DOI: 10.24996/ijs.2018.59.1A.19

ISSN: 0067-2904

An Improve Image Encryption Algorithm Based on Multi-level of Chaotic Maps and Lagrange Interpolation

Salam Abdulnabi Thajeel*[1], Mohammed Sabbih Hamoud Al- Tamimi[2]
[1]Department of Computer Science, College of Education, University of Al-Mustansiriyah, Baghdad, Iraq.
[2] Department of Computer Science, College of Science, University of Baghdad, Baghdad, Iraq.

Abstract

Currently no one can deny the importance of data protection, especially with the proliferation of hackers and theft of personal information in all parts of the world .for these reasons the encryption has become one of the important fields in the protection of digital information.

This paper adopts a new image encryption method to overcome the obstacles to previous image encryption methods, where our method will be used Duffing map to shuffled all image pixels ,after that the resulting image will be divided into a group of blocks for perform the shuffling process via Cross Chaotic Map.

Finally, an image called key image was created by using Quadratic number spirals which will be used to generate numbers of polynomial equations via Lagrange interpolation to perform pixel diffusion.Simulations have been accomplished in order to evaluate the effectiveness of suggested technique, the Experimental results demonstrate that the proposed method can supply sufficient security for the confidentiality of images.

Keywords: Image Encryption, Chaotic Map, Duffing map, Cross Chaotic Map Lagrange Interpolation.

تحسين خوارزمية تشفير الصور اعتمادا على دوال فوضوية متعددة المستويات واستيفاء لاكرانج

سلام عبدالنبي ثجيل*[1]، محمد صبيح حمود التميمي[2]
[1]قسم علوم الحاسبات، كلية التربية، الجامعة المستنصرية، بغداد، العراق
[2]قسم علوم الحاسوب، كلية العلوم، جامعة بغداد، بغداد، العراق

الخلاصة

حاليا لا يمكن لأحد أن ينكر أهمية حماية البيانات، وخاصة مع انتشار القراصنة وسراق المعلومات الشخصية في جميع أنحاء العالم .لهذه الأسباب أصبح التشفير واحدة من المجالات الهامة في حماية المعلومات الرقمية.في هذا البحث اقترحنا طريقة جديدة لتشفير الصور الرقمية للتغلب عل المشاكل الموجودة بالطرق السابقة ، حيث تم استخدام طريقة Duffing map لغرض تغيير مواقع جميع بكسلات الصورة وبعد ذلك سيتم تقسيم الصورة الناتجة إلى مجموعة من الكتل لغرض تنفيذ عملية اعادة نشر لهذة الكتل (shuffling) . أخيرا سيتم استخدامQuadratic number spirals لغرض توليد صورة سميت بالصورة

*Email: [1]sath72@gmail.com

المفتاحية و التي تم استخدامها لتوليد عدد من المعادلات متعدد الحدود بواسطة الاستيفاء لاغرانج
Lagrange interpolation حيث تم استخدام هذه المعادلات بتغيير قيم نقاط الصورة المبعثرة . تم تنفيذ
النظام المقترح واثبتت النتائج العملية بان النظام المقترح يوفر حماية كافية وموثوقية للصور.

1. Introduction

Currently in the digital age, where the technology in both of the communication networks and digital image processing were evolving rapidly and continuously.as we known the digital image is one of the most significant means of transmitting large amounts of information [1] . This has increased the amount of encryption images whether private or public, which are transmission over the Internet. Nonetheless, because the network its open environment and the network data is easy to sharing, for these reasons, the problems concerning of the unauthorized access became a public threat in our time[2]. As a result, Digital image security has now attracted more and extra attentiveness, therefore in order to overcome the problem of digital image protection, different techniques have been proposed such as steganography and cryptography[3].

In the recent decades it can be consider image encryption as a hot research area[1], where a numerous schemes of digital image encryption have been proposed based on different principles such as such as quantum chaotic map, scan pattern ,quantitative cryptanalysis, linear hyperbolic chaotic ,a linear quad tree compression , etc. [4-7]. all of image encryption schemes can be essentially categorized into three different types which are: pixels value conversion, permutation of pixel position and finally integration of them [8].

Presently, researchers have been increasingly emphases on the image encryption based on is chaotic encryption such as hyper-chaotic systems, chaotic nonlinear adaptive filtered, Etc. [8, 9] Commonly, the chaotic system have fast with minimal costs, making it better than most traditional methods which are used to encrypt digital images[6]. In the subsequent paragraphs, will provide a brief explanation of some significant improvements that have been occurs on image encryption methods using chaotic system.

For the first time in 1989, Matthew[10] introduced a new encryption algorithm based on a logistic map. Then Fridrich followed him in 1998, proposed for the first time a new architecture for chaotic image encryption which are consisting of two stage namely a permutation- diffusion .where in the a permutation stage all image pixels are moved to new locations utilizing 2D chaotic map ,while 1D chaotic map has been used to alter the values of image pixels in diffusion stage[11].

As well. Guan et al.(2005) has been used the same technique, but applied 3D Arnolad's catmap and Chen chaos system to carry out simultaneously both of the permutation and diffusion [12] . After that, Pareek et al., (2006) suggested a new method based on two logistic map ,Which has been used with 80-bit key .in this method 8 various kinds of operations utilized to accomplish the encryption process that carry out on each pixel[13]. In [14] method of image encryption was introduced depending on multi-chaotic functions, where Logistic map with Rossler attractor has been utilized to generate the key which has been used for a purpose of perform permutation the all image pixels (where alteration has been done to the position and value of the pixels). this paper , suggested a new image encryption method to overcome the obstacles to previous image encryption methods, where the proposed method will be used Duffing map to shuffled all image pixels ,after that the resulting image will be divided into a group of blocks for perform the shuffling process via Cross Chaotic Map. Finally an image called key image will be created by using Quadratic number spirals that will be used to generate numbers of polynomial equations via Lagrange interpolation to perform pixel diffusion.

The reset of this paper is organized as follows. In section 2, present an overview which include: Duffing Map Based, Cross Chaotic Map, Quadratic number spirals and Lagrange interpolation Section 3 is devoted to a detailed description of the proposed scheme. In Sections 5 provide a thorough security and statistical analysis of the proposed scheme followed by comparison with existing works in Section 6. Finally, we end the paper with some concluding remarks.

2. Preliminaries Works

In this section, four main subjects (which are Duffing Map, Cross Chaotic Map, Quadratic number spirals technique and Lagrange Interpolation Method) will be explained in detail to clarify the concept of using each one of them.

2.1 DUFFING MAP BASED PIXEL PERMUTATION

Essentially, Duffing map (which are as well is called sometimes as Holmes Map) is a one of the kinds of chaotic map which show chaotic demeanor ,and across time domain it is discrete and has a dynamic impression[15]. essentially , when take any certain pixel coordinates such as (x_m, y_m) and then has been passed it as an input to the Duffing map,so this will lead to generates a new pixel coordinates(x_{m+1}, y_{m+1}) this is perform by the following equations[15] :

$$x_{m+1} = y_m \quad (1)$$

$$y_{m+1} = -ax_m + by_m - y_m^3 \quad (2)$$

Where a and b are constant and on which the map depends, these constants are normally set to 0.2 and 2.75 respectively in order to make the map have a chaotic behavior. According to[16] ,the Duffing map is preferable to acquire shuffled pixels as well as easy to implement In addition to reflectivity in nature ,for these reasons we adopted it to used it in image block shuffling.

2.2 Cross Chaotic Map

At present in order to reduce the multiple calculations that lead to time complexity and ameliorate the security. Wang, Ye et al. [17] was invent new variant of chaotic maps called cross chaotic map ,where two types of chaotic maps used which one dimensional and non-linear dynamic systems (Logistic, and Chebyshev) has been merged this lead to fulfilled superior level of security via utilizing the eventual map which was in two dimensions. The formula of Cross chaotic map that has been constructed is defined by the following equations

$$x_{i+1} = 1 - \mu y_i^2 \quad (3)$$

$$y_{i+1} = \csc(k . \cos^{-1} x_i) \quad (4)$$

Where μ and k indicate to the control parameters of the Cross Chaotic Map system, the system give a great and diversity of the dynamics attitude When μ =2 and k =6 . while x and y represent the initial pixel that has been selected randomly .

2.3 Quadratic number spirals Technique

Presently many researchers adopted to use different techniques for selecting the initial seeds to utilize it in various image encryption methods. For example [18, 19] proposed a novel strategy for selecting the initial seeds automatically based on the Sunflower spiral points. This created the positions of a large number of seeds based on specified radius (r) and total number of seeds (R). Predominantly, Spirals can be categorized via the mathematical rapport between both of angle and radius length .in this paper we proposed to use Quadratic number spirals in order to create another types of spiral[20].

A quadratic spiral [20]likewise the basic spiral with simple difference, where it use the quadratic polynomials to draw spiral that make it appropriate for propose encryption method (Lagrange interpolation). Mathematically we can create Quadratic number spirals via the following equations[20].:

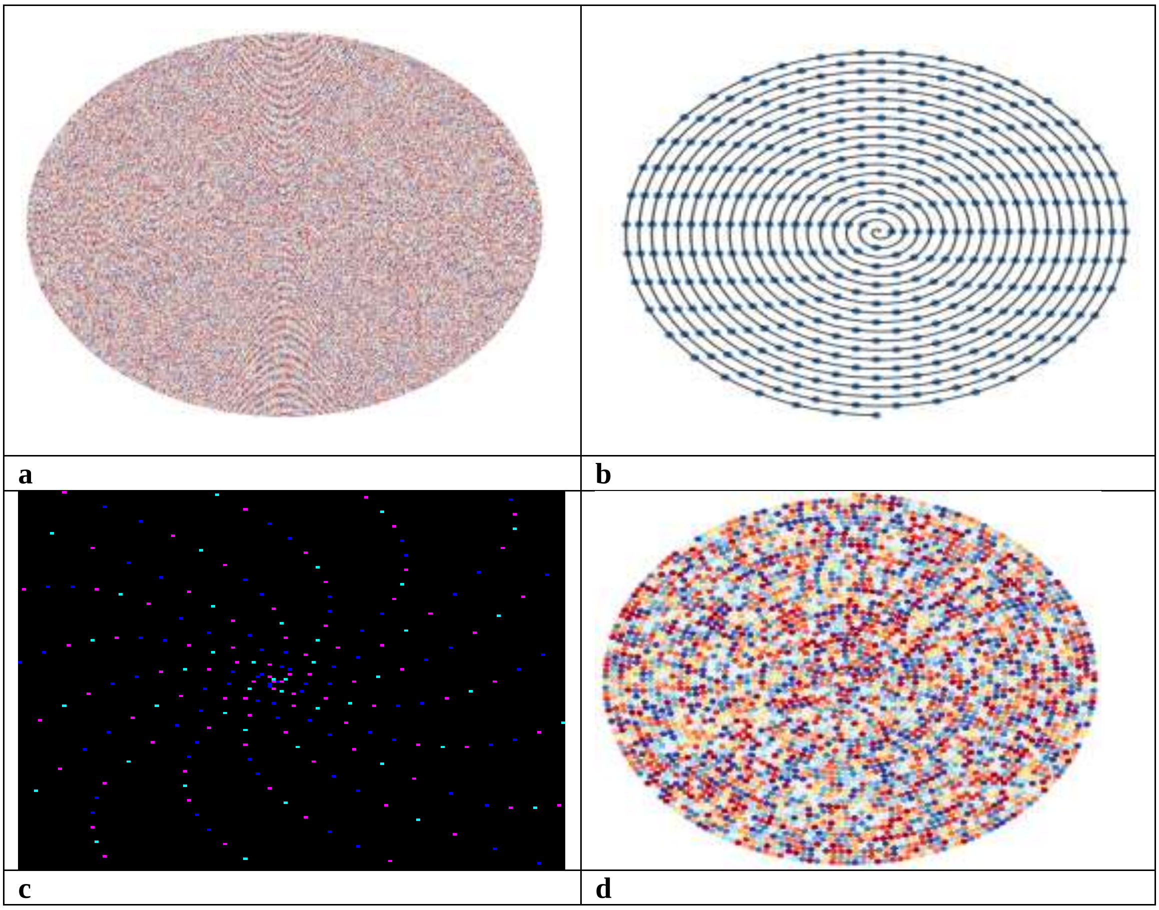
$$\mathrm{x} = \mathrm{r_n} \cos(\mathrm{a_n}) \quad (5)$$

$$\mathrm{y} = \mathrm{r_n} \sin(\mathrm{a_n}) \quad (6)$$

$$\mathrm{r_n} = \sqrt{\mathrm{n}} \quad (7)$$

$$\mathrm{a_n} = 2\pi\sqrt{\mathrm{n}} \quad (8)$$

Where n indicate the number of iterations which represent the numbers of points in spirals. It is worth mentioning that the following strategy has been proposed to make squared square loops have multi-color by taking the initial point's color which has previously chosen in Confusion stage. Next, by rising up the intensity value of pixel color with each iteration. Figure-1(part a), shows example of Quadratic number spirals which have about 275625 points. It's is so clear that this Figure does not match to a spiral, however it clearly shows the spiral (part b) when make linking for all these dots. For the sake of simplification only, it will be used the color sequence consisting of only five colors which are: blue, green, cyan, red, and magenta (part c), while part d represent a section for enlarged portion of the shape in part a. This paper suggested to use the shape in part (a) in order to generate a numbers of polynomial equations via Lagrange interpolation which will then be used as a suggested method for implementing pixel diffusion.



a　b　c　d

Figure 1- Quadratic spirals architecture (a) General view (b) spirals points(c) spiral at the initial stages (d) enlarged clip of part a[20].

2.4. Lagrange Interpolation Method

Many of the cases that are facing in practice required to guess the value of the unknown values in the light of information for a variety of information. The process of guessing this is called interpolation and extrapolation. There are many methods used in order to guessing interpolations ,one of them is Lagrange polynomial method[21].

In many issues of interpolation and extrapolation, we have a set of tandem values for two variables and there is a mathematical model that describes in the general form the relationship between these two variables, and is usually this model in the form of a function to one of the two variables and is based on some unknown constants, in Lagrange the formula as the following form [21]

$$f(X) = \sum_{j=0}^{n} f(x_j) \prod_{\substack{i=0 \\ i \neq j}}^{n} \frac{(x^* - x_i}{(x_j - x_i)} \qquad (9)$$

If the required guess the value of the function in the new points, first, it must find the values of the constants in the mathematical model that selected in order to obtain the mathematical relation between the two variables in the full form[22] .

In this research, we used the Lagrange polynomial (equation 9). To estimate the new values of the image encrypted. So we will take the values of the first five pixels from the first column in the key image (part a in Figure-1) that will represent x value, while y value represent the color values of corresponding pixels in the second column. Using the Lagrange polynomial can be obtained optimal functions that can be used to guess the value of y by giving x value. So, if we have the following value

X	0	3	6	8
Y	40	7	163	243

We can obtain the Lagrange's polynomial as following

$$f(x) = f(x_0)\frac{(x-x_1)(x-x_2)(x-x_3)}{(x_0-x_1)(x_0-x_2)(x_0-x_3)} + f(x_1)\frac{(x-x_0)(x-x_2)(x-x_3)}{(x_1-x_0)(x_1-x_2)(x_1-x_3)}$$
$$+ f(x_2)\frac{(x-x_0)(x-x_1)(x-x_3)}{(x_2-x_0)(x_2-x_1)(x_2-x_3)} + f(x_3)\frac{(x-x_0)(x-x_2)(x-x_2)}{(x_3-x_0)(x_3-x_1)(x_3-x_2)}$$
$$f(x) = 40\frac{(x-3)(x-6)(x-7)}{(0-3)(0-6)(0-7)} + 7\frac{(x-0)(x-6)(x-7)}{(3-0)(3-6)(3-7)} + 136\frac{(x-0)(x-3)(x-7)}{(6-0)(6-3)(6-7)}$$
$$+ 243\frac{(x-0)(x-3)(x-6)}{(7-0)(7-3)(7-6)}$$

Where n represents the number of values are given for x, or y. After the implementation of the equations above on the values that we have (this represents the color values for the image key) will get on the optimal function for these values as show in equation10

$$f(x) = x^3 - 20x + 40 \tag{10}$$

Finally ; will be have the number of equations represents the relations between all the color values of key- image(part a in Figure-1) Which will be used for image encryption purposes as will be explained in the encryption algorithm

3. Image Encryption

The proposed method of image encryption consists of two main phases confusion and diffusion as show in Figure-2 .where ,the first phase aims to disarrange the correlation amongst the neighboring pixels that will performed via implement both of Duffing and Cross chaotic map on the pixels and blocks of original image. While in the second stage, a new technique is implemented to encrypt the shuffled image using Lagrange Interpolation. At the beginning, a pixel will be randomly selected where the pixel position will be used as a key in Confusion stage (for Duffing & Cross chaotic map), while the pixel position and color value will be used for generate Key-image using Quadratic number spirals.

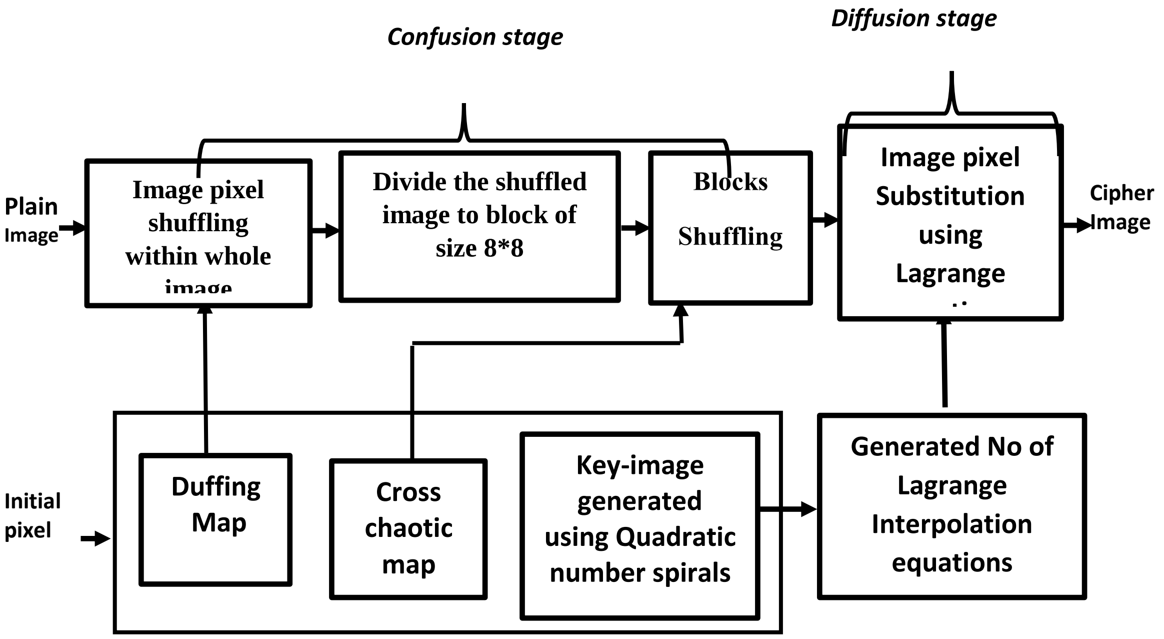

Confusion stage
Diffusion stage
Plain Image
Image pixel shuffling within whole image
Divide the shuffled image to block of size 8*8
Blocks Shuffling
Image pixel Substitution using Lagrange
Cipher Image
Initial pixel
Duffing Map
Cross chaotic map
Key-image generated using Quadratic number spirals
Generated No of Lagrange Interpolation equations

Figure 2-General Diagram of the Proposed Encryption Scheme.

3.1 Confusion stage

Depending on the knowledge of the principles of digital images, the digital image is formed based on the strength of the correlation among the neighboring pixels. Therefore, it is best to demolished correlation among pixel for get secrecy and security. In theory, when the pixels correlation become close to zero this will lead to image appear closer to a noise[7]. For this reason this stage aims to demolish correlation among pixel through Crush the position of the pixels over the whole image without altering its values. Here in confusion phase we employed two level of shuffling to boost the level of randomness and security as in the following steps:

Step1: The pixels in the whole image are shuffled using Duffing map.

Step2: then, the resulting image will be divided into 8x8 sized blocks

Step3: All the 8x8 blocks within an image are shuffled using Cross chaotic map.

3.2 Diffusion stage

The image histogram remains unchanged even after the Permutation has been performed on the image pixels. Therefore, it is best to be implemented alteration process also on the value of image pixels .Accordingly, It is suggested to implement the process of changing the values of the image pixels here using a new method based on the equations generated via Lagrange interpolation (which have been explained previously in section 2.4).

The Lagrange interpolation equations which has previously calculated will be used to get the new values of image pixels (encrypted image).This step will be performed by offsetting the value of the pixel in the plain image instead of the x value in the right-hand side of each Lagrange Interpolation equation (For example equation 10) .then the Y value in the left side of the equation which have been obtained from the compensation process will be represent the encrypted pixel value of the ciphering image .

As mentioned earlier, each equation will represent 5 pairs of opposite pixels which has been take from the key-image. Therefore, the number of equations will be less than the number of plain image pixels .For this reason, it will encrypt the first pixel of the plain image by the first equation and then via the second equation will be encrypt the second pixel and so on This process is performed using the aforementioned equations until all image values are encrypted

4. Decryption

The same steps implemented in encryption process will be performed in decryption phase, but in the reverse order, where all the keys are plugged into receiver. Then in the same way as encryption process, will be again generate the key-image to use it to generate the Lagrange equations.

These equations are used as in diffusion stage with a slight difference by put the pixel values of the cipher image in the right side of the equation (for example equation 10) to find the value of X through the implementation of the inverse lagrange interpolation equation. Finally implement the reverse the shuffling for both the blocks and pixels using the Cross chaotic map and Duffing map respectively to retrieve the source image. Figure-3 shows the implementation of decryption process

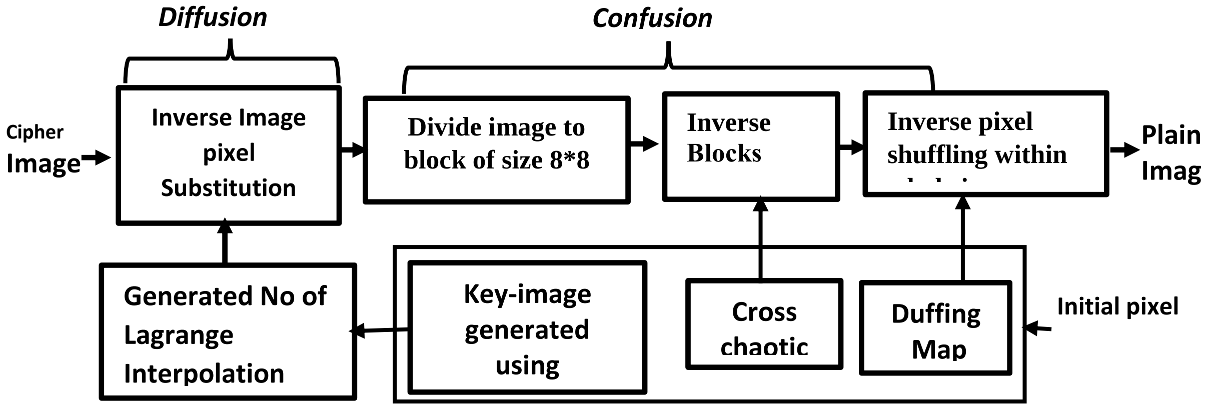

Diffusion
Confusion
Cipher
Image
Inverse Image pixel Substitution
Divide image to block of size 8*8
Inverse Blocks
Inverse pixel shuffling within
Plain Imag
Generated No of Lagrange Interpolation
Key-image generated using
Cross chaotic
Duffing Map
Initial pixel

Figure 3-General Diagram of the Proposed Decryption Process.

5. EXPERIMENTAL ANALYSIS

In this paper to evaluate the performances of our encryption method, the eight traditional images obtained from standard USC-SIPI Image Database[23] are encrypted by the proposed image encryption method. Accordingly, various measures such as, Statistical Analysis, sensibility analysis (Differential Attack), key space analysis and randomness tests were used in order to analyze the security efficiency of the proposed image encryption method.

5.1 Statistical analysis

As we know, a good encryption method must be strong versus any statistical attack[13]. For this reason, here we will conduct statistical analysis of the proposed scheme.in this experimental various measures such as Histogram analysis, entropy, correlation coefficient, Peak Signal to Noise Ratio (PSNR) were used to analyze the proposed image encryption method. Figure-4 shows the Histograms of red, green and blue channel of two image samples for the original and encrypted images Lena and Peppers) respectively.

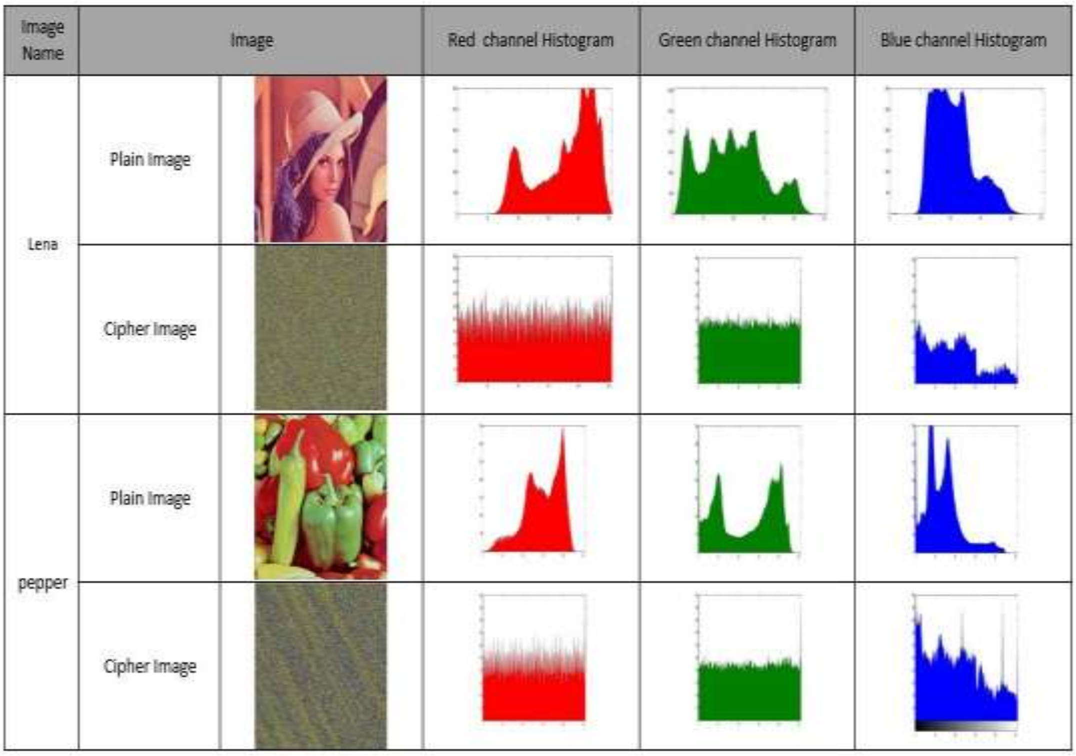


Figure 4-Encrypted Image and Histogram for Two Samples.

A careful visual inspection of these above histograms of the encrypted images by proposed method, it is clear that the histogram of the encrypted image is significantly unlike from the original image histogram. Where In the original image a few gray-scale values in the range 0 to 255 do not exist, while every gray-scale values in the range 0 to 255 are present and distributed uniformly in the ciphering image.

Furthermore, Table-1 enlists the PSNR, entropy and the correlation coefficient (CCs) of all standard dataset images of size (512 × 512) pixels.

Table 1-PSNR, Entropy, CC, NPCR and UACI values for all images

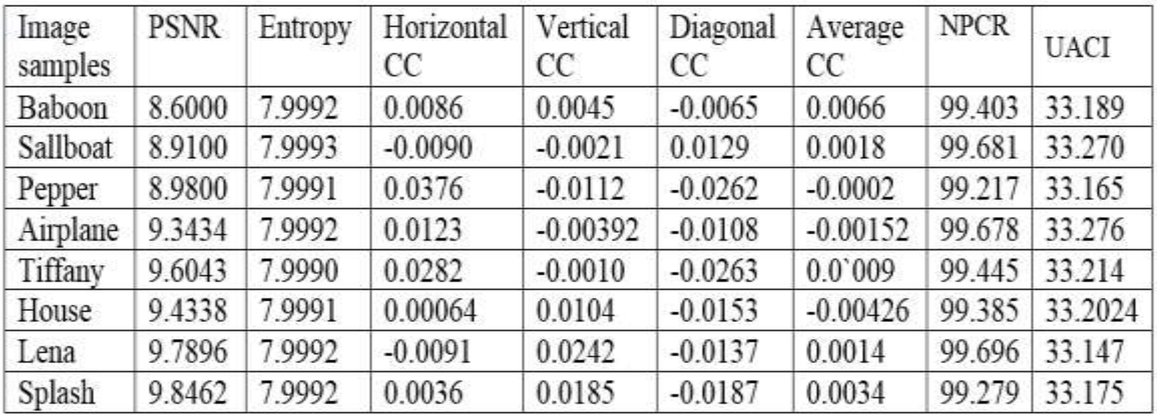


Image samples	PSNR	Entropy	Horizontal CC	Vertical CC	Diagonal CC	Average CC	NPCR	UACI
Baboon	8.6000	7.9992	0.0086	0.0045	-0.0065	0.0066	99.403	33.189
Sallboat	8.9100	7.9993	-0.0090	-0.0021	0.0129	0.0018	99.681	33.270
Pepper	8.9800	7.9991	0.0376	-0.0112	-0.0262	-0.0002	99.217	33.165
Airplane	9.3434	7.9992	0.0123	-0.00392	-0.0108	-0.00152	99.678	33.276
Tiffany	9.6043	7.9990	0.0282	-0.0010	-0.0263	0.0`009	99.445	33.214
House	9.4338	7.9991	0.00064	0.0104	-0.0153	-0.00426	99.385	33.2024
Lena	9.7896	7.9992	-0.0091	0.0242	-0.0137	0.0014	99.696	33.147
Splash	9.8462	7.9992	0.0036	0.0185	-0.0187	0.0034	99.279	33.175

From the above table, it is observed that the proposed encryption method has achieved very encouraging result. Where for all the images the PSNR values almost very low which mean the encryption quality is good and also indicates that the algorithm can tolerate various statistical attacks. Where according to [24, 25] when the obtained values of peak signal to noise ratio was small, This indicated to the difference between the plain and encrypted image is too high .Therefore to boost the ability to withstand versus data loss attacks the PSNR should be low value.

Also, from the same Table-1, it easy to notice that the entropy results are very close to the theoretical value of 8, this means that the information leakage in the encryption process is very little, and the image encryption scheme is secure enough to resist the entropy attack. Where when the entropy value closed to ideal value this mean it is difficult to retrieving the original image without knowing the key[26].

As a result, from the Table-1, yet again, the proposed encryption method performed superbly, where it is clear that the average CCs of three directions (Horizontal, Vertical, and Diagonal) are found to be absolute close to 0. this is another evidence of the proposed algorithm has the strong ability of resisting statistical attack.

To test the resistance of the proposed encryption system against differential attack, where Differential attacks is the study of how any tiny alteration in the plain image can cause a significant difference in the cipher-image.In this experiment we have measured NPCR (number of pixels change rate) and UACI (unified average changing intensity) which are widely used for for differential attack analysis[27].

From Table-1 is easy to note the values of NPCR and UACI are close to ideal value which are 99.61% and 33.46 % respectively[2] ,where for all testing image the NPCR value is found (>99%) and UACI (≈33%) .This indicated that the proposed encryption scheme can withstand against the differential attacks effectively.

5.2 Key space analysis

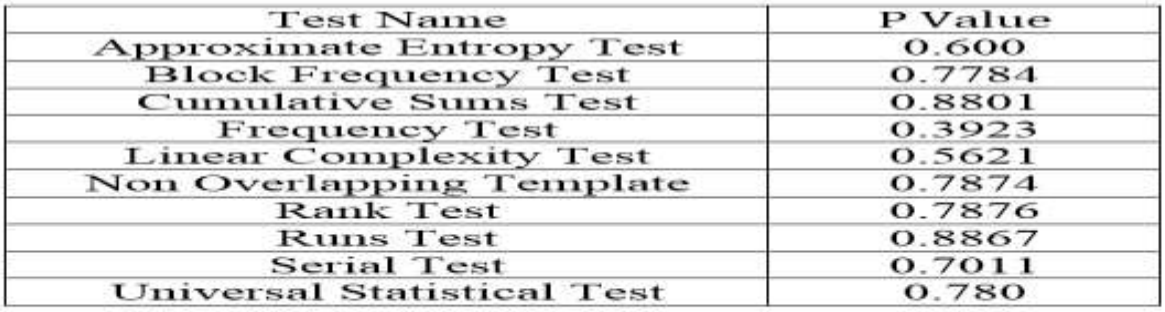
In any encryption system in order to make the encryption system constant against various types of security attacks, the key of the braiding must be large enough[28]. Theoretically the key space referred to the total number of various keys that can possible to be used in the encryption process. In the proposed encryption method the secret keys involve the initial values of the chaotic system that will be used in shuffling process it is performed on both of the pixel and blocks .additional to that, this initial value will be used to generate image which used as a key so that the size of key image is variable and depend on the size of original image, where size of key space increases accordingly to size of key image. This means that its proposed encryption scheme has:

$$\mathbf{2^{w \times h \times 24}}$$

Where w and h are represent the width and the height of key-image (in this experiment the image key with size 512x512), respectively; while 24 is a number of bits used to represent each pixel. It is worth mentioning when the key space large the 2^{100} this will be led to make the brute-force attack impractical or invalid [2, 28]. So accordingly and depending on the proposed key size (size of key-image) it is easy to conclude that the proposed encryption method has a sufficiently large key space to withstand versus to various types of brute-force attacks.

Also series of statistical tests suite provided by the National Institute of Standards and Technology (NIST) special publication is used to detect variation of a binary sequence from true randomness [3].in this experimental we used 10 tests which are list in Table-2

Table 2-NIST testing result



Test Name	P Value
Approximate Entropy Test	0.600
Block Frequency Test	0.7784
Cumulative Sums Test	0.8801
Frequency Test	0.3923
Linear Complexity Test	0.5621
Non Overlapping Template	0.7874
Rank Test	0.7876
Runs Test	0.8867
Serial Test	0.7011
Universal Statistical Test	0.780

From Table-2 can be conclude, that the proposed key have perfect randomness and successfully pass all the tests. Where It is clear from these results that the P Value is >= 0.01,according to [29] when the P-value larger than 0.01 this means that a sequence which passed the test is considered as random with 99% confidence. Thus, the new key are suitable for image encryption.

6. Conclusion

In this paper, a new image encryption scheme based on multi-level of chaotic in confusion stage has been proposed, where the proposed method employed both of the Duffing map and Cross chaotic map to perform the hash operation for both pixels and blocks, respectively. Moreover, in order to improve performance of the proposed encryption method. a new technique has been proposed in diffusion stage using number of equations that have been generated via Lagrange Interpolation from key-image.Finally, many experiments and security analysis has been applied to the proposed system .where histogram analysis, information entropy calculation, correlation coefficient ,PSNR ,differential analysis and key space evaluation has been used . The obtained results demonstrated that this method has an excellent performance in terms of security, sensitivity, and robustness. Of image encryption and resist to the different security attacks such as statistical attack, differential attack and entropy attack. Moreover, the proposed method also provide a large key space that made it withstand against the brute-force attack.

References

1. Qin, Y., et al. **2016.** Optical color-image encryption in the diffractive-imaging scheme. Optics and *Lasers in Engineering*,**77**: 191-202.
2. Li, Y., Wang, C. and Chen, H. **2017**. A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation. *Optics and Lasers in Engineering*. **90**: 238-246.
3. Ghebleh, M., Kanso, A. and Stevanović, D. **2017**. A novel image encryption algorithm based on piecewise linear chaotic maps and least squares approximation. *Multimedia Tools and Applications*: 1-22.
4. Fu, C., et al. **2011**. A novel chaos-based bit-level permutation scheme for digital image encryption. *Optics communications*, **284**(23): 5415-5423.
5. Li, C. and K.-T. Lo, **2011**. Optimal quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks. *Signal processing*, 2011. **91**(4): 949-954.
6. Wang, X., Teng, L. and Qin, X. **2012**. A novel colour image encryption algorithm based on chaos. *Signal Processing*, **92**(4): 1101-1108.
7. Zhang, Y., et al. **2013**. A novel image encryption scheme based on a linear hyperbolic chaotic system of partial differential equations. *Signal Processing: Image Communication*, **28**(3): 292-300.
8. Norouzi, B. and Mirzakuchaki, S. **2014**. A fast color image encryption algorithm based on hyper-chaotic systems. *Nonlinear Dynamics*, **78**(2): 995-1015.
9. Hua, Z. and Zhou, Y. **2017**. Design of image cipher using block-based scrambling and image filtering. *Information Sciences*, **396**: 97-113.
10. Matthews, R. **1989.** On the derivation of a “chaotic” encryption algorithm. *Cryptologia*, 1989. **13**(1): 29-42.
11. Fridrich, J. **1998.** Symmetric ciphers based on two-dimensional chaotic maps. *International Journal of Bifurcation and chaos*, **8**(06): 1259-1284.
12. Guan, Z.-H., Huang, F. and Guan, W. **2005.** Chaos-based image encryption algorithm. *Physics Letters A*, **346**(1): 153-157.
13. Pareek, N.K., Patidar, V. and Sud, K.K. **2006.** Image encryption using chaotic logistic map. *Image and vision computing*, **24**(9): 926-934.
14. Alsafasfeh, Q.H. and Arfoa, A.A. **2011.** Image encryption based on the general approach for multiple chaotic systems. *J. Signal and Information Processing*, **2**(3): 238-244.
15. Srinivasu, P.N. and Rao, S. **2015**. A Multilevel Image Encryption based on Duffing map and Modified DNA Hybridization for Transfer over an Unsecured Channel. *International Journal of Computer Applications*, **120**(4).
16. Stoyanov, B. and Kordov, K. **2014**. Novel image encryption scheme based on Chebyshev polynomial and Duffing map. *The Scientific World Journal*, **2014**.

17. Wang, L., et al. **2008**. An image encryption scheme based on cross chaotic map. in Image and Signal Processing, 2008. CISP'08. Congress on. IEEE.

18. Zeng, L. and Pu. Q. **2010.** Interactive flower modeling based on phyllotactic pattern. in Natural Computation (ICNC), 2010 Sixth International Conference on.IEEE.

19. Segerman, H. **2010.** The sunflower spiral and the Fibonacci metric. Proceedings of Bridges 20 10: Mathematics, Music, Art, Architecture, Cul− ture,: p. 483-486.

20. Zhu, Y., Shen, X. and Chen, H. **2016**. Copy-move forgery detection based on scaled ORB. *Multimedia Tools and Applications*, **75**(6): 3221-3233.

21. Dahiya, V. **2014**. Analysis of Lagrange Interpolation Formula. IJISET - *International Journal of Innovative Science, Engineering & Technology*, . **1**(10): 619-624.

22. Xiao, J., et al. **2006**. Adaptive interpolation algorithm for real-time image resizing. in Innovative Computing, Information and Control, ICICIC'06. First International Conference on. 2006. IEEE.

23. Weber, A.G. **1997.** The USC-SIPI image database version 5. USC-SIPI Report, **315**: 1-24.

24. Deng, P., et al. **2016.** Multiple-image encryption using spectral cropping and spatial multiplexing. *Optics Communications*, **359**: 234-239.

25. Das, S., Mandal, S.N. and Ghoshal. N. **2015.** Diffusion and Encryption of Digital Image Using Genetic Algorithm. in Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA). Springer.

26. Mannai, O., et al. **2015.** A new image encryption scheme based on a simple first-order time-delay system with appropriate nonlinearity. *Nonlinear Dynamics*, **82**(1-2): 107-117.

27. Mondal, B. and Mandal, T. **2017.** A light weight secure image encryption scheme based on chaos & dna computing. *Journal of King Saud University-Computer and Information Sciences*, **29**(4): 499-504.

28. Seyedzadeh, S.M., et al. **2015**. A novel color image encryption algorithm based on spatial permutation and quantum chaotic map. *Nonlinear Dynamics*, **81**(1-2): 511-529.

29. Pareschi, F., Rovatti, R. and Setti, G. **2012**. On statistical tests for randomness included in the NIST SP800-22 test suite and based on the binomial distribution. *IEEE Transactions on Information Forensics and Security*, **7**(2): 491-505.