J. Appl. Environ. Biol. Sci., 5(3)174-180, 2015
© 2015, TextRoad Publication

ISSN: 2090-4274
Journal of Applied Environmental and Biological Sciences
www.textroad.com

Presentation of a method for Watermarking by Multi-dimensional Chaotic Functions

Hamid Maleki[1], Mohammad Tahghighi Sharabyan[2]

[1,2] Department of Computer Engineering, Zanjan Branch, **Islamic Azad University**, Zanjan, Iran

Received: November 6, 2014
Accepted: January 15, 2015

ABSTRACT

Watermarking is the art and science of placing of information in a carrier medium and its applications have been increasing considering the considerable advancements in digital communications. Today, watermarking is considered as serious in different scientific branches. Watermarking makes use of different algorithms in order to acquire security, resistance and capacities. One of the methods of watermarking is the use of chaotic algorithms. Chaos is a phenomenon that is embedded indefinable non-linear systems and is very sensitive too primary conditions and demonstrates quasi-random behavior. These systems are influenced by two important factors: system primary value and system control parameters which are in fact effective values in determination of chaos mode. In the present paper, a method based on chaotic functions has been presented in order to improve evaluation criteria. Results of comparisons indicate the effectiveness of the recommended method from different aspects like maintenance of the Host image quality and higher resistance against destruction and discovery attacks.

KEYWORDS: chaotic function, logistic function, Lorenz function, Henon Function, watermarking

1. INTRODUCTION

As network multimedia systems develop, it seems necessary to have information security and support for copyright in digital media. Watermarking is an appropriate method for this. Digital watermarking refers to the process of concealing information in a digital datum which exerts the lowest change in host data. This allows for image labeling, copyright doing and protection of forgery (Asvadi, 2008). Since both steganography and watermarking hide a datum in another datum and therefore carry one datum by another datum and are similar; however, they are different in terms of design target. Steganography aims to cover a datum so that the presence of the datum is not visible and its goal is not resistance against changes (V.Nagaraj et al, 2013). However, watermarking aims to exercise ownership and carries information not necessarily in hidden form and it is resistant against changes on coverage and in case there are some changes, the hidden data are recoverable. In watermarking, the goal is not remaining hidden and watermark presence may be visible in coverage (Rui Ye, 2013). In the present research, we investigate relationship between chaos and watermarking and try to receive an image file as logo and embed it in host image using chaos functions so that image quality is reserved and data remain in the image in hidden form.

2. DEFINITIONS AND METHODS

2.1. Watermarking

Digital watermarking refers to the process of concealing data in a digital datum such that the minimum change is exercised to host datum. This can be used in image labeling, copyright doing and protection from forgery. This is done by virtue of signaling in every image cell contents. Encrypting protects contents in data transfer from transmitter to receiver. Watermarking has many applications the most important of which is proving copyright and ownership right towards a digital data. Digital data owner can provide its ownership by virtue of extraction of hidden information. Watermarking has some features like Invisibility, Robustness, Security, Capacity and Complexity (Nasab Haji, 2010). For short, it can be said that Robustness shows the level of invariability of watermarked signal in digital image to intentional and unintentional manipulation and Invisibility shows resemblance of the Host image and watermarked image. These two features are in contradiction to each other. When Invisibility increases, Robustness decreases and vice versa. Relationship between Invisibility and Robustness of watermark is specified by means of watermark Strength parameter. Watermark Strength is in fact is the intensity of putting watermark image into Host image. Therefore, we can establish a trade-off between invisibility and robustness by selecting watermark power appropriately. Watermark design has two stages: image watermark concealing and identification (whether the watermark can be detected or not). In concealing stage, unmarked Host image is transferred to an environment in which we

***Corresponding Author:** Hamid Maleki**,** Department of Computer Engineering, Zanjan Branch, **Islamic Azad University**, Zanjan, Iran**.**
Email: hamidmaleky.uni@gmail.com, Tel: (+98)24-34221003

intend to hide the watermark. Then, we create watermark by means of encryption key. In the next step, the watermark is embedded into the final environment and we inverse the transfer to obtain watermark image (Rui Ye, 2013). We use a key in watermarking to embed watermark in the host medium. The key may control locations in which the host medium changes (placing location). If enemy does not have access to the key, it has many problems with eliminating it; therefore, watermarking algorithm can be created without endangering security of watermark and by protecting encryption key.

2.2. Chaos theory

Chaos theory deals with the study of chaotic dynamic systems. Chaotic systems are non-linear dynamic systems which are very sensitive to their primary conditions. Small changes in primary conditions of such systems result in great changes in future. In chaos theory, this phenomenon is called butterfly effect (Rui Ye, 2013). Chaotic systems apparently have random behaviors but there is no need to the presence of accidentally element in chaotic behavior and special dynamic systems can also express chaotic behaviors. Hilz (1990) defined chaos as: "chaos or irregularity is a kind of regular irregularity or order in irregularity. It is irregular because its results are unpredictable and it is regular because it has some kind of certainty"(E Ott, 2002). Chaotic is a mathematical concept and cannot be defined exactly but it can be considered as a kind of randomness along with certainty. Its certainty is because chaos has many internal reasons and does not occur as a result of external disorders and randomness is because chaotic and irregular behavior is unpredictable. If we want to classify chaos theories in terms of the number of primary values and the number of chaotic sequences in output, we will have one-dimensional chaos functions, two-dimensional chaos functions, three-dimensional chaos functions and spatial chaos functions. It must be noted that functions which are introduced as chaos functions do not produce chaotic behaviors in all states but they produce chaotic signals in special states and for constant values of some parameters. One of the most famous functions which can have chaotic behavior is logistic map chaos function. This function is a one-dimensional chaos function and receives only one single primary value as input and produces one chaotic sequence as output. The formula of this function is as follows (N.K.Pareek et al, 2006):

$$X_{n+1} = rX_n(1 - X_n) \qquad \text{equation (1)}$$

If we want to produce a chaotic sequence by means of logistic map function, we must assume r value in [3.57, 4] period for primary value X_0=0.3 (Pourdelan, 2011).

Henon mapping is a reversible two-dimensional chaotic mapping which was introduced by Henon in 1976. It is defined as follows:

$$\begin{cases} X_{n+1} = 1 + Y_n - \alpha_n^2 \\ Y_{n+1} = bX_n \end{cases} \qquad \text{equation (2)}$$

The starting point is (x_0, y_0) and (x, y) is a two-dimensional state of the system, when a=1.4 and b=0.3 (Mirghadri et al, 2011).

The following non-linear equations are called Lorenz equations. When he simulated weather by his computer in 1961, he noticed the high level of intensity of equations to primary conditions. He found that insignificant changes in primary parameters of weather result in different patterns:

$$\begin{cases} x = a(y - x) \\ y = cx - xz - y \\ z = xy - bz \end{cases} \qquad \text{equation (3)}$$

This function contains three control parameters all of which receive positive values. Lorenz chaos system has chaotic behavior only when its parameters values are c=28, b=8/3 and a=10.

It is clear that when we use functions with high dimensions we increase the complexity and security of the algorithm because chaotic functions with higher number of dimensions require more primary values. Consequently, key space also increases and this makes encryption algorithm resistant and stable against many deciphering attacks like runaway attacks (pourdelan, 2012).

3. Previous studies

Chaotic mapping can be used in two stages of watermarking. One of these stages is when we first encrypt the input data or text by means of chaotic maps and then embed in the image. The other use is when we embed the input text or data in the image and then we displace image pixels by chaotic maps. As it is obvious, in the

first kind ofuse, the goal is not to reduce image quality and in the second kind of use, the image completely disappears. Pourdelan (2012) proposed a rapid algorithm for image encryption by combining permutation and distribution stages. First, the image is divided into blocks of pixels. Then, the logistic chaotic function is produced by means of quasi-random numbers in order to disturb the blocks and change pixels values. Pawan N. Khadeh and Manish Narnaware (2012) used 3D map logistic map and Chebyshev map and also 2D and 3D map Arnold Cat Map for encrypting input image. Arnold Cat Map is a 2D map which is used for disturbing pixels of input image and its 3D map is used for placing R, G and B components. Chebyshev 3D map is used for producing key and logistic 3D map is used for disturbing image pixels. Use of logistic 3D map provide encryption algorithm with high security (Rasoul Enayati Far et al, 2008). Binary search tree is used for making encryption algorithm more complex, increasing encryption algorithm security and changing gray surface of every main pixel. In this method, we produce numbers 0 to 255 in a random manner by means of logistic map chaotic function and put the numbers in a binary tree. We use a key with a length equal to 80 bits for producing primary key in order to start and increase security. This method expresses appropriate stability against different attacks like decryption attacks, statistical attacks and runaway attacks. The entropy value 7.9926 in this method indicates high effectiveness of the recommended method.

Reversible watermarking can protect important digital media like medical and military images and allows for extraction of watermark and returns the Host image completely. QiaolunGu and TiegangGao (2013) introduced a reversible watermarking algorithm based upon chaos system. Chaos system is used for selecting watermark location placing randomly. Empirical results showed that dependence and sensitivity of primary values play important roles in reversible watermarking algorithm and the proposed method can establish a balance between return and powerfulness by means of chaos system. In order to implement algorithm, it is assumed that the input image X is a gray N*N gray image. First we separate C_0 image margin pixels width. Therefore, the smaller image X' is obtained with a size equal to $(N-2C_0)*(N-2C_0)$. Then, the image is divided into non-overlapping sub-blocks with sizes equal to 6*6. In order to embed the watermark, chaotic subsequence will be produced by X_0 and after 1000 times of repeat in chaos relationship.

$X_{n+1}= 4X_n(1-X_n)$ equation (4)

A 3*3 matrix is obtained by low frequency LL1 for each sub-block by sized 6*6 in X' image which has been analyzed by wavelet conversion.

The other state in watermarking method involves finding optimum points of the Host image and placing watermark image in these points. Agraval et al (2014) used evolutionary algorithm of firefly and filters to find an optimal algorithm for watermarking. Glowworm optimization algorithm was developed by Ghose and Krishnanand (2005) in order to find all optimums of a function. In this algorithm, firefly are points in search space which produce a light at a special radius considering the level of a material called luciferin which is the very efficiency. These worms move towards neighboring worms when they see more light in their neighborhood. Agraval et al emphasized on optimization of relationship between the two important parameters in watermarking i.e. invisibility and robustness and used firefly algorithm in order to find this relationship.

4. Presented method for watermark

We assume the image size to be M*N and each pixel is indicated by (x, y). therefore, all present pixels are as follows:

$A_{MN}= \{(x,y):0\leq x<M,0\leq y<N\}$

For colored images, we have three matrices with dimensions M*N and each element corresponds to a pixel of the image, Matrices are Matrix R, Matrix G and matrix B.

Watermark image is a gray image of Logo matrix.

Stages for doing the proposed method are depicted in 5 phases:

-first phase: we enter the Host image and watermark image into system. The watermark image which is in the form of stored matrix is converted into one array or vector and we call it Logo Vertex.

- second phase: Logo-vertex array is converted into binary and it is denoted as binary_logo_vertex.

- third phase: we produce enough sequence by means of one of the chaotic functions. In this stage, it must be noted that function parameters and primary values must be sent to the receiver along with watermark image size as a key.

- fourth phase: we select decimal numbers from Host image frames by means of chaotic sequence and convert it to binary form.

-fifth phase: we embed each of the bits of watermark image in low-value bit of the selected numbers in order of chaotic sequence (Seyyed Amin Seyyedi et al, 2013).

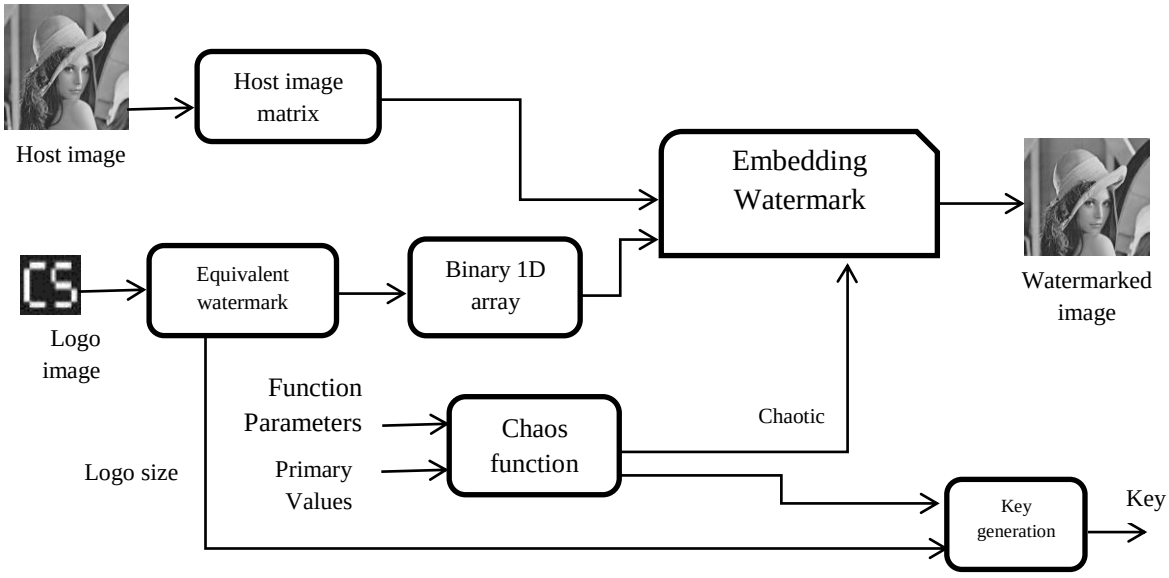


Figure 1: Flowchart of the phases of the proposed method

After doing the above phases, total watermark image is embedded into the Host image in a hidden manner.

The key is used for sending to the receiver in order to extract text from the watermarked image, primary value of the function, function parameter and rows and columns of the watermarked image.

In Henon two-dimensional function, since x and y are outputs of the function, the ordered pair (x, y) can be used for selecting image pixels in order to embed into the text. As we know, colored images have been composed of three layers: red, green and blue (R, G, B). we can use the selected ordered pair for placing watermark in each of the layers. This has been also investigated. Considering the fact that three outputs are produced in Lorenz three-dimensional function, we use x and y outputs for using in pixel embed ordered pair and we use z output for selecting one of the three layers (R, G, B) (V. Nagaraj et al, 2013).

4.1. simulation results

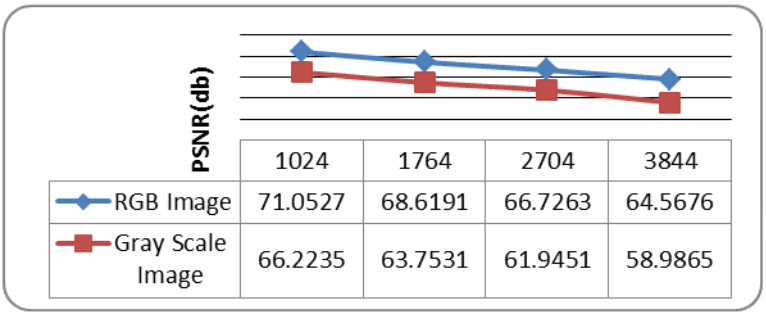
Matlab R2012b software was used for simulation. The algorithm performance on six gray images with dimensions 256*256 was evaluated. A binary image with dimensions 32*32 was also considered as watermark image. The parameters assumed for logistic function were x=0.5 and r=3.9999. the six selected images (Agraval et al, 2014) can be observed in figure 4 along with the logo. Furthermore, the images produced after implementation of the proposed watermarking algorithm can be observed in figure 5.
Results of the proposed algorithm and Agraval et al's algorithm (2014) have been listed in Table 1.

Table 1: PSNR and NC values obtained from the proposed algorithm and related works

Image	Algorithm	PSNR(db)	NC(W,W')
Baboon	CharuAgarwal et al.	50.76746	1.000
	Proposed algorithm	**66.1557**	**1.000**
Boat	CharuAgarwal et al.	51.49438	1.000
	Proposed algorithm	**66.1683**	**1.000**
Cameraman	CharuAgarwal et al.	53.65498	1.000
	Proposed algorithm	**66.2000**	**1.000**
Lena	CharuAgarwal et al.	55.7296	1.000
	Proposed algorithm	**66.1315**	**1.000**
Man	CharuAgarwal et al.	51.1733	1.000
	Proposed algorithm	**70.9947**	**1.000**
Peppers	CharuAgarwal et al.	52.15925	1.000
	Proposed algorithm	**66.1107**	**1.000**

Considering the above results, it can be concluded that transparency test value (or the very PSNR) has better values in comparison with Agraval et al's algorithm (2014). Furthermore, values between 66 and 71 are acceptable. For the case of resistance or NC test, as it can be seen the algorithm has a high resistance and the obtained value is equal to 1 just like that of Agraval et al (2014).A considerable amount of scattering has been created within the Host image due to use of a sequence for placing logo image bits which are derived from logistic chaotic function. This chaotic sequence can be produced in receiver's side only by primary values and

parameters in key which has been created by transmitter and logo image has been extracted from it. One of the strengths of the proposed algorithm is the ability to watermark on colored images as well as gray images (Qiaolun et al, 2013). Furthermore, the size of watermark image can also be increased to increase watermark capacity. Figure 2 indicates PSNR change versus an increase in the number of watermarked bits.



	1024	1764	2704	3844
RGB Image	71.0527	68.6191	66.7263	64.5676
Gray Scale Image	66.2235	63.7531	61.9451	58.9865

Figure 2: transparency versus watermark bit increase

As it would be predicted, an increase in the number of watermark bits for placing in the Host image results in a reduction in transparency of the every PSNR. Figure 2, also indicates that the proposed algorithm performance better in colored images quality maintenance than gray images. Considering the fact that the colored images are made up of three layers red, green and blue, we will have more locations for watermarking and watermarking can be conducted separately on all layers and in combinational form.

In the next sentences, we deal with four common types of attacks regarding image watermarking: Salt and Pepper noise (5%), Sharpening (aperture=0.2), Scaling, Cropping (1/8). The results can be used for measuring the criterion of the proposed algorithm resistance. Table 2 indicates the comparison of resistance criterion or the very NC (W, W') in 6 studied images using Agraval et al's algorithm (2014) and the proposed algorithm.

A comparison of the two algorithms can reveal that the proposed algorithm yields better results in attacks like Salt and pepper noise and Scaling and it is a little bit weaker in the other two stages. Bit replacement method is a little bit vulnerable to attacks like manipulation of images.

Table 2: Comparison of resistance against attacks between the proposed method and Agraval et al's algorithm (2014)

Cropping	Scaling	Sharpening	Salt and pepper Noise	algorithm	image
0.699	1	0.991	0.9991	Agarwal et al.	**Baboon**
0.6984	1	**0.9736**	**0.9941**	**Proposed algorithm**	
0.756	1	0.991	0.998	Agarwal et al.	**Boat**
0.6526	1	**0.9349**	**0.9988**	**Proposed algorithm**	
0.533	1	0.905	0.973	Agarwal et al.	**Cameraman**
0.5063	1	**0.8677**	**0.9970**	**Proposed algorithm**	
0.490	1	0.9957	0.991	Agarwal et al.	**Lena**
0.5194	1	**0.9272**	**0.9913**	**Proposed algorithm**	
0.724	1	0.9798	0.9585	Agarwal et al.	**Man**
0.924	1	**0.8598**	**0.9995**	**Proposed algorithm**	
0.758	1	0.954	0.995	Agarwal et al.	**Pepper**
0.7369	1	**0.9100**	**1.0000**	**Proposed algorithm**	

(a) (b) (c) (d)

Figure 3: Images extracted after attacks (a)Salt and pepper (b)Sharpening(c)Scaling(d)Cropping

We repeat the proposed algorithm by Henon two-dimensional function and Lorenz three-dimensional function. Since the proposed algorithm uses chaotic functions sequence for finding image watermark situation, it makes no difference which chaotic function we use and results of transparency and resistance are approximately the same. However, if we want to compare in terms of sensitivity to key and key space analysis, we had better use a large key space for preventing from attacks like runaway attack. As key space is greater, probability for defeat is lower. Moreover, considering the fact that watermark algorithm must be very sensitive to even changes in only one of the present values in the key, different attacks will be very difficult and impossible because of the presence of such long key (Zare, 2014).

In Henon two-dimensional function, key includes two input parameters a=1.4 and b=0.3 and two primary values x_0=0 and y_0=0, number of repetitions and watermark image column and row values which totally has 7 parameters.

In Lorenz's three-dimensional function, the key contains three input parameters r=28, b=8/3 and a=10 and three primary values x_0=1 and y_0=1 and z_0=20, number of repetitions and watermark image column and row value which totally makes 9 parameters.

Table 3 indicates different combinations of key using three chaotic functions with different dimensions. As it could be predicted, the number of combinations was more in Lorenz's function. Consequently, Lorenz's method will have better performance against different types of runaway in terms of resistance.

Table 3: the number of different combinations of key with different chaotic functions with different dimensions

Number of different combinations of the key	Chaotic function
2^{40}	**One-dimensional logistic**
2^{56}	**Two-dimensional Henon**
2^{72}	**Three-dimensional Lorenz**

5. Conclusion

Chaotic functions have played important roles in image watermarking for secure transfer and ownership maintenance of image. High sensitivity to key, being quasi-random and definite is advantages of chaotic functions. We used chaotic functions in the proposed algorithm for finding watermark situation. It had acceptable performance in transparency and resistance against some attacks. Furthermore, an increase in chaotic function dimension increases key size. This results in an increase in resistance against runaway attacks.

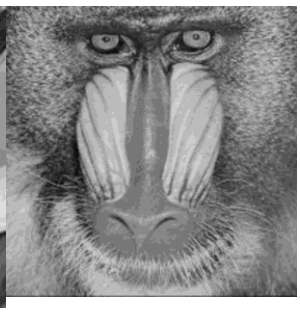
Chaotic maps are used in two stages of watermarking. One is when we first encrypt input text or data by chaotic maps and then we embed them into image and the other is when we first embed the input data or text in the image and then displace image pixels by means of chaotic map. In the recommended algorithm, however, we use chaos for finding watermark locations. This watermark algorithm is invisible, semi-fragile, symmetrical and smart. Smartness of this method helps with extracting watermark logo without having host image. This kind of watermarking can be used in ownership verification, documents verification, identification of unlicensed production device and so on.

6. Recommendations

Considering the capabilities of chaotic functions, two-dimensional and three-dimensional chaotic functions can also be used in watermarking. This results in increasing complexity and security. Furthermore, use of signal processing instead of pixel processing and bit processing of images can reveal capabilities of chaotic functions. Future studies can generalize watermark methods by chaotic functions in sound and video which is very effective in reserving ownership right.

(c)

(d)



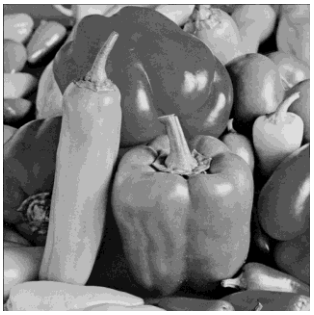
(a)

(b)

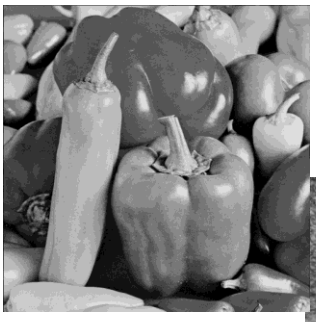
(c)

(d)

(e)



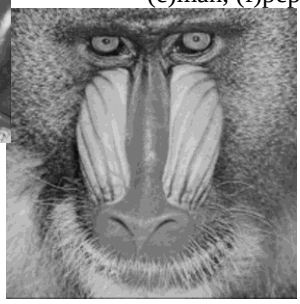
(f)



(g)

Figure 4: host images
(a)baboon, (b)boat, (c)cameraman, (d)Lena,
(e)man, (f)pepper, (g)Logo image

Figure 5: watermarked images (a)baboon, (b)boat,
(c)cameraman, (d)Lena, (e)man, (f)pepper



(a)

(b)

REFERENCES

Agarwal Charu,Mishra Anurag, Sharma Arpita,"Optimized gray-scale image watermarking using DWT-SVD and firefly Algorithm", ELSEVIER,Expert system with aplications,2014.

Asvadi, Ali Reza, "introduction of watermark methods in sound and implementation of LSB coding method in Matlab software", technical and engineering faculty of Isfahan University, 2008.

Mir Ghadri, AbdolRasul, Jolfayee, Ali Reza, " new design of image encryption by means of chaotic mapping", scientific-research journal of passive defebce sciences and technologies, second year, number 2, summer 2011: pp: 111-124.

N.K.Pareek,Vinod Patidar,K.K.Sud, "Image encryption using chaotic logistic map",ELSEVIER,Image and Vision computing 24(2006) 926-934.

Ott E.,2002,"Chaos in Dynamical Systems ",Paperback, chapter 4.

Nasab Haji, MohamamdKazem, "nuyer-seller watermark protocols", master degree thesis, shahidBeheshti University, mathematical sciences faculty, November 2010.

pourdelan, Hadi, "a novel algorithm for image encryption and decryption based on chaos", international conference on non-linear modeling and optimization, Sari Islamic Azad University, 2012.

PawanN.Khade, Manish Narnaware,"3D Chaotic functions for image encryption", IJCSI International Journal of Computer Science Issues,Vol.9,Issue 3,No 1,2012.

QiaolunGu, TiegangGao, "A novel reversible robust watermarking algorithm based on chaotic system", ELSEVIER, Digital signal processing 23(2013) 213-217.

Seyyed Amin Seyyedi,Rauf.khsadykhov, "Digital Image Steganography Concept and Evaluation", International Journal of Computer Application(0975-8887),Volume 66-No.5,2013.

V.Nagaraj,Dr.V.Vijayalakshmi,Dr.G.Zayaraz, «'Color Image Steganography based on pixel value modification method using modulus function", Elsevier,International on electronic engineering and computer science,2013.

XipingHe,QionghuaZhang,"ImageEncrypyion Based on Chaotic Modulation of Wavelet Ceofficients",IEEE Computer Society, Congress on Image and Signal Processing,2008.

Ye, Rui,"Image watermarking using chaotic watermark scrambling and perceptual quality evaluation",IETR, 2013.

Zare, Jamileh, "optimization of image encryption algorithm based upon a combination of ultra-chaotic functions and discontinuous Cosine conversion", master degree thesis, Islamic Azad University, Zanjan Branch, 2013.