International Journal of Civil Engineering and Technology (IJCIET)
Volume 9, Issue 13, December 2018, pp. 224-231, Article ID: IJCIET_09_13_025
Available online at http://www.iaeme.com/ijciet/issues.asp?JType=IJCIET&VType=9&IType=13
ISSN Print: 0976-6308 and ISSN Online: 0976-6316

© **IAEME** Publication **Scopus** Indexed

NEW METHOD FOR USING CHAOTIC MAPS TO IMAGE ENCRYPTION

Salah T. Allawi
Computer Science Dept., College of Science, Mustansiriyah University, Baghdad, Iraq

May M. Abbas
Ministry of Higher Education and Scientific Research, Legal and Administrative Directorate, Baghdad, Iraq

Reyadh Hazim Mahdi
Computer Science Dept., College of Science, Mustansiriyah University, Baghdad, Iraq

ABSTRACT

When applying the algorithms that depend upon the use of Chaotic Maps in the image encryption operation a number of advantages are provided such as high security, speed and computational power. This paper suggests a new method combines between 1D-Logistic maps and 2D Cat Mapping to encrypt the color image. This method depends upon using 1D-Logistic maps to generate random numbers to encrypt the information of image through generating three keys (R_k, G_k, B_k) one for each color (R, G, B) in the first stage. In the second stage using the 2D Cat Mapping to generate random numbers to change the position of the pixels in the image that got from previous step.

Keywords: Chaotic Map, 1D-Logistic maps, 2D Cat Mapping, Image encryption

Cite this Article: Salah T. Allawi, May M. Abbas and Reyadh Hazim Mahdi, New Method for Using Chaotic Maps to Image Encryption, International Journal of Civil Engineering and Technology, 9(13), 2018, pp. 224–231

http://www.iaeme.com/IJCIET/issues.asp?JType=IJCIET&VType=9&IType=13

1. INTRODUCTION

With the advances of science and technology, the interest in applications of the digital image has become increasing after it was a small branch. Where it has become one of the most important media used in many fields such as economics, politics, education and defense [1].Data security has become a problem of great importance. One of the methods used to protect important data when sending it through insecure channels is to hide data. Encrypting digital image data has become an important part of data hiding methods [2]. Modern

cryptography methods have been adopted on computer science as well as mathematical theory. Many cryptographic algorithms were designed to protect data from people who are not authorized to rely on computational hardness assumptions making it difficult to break these algorithms by anyone. [3].the best way to avoid traditional analysis methods based on differential cryptanalysis and statically are use diffusion and permutation.in recent times, many research on the image encryption using the chaos theory are submit. Some of these research are used multi-dimensional chaotic map for redistribution the pixel position and another methods used (1D) chaotic map for data encryption [2].

2. RELATED WORK

K. Sakthidasan and B. V. Santhosh Krishna in [4] suggested A new way to encrypt the image is based mainly on three chaotic systems (Chen or LU or Lorenz chaotic system which depends on 16-byte key). One of these methods is used to change the position of the pixels in the image. *In* the second stage used one of the same three maps to break the relationship between pixels in the image that resulted from the first stage. This method has a set of characteristics that make it resistant to attacks, giving it strength and efficiency such as (smaller iteration times, bigger key space, and high security analysis)

AbirA. In [5], a new system for encrypting a secure image is proposed. This system uses two methods of chaos. The process of encoding and decoding uses two chaotic methods to scramble the bits of image pixels and controls the shuffle process by using the PWLCM map. The perturbing orbital technique is used to confirm the dynamic statistical properties of the chaotic sequences generated. Several standard tools have been applied to determine the safety level of the proposed system as the results showed a high level of security.

Abolfazl Y. N. and Majid V. J. in [6], suggest an encryption method is composed of two stages, firstly split the color image into the essential components R, G, B, and then encrypted each component by using chaotic maps through generate a chaotic sequence, as a result of this stage get a matrix of DNA sequences through convert each component and the chaotic sequences into DNA code. Secondly, DNA array of the color image is shuffle by using the Chen's hyper chaos system. Thirdly, apply XOR operation on to the resulting DNA matrix from the previous step. Then, get three grayscale images through decoding. Finally, merge the components R, G, B to get encrypted color images.

Vivek S., Hariom C. A., and Chetan H. P. in [2], suggest a method to encryption and decryption color image depend on a chaotic system. The proposed method depend on two chaotic systems. The technique combines the traditional stream cipher technology and the spatial – domain encryption of digital images. The main advantage of using two chaotic systems is the very wide encrypting space. In addition to chaotic sequences are easy to generate and easy to control. The image encryption stage uses two chaotic sequences. in the decoding stage to restore the original images the encryption process is reversed.

3. CHAOTIC MAPPINGS

3.1. One-D Logistic maps

The 1D logistic map is one of the widely using methods, described in in Eq. 1 [6][7].

$$N_{q+1} = z * N_q(1 - N_q) \quad (1)$$

Where $z \in [0, 4]$, $N_q \in (0, 1)$, q=0, 1, 2, ... After conducting research it emerged that the method would be in a good chaotic under condition $3.56994 \leq z \leq 4$ [7].

3.2. Two-D Cat Mapping

Method 2D Cat map was submitted by V.I. Arnold in the research of ergodic theory. Suppose the coordinates of pixels position in the image are H = {(i, j) | i, j = 1, 2, 3, m}, two control parameters are used in 2D Cat map [7] is as follows:

$$i^1 = (i + p*j) \bmod (m) \quad (2)$$

$$j^1 = (q*i + (p*q+1)\, j) \bmod (m) \quad (3)$$

Where (i, j) original pixel position, (i^1, j^1) is the new position, (p, q) are positive integers represent control parameters and m x m plain-image when 2D Cat map is carried out one time to the original.

Cat map using to reordering the original image pixels position based on generating new coordinates. After several repetitions, the correlation between the contiguous image pixels becomes disjointed and the image becomes meaningless. But after repeated work several times the original image is return [7].

4. PROPOSED ALGORITHM

4.1. Encryption Stage

The outline for the proposed algorithm illustrated in Fig. 1. This stage divided into several main steps: first step includes split the entered image into original components color RGB, second step includes data encryption for each component by doing XOR operation with Special mask key, thus three mask keys (R_k, G_k, B_k) are generated by using 1D Logistic maps, so the result of this step is an encrypted image. Third step includes reordering the pixels position of the result image from the previous step through generating random numbers by using 2D Cat Mapping. Finally the result of the proposed algorithm will be an encrypted image with the rearrangement of the pixels position.

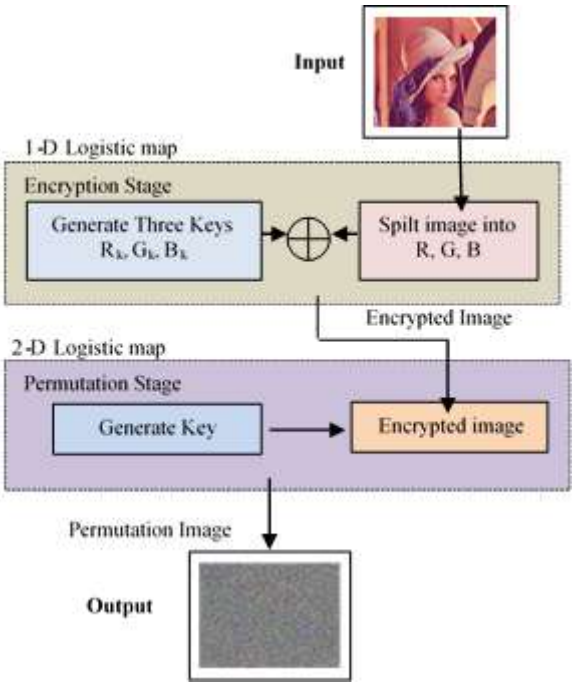

Figure 1 The general outline of Encryption Stage

The algorithm bellow illustrate the main steps of image encryption:

Step 1: Input color image (P) of size wid * hig.

Step 2: Split the input image (P) into essential components R, G, and B.

Step 3: Convert the color value for each component to 1D array (Pr, P_g, P_b)).

Step 4: Encrypt the color values of each component using 1D Logistic maps.

The following algorithm illustrates the method of encoding the R color

$R_{k\,(0)} \leftarrow 0.78916$
Sz ← hig *wid
For i ← 1 to Sz
  $R_k(i) \leftarrow 3.99995 * R_{k\,(i-1)} * (1 - R_{k\,(i-1)})$
  $R_k(i) \leftarrow (R_k(i) * 10 \wedge 14) \bmod 255$
  $C_r(i) \leftarrow R_k(i)$ XOR $P_r(i)$
End For

Where :(Sz) represents the size of the image, hig image height, wid width image,

($K_{r\,(0)}$) Initial value, (K_r) Encryption key, P_r original color value, C_r Color value after encryption. Initial values for (K_r= 0.78916, K_g =0.12345, K_b = 0.45678).

Step 5: The previous step is repeated with all three components

Step 6: Convert the color value for each component to 2D array after ending the previse step.

Step 7: Grouping color components after they are encrypted to form an encrypted image (PE).

Step 8: Change the pixels position for the encrypted image (PE) to get the image that represents the result of the implementation of the suggested method (PS).

The following algorithm illustrates the method of rearrange the pixels position.

a ← 6
b ← 8
For i ← 0 To (wid) - 1
For j ← 0 To (hig) - 1
  $i^1 \leftarrow (i + a * i) \bmod (wid)$
  $j^1 \leftarrow (b * i + (a * b + 1) * j) \bmod (hig)$
  PS (i^1, j^1) ← PE (i, j).
 End For
End For

Where :(a, b) positive integers (control parameters), (x^1, y^1) the new position, (x, y) the original position, (PE) encrypted image, (PS) final result image.

Step 9: Saving the result image (PS)

4.2. Decryption Stage

This stage include several main steps: First step includes input the stego-image, second step includes generate the same random numbers by using 2D Cat Mapping to reconstruct the original position of the pixels for the stego image, third step includes using the same initial values to generate three mask keys (K_r, K_g, K_b) by using the 1D Logistic maps to decrypted the stego image for reconstructed the original image.

The following algorithm illustrates the main steps of image decryption:

1. Input encrypted image
2. Reconstruct the original pixels position by using 2D Cat Mapping
3. Split the encrypted image into the essential components (R, G, B)
4. Convert the color value for each component to 1D array
5. Generating three keys (K_r, K_g, K_b) using the same initial values by using 1D Logistic maps.
6. Applying XOR operation between the mask keys with color value
7. Convert the color value for each component to 2D array after ending the previous step.
8. Grouping color components to reconstruct the original image
9. Save the result image.

5. PROPOSED METHODES TEST

In the suggested method, Lena image is used as the test image with size (352*288). In the image encryption stage, the 1D logistic Map method was used. In the pixel position rearranged stage, the 2D Cat Map method was used Fig. 4 shows the result of applying the proposed.

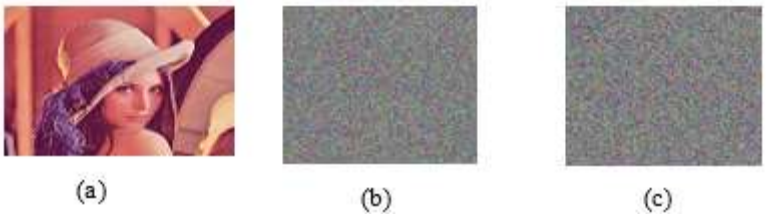

Figure 4: Result of implementing the proposed method

5.1. Histogram

Histogram used to present the statistical features for the image. After applying the proposed method, the image information histogram is uniformly shown to protect the encrypted image from statistical attacks. Fig. 5 and 6 shown the histogram of the original and stego image.

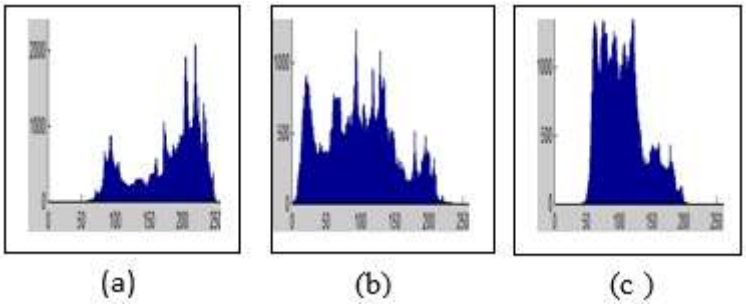

Figure 5 (a, b, c) Histogram of the essential components before encryption

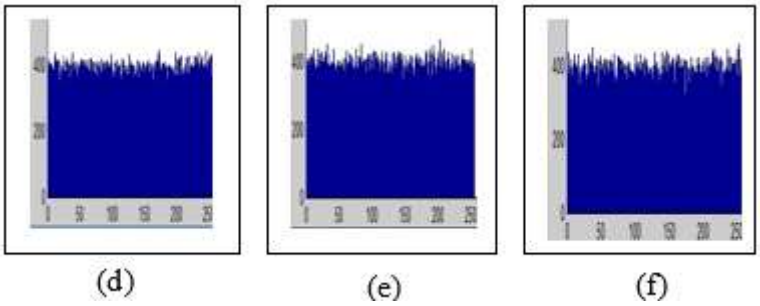

Figure 6 (d, e, f) Histogram of the essential components after encryption

5.2. NPCR & UACI

To calculate the rate of change in pixels (NPCR) between the plain and stego image pixels are used eq. 4 and 5 [8] [9]:

$$\boldsymbol{NPCR} = \frac{\sum_{i,j} \boldsymbol{D}(\boldsymbol{i},\boldsymbol{j})}{\boldsymbol{M} * \boldsymbol{N}} * \mathbf{100} \qquad (\mathbf{4})$$

$$\boldsymbol{D}(\boldsymbol{i},\boldsymbol{j}) = \begin{cases} \mathbf{0}, & \boldsymbol{if}\ \boldsymbol{C_1}(\boldsymbol{i},\boldsymbol{j}) = \boldsymbol{C_2}\,(\boldsymbol{i},\boldsymbol{j}) \\ \mathbf{1}, & \boldsymbol{if}\ \boldsymbol{C_1}(\boldsymbol{i},\boldsymbol{j}) \neq \boldsymbol{C_2}\,(\boldsymbol{i},\boldsymbol{j}) \end{cases} \qquad (\mathbf{5})$$

The rate of difference between the plain and stego image (UACI) is calculated by applying the eq.6 [9] [8]

$$\boldsymbol{UACI} = \sum \frac{|\boldsymbol{C_1}(\boldsymbol{i},\boldsymbol{j}) - \boldsymbol{C_2}(\boldsymbol{i},\boldsymbol{j})|}{\mathbf{255}} * \mathbf{100} \qquad (\mathbf{6})$$

Table (1) shows a comparison between the rate of difference of (NPCR) of the suggested way and other ways

TABLE 1 Showing the difference of NPCR

Encryption Method	NPCR
Proposed Method	99.77
Abir Awad et. al.[5]	99.62
Khaled L. et. al. [10]	99.58
T. Sivakumar et. al. [11]	99.54
Musheer A. et. al [12]	99.59

Table (2) shows a comparison between the rate of difference of (UACI) of the suggested way and other ways

TABLE 2 Showing the difference of UACI

Encryption Method	UACI
Proposed Method	30.66
Abir Awad et. al.[5]	29.99
Khaled L. et. al. [10]	28.62
T. Sivakumar et. al. [11]	28.80
Musheer A. et. al [12]	33.45

5.3. Entropy

Use the entropy to calculate the level of uncertainties in the system, the eq. 20 used to calculate the entropy value [8].

$$\boldsymbol{H(p) = -\sum_{i=0}^{255} q(p_i)\ log_2\ q\,(p_i)} \qquad (7)$$

Where: q (p_i) the probability of (pi), and the entropy is described by bits. The entropy value of the encrypted image is better as you get closer to the number 8. Table (3) shows a comparison between the value of entropy for the suggested way and other ways.

TABLE 3 Showing the difference of Entropy value

Encryption Method	Entropy
Proposed Method	7.998
Abir Awad et. al.[5]	7.999
Khaled L. et. al. [10]	7.996
T. Sivakumar et. al. [11]	7.992
Musheer A. et. al [12]	7.997

6. CONCLUSION

A new method for color Image encryption and decryption depending on chaotic maps presented in this paper. This method consists from two levels, encryption the image by using 1D logistic maps in the first stage and then rearrange the pixels position in the second level by using 2D cat mapping. The experience of the suggested way has shown several advantages: this way consists of several levels to make security more, provide an encrypted image with a low level correlation between the pixels, high degree of entropy and a histogram has distributed uniform.

ACKNOWLEDGMENT

The author's wild like to thank Mustansiriyah University (www.uomustansiriyah.edu.iq) Baghdad-Iraq for the support in the prevent work.

REFERENCES

[1] Jian Z.g, DongXin F., and Honge R. "Image Encryption Algorithm Based on DNA Encoding and Chaotic Maps ",Hindawi Publishing Corporation, Mathematical Problems in Engineering, Volume 2014, Article ID 917147, 10 pages.

[2] Dr. Vivek S., Hariom C. A., Chetan H. P. "An Image Encryption and Decryption Techniques Using Two Chaotic Schemes ",International Journal of Research in Advent Technology, Vol.2, No.2, February 2014.

[3] Nitin K.[1], Deepika[2], Divya W.[3] "Review on Different Chaotic Based Image Encryption Techniques", International Journal of Information and Computation Technology. ISSN 0974-2239 Volume 4, Number 2 (2014), pp. 197-206.

[4] K. Sakthidasan S., B. V. Santhosh K. "A New Chaotic Algorithm for Image Encryption and Decryption of Digital Color Images ", International Journal of Information and Education Technology, Vol. 1, No. 2, June 2011.

[5] AbirAwad "A New Chaotic Image Encryption Algorithm using a New Way of Permutation Methods "IAENG International Journal of Computer Science, November 2010

[6] Abolfazl Y. N., Reza M. Hei Hei, Majid V. J. "A RGB image encryption algorithm based on DNA sequence operation and hyper-chaotic system " , Conference Paper · October 2015.

[7] Musheer A., M. S. Alam "A New Algorithm of Encryption and Decryption of Images Using Chaotic Mapping ", International Journal on Computer Science and Engineering, Vol.2 (1), 2009, 46-50.

[8] Mohamed E., Ismail A., Abderrahim S. and Ali M. "A new color image encryption algorithm based on iterative mixing of color channels and chaos ",Advances in Science, Technology and Engineering Systems Journal Vol. 2, No. 5, 94-99 (2017).

[9] Himan K. · Mohammad E., Shahram E. B. "Image Encryption Using Random Bit Sequence Based on Chaotic Maps ", Arab J Sci Eng (2014) 39:1039–1047.

[10] Khaled Loukhaoukha, Jean-Yves Chouinard, and Abdellah Berdai, "A secure image encryption algorithm based on Rubik's cube principle", *Journal of Electrical and Computer Engineering*, Vol. 20, No. 12, pp1-13, 2011.

[11] T. Sivakumar, R. Venkatesan "Image Encryption Based on Pixel Shuffling and Random Key Stream ", International Journal of Computer and Information Technology. Volume 03, Issue 06, November 2014.

[12] Musheer Ahmad "Security Improvement of an Image Encryption Based on mPixel-Chaotic-Shuffle and Pixel-Chaotic-Diffusion " , European Journal of Scientific Research, ISSN 1450-216X ,(2013),