A NOVEL STEGANOGRAPHY METHOD BASED ON 4 DOMINATIONS STANDARD CHAOTIC MAP IN SPATIAL DOMAIN

[1] Dr. ANWAR ABBAS HATTAB,[2] Dr. SADIQ A. MEHDI

[1] Mustansiriya University, Computer Science, Iraq

[2] Mustansiriya University, Computer Science, Iraq

E-mail: [1]Anwarabbas76@ uomustansiriyah.edu.iq, [2]sadiqmehdi71@ uomustansiriyah.edu.iq

ABSTRACT

The goal of steganography is to embed secret information in a data is considered as a cover in a way that unparticipating users can not able to discover the content of this information by estimating the data. In this paper, new method of stenography has been suggested to hide text in cover image as dynamic method in which combine cryptograph with information hiding to do high level security. In this method chaotic theory is used to choose randomly pixel in image based on initial control parameters. Some operations of number theory are used to generate keys from text's characters with these coordinates of the location of chosen pixel which are used to change these characters from the text which is stored in this location as four dominations to make diffusion and confusion in text and hide in cover image randomly. The result experiments show strongest of this method based on value of Mean Square Errors (MSE), Pack Signal to Noise Ratio (PSNR) when compared with other methods.

Keywords: *Steganography Method, Standard Chaotic Map, PSNR, MSE, Histogram.*

1. INTRODUCTION

With the rapid development of digital technology and communication media, data such as text, images, audio, video, etc. are growing importance in day to day life. A large amount of data is being transmitted over internet. There is always a threat of an intruder accessing the private information. So a mechanism needs to be implemented in order to keep the integrity and confidentiality of the information. This has led to an explosive growth in the field of information hiding. Cryptography is the most common word that is used in information hiding. Cryptography means converting the text from readable format to unreadable format. Cryptography applies encryption techniques to convert the message into non-readable form but it does not hides the message i.e., the encrypted message is visible [1]. It would be great to have something that can embed the secret message into some media in such a way that analogously stochastic and deterministic process appearing a nonlinear dynamical system [6, 7]. This theory discusses the system's behavior which follow deterministic laws, but in the same time appear unpredictable and random system which has a sensitive dependence on its basic conditions, no one can guess whether anything is hidden or not [2]. Steganography can be used for wide range of applications such as, in defense organizations for safe circulation of secret data, in military and intelligence agencies, in smart identity cards where personal details are embedded in the photograph itself for copyright control of materials [3]. In medical imaging, patient's details are embedded within image providing protection of information and reducing transmission time and cost, in online voting system so as to make the online election secure and robust against a variety of fraudulent behaviors, for data hiding in countries where cryptography is prohibited, in improving mobile banking security, in tamper proofing so as to prevent or detect unauthorized modifications and other numerous applications [4].

Edward Lorenz developed a mathematical physics which is called Chaos theory [5]; which is

if these conditions are changes (even in small way) a huge different outcomes can be made [8]. Sensitivity to basic conditions is the initial principles of chaotic theory.

If we make a little variation in the initial parameters of the task will produce to a huge variance in the manner which is produced after iterations. These dynamical system sensitivities have a fractal nature that can be applied to discover whole solutions of an equation [9]. Dependent on area of employ critical fractal to determine whole results in one way of variable-space; a way of searching global minima would be introduced in optimization-problems [10]. The using of chaotic sequence doesn't have any mathematical proofs about its benefits of using it [11]. The basic advantages of utilizing chaos theory in technique of steganography are randomness, confidentiality, non-periodicity, and easy implementation. In many fields, the using of chaotic systems is notice as an idea. If this new method is used non-linear dynamics a great number (in real systems) of implementations, each natural and man-made, are being investigated [12]. For the last years many researchers discussed and proposed methods of chaos steganography. K Ganesan et.al. [13] depending on improving algorithm which can utilize to cover messages by uitizing logic of casual number. They have focused on using LSB (least signification bit) method. In [14], 2D logistic and Arnold methods are proposed. So, the secret message is ciphered chaotically and after that covered by using 2-steganography approaches. In [15], a steganography approach is suggested to cover data randomly within an encrypted-image. It gives strong and simple method to cover the data within the cipher image. So that, decreasing the chance of the encrypted image be detected and after that enhance the encrypted images' security. In [16], in dependent on human begin visual-characteristics and chaotic mapping, a huge of steganography technique capacity is suggested and also it can cover secret-information adaptively into the picture (which is stilled). A's results of this experimental, the results appear substantial improvement in invisibility and capacity, and that is very robust for the techniques of image processing as compression of image cropping, etc. In [17] we can use the logistic map to make a sequence like the watermark. As well as the logistic map can be used to mix the bits arrange for the message in [18]. In [19], in dependent on the fractal theory; the modifying chaos optimization algorithm (COA) presented an optimization technique. In [20] a fractal image has been used by the proposed technique as the host- image and then produced a casual like sequence by chaotic method as the reference for covered locations, and uses a wavelet transform to achieve the embedding procedure. In [21] a Haar wavelet transform has been utilized to illustrate the image into differencing and averaging components. In [22] firstly the message has been covered within the hide image; and the message is ciphered by using (triple-key) of chaotic method. in [23] presents cellular automata and a hybrid model of chaotic function; by utilizing a position of N-bits mask pixel is limited in the hide image for cover one bit for secret message. In each stage logistic map and cellular automata generate the mask. In [24] a new method is presented based on chaotic steganography and cipher image in spatial domain for images.

The reminder of research is order as: steganography methods in spatial domain is explained in section 2, chaotic systems is explained in section 3, In part 4, the proposed steganography technique has been explained. The evaluation technology is explained in part 5. Tests finding are explained in part 6; conclusions are explained in part 8.

2. STEGANOGRAPHY METHODS IN SPATIAL DOMAIN

The spatial domain steganography methods point out to the ways in which the information hiding is treated immediately on the pixel values of the cover picture in a way that the effectiveness of the text is not visual on the hiding image. To treat such a hiding many methods are utilized but popular of all is they all use the immediate pixel hiding although the pixel chosen criterion varies. The popular ways utilized in spatial domain are [25]:

1. Least significant bit -LSB
2. Pixel intensity or gray level value –GLV based method
3. Texture based method `
4. Histogram based methods
5. Spread Spectrum based methods
6. Color Palette based methods
7. Pixel value differencing -PVD
8. Edges based data embedding method -EBE
9. Random pixel embedding method -RPE
10. Mapping pixel to hidden data method –PMM
11. Labeling or connectivity method

1. LSB method: It is one of the widely popular and simple methods for text covering. In this way, text is covered in the least specific bits of picture pixels. Modifying the LSB of the pixels does not cause more variations in the picture and so that the stego-image looks like to the premier image. In state of images (24-bit) 3- bits of pixel can be utilized for LSB exchange as each pixel include discrete elements for red, green and blue.

2. PIXEL INTENSITY: Method which is utilized to map information by altering the gray level of pixels in image. This method uses the idea of even and odd numbers to modify data within an image. From a resulted image a some of pixels are chosen according to an arithmetic method.

3. TEXTURE BASED: In this method the host pictures are split into bulks of particular size and each bulk in picture is picked as a texture pattern for which the extreme similar bulk is accrued between the bulks of the host picture. The hiding way is achieved on by exchange these littles bulks of the confidential image with bulks in host picture

.

4. HISTOGRAM BASED: In this method the sensitive information is hided into the histogram of image. Couples of peak pixels and zero-points are utilized to make low hiding distortion with consideration to providing low information embedding capacity.

5. SPREAD SPECTRUM: The root of this method is an expansion spectrum encoder. These unites run by modulating a tight band signal through a carrier. The frequency of carrier is transferred using a noise- generator feeded with a confidential key. To recover the hided message, the user should utilize the similar noise and key generator to tune on the demodulate and frequencies the premier signal. An accidental user can not able even to discover the embedding communication because of noise utilizing.

6. PALETTE BASED: This method is like to the used LSB method for images (24-bit) or grayscale pictures (8-bit). After the palette colors are saved by luminance, it hides the text into the LSB of indices reffering to the palette colors. Message discovery is achieved by choosing the similar pixels and collecting the LSBs of all indices to the ordered palette.

7. PVD method: user view is sensible to small modifications in the sleek parts, but can resist more sharp modifications in the brink parts. Therefore, the PVD ways have suggest promoting the hiding ability without insert clear visible changes into cover pictures. PVD, the size of hiding bits is specific by among the neighbor and its pixel. The greatest the variance quantities are the more bits of text can be hiding. Therefore, PVD method can make more imperceptible effects contrast with LSB ways with the same hiding power. While, according to experiments and analysis, we detect that PVD method achievement poor to combat some statistical-attack.

8. EDGE BASED: Edge Detection method covers secret information into the pixels that determine the brinks of the carrier picture. The confidential information can be of any kind, not indispensable text, and they are truly hided into the 3-LSBs of the pixels of the cover picture, however not in whole pixels, just in the pixels that are section of the brinks discovered by the brink detection method.

9. RANDOM PIXEL SELECTION: In this technique information is unobserved at random i.e., data is invisible in some randomly chosen pixel. Random pixel is produced by utilizing Fibonacci technique.

10. PIXEL MAPPING METHOD: The way for information hiding within the spatial-domain of a picture. Hiding pixels are chosen according to on several arithmetic functions which build on the pixel intensity amount of the kernel pixel and its 8 neighbors are chosen in counter clockwise orientation. Before hiding an examining has been accrued to detect whether the chased hiding pixels or its neighbors lies at the edge of the picture or not. Data hiding are achieved by mapping each four or two bits of the secret text in each of the neighbor pixel according to some attributes of that pixel.

11. PIXEL CONNECTIVITY: A hiding operation starts at the tops in the score image and expansion throughout the remainder of the picture according to the connectivity of the pixels. Connectivity knows that pixels are linked to other pixels.

3. CHAOTIC SYSTEMS

Chaotic system has attributes such as: initial conditions sensitivity, parameter sensitivity, state ergodicity, similar randomness and mixing, these make chaotic system are important in encryption operations [26]. These attributes can explain in following section [26]:-

1. Butterfly impact is the feature of susceptibility to premier terms; anywhere two randomly close premier terms expand with safely diverse paths.
2. Aperiodicity: It refers to, the system extends a tropic (that does not reiterate same self) and tropics are not always cyclic.
3. Ergodicity: The dynamics shows alike statistics while calculated through space or time.

That is to say the variables statistical scales hand like results in any case if they are executed through space or time

4. Topological mixing: It refers to, the method will improve in time, and thus any specific region of different usually exchanges or interferes for any other specific region.

5. Self-similarity: within space or time, the method expansion offers alike appearance at various scales of perception. According to this attribute the system is made to show auto-repetitive at various scales of perception.

The methods of chaotic are accrued by summation of twain methods named permutation and diffusion of the both operations are frequently tautened until the appropriate cipher-level is accomplished [28, 29].Thus, one of chaotic methods are utilized for security (cipher), standard map (2D) was described in [26,30], it is explained as:

$$A_{i+1}= (A_i+B_i) \bmod 2\pi$$
$$B_{i+1}=(B_i+K\sin(A_i+B_i))\mathrm{mod}2\pi \qquad (1)$$

ith various situations Ai and Bi get values in [0,2π) for whole i and K are a control factor takes a value greater than zero. The standard map method is discretized by exchanging x = aN/2π, y = bN/2π, K = kN/2π into equation (2) which maps from [0,2π) × [0,2π) to N × N. After that, the chiastic can explain as: -

$$X_{i+1}= (X_i+Y_i) \bmod N$$
$$Y_{i+1}=(Y_i+K\sin X_{i+1}N2\pi)\mathrm{modN} \qquad (2)$$

Pixel in the equation above at location (0, 0) stays in accordance with any set of rounds. Therefore, (0, 0) is represents the first (pixel) location in an ordinary examine operation, this is a failures of the permutation operation according to these method. So that the permutation operation is almost hardened by a diffusion process for preventing it, an easy method is suggested here to exchange the locations of the pixels at the ((0, 0), (N- 1,0), (0,N-1) and (N- 1, N-1)). This mean, to alteration the ordinary examine order into a random mode. After the set of rounds of these way, rx and, ry is utilized, that explains the location of a randomly chosen pixel in the cover image, which is shown in Figure (1) [30]. Thus, the chaotic method is adjusted to [29]: -

$$X_{i+1}= (X_i+rX+Y_i+rY) \bmod N,$$

$$Y_{i+1}=(Y_i+rY+K\sin_{X_{i+1}}N2\pi)\mathrm{modN} \qquad (3)$$

The adjusted equation (3) is discretized method , therefore, it is used as cipher system, key (K) has a great space, and the disruption modes depends on these factors are diverse from each one, the random couple can be produced under the parameters control. The space of key of the random-pair is 2 × N (N is width or the height) and it is hard to fracture the propagation key down known-plaintext attacks on account of utilizing the random-scan operation. That mean, the random-scan operation discomposes the place of the initial-pixel, which m accrues it hard for intruders to bring the initial cipher-pixel, and so grows the hardness of breaking the propagation key [29], and its 3D standard map expansion is showed as [26]:

$$A1\ (x, y, z) = (x+ z) \bmod N$$
$$A2(x, y, z) = (y + z + K1 \sin\frac{S_1N}{2\pi}) \bmod N \qquad (4)$$
$$A3(x, y, z) = (z+K2 \sin \frac{S_1N}{2\pi}+K3 \sin \frac{S_2N}{2\pi}) \bmod N$$

Where, K1, K2, K3 > 0.

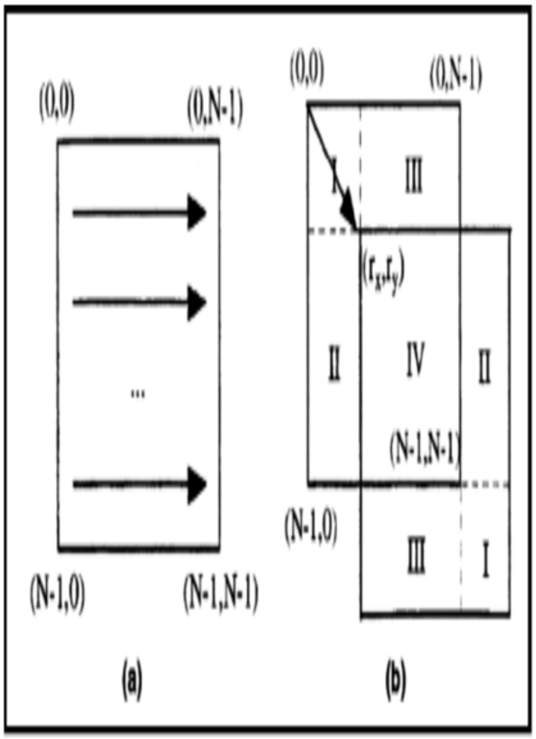

Figure 1: (A) Normal Examine Operation, (B) Random Examine Operation.

4.1 Proposed method

In this paper, text is hidden in color image in which each pixel have three channels (red, green, blue) and 4 domination standard map (4D) which is described in section (4.2) is new chaotic method is used to choose randomly pixels in color image based on initial control parameters, The coordinates of that point in the image are used as a key to change the text before storing it in randomly pixels in the cover image by using some operation in number theory as modular operation (mod). 4D is used to increase level of security of image stereography by encrypting characters of then embedded randomly in cover image. Each byte of text is embedded by using Least Signification Bit method (LSB) in pixel of cover image (3, 3, 2) order respectively. The 3 bit of text are stored in LSB in red channel , next 3 bits are stored in LSB of green channel, finally the 2 bits of text are stored in LSB of blue channel as explain in figure(2) bellow:

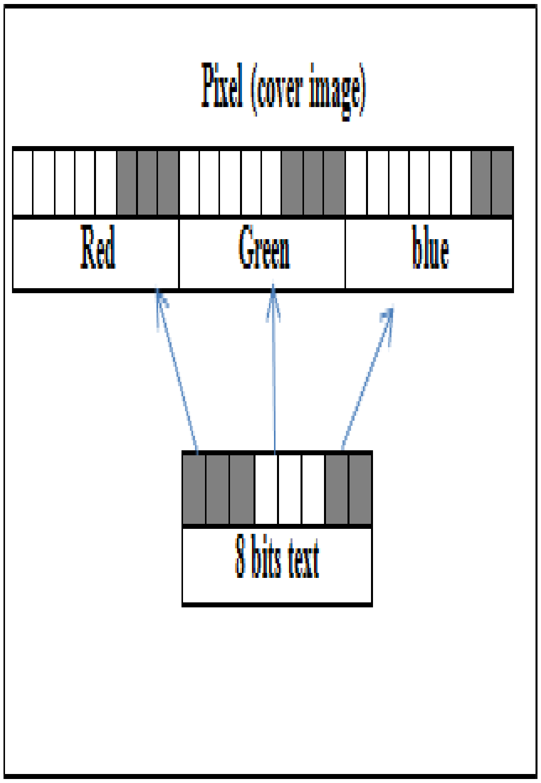

Figure 2: Byte Text (3, 3, 2) Embeds In Cover Image (Pixel)

4.2 D Standard Map Chaotic:

4D standard map which is described in [32] base on 2 domination standard map (2D) as shown in equations(3).

X_{i+1}= (x_i+rx+y_i+ry) mod N,
Y_{i+1}=$(y_i+ry+ksinx_{i+1}N2\pi)$modN (3)

Mod operation (number theory) can be defined:

Z= $h_{11} + h_{22}$ * Set (5)
h1= h_{11} + Xi + 1 (6)
h2 = h_{22} + Yi + 1 (7)

Where rx, ry and k are control parameters, Xi+1, Yi+1, h1 and h2 are four new values generate from different initial value are un-correlation statically and set any value. Figure (3) shown behavior of set iterations of 4D standard map method, figure (3.a) shown topological transitivity of 4D standard map and figure(3,b) shown dense of 4D standard map.

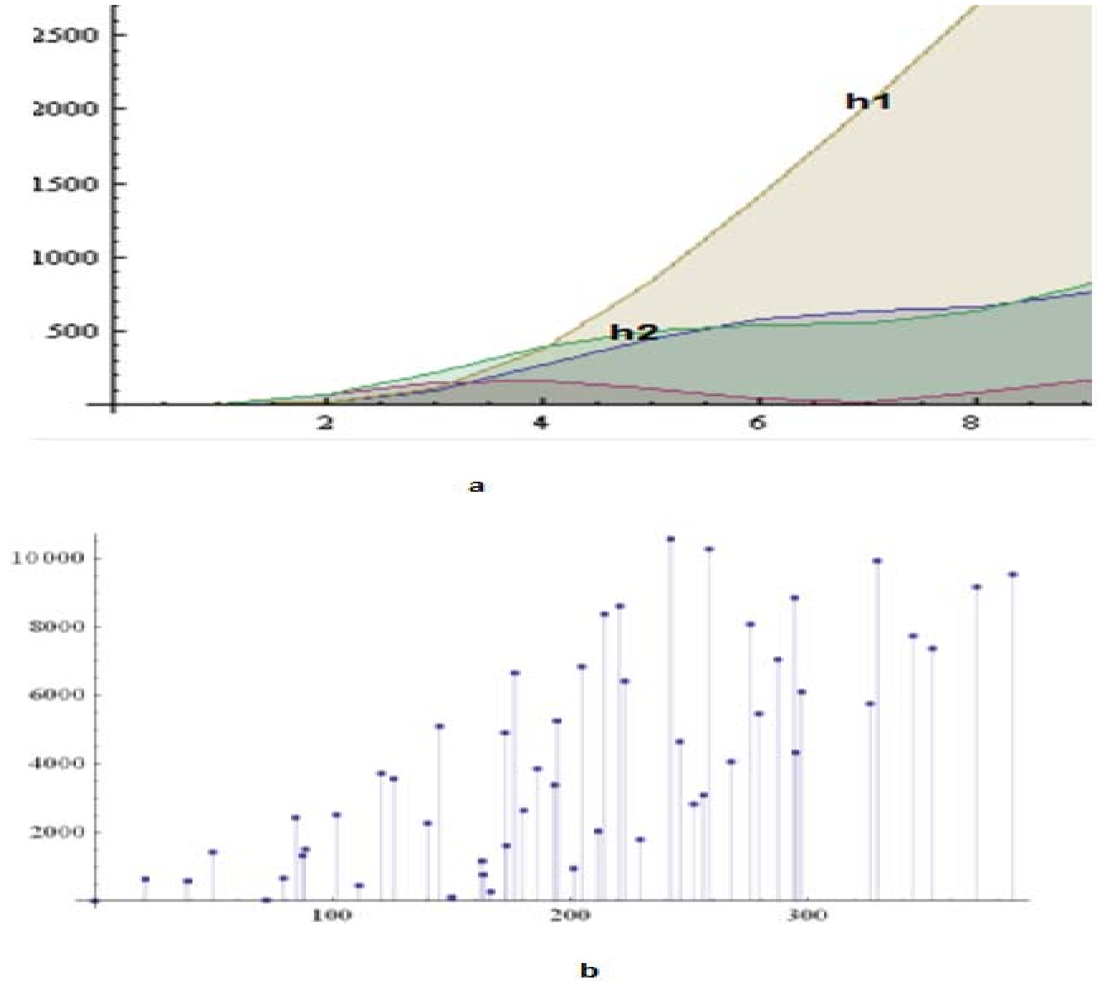

Figure 3: (a) Distributed with topological transitivity (b) 15-reiterations, 10-reiterations and 5 reiterations, four dominations standard map is dense

4.3 Novel Steganography Method:

Our steganography method is shown in figure (4), in which 4D standard map with different initial control values (rx, ry, key) is used to generate unpredicted and randomly locations(x, y) in cover image.

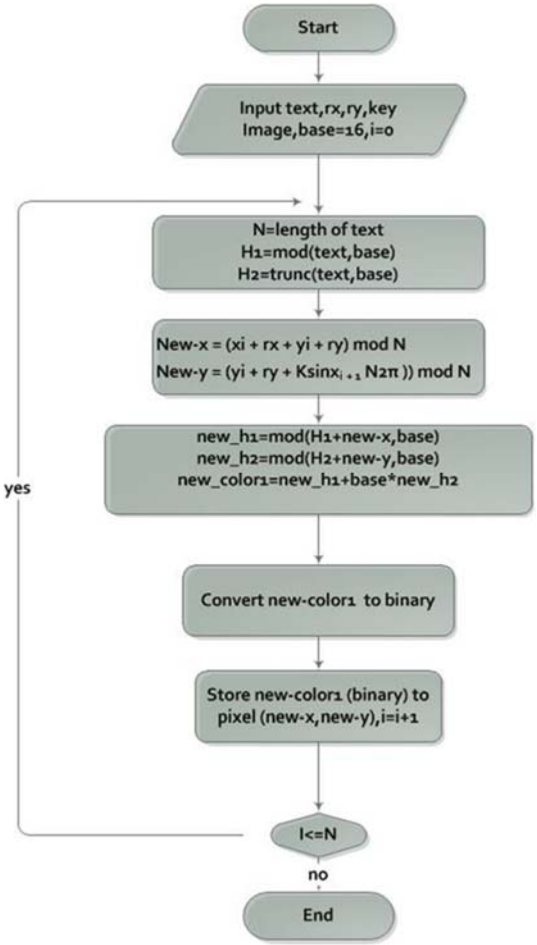
Start
Input text,rx,ry,key
Image,base=16,i=o
N=length of text
H1=mod(text,base)
H2=trunc(text,base)
New-x = (xi + rx + yi + ry) mod N
New-y = (yi + ry + Ksinx$_{i+1}$ N2π)) mod N
new_h1=mod(H1+new-x,base)
new_h2=mod(H2+new-y,base)
new_color1=new_h1+base*new_h2
Convert new-color1 to binary
Store new-color1 (binary) to
pixel (new-x,new-y),i=i+1
I<=N
yes
no
End

Figure 4: Flowchart of novel Steganography Method

Value of x and y used as keys to change character (char) from text, each char in text is 255 is the largest number represented by eight bits so to represent it by equation (2) is as follows:

EX: Z= C1 + C2 * Set

255=15+15*16

16 is used in the method as a base (base or set=16). C1 value can be produced as a result from mod operation as: C1=Z mod base; C2 value can be produced as a result from trunc operation (The number represents the product of the partition without the rest). After generate new-C1 and new-C2 by using eq (6 and 7), eq (5) is used to generate new value of text (one byte), then it will be converted to binary with store in location (x,y) in cover image. Algorithmic (1) shown novel steganography method.

convert to different value based on mod operation and it (new value) is stored in location(x, y). 8 bits in each color channel(R, G, B) are used to represent numbers from (0-255), equation (2) represent modular operation is used to generate C1 and C2.

4.4 Novel Steganography Method Algorithm(1):

Input: Text, Cover image.

Output: Text embeds in cover image.

Step1: Converting text to asci code and storing it in a one-dimensional text matrix.

Step2: Standard map is used as a first step to distribute text to particular amount to the Y-axis and X-axis by utilizing keys which produce new position (new x and y) which are utilized to store element from text array. This work is a permutation process, as shown in the following equations:

i.$Xi + 1 = (Xi + rx + Yi + ry) \bmod H$

ii.$Yi + 1 = (Yi + ry + K\sin X_{i+1} N2\pi) \bmod W$

Where xr, yr, key keys, xi and yi are coordinates of pixel in image, H and W are high and width of image.

Step3: Change the value of an element of the text matrix based on a number theory operations and use (Xi + 1, Yi + 1) as the keys to change characters of text. This represents the work of the substation. As shown in the following equations:

i. C1 = mod (p, 16) , p represent an element in text matrix
ii. C2 = trunk (p / 16) ,
iii. New-C1 = mod(C1 + Xi + 1, 16)
iv. New-C2 = mod(C2 + Yi + 1,16)

Equation (7) is used to make new colour as:

New-C = New-C1 + New-C2 * 16

New-C save in the recent position (of the output) is equal to standard map (four dimensions 4D) here it make replaces positions and the colour of the picture and colour stores in a new position as in eq (7).

Step4: Store of the new values which are generated by the step (3) in the location (xi+1, yi+1) representing the stage of hiding the data.

5. EVALUATION TECHNOLOGY

Human viewing cannot determine few differences in the images when matching a stego image and normal image. In case of putting in text into the image, the data of image will be modified a little. But there are many estimation methods which can be utilized to determine the variances between original and the stego images, these are:

5.1. Histogram

The histogram illustrates the amount of pixels in a picture at difference intensity values. Histogram displays the numbering of pixels for each grey value in the pictures [26].

5.2 Peak-Signal to Noise Ratio (PSNR)

Peak Signal to Noise Ratio (PSNR) is computed to detect the noise of the picture. Mean Squared Error (MSE) is the firstly value to be computing utilizing the equation [8]:

$$\text{MSE}=\frac{1}{\text{HXW}}\sum_{i=1}^{H}\sum_{j=1}^{W}(\,H_1(i,j)-H_2(i,j))^2 \qquad (8)$$

Let H_1 and H_2 , two pixels at the i-row with j-column of a H×W two images [33]

The PSNR is defined as [34]:

$$\text{PSNR}=10.\log10\left[\frac{255^2}{MSE^2}\right] \qquad (9)$$

If the value of MSE between two given images is small, mean these two images are having same kind. If the value of PSNR between two images is higher, mean the PSNR-value means the rebuilding is of high quality.

5.3 Mean Squared Error

The mean squared error (MSE) of an estimator which explains the rate of the squares of the "mistake". MSR can compute by using equation (8) which explained above.

6. TEST RESULTS

In this section, we will estimate our steganography technique and analyzing the other methods. The examples images are utilized for testing are shown in table (1) as below. As a section of our examinations a text of 4096 byte was embed into the images and then histogram, PSNR and MSE value were computed.

The results are match with the similar methods base embedding method without and with chaos.as 8-bits are embedded per 24-bit, so data size is 2.7 bpB. Comparing the finding it can be observed that, though data size is same as that of the other methods. However, there is refinement in PSNR and MSE values as shown in Table (2) which explain the performance evaluation of our proposed method with other methods.

Table 1: images information

No.	Cover images		
	Name	size	type
1	Baboon	256x256	Jpg
2	Lena	256x256	Jpg
3	Jet	512x256	Jpg
4	Scene	512x512	jpg

Figures (5) and (6) shown histogram comparison utilized by stego-analyst to determine the stego picture by comparing the histogram of cover picture and stego image.

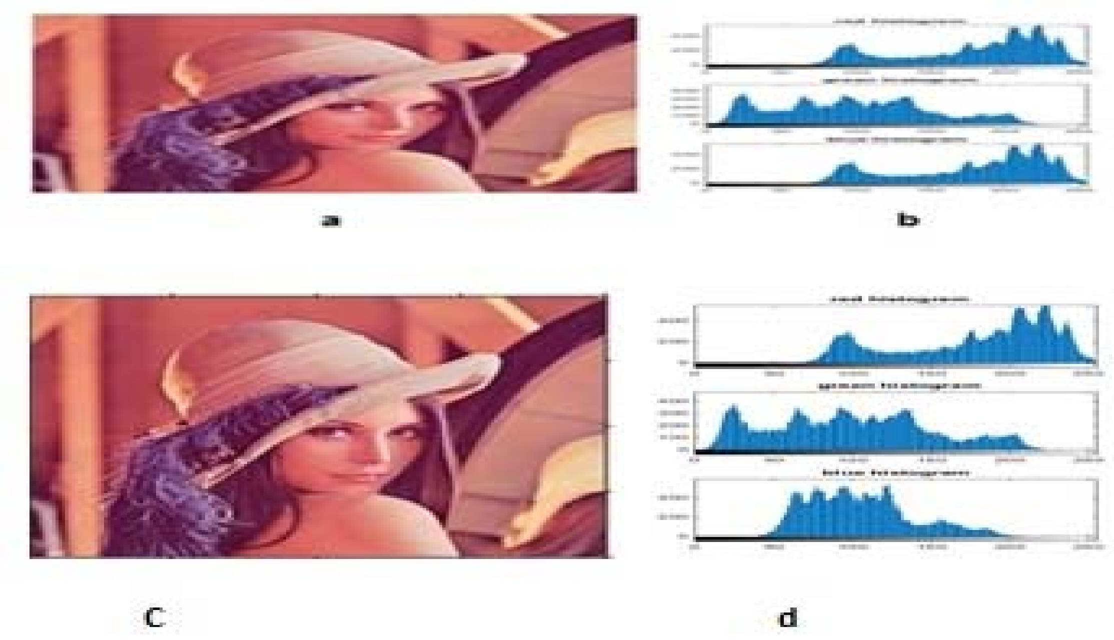

Figure 5: A. Lena Image B. Histogram Of Lena Image (R,G,B) Channels C. Lena (Stego) Image After Insert Text D. Histogram Of Lena (Stego) Image (R,G,B) Channels

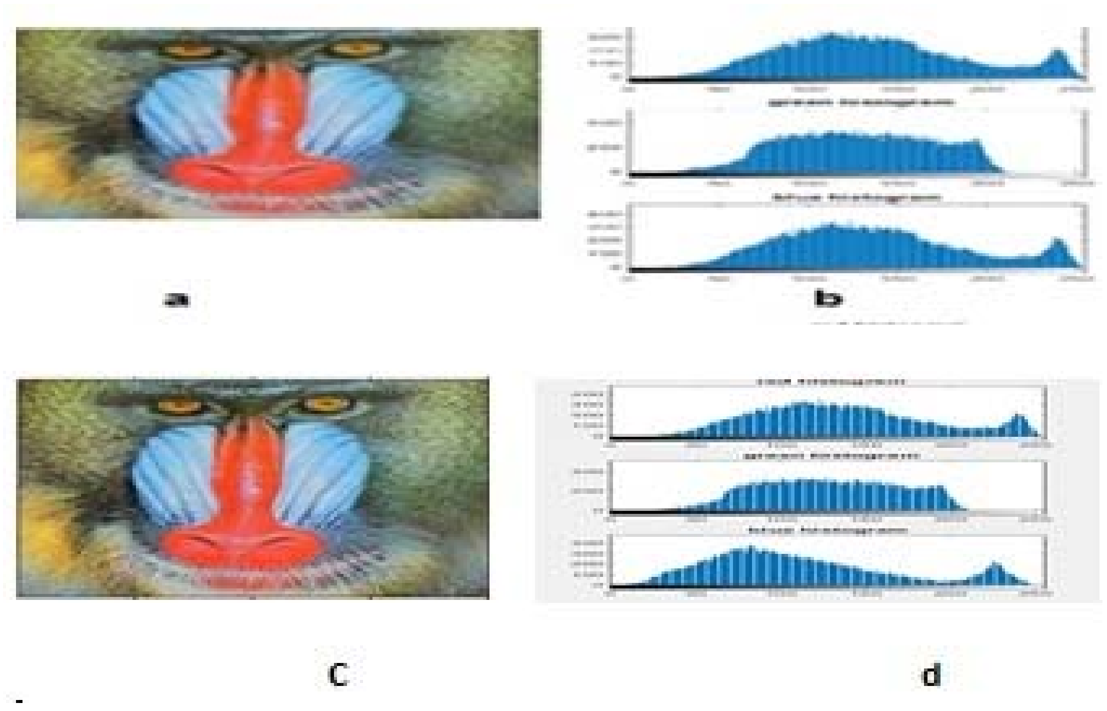

Figure 6: A. Baboon Image B. Histogram Of Baboon Image (R,G,B) Channels C. Baboon (Stego) Image After Insert Text D.Histogram Of Baboon (Stego) Image (R,G,B) Channels

Table 2: Performance Evaluation Of Our Proposed Method With Other Methods

Image name	Result using our method			Result using method(3,3,2)LSB method[24]			Result using chaotic theory (3,3,2)[24]		
	PSNR	MSE	Data size	PSNR	MSE	Data size	PSNR	MSE	Data size
Baboon	61.55	0.022	2.7	48.07	1.01	2.7	49.12	1.00	2.7
Lena	61.39	0.025	2.7	48.01	1.02	2.7	49.08	1.01	2.7
jet	59.69	0.14	2.7	50.97	0.51	2.7	56.11	0.15	2.7
scene	59.44	0.062	2.7	54.10	0.25	2.7	58.94	0.08	2.7

7. DIFFERENCE FROM PRIOR WORKS

In the previous works, we found the using of the various methods of chaotic in the process of hiding the information in the text or image either for: a. generate random numbers used to select positions randomly in text or image and those positions are used to hide information.

b. Or generate random numbers used to encrypt data before hiding it in cover (text or image) .In the sense of previous work, the using of chaotic either in locating random sites or encrypting data before hiding.

In this research, the first and second steps (a and b) are combined in one way in which we use four-dimensional chaotic method, producing four values (x, y, c1, c2) used in the process of hiding information as: x and y are used in random positioning in cover (text or image). Some operations in number theory such as modular and trunk method are used to generating c1, c2 of the same data by using x, y to generating c1, c2 Thus changing the new values of the data before hiding them in x, y. Here, four diminutions chaotic are used to select random positions and then change the data before storing them in random locations. Our method is fast, more complicated and strong to hide data without any statically errors from other previous works.

8. CONCLUSIONS AND FUTURE STUDIES:

Stenography process is utilized to cover data in to image without outraging suspiciousness to hacker. In this paper suggest, new dynamic stenography method based on chaotic method which is highly sensitive to initial values and parameters of system with some operation of number theory and some keys generated from image data. Previous works are used chaotic as: either in locating random sites or encrypting data before hiding. In our paper, four diminutions chaotic are used to select random positions and then change the data before storing. It makes high level of diffusion and confusion. In the tests were done shows strongest of this method when comparing these results with results from other methods as LSB (3, 3, and 2) method and stego with chaos. The result of our tests we find our method is strong to hide data without any statically errors.

The future work can be extended to use six dimensions or eight dimensions chaotic method to make information hiding in more complicated and strong. That makes high level of diffusion and confusion to make more secure data

ACKNOWLEDGMENTS

The authors would like to thank of Mustansiriya University, Computer Science (Iraq) for giving us the opportunity to perform and publish this research work.

REFERENCES

[1] N. Provos and P. Honeyman, "Hide and seek: An introduction to Steganography", IEEE Conference on Security and Privacy, , 2003 , pp. 32-44.

[2] Rajput A.S., Mishra N., and Sharma S., " Towards the growth of image Encryption and Authentication Schemes", International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2013.

[3] V.Sathyal, K. Balasuhramaniyam, N. Murali and M. Rajakumaran Vigneswari, "data hiding in audio signal, video signaltext and jpeg images", IEEE-International Conference on Advances in Engineering, Science and Management (ICAES), 2012.

[4] J. Fridrich and J. Kodovsky, ―Rich Models for Steganalysis of Digital Images‖,IEEE Transactions on Information Forensics and Security, Vol. 7, No. 3, 2012, pp. 868-882.

[5] E. Lorenz, "The Essence of Chaos", CRC Press, 3rd edition, ISBN 978-0295975146, 1995.

[6] Z. Liu and L. Xi, "Image information hiding encryption using chaotic sequence," in Proc. of the 11th International Conference on Knowledge-Based Intelligent Information and Engineering Systems and the XVII Itallian Workshop on Neural Networks, 2007, pp. 202-208.

[7] Y. Zhang, F. Zuo, Z. Zhai, and C. Xiaobin, "A new image encryption algorithm based on multiple chaos system", in Proc. of the International Symposium on Electronic Commerce and Security (ISECS '08), 2008, pp. 347-350.

[8] J. M. Amigo, L. Kocarev, and J. Szczepanski, "Theory and Practice of Chaotic Cryptography", in Proc. of Physics Letters A 366, 2007, pp. 211-216.

[9] V.T. Jovanovic and K. Kazerounian, "Using Chaos to Obtain Global Solutions in Computational Kinematics", in Proc. of Journal of Mechanical Design, Vol. 120, No. 2,1998, pp. 299-304.

[10] V.T. Jovanovic, and K. Kazerounian, "Optimal Design using Chaotic Descent Method", in Proc. of Journal of Mechanical Design, Vol. 123, No. 2, 2000, pp. 265-270.

[11] M. Bucolo, R. Caponetto, L. Fortuna, M. Frasca, and A. Rizzo,"Does chaos work better than noise?", in Proc. of IEEE Circuits and Systems Magazine, Vol. 29, No. 4, 2002, pp. 409-419.

[12] Bhavana. S and K. L. Sudha, "Text Steganography using LSB insertion Method Along With Chaos Theory", in Proc. of International Journal of Computer Science, Engineering and Applications (IJCSEA), Vol. 2, No. 2, 2012, pp. 145-149.

[13] K. Ganesan, B. Venkatalakshmi, and R. Krishna Moothy, "Steganography using enhanced chaotic encryption technique",

Available: http://www.niitcrcs.com/iccs/iccs2004/Papers/145%20B%20Venkatalakshmi.pdf. , 2004.

[14] K. L. Sudha, and Manjunath Prasad, "Chaos image encryption using pixel shuffling with henon map," in Proc. of Elixir Elec. Engg. 38, 2011, pp. 4492-4495.

[15] M. A. Bani and A. Jantan, "A new steganography approach for image encryption exchange by using least significant bit insertion", in Proc. of International Journal of Computer Science and Network Security(IJCSNS), Vol. 8, No. 6, 2008.

[16] P. Liu, Z. Zhu, H. Wang, and T. Yan, "A novel image steganography Using chaotic map and visual model", Available: www.atlantispress.com/php/download_paper.phpid=1452.

[17] Z. Dawei, C. Guanrong, and L. Wenbo, "A Chaos-based robust wavelet-domain watermarking algorithm", in Proc. of Chaos, Solitons and Fractals, Vol. 22, No. 1, 2004, pp. 47-54.

[18] L. Yu, Y. Zhao, R. Ni, and T. Li, "Improved Adaptive LSB Steganography Based on Chaos and Genetic Algorithm", in Proc. of EURASIP Journal on Advances in Signal Processing, Vol. 10, 2012.
pp. 1-6.

[19] M. Saleh Tavazoei and M. Haeri, "An optimization algorithm based on chaotic behavior and fractal nature", in Proc. of Journal of Computational and Applied Mathematics (206), 2007, pp. 1070-1081.

[20] Y. Wu and Joseph P. Noonan, "Image Steganography Scheme using Chaos and Fractals with the wavelet Transform", in Proc. of International Journal of Innovation, Management and Technology, Vol. 3, No. 3, 2012, pp. 285-289.

[21] N. Sethi and D. Sharma, "A novel method of image encryption using logistic mapping", in Proc. of International Journal of Computer Science Engineering (IJCSE), Vol. 1, No. 2, 2012, pp. 115-119.

[22] Arun A.S. and George M. Joseph, "High Security Cryptographic Technique uses Steganographjy and Chaotic Image Encryption", in Proc. of Journal of Computer Engineering (IOSRJCE), vol 2, 2013, pp 49-54.

[23] M. Alirezaanejad and R. Enayatifar, "Steganography by using logistic map function and cellular automata" in Proc. of Research Journal of Applied Sciences, Engineering and Technology, 2012, pp. 4991-4995.

[24] Debiprasad B., KousikD., J. K. Mandal."a Novel secure Image Steganography Method based on Chaos Theory in Spatial Domain", International Journal of Security, Privacy and Trust Management (IJSPTM) Vol 3, No 1, 2014.

[26] S. Lian, Y. Mao and Z. Wang,"3D Extensions of Some 2D Chaotic Maps and Their Usage in Data Encryption", the Fourth International Conference on Control and Automation (ICCA'03), Montreal, Canada, 2003.

[27] E. Abba Albaharany, "Image Encryption Using Substitution-Permutation Network with Chaotic Mapping", Ph. D dissertation, University of Technology, 2015.

[28] S. Ansari, N. Gupta, S. Agrawal, "A Review on Chaotic Map Based Cryptography",international Journal of Scientific Engineering and Technology, Volume No.1, 2012.

[29] K. Wong, B. Sin-Hung Kwok, and W. Shing Law, "A Fast Image Encryption Scheme based on Chaotic Standard Map", https://arxiv.org/pdf/cs/0609158v1 2006.

[30] S. Lian, J. Sun and Z. Wang, "A block cipher based on a suitable use of the chaotic standard map", Elsevier, 2004.

[31] Hanaa M. A. and Anwar A. H. ,"Formal Language Space Time Block Code for Mobile Network", diyala journal for pour sciences (DJPS), Vol: 13 No:2 , 2017, pp. 147-166.

[32] G. Hanchinamani and L. kulakarni," A Novel Approach for Image Encryption based on Parametric Mixing Chaotic System", International Journal of Computer Applications , Vol: 96– No. 11, 2014.

[33] E. Abba Albaharany, "Image Encryption Using Substitution-Permutation Network with Chaotic Mapping", Ph. D dissertation, University of Technology, 2015.

[34] J. Ahmad and F. Ahmed "Efficiency Analysis and Security Evaluation of Image Encryption Schemes", International Journal of Video & Image Processing and Network Security IJVIPNS-IJENS Vol: 12 No: 04, 2012.