [8] produced a robust watermarking algorithm which proposed to embed the watermark in encrypted image. They used AES for encryption. It improves the security of system even though it is symmetric and security of this algorithm can be further improved simply by adding more rounds into it at the cost of increase in computation time. Their proposed method also ensures the confidentiality of content since encryption is combined with watermarking. Correlation between embedded and recovered watermark for various images were analyzed. Decryption after watermark extraction was done which is very challenging since the embedded watermark could alter the pixel values. They used Block DCT based watermarking algorithm is used to embed binary watermark in image. This watermark not related to the owner of the image.

Ashraf Darwish et al in [9] presented a securing patient medical images and authentication system to increase the security, confidentiality and integrity of medical images transmitted through the Internet. A public key encryption technique was used to encrypt the patient capturing fingerprint and then embed it into the patient medical image. The fingerprint has been encrypted using the Rivest-Shamir-Adelman (RSA) public-key encryption algorithm. Then, by embedding the encrypted patients fingerprint using a technique for digital watermarking in the Discrete Cosine Transform (DCT) domain makes the medical image be robust to several common attacks.

3. METHODOLOGY

This section declares the steps and algorithms used to secure medical image when transmitting it via internet. Secure medical image done in two phase, first at sender and second at receiver.

3.1. Prepare medical image for sending at sender

Sender applies some steps to secure image before sending it, the following steps declare the security techniques used.

3.1.1 DWT

To reduce run time of our program or instead of applying algorithms on each image, apply algorithms on part of image, this will reduce the time taken by program. Because of that we used DWT [10], the input image is separated into wavelet sub-bands using 1-level discrete transform which separates an image into a lower resolution approximation image (LL), horizontal (HL), vertical (LH) and diagonal (HH) detail components.

3.1.2 Encrypt LL image using AES technique

The encryption is performed on most significant bit planes (LL band) are chosen for encryption since most of the image energy is concentrated at lower frequency. AES-128 [11] encryption algorithm is used for encrypting the LL sub-band. The initial step of AES is to convert the input plaintext matrix into state matrix. State matrix is obtained by calculating hexadecimal value of input matrix which is given as input to the forth coming steps of encryption. The plaintext matrix is rearranged into state matrix and iteratively loops the state through 4 steps for 10 rounds:

A. Addroundkey
B. Subbytes
C. Shiftrows
D. Mixcolumns

3.1.3 Embed Encrypt name and secret number using RSA technique [12] into LH image.

RSA encryption is a public-key encryption technology developed by RSA Data Security. The RSA algorithm is based on the difficulty in factoring very large numbers. Based on this principle, the RSA encryption algorithm uses prime factorization. Deducing an RSA key, takes a huge amount of time and processing power. RSA is the standard encryption method for important data, especially data that's transmitted over the Internet. Use RSA to encrypt patient information then embed Encrypted name and secret number into LH image using this formula in equation 1.

$$\overline{LH} = LH + \alpha * Watermark \quad (1)$$

Where α (alpha) is embedding factor

3.1.4 Get features from ear image which related to patient.

We try to take unique print from patient to embed it in patient medical image. In this paper we took about the ear print for embedding. Extract seven values as feature vector from the ear image [13]. Figure 1 declares the main steps to extract these features.

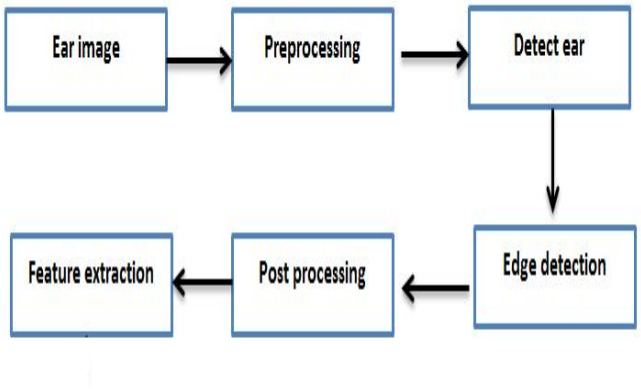

Figure 1: Model as black box

3.1.5 Embed encrypted ear features into HL image.

Because of the ear print is the important information about patient because of that we must secure it before embed it into image then encrypt the feature vector of ear image that shown in figure 2 using RSA. Use formula in equation 2 to embed the encrypted numbers in the HL image.

$$\overline{HL} = HL + \alpha * Watermark \quad (2)$$

Where α (alpha) is embedding factor

185.2188
113.6354
135.5950
117.2732
174.3120
120.0163
20.9048

a) b)

Figure 2: a) ear image. b) Feature values extracted from ear image

3.1.6 Apply IDWT

Inverse DWT is used for obtaining the encrypted watermarked image which be transmitted at the transmitter side. At the receiver side, watermark recovery and decryption is performed in respective sub-bands.

3.1.7 Compress encrypted watermarked image using LZW and BCH techniques.

Data compression implies sending or storing a smaller number of bits. Although many methods are used for this purpose. Compression can be categorized in two types [14]:

- **Lossy Compression**
  Removes data from the original file, the resulting file often takes up much less disk space than the original. Lossy Compression eliminates redundant information. Although the user may not notice the change between compressed and uncompressed image.
- **Lossless Compression**
  Where data is compressed and can be uncompressed without any loss of information. Because we took about medical images and these images are sensitive and all details are important, the key idea here is to remove redundancy of data presented within an image to reduce its size without affecting on the information of it. We are concerned with lossless image compression in this paper.

Here in this phase we used the algorithm proposed by A. Alarabeyyat et.al in [15]. Their proposed approach is a mix of a number of already existing techniques. Their approach works as follows: first, they applied the LZW algorithm on the image. What comes out of the first step is forward to the second step where the BCH error correction and detected algorithm is used. To improve the compression ratio the author applies the BCH algorithms repeatedly until inflation detected. Comparing with the standard compression algorithms their experimental results achieved an excellent compression ratio without losing data.
We can see the overall model for the algorithm 1 in figure 3.

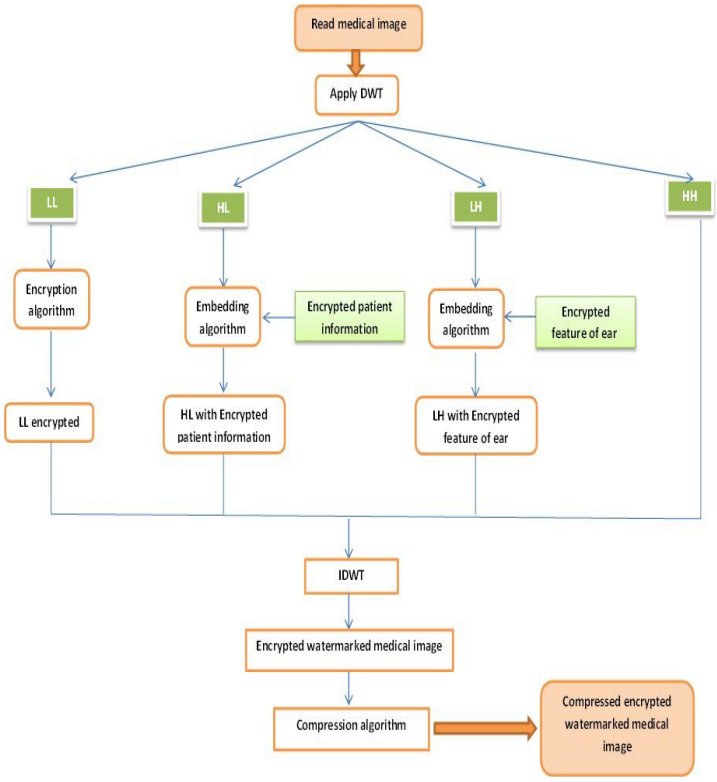

Figure 3: model to get compressed encrypted watermarked medical image

Algorithm 1 secure image at sender.

1: Apply DWT
2: Encrypt LL image using AES technique
3: Encrypt name and secret number using RSA technique
4: Embed Encrypted name and secret number into LH image
5: Get features from ear image which related to patient
6: Encrypt ear features using RSA technique
7: Embed encrypted ear features into HL image
8: Apply IDWT
9: Compress encrypted watermarked image using LZW and BCH techniques

3.2 Return to the original image at the receiver

This section shows how to return from the compressed encrypted watermarked image to the original image at receiver. Receiver can do this throw few steps as shown in figure 4.

3.2.1 Decompress image using LZW and BCH techniques

Decompression is done using the inverse of the compression process. Return to the original image without any loss of data (Lossless). Decompression of the proposed methods using combination of inverse of LZW algorithm and inverse of BCH algorithm [15]

3.2.2 Apply DWT.

We applied DWT to decompose encrypted watermarked image in to $\overline{LL}$ (encrypted approximation image), $\overline{LH}$

(horizontal image with encrypted patient information), $\overline{HL}$ (vertical image with encrypted ear print), and HH.

3.2.3 Decrypt LL image using AES technique.

To return to the original LL part of the original image, we must do the reverse steps of encryption algorithm using the same key. We will see in the experimental result that no difference between the recovered approximation image and the original approximation image.

3.2.4 Extract encrypted name and secret number from $\overline{LH}$ image.

First, we want to extract watermark that we embedded before using the formula in equation 3.

$$Watermark\_Extracted1 = (\overline{LH} - LH)/\alpha \quad (3)$$

Where $\overline{LH}$ is watermarked image (LH) and α is embedding factor

3.2.5 Extract encrypted features of ear image from $\overline{HL}$ image.

We extracted watermark from $\overline{HL}$ image using formula in equation 4, decrypt the watermark extracted using RSA then compare it with the feature of the ear image.

$$Watermark\_Extracted2 = (\overline{HL} - HL)/\alpha \quad (4)$$

Where $\overline{HL}$ is watermarked image (HL) and α is embedding factor

3.2.6 Apply IDWT.

Now we decrypt the approximation part, extract watermarks from $\overline{LH}$ and $\overline{HL}$ then we can apply IDWT to return to original image.

Now we will see the overall model in figure 4 to remember all steps which done in this proposed approach at receiver.

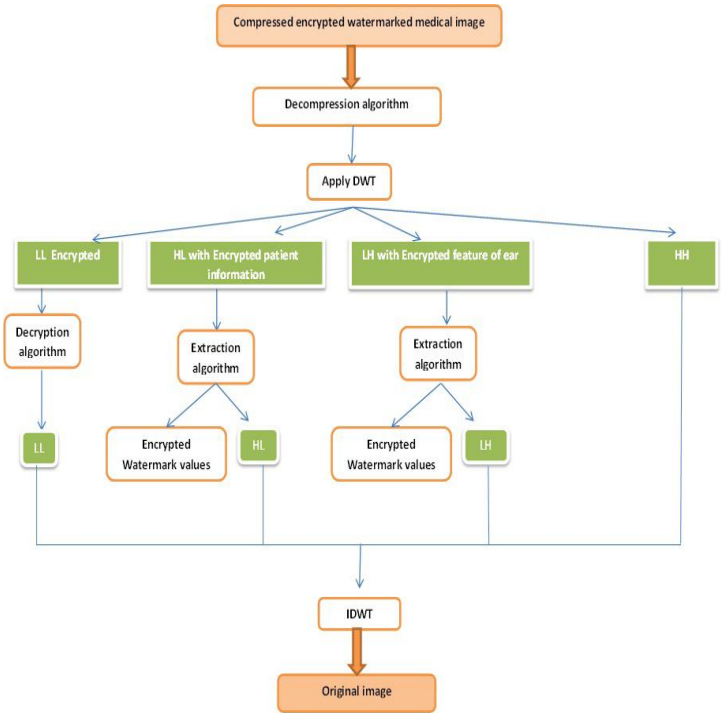

Figure 4: model to return to original image

Algorithm 2 Get original image at receiver.

1: Decompress image using LZW and BCH techniques
2: Apply DWT
3: Decrypt LL image using AES technique
4: Extract encrypted name and secret number into LH image
5: Extract encrypted features of ear image from HL image
6: Apply IDWT

4. EXPERIMENTAL RESULTS AND DISCUSSION

We used medical images to test our model we can show sample of those medical images in figure 5. First, we applied DWT to decompose image to 4 parts LL, LH, HL and HH as shown in figure 6. In the first part we applied AES encryption technique. The AES key expansion algorithm takes as input a 4-word (16-byte) key and produces a linear array of 44 words (176 bytes). This is sufficient to provide a 4-word round key for the initial Add Round Key stage and each of the 10 rounds of the cipher. We choose key= [0 1 10 3 12 5 14 15 8 9 2 11 4 13 6 7]. We can see the approximation image before encryption and approximation image after encryption in figure 7. We can use these metrics to evaluate our model in encryption and decryption part. The encryption and decryption based on the error between decrypted part and original part. Here we used 6 type of error from equation 5 to 10 to evaluate our model.

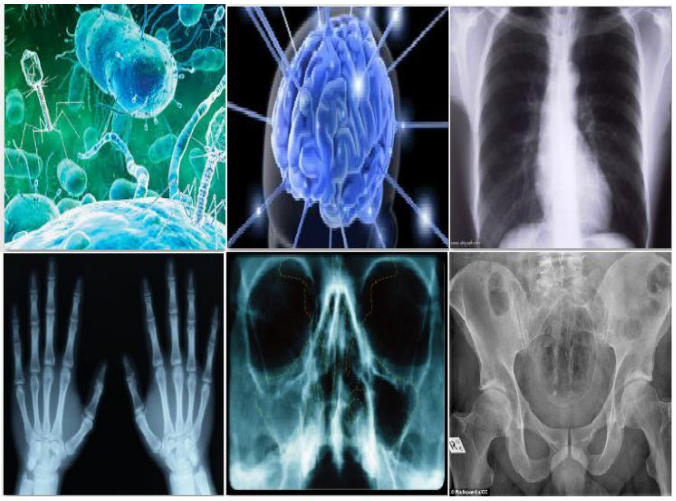

Figure 5: sample of medical images used

$$MSE = (\sum_{i=1}^{r}\sum_{j=1}^{c} (X(i,j) - Y(i,j))^2)/r * c \quad (5)$$

Where MSE is mean square error, X is the original image, Y is the decrypted image, r is number of rows and c is number of columns in image.

$$AD = (\sum_{i=1}^{r}\sum_{j=1}^{c} X(i,j) - Y(i,j))/r * c \quad (6)$$

Where AD is Average difference, X is the original image and Y is the decrypted image.

$$NCC = (\sum_{i=1}^{r}\sum_{j=1}^{c} X(i,j) - Y(i,j))/\sum_{i=1}^{r}\sum_{j=1}^{c} (X(i,j))^2 \quad (7)$$

Where NCC is normalized cross correlation, X is the original image and Y is the decrypted image.

$$MAE = \left|\sum_{i=1}^{r}\sum_{j=1}^{c} X(i,j) - Y(i,j)\right| / r * c \quad (8)$$

Where MAE is Mean Absolute Error, X is the original image and Y is the decrypted image.

$$NAE = \left|\sum_{i=1}^{r}\sum_{j=1}^{c} X(i,j) - Y(i,j)\right| / \sum_{i=1}^{r}\sum_{j=1}^{c} (X(i,j))^2 \quad (9)$$

Where NAE is Normalized Absolute Error, X is the original image and Y is the decrypted image.

$$SC = \sum_{i=1}^{r}\sum_{j=1}^{c} (X(i,j))^2 / \sum_{i=1}^{r}\sum_{j=1}^{c} (Y(i,j))^2 \quad (10)$$

Where SC is Structural Content, X is the original image and Y is the decrypted image.

We saw that all errors used for evaluation equal to zero as shown in Table 1 for all medical images used, this declares that there is no difference between the decrypted images and the original images. About Structural content this mean original image / decrypted image which equal to 1, also this declares that no difference between the medical image before encryption and the same image after decryption. Those result for all medical images used.

Table 1: Metrics to evaluate encryption algorithm

Error	Result for all images used
Mean Square Error(MSE)	0
Average difference(AD)	0
Normalized cross correlation(NCC)	0
Mean Absolute Error(MAE)	0
Normalized Absolute Error(NAE)	0
Structural Content(SC)	1

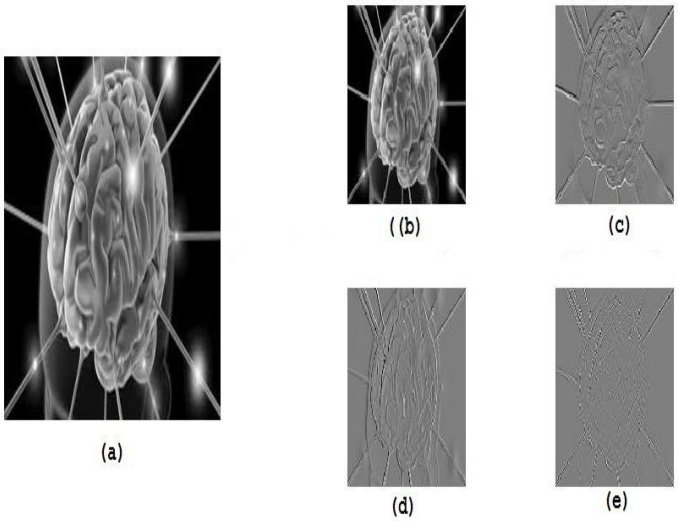

Figure 6: DWT: a) original image. b) Approximation image. c) Horizontal image. d) Vertical image. e) Diagonal image.

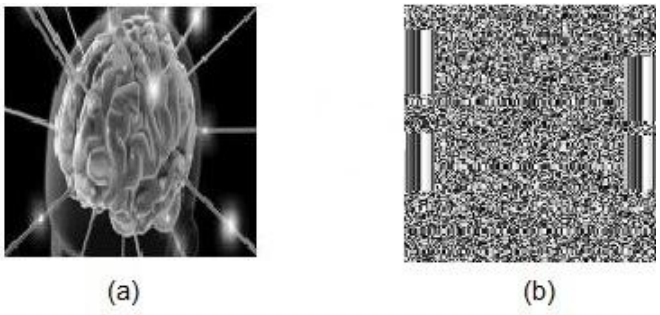

Figure 7: AES encryption results. a) Approximation image before encryption. b) Approximation image after encryption.

Second, we used horizontal image to embed the encrypted patient information on it. We used "Patient Name: XXXX YYYY Secret Number:123456789" as a watermark but after encrypt it using RSA. Figure 8 show the image before embedding and after embedding watermark. We do not notice any difference with naked eyes because the difference between them is very small. We captured the ear print from the patient then get feature vector from it [13]. After that encrypt this feature vector using RSA. We can see the image before embedding watermark and after embedding watermark in figure 9. We cannot see any difference with our eyes this is required.

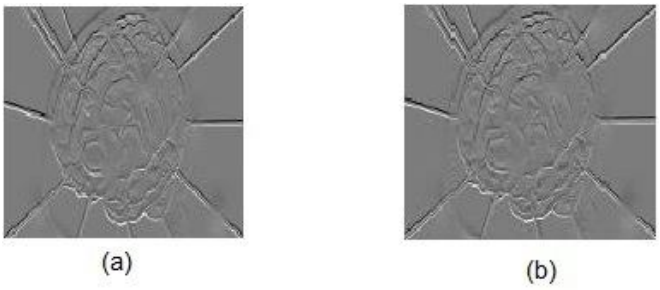

Figure 8: Embed watermark into LH image. a) LH before embedding watermark (encrypted name and serial number) b) LH after embedding watermark.

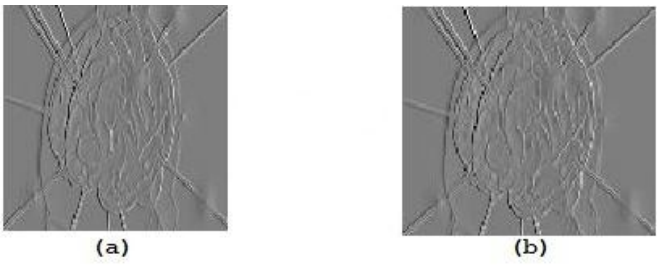

Figure 9: Embed watermark into HL image. a) HL before embedding watermark (encrypted ear print) b) HL after embedding watermark.

Applying IDWT to collect the four images into one image as shown in figure 10.

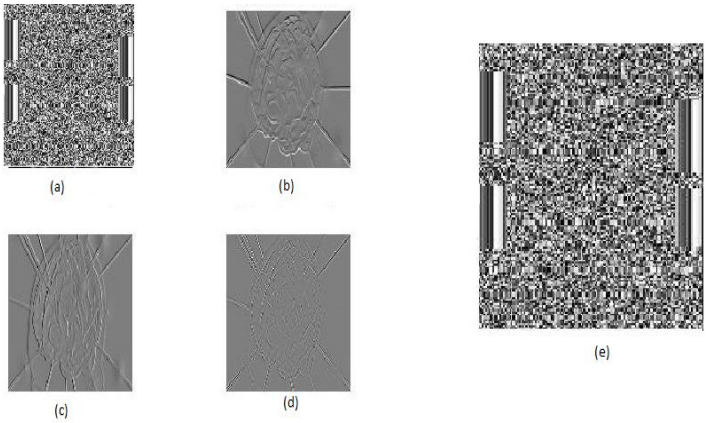

Figure 10: IDWT. a) LL encrypted. b) LH with encrypted name and secret number as watermark. c) HL with encrypted features of ear. d) Original HH image. e) Encrypted watermarked image.

We used these metrics to evaluate our model in watermark embedding and extraction. We depended on more than one metric. Mean square error used to show the difference between the image before embedding watermark and the image after embedding watermark. If this value equal to small number this is will be better. In our Experiment MSE equal to 0.0013 which declare that the difference is very small and does not notice with naked eyes.

1. Mean Squared Error (MSE) is one of the earliest tests that were performed to test if two pictures are similar. A function could be simply written according to the following equation.

$$MSE = (\sum_{i=1}^{r}\sum_{j=1}^{c} (X(i,j) - Y(i,j))^2)/r*c \quad (11)$$

Where X is the original image, Y is the Watermarked image, r is number of row in image and c is the number of column in image.

2. The signal-to-noise ratio (SNR) is used in imaging as a physical measure of the sensitivity of imaging system. The following equation describes how this value is obtained.

$$SNR = 10\ log\left(\frac{max(max(X),max(Y))^2}{MSE}\right) / log\ 10 \quad (12)$$

Where X is the original image and Y is the Watermarked image.

3. Pick Signal to Noise Ratio (PSNR) is a better test since it takes the signal strength into consideration (not only the error). Equation 13 describes how this value is obtained.

$$PSNR = 10\ log10\ \left(\frac{((max(X))^2}{MSE}\right) \quad (13)$$

Where X is the original image.

As shown in table 2 and show more clear in figures (11,12) , we noticed that MSE is be smaller if embedding factor is smaller but at the embedding factor equal to 0.01 the SNR is be stable and MSE not change after this number by large number, So we decide to use embedding factor equal to 0.01.

Table 2: MSE, SNR and PSNR via Embedding factor (alpha)

Embedding factor	MSE	SNR	PSNR
0.1	0.1338	24.0654	56.7648
0.05	0.0334	24.0654	62.7854
0.01	0.0013	24.0654	76.8676
0.005	$3.3439*10^{-4}$	24.0654	82.7854
0.001	$1.3376*10^{-5}$	24.0654	96.7648

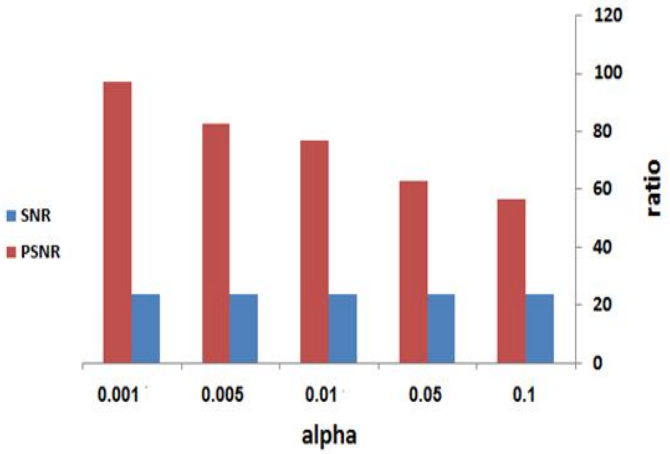

Figure 11: the effect of embedding factor on the Ratio.

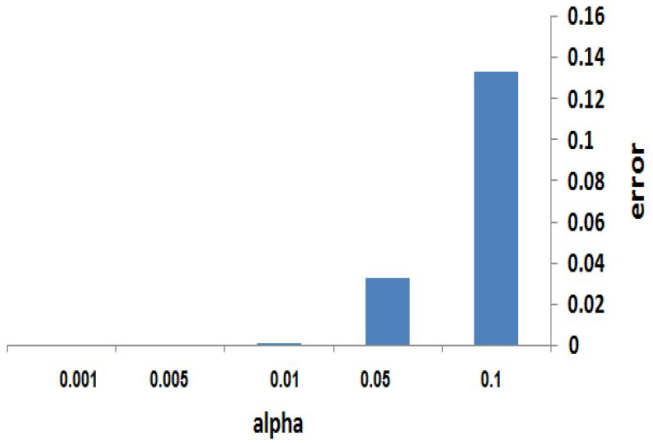

Figure 12: the effect of embedding factor on the error.

Third, the compression ratio is the metric which detect if the compression technique is good or not. The comparison is based on the compression ratio. The compression ratio=size of original image / size of compressed image = 1.5 approximately which is good result for compression.

5. CONLUSION AND FUTURE WORKS

This paper aimed to improve the security of medical images through sending it via internet. We used mix of algorithms to be sure that the medical image is good secured and not accessed via any unauthorized person. But to reduce running

time of our program, divide image to four parts using DWT. first one is approximation image that contain the most important pixels in the image.

In this part we applied the AES 128 encryption technique and get no difference between decrypted image and original one also used 6 metrics to evaluate this part. All error used to evaluate the difference get result= 0. Second part is horizontal details, used it for embedding encrypted information related to patient on it, we encrypted patient information using RSA because it is strong technique in encryption techniques. Third part is vertical detail, used it for embedding encrypted ear print of patient also encrypt ear print using RSA.

Fourth part is diagonal part, we does not make any change on it. We used metrics to evaluate error between watermarked image and original image, we found that if we used embedding factor=0.01 then MSE= 0.0013, SNR=24.0654 and PSNR=76.8676 after that we apply IDWT to get the big image again. Compression techniques used by A.Alarabeyyat et al applied in this paper to compress the image before sending it via internet to reduce its size. We took about medial image and every pixel is important so used lossless compression techniques. Compression ratio is approximately (1.5).

REFERENCES

1- Lu-Chou Huang, Huei-Chung Chu, Chung-Yueh Lien, Chia Hung Hsiao and Tsair Kao, **Privacy preservation and information security protection for patients' portable electronic health records**, *Computer sin Biology and Medicine*, vol.39, No.9, pp.743-750, 2009.

2- Corey M. Angst, **Protect My Privacy or Support the Common-Good? Ethical Questions about Electronic Health Information Exchanges**, *Journal of Business Ethics*, vol.90, No.2, pp.169–178, 2010.

3- Ahmed Mahmood, Charlie Obimbo, Tarfa Hamed and Robert Dony, **Improving the Security of the Medical Images**, *International Journal of Advanced Computer Science and Applications*, Vol.4, No.9, PP.137-146, 2013.

4- Gonzalo Alvarez, Shujun Li and Luis Hernandez, **Analysis of security problems in a medical image encryption system**, *Computers in Biology and Medicine*, vol.37, No.3, pp.424-427, 2007.

5- Rajendra Acharya, P. Subbanna Bhat, Sathish Kumar and Lim Choo Min, **Transmission and storage of medical images with patient information**, *Computers in Biology and Medicine*, vol.33, No.4, pp.303-310, 2003.

6- Bibhudendra Acharya, Saroj Kumar Panigrahy, Sarat Kumar Patra3 and Ganapati Panda, **Image Encryption Using Advanced Hill Cipher Algorithm**, *ACEEE International Journal on Signal and Image Processing*, Vol.1, No.1, PP.37-41, 2010.

7- Chin-Chen Chang, Min-Shian Hwang and Tung-Shou Chen, **Anew encryption algorithm for image crypto systems**, *The Journal of systems and software*, vol.58, No.2, pp.83-91, 2001.

8- V.Chandra Prasad and S.Maheswari, **Robust Watermarking Of AES Encrypted Images For Drm Systems**, *IEEE International Conference on Emerging Trends in Computing, Communication and Nanotechnology*, Tirunelveli, 2013, pp.189-193.

9- Ashraf Darwish, Aboul Ella Hassanien, Qing Tan, and Nikhil R.Pal, **Securing Patients Medical Images and Authentication System Based on Public Key Infrastructure**, in *6th International Conference SOCO*, vol.87, E.corchado et al Eds, Springer Berlin Heidelberg, 2011, pp.27–34.

10- A.N.Akansu, W.A.Serdijn, and I.W.Selesnick, **Wavelet Transforms in Signal Processing: A Review of Emerging Applications**, *Physical Communication, Elsevier*, vol.3, No1, pp.1-18, 2010.

11- William Stallings, **Cryptography and Network Security Principles and Practices**, Prentice Hall, 5th edition, 2010.

12- Rivest,R.L, Shamir,A and Adleman, **A Method for Obtaining Digital Signatures and Public-Key Cryptosystems**, *Communications of the ACM*, Vol.21, No.2, pp.120-26, 1978.

13- Asmaa Sabet Anwar, Kareem Kamal A.Ghany, Hesham Elmahdy, **Human Ear Recognition Using Geometrical Features Extraction**, *In proceeding of International Conference on Communication, Management and Information Technology (ICCMIT 2015)*.

14- K. D. Sonal, **Study of Various Image Compression Techniques**, in *Proceedings of COIT*, RIMT Institute of Engineering& Technology, Pacific, 2000, pp. 799-803.

15- A. Alarabeyyat, S. Al-Hashemi, T. Khdour, M. HjoujBtoush, S. Bani-Ahmad and R. Al-Hashemi, **Lossless Image Compression Technique Using Combination Methods**, *Journal of Software Engineering and Applications*, Vol. 5, pp. **752-763,** 2012.