

## Encryption and Hiding Watermarking Using A Chaotic Modified Wavelet Transform

Shaimaa Sh. Mohammad

College of Computer Sciences and Mathematics  
University of Mosul, Iraq

Received on: 02/01/2011

Accepted on: 16/05/2011

### ABSTRACT

In this letter, a new digital watermarking algorithm is proposed to hide binary image watermark inside gray image to increase authentication and robustness, DWT are used in embedding because it has many features in image processing. To increase the effective of this algorithm chaotic logistic map are used to select the embedding position in host chaotically which increase the security and make it hard to be detected, experimental result which be measured by using (Mean Square error, Peak signal to noise ratio , Signal to Noise Ratio, CORLLATION) has value (0.3195, 53.0867, 45.9152, 0.9998) respectively reflect the effective of this algorithm, the watermarked image has no noticeable change, some image processing operation such as(filter ,noise and compression) are used to test the robustness which measured by calculate similarity between extracted watermark after attack and the original one, Programming based on Matlab9.

**Keywords:** Encryption, Hiding, Watermarking, Wavelet Transform, Chaotic.

تشفير وإخفاء العلامة المائية باستخدام التحويل الموجي الفوضوي المعدل

شيماء محمد

كلية علوم الحاسوب والرياضيات، جامعة الموصل

تاريخ قبول البحث: 2011/05/16

تاريخ استلام البحث: 2011/01/02

### المخلص

يتم خلال هذا البحث تم اقتراح طريقه لإخفاء صوره ثنائيه كعلامة مائيه داخل صوره رمادية لغرض زيادة الوثوقية والتحصين ضد الهجمات، تم استخدام التحويل الموجي في الإخفاء لما يتميز به من خصائص عده في مجال معالجة الصور ولزيادة قوة وفعالية هذه الخوارزمية تم استخدام الدالة اللوجستية الفوضوية لتحديد مواقع الإخفاء داخل الصورة بصوره عشوائية مما يزيد سرية هذه الخوارزمية إذ انه من الصعب جداً التنبؤ بمواقع الإخفاء داخل الصورة الناتجة من خلال النتائج العملية التي تم الحصول عليها باستخدام المقاييس  $psnr$  ,  $mse$  ,  $correlation$ ,  $snr$  والتي كانت نتائجها (0.3195, 53.0867, 45.9152, 0.9998) على التوالي عكست مدى جودة هذه الخوارزمية إذ أن الصورة بعد الإخفاء لم تحوي تغيير واضح للعيان. تم استخدام بعض عمليات معالجة الصور مثل (الفلتر، الضوضاء، الكبس) لقياس مدى قوة هذه الخوارزمية من خلال حساب التطابق بين العلامة المائية المستخرجة والعلامة الأصلية. أما برمجة وتنفيذ العمل فتم بالاعتماد على Matlab9.

الكلمات المفتاحية: تشفير، إخفاء، العلامة المائية، التحويل الموجي، الفوضى.

### 1- Introduction

Digital watermarking is defined as the process of hiding apiece of digital data in the cover data which is to be protected and extracted later for ownership verification. Some of the important applications of watermarking technique are copyright protection, ownership verification, finger printing, and broadcast monitoring [1]. Watermarking can be embedded in the spatial domain or a transform domain. In spatial domain, the

watermark is embedded directly by modifying the intensity value of pixels, In frequency domain, the watermark is embedded by changing the frequency coefficients. To transform image into frequency domain, the transformation technique such as discrete wavelet transformation (DWT), discrete cosine transformation (DCT) and discrete Fourier transformation are used. Spatial domain watermarking technique is easier and its computing speed is high, than transform domain. But the disadvantage is that it is not robust against common image processing operations. Transform domain technique are introduced to increase the robustness of the digital media [2]. There are three kinds of digital watermarking technique according to their embedding purpose: robust, fragile, and semi-fragile. A robust watermark withstands malicious attacks, such as scaling, rotating, filtering, and compression. This kind of watermarking is usually used for copyright protection. Fragile watermarks can detect any unauthorized modification in an image, and therefore, they are quite suitable for an authentication purpose. However a semi-fragile watermark is adopted to detect the unauthorized modification, and at the same time, it must survive some authorized image processing operations [3]. In addition, non Blind, semi-Blind, and Blind methods are the division of watermarking. In non-Blind methods the original image itself are employed for the extraction of watermark, While the certain characteristics of the original image are engaged by the semi-Blind methods, whereas the detection process in the Blind methods do not necessitate the original image. A good watermarking scheme should be robust enough to define against attacks while being invisible such that the dissimilarity between the watermarked image and the host image should not be distinguishable by the human eyes [4]

In this paper a simple and efficient security system is introduced to protect the ownership of digital image using non-blind imperceptibly encrypted binary image watermarking based on DWT using chaotic function to generate random sequence used to select DWT coefficient that will be used in embedding. Chaotic Logistic map function was used twice, first time for watermarking encryption and second for watermarking hiding in host image.

The rest of this paper is organized as follows: section 2 introduces the related works. Section 3 defines different notations used in this paper. Section 4 illustrated the steps of using chaotic in watermarking encryption. Section 5 defines how to use chaotic in embedding. Section 6 and 7 introduce watermarking embedding and extraction respectively. Experimental results and attack analysis are discussed in section 8 and 9 respectively. Finally concluding remarks are made in section 10.

## **2- Related works**

1. In 2006, S. Mabtoul, E. Ibn-Elhaj and D. Aboutajdin present a Blind watermarking procedure for digital image in complex wavelet domain. The procedure has many steps: first a watermark image as copyright sign is preprocessed with a random location matrix then split the host image into many non-overlapping small blocks with 8\*8 pixels and by using chaotic logistic map function generate a random sequence which is used to select the blocks to construct sub image, perform a Dual tree Complex Wavelet Transform on sub image then hide the watermark into coefficients by compare each pixel of low pass subband with its eight neighbors [5].
2. In 2007, Xianyong Wu and Zhi-Hong Guan, proposed anew watermarking algorithm by using two type of chaotic maps function first Arnold cat map was used to select the embedding position in host image, second using logistic map to

determine the pixel bit of host image for watermark embedding, they use spatial domain for embedding [6].

3. in 2009,Guang yang and yang zhon present research to compress watermark using Huffman coding and embedding it using LSB and chaotic logistic function [7].
4. In 2009, Chen yongqiang and others present an algorithm to encrypted binary image watermarking using chaotic stream encryption and embedding it by selecting and modifying DWT coefficient using genetic algorithm and used neural network in watermarking identification [8].

### 3- Notation and Background

- a. **Chaotic:** the word 'chaos' has appeared since 800 BC and was derived from the Greek  $\chi\alpha\omicron\varsigma$ , which mean complete absence of order. In the past decades, many research started to adopt chaos theory into cryptosystem the reason of applying chaotic algorithm on data encryption because of two intrinsic characteristics of chaotic algorithm [9]

- Highly complex and nonlinear behaviors.
- Sensitive dependence on initial condition.

- **Logistic Map:** Logistic Map is simple, fast, sensitive to the initial conditions, unpredictable and it is a one-way-function. Logistic Map is a recursive function which takes a real number ( $X_n$ ) ,  $0 \leq X_n \leq 1$  as an input, and produce real number,  $X_{n+1}$ , between 0 and 1 (inclusive) as indicated by Equation 1. Various sequences of the Logistic Map can be generated from different initial value of  $X_0$  and  $r$  [6][10]. Figure 1 shows the graph of the Logistic Map plotted from Equation 1.

$$X_n = r(1 - X_{n-1})X_{n-1} \quad \dots(1)$$

Where  $r \in [0,4]$ ,  $X_n \in (0,1)$ , and  $n \in N$  [6][10]

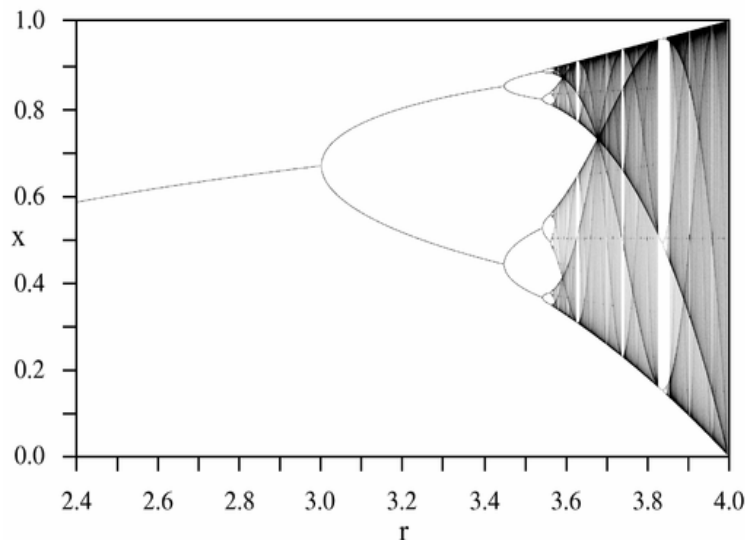


Figure 1: Bifurcation diagram for the Logistic Map [10]

- b. **Wavelet Transform:** Wavelet are recently developed signal processing tool enabling the analysis on several time scales of the local properties of complex signals that can present non stationary zones. They lead to a huge number of applications in various fields, such as for example geophysics, astrophysics,

telecommunication, imagery and video coding. They are the foundation for new techniques of signal analysis and synthesis and find beautiful application to general problems such as compression and denoising [11]. The Discrete wavelet transform (DWT) is a powerful and a popular transform familiar to image processing community. In two dimensional applications, The DWT decomposes a given image into four subbands (i.e. LL1, HL1, LH1, and HH1). The subbands (LL1) represent the low frequency part where most energy is concentrated, while the other subbands represent the high frequency content in the horizontal, vertical, and diagonal directions. To obtain the next wavelet level, the subband (LL1) is further decomposed into another four subbands. This process can be repeated several times until the required decomposition level is reached. Figure 2 shows an example of three level wavelet decomposition subbands [12] [13]

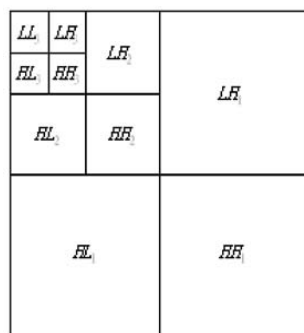


Figure 2: Three level DWT decomposition [12][13]

#### 4. Watermarking encryption

Watermarking encryption algorithm is proposed as following steps:

Step1: Read a binary watermarking image W of size M\*M.

Step2: Locate  $X_0$  and r value which is key for encryption,

$$\text{Where } 0 \leq X_0 \leq 1 \text{ and } r \in [3.5, 4].$$

Step3: Use Equation1 to generate real value sequence(S) of size  $M^2$ .

Step4: Transfer sequence S generated by step 3 to binary sequence by using the following equation:

$$S'_k = \begin{cases} 1 & \dots S_k > 0.5 \\ 0 & \dots S_k < 0.5 \end{cases} \quad \dots(2)$$

$$\text{Where } k=0, 1, 2, \dots M^2$$

Step5: Encrypt watermarking using following equation

$$W'(i, j) = W(i, j) \oplus S'_k \quad \dots(3)$$

$$\text{Where } 0 \leq i \leq M - 1, 0 \leq j \leq M - 1, 0 \leq k \leq M^2 - 1$$

In decryption algorithm, The same pervious steps with the same initial value of  $X_0$  and r must be used.

#### 5. Chaotic algorithm

The chaotic algorithm in embedding is proposed by [7] as follows:

Step1: Choose the original number  $X_0$ , which is the seed of the Logistic mapping, and it is another key of the embedding algorithm.

Step2: Using the Logistic Mapping n-1 times to create a sequence  $\{x_1, x_2, \dots, x_{n-1}\}$ .

Step3: Sorting the previous sequence and create anew sequence  $\{x'_0, x'_1, \dots, x'_{n-1}\}$ .

Step4: Find out the position of every element of the sequence  $\{x_0, x_1, \dots, x_{n-1}\}$  in the sequence  $\{x'_0, x'_1, \dots, x'_{n-1}\}$ , and then create a transform sequence

$$T = \{t_0, t_1, \dots, t_{n-1}\}.$$

Sequence T, which produced from this algorithm contain value from 1 to n sorted at random and not serial.

## 6. Watermarking Embedding

An embedding algorithm in DWT domain can be presented in following:

Step1: Read host gray image (Y) with size N\*N.

Step2: Read a watermarking binary image (W) of size M\*M.

Step3 Encrypt watermarking image using chaotic encryption algorithm to produce (W').

Step4: Change an encrypted watermarking into sequence (W''), where

$$W'' = \begin{cases} -1 \rightarrow W' = 0 \\ 1 \rightarrow W' = 1 \end{cases} \quad \dots(4)$$

Step5: Perform one level DWT (db1) on host image(Y) to get approximation(LL subband) and details coefficients(HL,LH,HH subbands).

Step6: Generate a chaotic sequence (T) of size  $N^2$  by perform chaotic algorithm.

Step7: Change each DWT approximation coefficient selected by ( $T_i$ ) using equation5

$$Y'_i = Y_i(e^{\alpha W''_i}) \quad \dots(5)$$

Where  $Y'_i$  : DWT coefficient after embedding.

$Y_i$  : Original DWT coefficient.

$W''_i$  : Encrypted watermarking value  $\{-1, 1\}$ .

$\alpha$  : Small value  $0 < \alpha < 1$ .

Step8: Perform IDWT and save the watermarked image.

## 7. Watermarking Extraction:

Step1: Read watermarked image  $I'$  and host image I.

Step2: Perform DWT on  $I'$  and I.

Step3: Choose the same value for  $X_0$  that was used in embedding and run chaotic algorithm to produce a sequence T.

Step4: Select each  $T_i$  position in approximation coefficient of  $I'$  and I.

Step5: extract the encrypted watermarking as following condition:

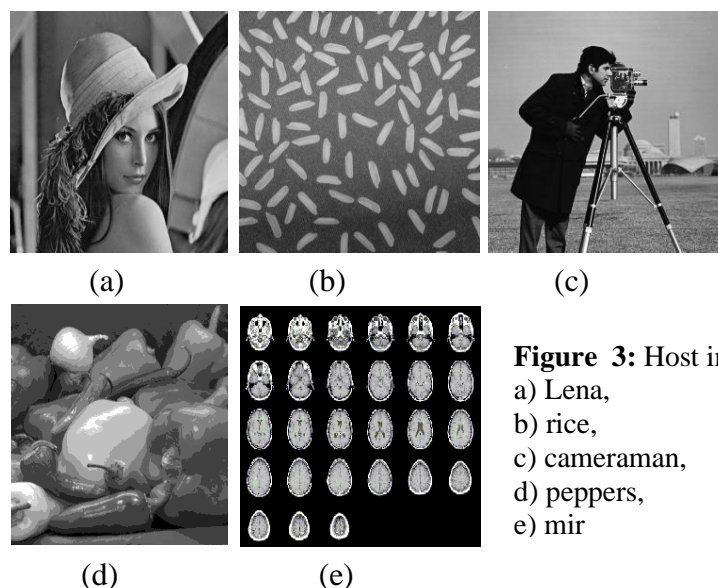
$$\begin{cases} Y'_i > Y_i \longrightarrow W_{s,t} = 1 \\ Y'_i \leq Y_i \longrightarrow W_{s,t} = 0 \end{cases} \quad \dots(6)$$

Step5: Using decryption algorithm to decrypt the extracted encrypted watermarking.

## 8. Embedding Implementation and Security Analysis

In order to evaluate validity of the proposed schema, five grayscale images samples used as host images shown in figure3. A binary image of size 64\*64 used as a watermarking is shown in figure4a.

First the binary image is encrypted by chosen  $X_0[0 \leq X_0 \leq 1]$  and  $r[3.5 \leq r \leq 4]$ , Which are the two keys for encryption. Figure4b is an encrypted watermarking using  $X_0 = 0.89$  and  $r=4$ .

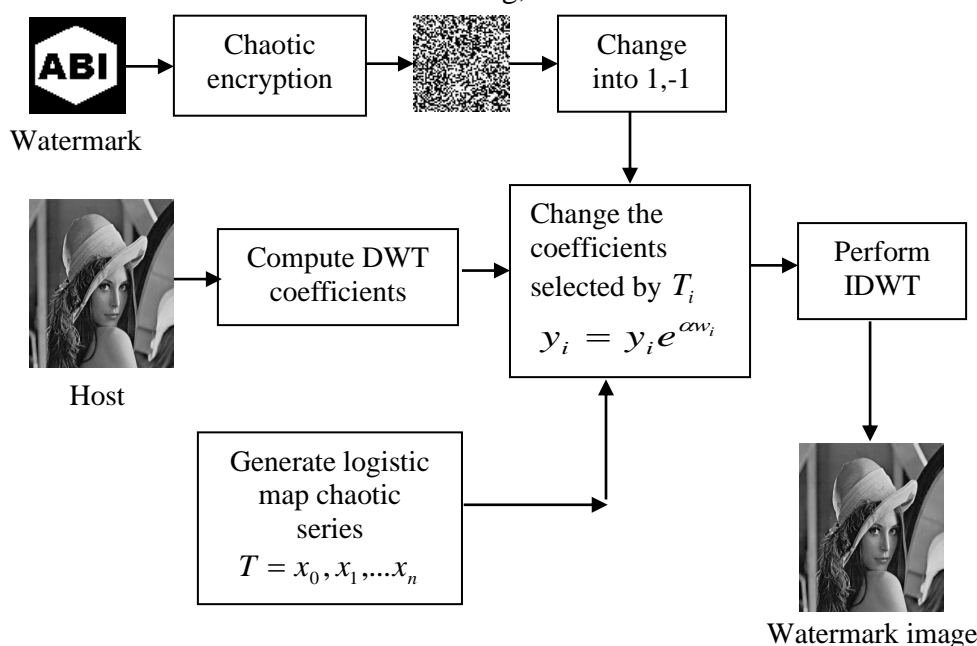


**Figure 3:** Host images  
 a) Lena,  
 b) rice,  
 c) cameraman,  
 d) peppers,  
 e) mir

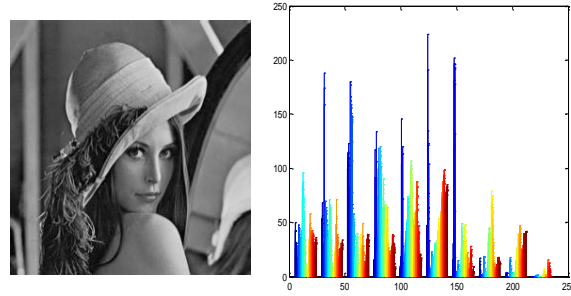


**Figure 4:** a) original watermarking, b) encrypted watermarking

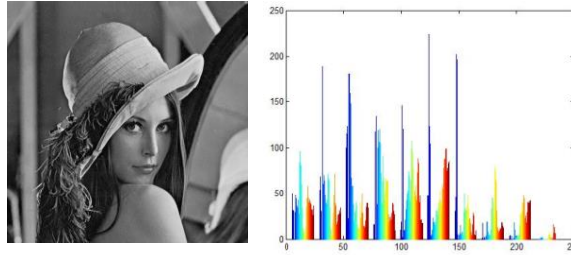
In embedding selection  $r=4$ (which means maximum chaotic) and  $X_0$  is chosen as 0.683 which is the two key for embedding. Then By implementing the best value for  $\alpha$  which is equal to 0.01, Figure5 shows embedding process and Figure6 shows the histogram of Lena before and after embedding,



**Figure 5:** Embedding Process



a. host image with its histogram



b. Watermarked image with its histogram

**Figure 6:** Lena before and after embedding

From Figures 6 (a and b), It can be seen that they are almost the same. This means that the algorithm did not damage the host image. To test the quality of the watermarked image the following measures are used

**a. Mean square error:** is one of many ways to quantify the difference between an estimator and the true value of the quantity being estimated and its equation is [2][14]:

$$MSE = \frac{1}{n * n} \sum_{i=1}^n \sum_{j=1}^n (f(i, j) - g(i, j))^2 \quad \dots(7)$$

Where  $f$  : Host image.

$g$  : Watermarked image.

**b. peak signal to noise ratio(db):** often abbreviated **PSNR**, is an engineering term for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation [2][14]

$$psnr = 10 \log_{10} \left( \frac{255^2}{mse} \right) \quad \dots(8)$$

**c. Signal to noise ratio(db):** (often abbreviated **SNR** or **S/N**) is a measure used in science and engineering to quantify how much a signal has been corrupted by noise. It is defined as the ratio of signal power to the noise power corrupting the signal [14].

$$SNR = 10 \log_{10} \left( \frac{\sum (Y_i^2)}{\sum (Y_i - Y'_i)^2} \right) \quad \dots(9)$$

Where  $Y$  and  $Y'$  are original and watermarked image respectively.

**d. Correlation(corr):** compute the correlation coefficient between the original image (A) and the watermarked image(B)[4]:

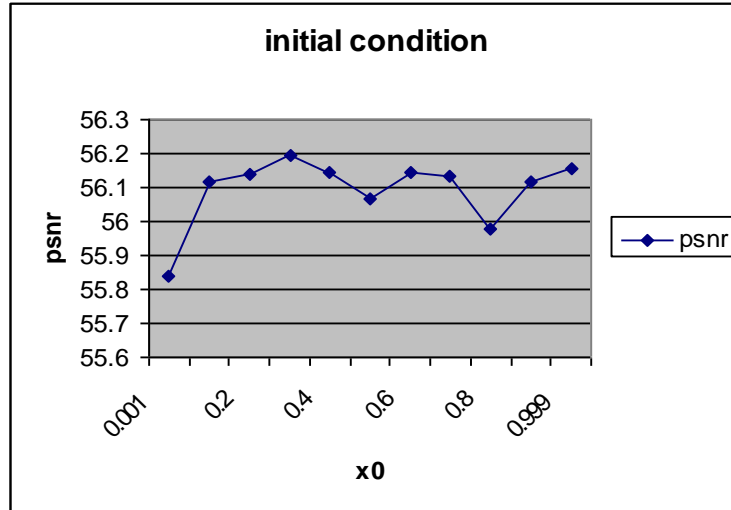
$$corr(A, B) = \frac{\sum_m \sum_n (A_{mn} - \bar{A})(B_{mn} - \bar{B})}{\sqrt{(\sum_m \sum_n ((A_{mn} - \bar{A})^2)(\sum_m \sum_n (B_{mn} - \bar{B})^2)}} \quad \dots(10)$$

Where  $\bar{A} = \text{mean2}(A)$ , and  $\bar{B} = \text{mean2}(B)$ .

The following table illustrates the value of the four measures for five samples. And figure 7 illustrated that any change in initial condition of logistic map has a slight affected on watermarked image quality.

**Table 1:** Quality measures of the watermarked image and extract

Samples	MSE	PSNR	SNR	CORR
Lena	0.3195	53.0867	45.9152	0.9998
rice	0.3917	52.2017	45.5881	0.9989
cameraman	0.5237	50.9401	45.3577	0.9999
Mir	0.1610	56.0614	47.7851	0.9888
peppers	0.4719	51.3924	45.4282	0.9988



**Figure 7:** Effect of initial condition on embedding

### 9. Attack analysis

In order to test the robustness of the algorithm, four types of attacks are used:

1. Salt & pepper attack with various densities.
2. Gaussian attack with mean=0 and various variance.
3. Median filter attack.
4. JPEG2000 compression with various ratios.

After each attack and after extract watermark the similarity is checked between original and extract watermark by the following equation [15]:

$$sim(W, W') = \frac{\sum_{i=1}^{m1} \sum_{j=1}^{m2} W(i, j)W'(i, j)}{\sqrt{\sum_{i=1}^{m1} \sum_{j=1}^{m2} W(i, j)^2} \sqrt{\sum_{i=1}^{m1} \sum_{j=1}^{m2} W'(i, j)^2}} \quad \dots(11)$$



















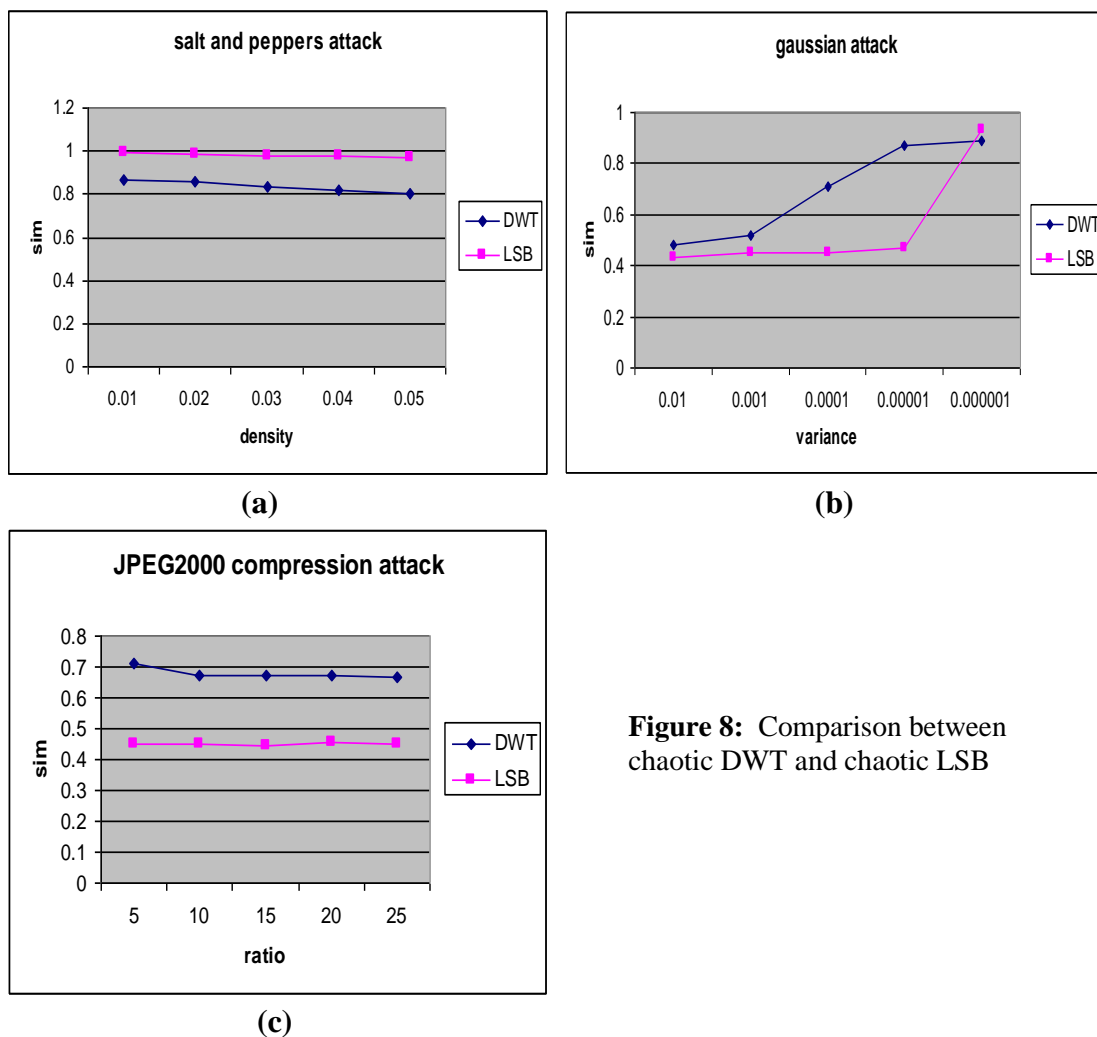
Where  $W$  and  $W'$  are original and extracted watermarks respectively the maximum value of sim is 1 correspond to perfect match.

Table2 illustrates the watermarked image after various attacks and the extracted watermark.

The comparison are made between this watermarking approaches with chaotic LSB watermarking after exposure to attacks, the results are gathered in figure8 (a, b and c) which illustrated the robustness of chaotic DWT over chaotic LSB against noises and JPEG2000 compression attacks.

**Table 2:** Watermarked image after attack

Watermarked Image after attack	Extracted watermarking		
	0.01	0.02	0.03
			
Salt & pepper attack	Sim=0.8692	Sim=8620	Sim=8375
	0.0001	0.001	0.01
			
Gaussian attack. Mean=0	Sim=0.7123	Sim=0.5185	Sim=0.4789
	1*1 neighborhood	2*2 neighborhood	3*3 neighborhood
			
Median filter.	Sim=0.8957	Sim=0.5615	0.6255
	5%	10%	15%
			
JPEG compression	Sim=0.7108	Sim=0.6744	Sim=0.6712



**Figure 8:** Comparison between chaotic DWT and chaotic LSB

## 10. Conclusion:

In the proposed algorithm the following conclusion are made:

1. This algorithm is simple, fast but efficient and has high imperceptivity.
2. chaotic logistic map has been used in encrypting and embedding with DWT which increase the security and imperceptivity because the sensitivity of logistic map to initial condition lead to generate different sequence with different initial value, therefore watermark signal spread in all regions of the host chaotically, which make embedding hard to be detected with out known initial condition.
3. after application changing in initial condition of chaotic logistic map in embedding the sequence sort will be effected but it has slight effect on watermarking quality and robustness
4. as seen in experimental results using DWT in embedding will not damage cover which reflect by value of correlation that near to 1, it mean the high identical between the covers before and after embedding.
5. Using chaotic DWT better than using chaotic LSB because it has more robustness against attacks.

**REFERENCES**

- [1] Santhi V. Thangavelu Arunkumar, 2009, "DWT-SVD combined full band robust watermarking technique for color image in YUV color space", International Journal of computer Theory and Engineering, Vol. 1, No.4
- [2] Rajkumar Franklin, GRS Manekandan, Santhi V, 2011, "Entropy based Robust Watermarking Scheme using Hadamard Transformation Technique", International Journal of computer Application, Vol12, No.9.
- [3] Saryazdi Saeid, Nezamabadi-pour Hossein, 2005, "A Blind digital Watermarking in Hadamard Domain", World Academy of science Engineering and Technology.
- [4] Reddy V.padmanabha, Varadajan S., 2010, "An effective Wavelet-Based Watermarking Scheme using Human Visual system for Protection Copyright of Digital Images", International Journal of computer and Electrical Engineering, Vol.2, No.1.
- [5] Mabtoul S., Ibn-Elhaj E., Aboutajdin D., 2006, "Ablind Chaos Based Complex Wavelet Domain Image Watermarking Technique", IJCSNS international journal of computer science and network security, vol.6,no 3.
- [6] Wu Xianyong, Guan Zhi-Hong, 2007, "Anovel digital watermark algorithm based on chaotic maps", Elsevier B.V.
- [7] Yang, Guang-ming, zhon, yang, 2009, "LSB algorithm research based on chaos", "ninth international conference on hybrid intelligent system" doi.ieeecomputersociety.org/10.1109/HIS.2009.201
- [8] Yongqiang, Chen, Yanqing, Zhang,Lihna, peng, 2009, "ADWT domain image watermarking scheme using genetic algorithm and synergetic neural network", www.academy ublisher.com/proc/isipog/papers/isipogp298.pdf
- [9] S.T. lee, Raymond, W.S. lam, henry, Augest 2006, "Achaotic Real\_time cryptosystem using a switching algorithm- based linear congruential generator(SLCG),"IJCSNS international journal of computer science and network security, Vol.6, No.8.
- [10] Maqableh,mahmoud, Bin samsudin, Azman, A.Alia, mohammed, February 2008"New hash function based on chaos theory (CHA-1)", IJCSNS international journal of computer science and network security, Vol.8, No.2.
- [11] Misiti, Michel, misiti, yves, oppenheim,Georges, poggi,Jean\_michel, 2007, "Wavelet and their application" , Britich library cataloguing-in-publication data.
- [12] El-rube Ibrahim, Abou-Elnasr Mohamad, Naim Mostafa, 2009, "Contourlet versus Wavelet Transform for a Robust Digital Image Watermarking Technique", World Academy of Science, Engineering and Technology.
- [13] Acharya Tinku, Ray Ajoy, 2005, "Image Processing Principles and Applications", A Wiley-Interscience Publication.
- [14] Sallow Amira B., Taha Zahraa M., Nori Dr.Ahmed S., 2010, "An Investigation for Steganography using Different Color System" third scientifically conference on information technology, University of computer and mathematic science, Mosul university.
- [15] Ketcham M, Vongpradhip S, 2007,"Intelligent Audio Watermarking using Gentic Algorithm in DWT Domain", Proceeding of world academy of science, Engineering and technology, Vol 20, ISSN 1307-6884