SECURITY SYSTEM FOR SAFE TRANSMISSION OF MEDICAL IMAGES

Mohammed Jamal al-Mansor MSc

Department of Electrical, Electronic and Systems Engineering, Iraq University College, Iraq

Abstract

This paper develops an optimised embedding of payload in medical images by using genetic optimisation. The goal is to preserve the region of interest from being distorted because of the watermark. By using this system there is no need to manually define the region of interest by experts as the system will apply the genetic optimisation to select the parts of image that can carry the watermark guaranteeing less distortion. The experimental results assure that genetic based optimisation is useful for performing steganography with less mean square error percentage.

Keywords: steganography**;** watermarking; discrete wavelet transform; medical images; advanced encryption standard; genetic algorithm

Introduction

Since the rise of the Internet one of the most important factors of information technology and communication has been the security of information. Cryptography was created as a technique for securing the secrecy of communications and many different methods have been developed to encrypt and decrypt data in order to keep the message secret. Unfortunately it is sometimes not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret. The technique used to implement this, is called steganography.[1] The word steganography is derived from the Greek words “stegos” meaning “cover” and “grafia” meaning “writing”.[2]

Steganography methods hide the secret data in a cover carrier so that the existence of the embedded data is undetectable. The cover carrier can be different kinds of digital media such as text, image, audio and video.[3] Many image steganography methods have been proposed. In these methods, the secret data is embedded into the cover-image by modifying the cover-image to form a stego- image. The most important requirement for a steganographic algorithm is for it to be imperceptible.[4] Imperceptibility involves three features.

Invisibility. The invisibility of a steganographic algorithm is the first and foremost requirement, since the strength of steganography lies in its ability to be unnoticed by the human eye.

Capacity. Steganography aims at hidden communication and requires sufficient embedding capacity. Capacity is measured in bits per pixel (bpp) in images.

Robustness against statistical attacks and image manipulation. The amount of modification the stego amount medium can withstand before an adversary can destroy the hidden information.

Achieving all these requirements simultaneously is difficult to a great extent. Steganographic methods can be broadly classified in to three categories. i) spatial transform, ii) transform domain, and iii) adaptive steganography methods.[5] Common approaches in the spatial domain method include Least Significant Bit (LSB) manipulation.

LSB insertion is the simplest method and is very weak in resisting even simple attack such as transform, compression, etc. The transform technique involves modulating the coefficients of the cover data in the frequency domain. There are a few methods in Fourier transform and it is not used for the JPEG image format.

In contrast Discrete Cosine Transform (DCT) is used extensively with image compression such as JPEG lossy compression. Although modification of properly selected DCT coefficients during the embedding process will not cause noticeable visual artefacts, they do cause detectable statistical degradations. Various steganography methods like YASS (yet another steganographic scheme), MB (model based), Outguess, and Perturbed Quantisation (PQ) have been proposed with the purpose of minimising the statistical artefacts which are produced by modifications of DCT coefficients. [6]

This paper proposes a method to embed data in discrete wavelet transform (DWT) coefficients using a mapping function based on genetic algorithm (GA) in 8x8 blocks on the cover image and, it applies the Optimal Pixel Adjustment Process (OPAP) after embedding the message to maximise the Pick signal to noise ratio (PSNR). There are only a few works on data hiding in DWT transform domain,[7,8] and there are some image steganography methods that have used GA.[9]

Related Works

Data hiding techniques are generally divided in two groups:

Spatial and frequency domain.[3,10,13] The first group is based on embedding the message in the least significant bit (LSB) of image pixel. The basic LSB method has a simple implementation and high capacity, however it has low robustness versus some attacks such as low-pass filtering and compression.[10]

Different methodologies have been proposed in the literature for End Point Reference (EPR) authentication. Some methods have performed an integration between EPR encryption and hiding in the image under the concept of watermarking (Joint watermarking\ encryption image for safe transmission).[1] EPR data are represented as ASCII of text files.

In terms of watermarking, some researchers have used spatial domain based digital watermarking scheme for adding patient information to medical images.[10,19]

There are two types of LSB insertion methods, fixed-size and variable-size. In the fixed-size methods the same number of message bits are embedded in each pixel of the cover image. The variable-size method embeds the variant number of LSBs in each pixel used for message embedding and depends on the image characteristics. A variant of the LSB method proposes an optimal pixel adjustment process (OPAP) in which imperceptibility of the stego-image can be improved.[6] Furthermore, this hiding method improves the sensitivity and imperceptibility problem found in the spatial domain.

The second group embeds the messages in the frequency coefficients of images. These hiding methods overcome the problem related to robustness and imperceptibility found in the spatial domain. JPEG, a standard image compression technique, employs DCT.[3] Several steganography techniques for hiding data in JPEG have been proposed. Recent research applies DWT due to its wide application in the new image compression standard, JPEG2000.[14] An example is the employment of an adaptive data embedding technique with the use of OPAP to hide data in the integer wavelet coefficients of the cover image.[9] Sekra et al presented a GA based steganography in discrete cosine transforms (GASDCT) domain and, GA based steganography using discrete wavelet transforms (GASDWT).[17] GASDWT has an improvement in bit rate error compared to GASDCT

While others have used frequency domain such as DCT[2,3] based watermarking scheme which is capable of hiding EPR related data into a marked image DWT[15] and others used Two Label DWT and a SVD (singular value decomposition) based watermarking technique for a more secure transmission of medical images.[7] Some have considered avoiding ROI (region of interest).[15,27]

This application discusses an exploration of the use of GA operators on the cover medium. Elitism is used for the fitness function. The model presented here is applied on image files, though the idea can also be used on other file types. Our results show this approach satisfied both security and hiding capacity requirements can increase the capacity and imperceptibility of medical image proposed a genetic algorithm evolutionary process to make secure steganography encoding on the JPEG images.[17]

Proposed Algorithm

The system consists of sender, and receiver. The electronic patient record (EPR) represents patient information to be inserted in an image for the patient. Patient information is encrypted for achieving the first level of security by hiding the meaning of the information. Next, encrypted data are inserted in the medical image, which represents a host image for the patient information, to achieve the second level of security by hiding the existence of the information. The whole process is performed at the sender side. Next, the host image is transferred through a communication channel to another party of the medical service. The goal of this operation is to meet two requirements. The first is to keep the patient information secured and inaccessible to a third party. The second is to enable an authentication of the host image that it is clean from any possible attack or corruption during transferring.

At the receiver side, the process is repeated in an inverted manner and the patient data are extracted. Next, the decryption of this data is applied in order to restore the plain patient information. The authentication can be based on matching the restored plain text with the agreed format of the patient information message. This procedure represents the typical crypto-steganography system. In this methodology the goal is to insert the patient information with lower effect on the imperceptibility. Therefore, the optimisation process of inserting the patient information is performed through using an evolutionary GA using an objective function: as a fitness function. This security system is evaluated in terms of imperceptibility by using two statistical measures: Mean Square Error (MSE) and peak signal to noise ratio (PSNR).

AES (Advanced Encryption Standard)

AES comprises three block ciphers, AES-128, AES-192 and AES-256. Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128-, 192- and 256-bits, respectively. (Rijndael was designed to handle additional block sizes and key lengths, but the functionality was adopted in AES.) Symmetric or secret-key ciphers use the same key for encrypting and decrypting, so both the sender and the receiver must know and use the same secret key. All key lengths are deemed sufficient to protect classified information up to the "Secret" level with "Top Secret" information requiring either 192- or 256-bit key lengths. There are 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys.

A round consists of several processing steps that include substitution, transposition and mixing of the input plain text and transforming it into the final output of cipher text.[14,17]

The main loop of AES performs the following functions:

Sub Bytes: Sub Bytes() adds confusion by processing each byte through an S-Box. An S-Box is a substitution table, where one byte is substituted for another, based on a substitution algorithm.

Shift Rows: Shift Rows() provides diffusion by mixing data within rows. Row zero of the State is not shifted, row 1 is shifted 1 byte, row 2 is shifted 2 bytes, and row 3 is shifted 3 bytes.

Mix Columns: Mix Columns() also provides diffusion by mixing data within columns. The 4 bytes of each column in the State are treated as a 4- byte number and transformed to another 4- byte number via finite field mathematics

*Add Round Key***:** The actual ‘encryption’ is performed in the Add Round Key() function, when each byte in the State is XORed with the sub key. The sub key is derived from the key according to a key expansion schedule.

The AES encryption flowchart is shown in Figure 1.

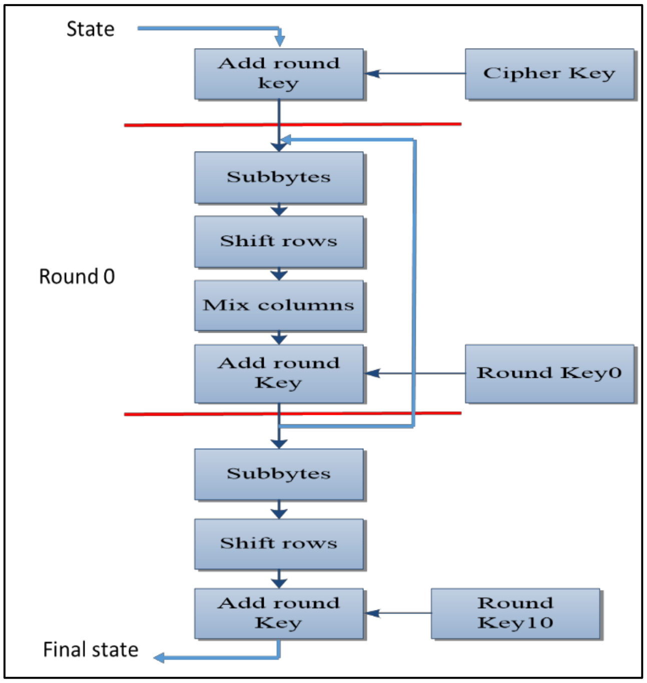

Figure 1. AES encryption flowchart.

Embedding Steganography

To embed the watermark inside the image, the watermark has to be converted to a binary format (sequence of ones and zeros). Next, a padding operation is performed on the host image to have a width and height divisible by 8. This is for converting it to an 8 x 8 pixels length of blocks. Then, the blocks of the image are converted to discrete wavelet domain and are scanned sequentially and the watermark is inserted in the pixel (8,8) according to the following logic:

1. If the watermark bit is 1, then do a quantisation to the nearest odd number.
2. If the watermark bit is 0, then do a quantisation to the nearest even number.

The same procedure has been used before.[3]

This quantisation function is defined as: Assume that f(i,j) represents the pixel of medical image , w(i,j) represents the binary pixel of watermark and

$F_k(u,v) = DWT\left\{f_{k(i,j)}\right\}$,

If W(i,j)=1 then

$$F_k(x,y) = \begin{cases} \Delta Q_e = \left(\frac{F_k(x,y)}{\Delta}\right) & \text{x,y} \in H_k \; 1 \le k \le N_{HB} \\ F_{k(x,y)} & \text{x,y} \notin H_k \; 1 \le k \le N_{HB} \end{cases}$$

If W(i,j)= 0 then

$$F_k(x,y) = \begin{cases} \Delta Q_e = \left(\frac{F_k(x,y)}{\Delta}\right) & \text{x,y} \in H_k \; 1 \le k \le N_{HB} \\ F_{k(x,y)} & \text{x,y} \notin H_k \; 1 \le k \le N_{HB} \end{cases}$$

Where Q_e is the quanitisation to the nearest even number and Q_o is the quantisation to the nearest odd number, Δ is a scaling quantity and it is also the quantisation step used to quantise either to an even or an odd number. The quantisation process is shown in Figure 2 and the embedding process in Figure 3.

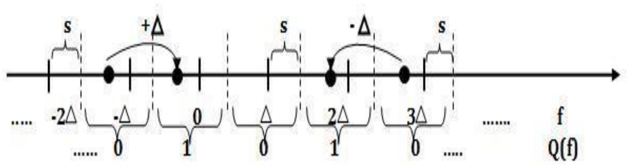

Figure 2. Quantisation procedure.

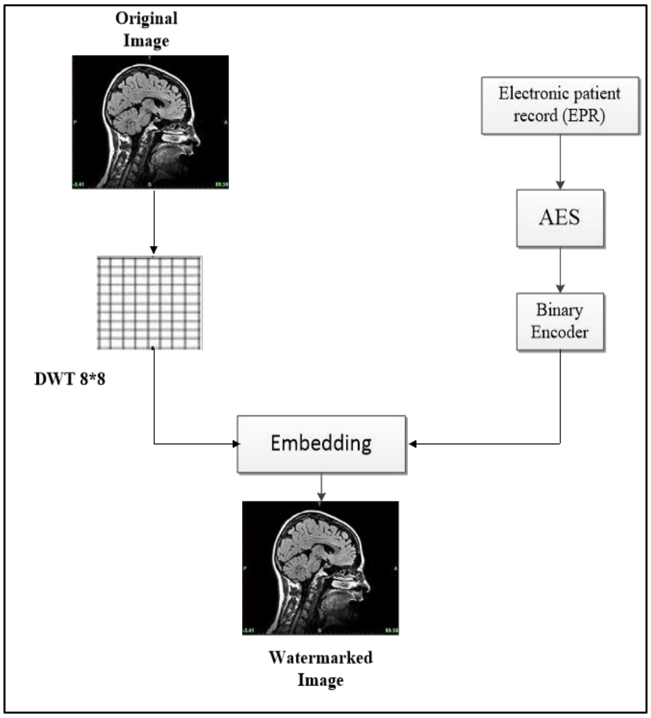

Figure 3. Graphical illustration of the embedding process.

Extractor

Extracting the watermark is performed in an inverted way to the embedding procedure. That is, the host image is partitioned to 8x8 pixels lengths of blocks. Next, the blocks are scanned sequentially, and converted to DWT domain. Next, the pixel (8,8) in each block is checked, and the following logic is performed to extract the corresponding watermark bit:

1. If the value of the pixel is odd, then the corresponding watermark bit is 1.
2. If the value of the pixel is even, then the corresponding watermark bit is 0.

If $Q\left(\frac{F_k(x,y)}{\triangle}\right)$ is odd when w(i,j) = 0

If $Q\left(\frac{F_k(x,y)}{\triangle}\right)$ is even when w(i,j) = 1

The extraction-restoration process is shown in Figure 4.

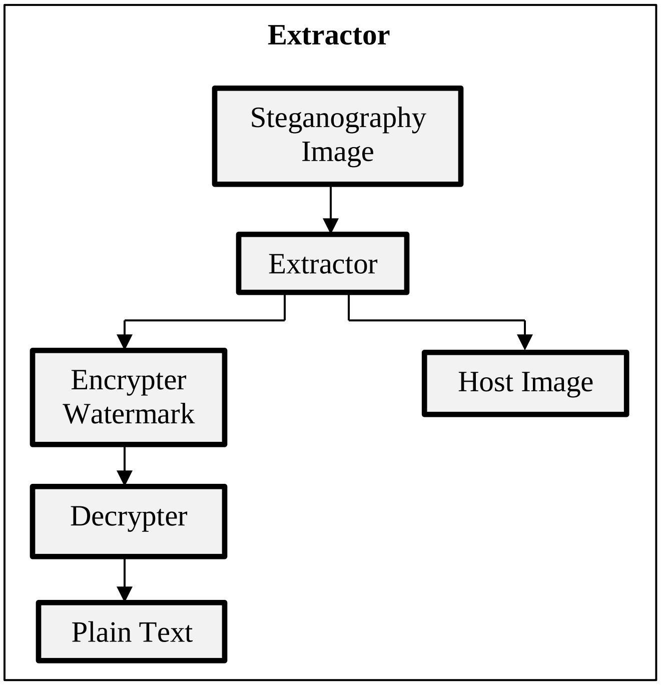

Figure 4. Illustration of the extraction-restoration process.

Genetic optimisation

It is desired in steganography to achieve the maximum value of PSNR, which leads to higher imperceptibility and better preservation of image information from tampering. This might be more important in medical images due to the fact that medical images contain diagnostic information of the patient. Any tampering or damaging to this information will lead to false diagnostic. An evolutionary optimisation algorithm is developed to embed the EPR in the image with maintaining higher PSNR. In order to do this, PSNR is regarded as the fitness function of the genetic optimisation. The process is described in the following.

Chromosome Representation

Considering that the image is divided into N blocks, each one is 8 X 8 pixels. The conventional approach is to embed EPR in the blocks in a sequential manner. The first block is b_1 and the last block is b_M where M denotes the length of the EPR message. This way of embedding EPR in the image is one possible solution. However, this solution might not correspond to the best value of PSNR.

Chromosome representation is the main part of any genetic model. We propose representing the chromosome by a vector of blocks index $chro = \{b_1, b_2, \ldots\ldots, b_N\}$. In this representation, the chromosome is a binary vector with length of the number of the blocks in the image. Each value might be 1, or 0. One denotes that a bit of the EPR message is embedded in the corresponding block, and 0 denotes that no bit in the EPR is embedded in the corresponding block.

Objective Function

The objective of this model is to maximise a well-known defined function

$$\text{PSNR} = 10\ log_{10}\ \ \frac{MAX\ I^2}{MSE}$$

Reproduction

The algorithm starts by creating a random population combined of a specific number of chromosomes. Each individual of the current population is scored based on the of fitness function. The population size is 40. Parents of the new generation will be selected based on the value of the fitness function and call them elite, the count of them is 10% of the population.

Crossover and Mutation

A single point crossover representation is used. The mutation is a random change for values in the chromosome based on a uniform distribution function.

Authentication

After extracting the watermark, and decrypting it, an authentication step is needed in order to validate that the host image has not been affected with any attack. In order to do this, the watermark plain data can be entered into a database in the system that includes information about all patient record numbers. The EPR should follow a predefined format. Any altering to the watermark bits will cause a change in the EPR format, and consequently, it can be used as a validation method for confirming that the image has not been exposed to any attack.

The format of the EPR is considered to consist of three types of fields: NAME, Date of Birth, and Record Number. A (#) delimiter separates each two consecutive field. Any violation of this format is used as an evidence of tampering with the image.

Evaluation

This study evaluates the performance of concealing data in the image using DWT applied to MRI, medical images based on statistical performance metrics like PSNR, mean square error (MSE), normalised correlation (NC).

$$\text{MSE} = \frac{1}{MN}\ \sum_{i=1}^{M}\sum_{j=1}^{N}\big(x(i,j) - y(i,j)\big)^2$$

Where x(i,j) represents the original image and y(i,j) is represent modified image and (i,j) are the pixel of position of the M*N , MSE is zero when x(i,j)=y(i,j).

$$\text{PSNR} = 10\ log_{10}\ \ \frac{MAX\ I^2}{MSE}$$

Where max I is the peak value of original image. The PSNR of an image is a typical measure used for assessing image quality by considering that the just noticeable distortions are uniform in all coefficients in a specific domain, such as special domain, frequency domain, or some transform domain. Since PSNR is more compatible and can be used to provide a generic bound for the watermarking capacity we used the PSNR to analyse the watermark embedding distortions on images.

Experimental results

In order to validate the developed system, a set of three images with a resolution of three has been used. Electronic records of three patients were encrypted using the advanced encryption system. Both embedding and extraction process were tested. After the patient's electronic record was embedded in the image, a calculation of MSE and PSNR was performed to verify the embedding quality or imperceptibility.

AES Encryption result

For the study the EPR had a predefined format with each field separated by # sign. The AES algorithm encrypted different EPR records. Table 1 shows the EPR plain texts and their encrypted results. This encryption step creates an initial security level before embedding the EPR in the patient image using the developed steganography.

Table 1. EPR plain text and cipher text.

EPR	**Encrypted EPR**
MohammedJamal#04-12-1989#0182-2683-4440-4421#	uH®{!b•#°I"y8±L½&Cz\2;dHW¨
KaramAlbeaty# 15-02-1957#0442-2148-4440-4421#	×´q¦'÷lX&iCt÷ûJén[¨²DnrY>-cLL
Saifalsamer#24-09-1984#0569-0000-1456-4999#	½PYH´´©,¢C¬qSétJz|)sHS%Y¬E¸n

Steganography performance

In order to evaluate the performance of the steganography, PSNR and MSE measures were generated for every image after inserting the EPR. PSNR is a good measure for imperceptibility while MSE is a measure for the amount of the noise that is interfered in the image. Table 2 shows each EPR, encrypted EPR, and its corresponding PSNR, MSE measures. In addition, the algorithm has been compared with a method from the literature in order to observe the relative performance with respect to the state of the art methods.[3]

Table 2. Encryption EPR and measures PSNR, MSE.

EPR	ENCRYPTED EPR	PSNR	MSE
MohammedJa mal#04-12- 1989#0182-2683-4440-4421#	uH®{! b•#°I"y8± L½&Cz\2;dHW¨	99.0369	4.3831e-^{04}
KaramAlbeaty#15-02-1957#0442-2148-4440-4421#	×´q¦"÷lX &iCt÷ ûJén[¨l²D nrY>-cL L	91.1411	0.0021
Saifalsamer#2 4-09-1984#0569-0000-1456-4999#	½PYH´´©,¢C¬qSét Jz¦)sHS% Y¬E¸n	92.4303	0.0015

Figure 5 shows results PSNR and MSE and Figure 6 the embedding process. A comparison of results between this study and others is shown in Table 3.

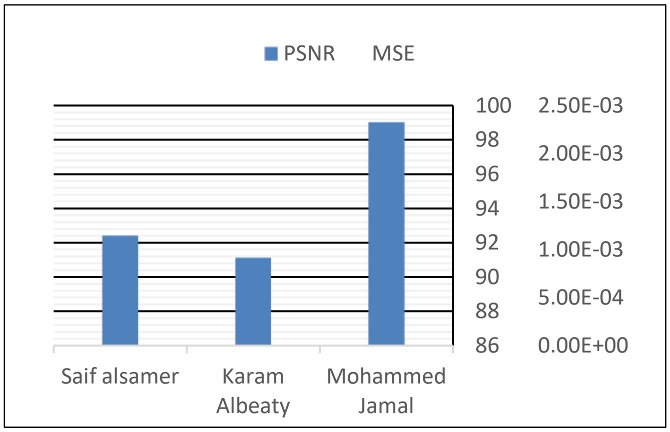

Figure 5. Evaluated EPR.

Steganography improved by using genetic algorithm

After being decrypted the watermark is fed along with the image to a genetic algorithm to define the best insertion scheme in the image. The chromosome is represented as series of ones and zeros with a size identical to the number of blocks in the image. The total number of ones is identical to the watermark size. The ones denote the location in which the embedding of the watermark will consider for steganography. The best chromosome which has most fitness value in the population is regarded as our optimal result. By genetic, taking the PSNR value as fitness function to be, optimised will lead to better performance in the imperceptibility aspect. For a watermark of size 50 bits the achieved PSNR by genetic is The genetic showed a slow performance because of the huge searching space in the current representation of the genetic algorithm.

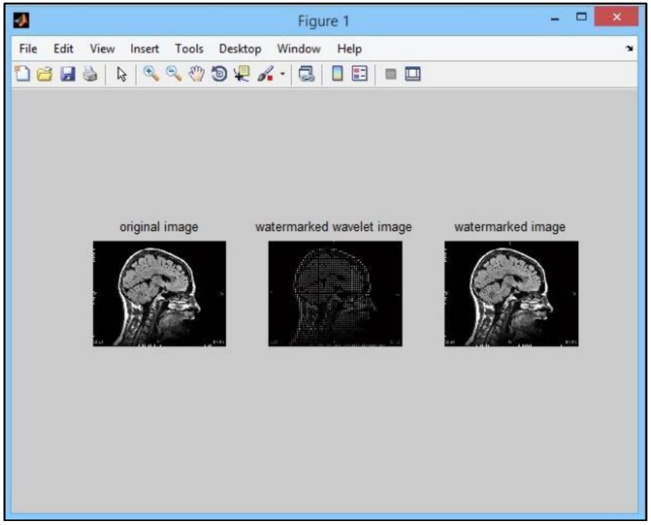
Figure 1
File Edit View Insert Tools Desktop Window Help
original image
watermarked wavelet image
watermarked image

Figure 6. Embedding DWT.

Authentication

Different types of attacks were applied on the images. The algorithm was used to perform an authentication by extracting the EPR from the image after applying the attack, decrypting the EPR, and comparing the format with the predefined format of the EPR. Figure 7 shows watermarked images and their corresponding attacked images. All authentication processes were applied successfully.

Table 3. Comparison of PSNR results with other studies.

Author	Objective	Domain	PSNR
This study	Authentication	Encryption and DWT with genetic algorithm	99.0369 dB
Sudeb Das et al (2013) [22]	Authentication, integrity and data hiding	Spatial	43.5-44.8 dB
Dalel et al (2012) [8]	Reliability	Spatial Encryption	53.9dB-60.15dB
Al-Gindy (2010) [3]	Authentication	Frequency (DCT)	73dB
Fontani et al (2010) [21]	Reliability	Frequency (Wavelet)	66-84dB
Viswanathan (2013) [23]	Confidentiality, Availability, Reliability	Spatial Encryption and biometric	45-62dB

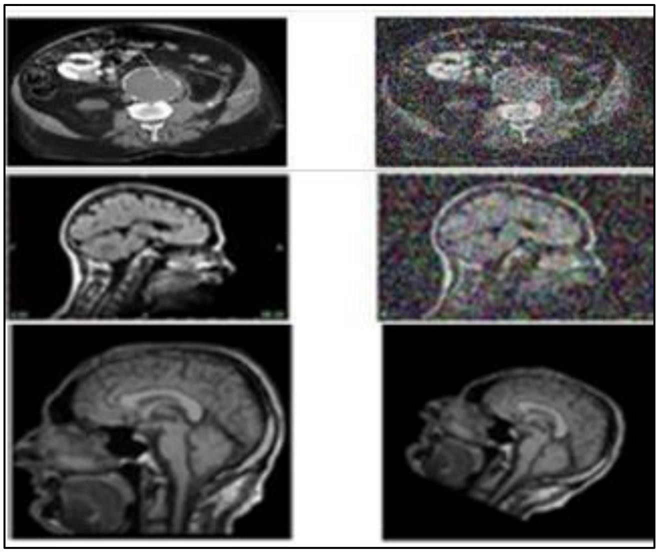

Figure 7. The images on the left are the originals and on the right are the attacks: top = Gaussian noise attack; middle = salt and pepper attack; and bottom, a rotation attack.

Conclusions

This paper presents a novel algorithm for embedding and extracting data in the DWT domain. A genetic algorithm based mapping function was employed to embed data in DWT Transform coefficients in 8x8 blocks on the cover image. The optimal pixel adjustment process was applied after embedding the message. Genetic Algorithm and Optimal Pixel Adjustment Process were implemented to obtain an optimal mapping function to reduce the difference error between the cover and the stego-image, therefore improving the hiding capacity with low distortions. This work is more suitable for low or medium size of images as large images cause a relatively high computational complexity for executing the optimisation.

…………………………………………………………

Corresponding author:
Mohammed Jamal al-Mansor
Department of Electrical, Electronic and Systems Engineering
Faculty of Engineering and Built Environment
IRAQ University College,
IRAQ
Email: m_j_2006_2009@yahoo.com

Conflict of interest. The author declares no conflicts of interest.

References

1. Ajili S, Hajjaji MA, Bouallegue B, Mtibaa A. Joint watermarking\encryption image for safe transmission: Application on medical imaging. In Computer & Information Technology (GSCIT), 2014 Global Summit on 2014 Jun 14 (pp. 1-6). IEEE.
2. Akter A, Ullah MA. Digital image watermarking based on DWT-DCT: Evaluate for a new embedding algorithm. In Informatics, Electronics & Vision (ICIEV), 2014 International Conference on 2014 May 23 (pp. 1-6). IEEE.
3. Al-Gindy A. A fragile invertible watermarking technique for the authentication of medical images. InSignal Processing and Information Technology (ISSPIT), 2010 IEEE International Symposium on 2010 Dec 15 (pp. 191-195). IEEE.
4. Furht B, Kirovski D. Protection of multimedia content in distribution networks. Multimedia watermarking techniques and applications. CRC Press, Taylor and Francis Groups, USA. 2006:1-60.
5. Paar C, Pelzl J. Understanding cryptography: a textbook for students and practitioners. Springer Science & Business Media; 2009 Nov 27.
6. Chan CK, Cheng LM. Hiding data in images by simple LSB substitution. *Pattern Recognit* 2004;37(3):469-474.
7. Pathak Y, Dehariya S. A more secure transmission of medical images by two label DWT and SVD based watermarking technique. In Advances in Engineering and Technology Research (ICAETR), 2014 International Conference on 2014 Aug 1 (pp. 1-5). IEEE.
8. Bouslimi D, Coatrieux G, Cozic M, Roux C. A joint encryption/watermarking system for verifying the reliability of medical images. *IEEE Trans Inf Technol Biomed* 2012;16(5):891-899.
9. El Safy RO, Zayed HH, El Dessouki A. An adaptive steganographic technique based on integer wavelet transform. InNetworking and Media Convergence, 2009. ICNM 2009. International Conference on 2009 Mar 24 (pp. 111-117). IEEE.
10. Eswaraiah R, Reddy ES. A fragile ROI-based medical image watermarking technique with tamper detection and recovery. In Communication Systems and Network Technologies (CSNT), 2014 Fourth International

Conference on 2014 Apr 7 (pp. 896-899). IEEE.

11. Shelly GB, Vermaat ME, Quasney JJ, Sebok SL, Jeffrey J. Multimedia and content sharing. *Discovering Computers*. 2009:294-297.
12. Sencar HT, Ramkumar M, Akansu AN. Communication with side information and data hiding. Data hiding fundamentals and applications: content security in digital media. ELSEVIER Academic Press, London, UK. 2004:35-39.
13. Jafari R, Ziou D, Rashidi MM. Increasing image compression rate using steganography. *Expert Syst Appl* 2013;40(17):6918-6927.
14. Gowtham M, Senthur T, Sivasankaran M, Vikram M, Sreeja GB. AES based steganography. *Int J Applic Innov Eng Manage* (IJAIEM). 2013;2:382-389.
15. Nilesh R, Ganga H. Securing medical images by watermarking using DWT-DCT-SVD. *Int J Comutp Trends Technol* 2014;12(2):67-74.
16. Raja'S A, Al Jaber A. A fragile watermarking algorithm for content authentication. *Int J Comput Inform Sci* 2004;2(1):27-37.
17. Sekra S, Balpande S, Mulani K. Steganography using genetic encryption along with visual cryptography. *IJCSIS* 2014;12(12):24.
18. Huang W, Ho AT, Pankajakshan V. Watermarking-based content authentication of motion-JPEG sequences in Proc VIE, 2008, p. 813- 818.
19. Wu CC, Kao SJ, Hwang MS. A high quality image sharing with steganography and adaptive authentication scheme. *J Syst Softw* 2011;84(12):2196-2207.
20. Duric Z, Jacobs M, Jajodia S. 6-Information Hiding: Steganography and Steganalysis. *Handbook Stat* 2005;24:171-187.
21. Fontani M, De Rosa A, Caldelli R, et al. Reversible watermarking for image integrity verification in hierarchical PACS. In Proceedings of the 12th ACM workshop on Multimedia and security 2010 Sep 9 (pp. 161-168). ACM.
22. Das S, Kundu MK. Effective management of medical information through ROI-lossless fragile image watermarking technique. *Comput Methods Programs Biomed* 2013;111(3):662-675.
23. Viswanathan P, Krishna PV. A joint FED watermarking system using spatial fusion for verifying the security issues of teleradiology. *IEEE J Biomed Health Inform* 2014;18(3):753-764.
24. Morkel T, Eloff JH, Olivier MS. An overview of image steganography. In Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005), Sandton, South Africa, 2005.
25. Moerland T. Steganography and steganalysis. Leiden Institute of Advanced Computing Science. 2003.
26. Liu CL, Liao SR. High-performance JPEG steganography using complementary embedding strategy. *Pattern Recognit* 2008;41(9):2945-2955.
27. Mohan M, Anurenjan PR, A Novel Data Hiding Method in Image using Contourlet Transform. *Recent Advances in Intelligent Computational Systems (RAICS)*, 2011:411-415.
28. Solanki K, Sarkar A, Manjunath BS. YASS: Yet another steganographic scheme that resists blind steganalysis. In *International Workshop on Information Hiding* 2007 Jun 11 (pp. 16-31). Springer, Berlin, Heidelberg.
29. Sajedi H, Jamzad M. Adaptive steganography method based on contourlet transform. In Signal Processing, 2008. ICSP 2008. 9th International Conference on 2008 Oct 26 (pp. 745-748). IEEE.
30. Ghasemi E, Shanbehzadeh J, Fassihi N. High Capacity Image Steganography Based on Genetic Algorithm and Wavelet Transform. InIntelligent Control and Innovative Computing 2012 (pp. 395-404). Springer US.
31. Cheddad A, Condell J, Curran K, Mc Kevitt P. Digital image steganography: Survey and analysis of current methods. *Signal Process* 2010;90(3):727-752.
32. Sajedi H, Jamzad M. ContSteg: contourlet-based steganography method. *Wireless Sensor Network* 2009;1(03):163.