Image Encryption Based on Fractal Geometry and Chaotic Map

Jamal Mustafa Al-Tuwaijari

Computer Sciences Department - College of Science - University of Diyala

Dr.altuwaijari@sciences.uodiyala.edu.iq

Received: 9 May 2017 **Accepted: 21 June 2017**

Abstract

Data security has become a critical issue nowadays. Sensitive data needs to be hidden from unauthorized users. In recent years, various types of images are stored and transmitted via internet. This make maintains the confidentiality, integrity and authenticity of images are a major task. Many techniques have been proposed to image encryption for the secure transmission of these images. One of the effective key of the image encryption is the using of fractal images because of the random and chaotic nature of fractals. This paper presents a proposed technique for image encryption based on fractal geometry and chaotic map. The proposed method includes encryption of color image at three stages. At first stage, the plain input image is encrypted by using the concepts of fractal geometry. In the second stage, the same picture is encrypted using the one-dimensional logistic mapping functions to generate a random image depend on the randomness nature of logistic function. Finally, in the third stage, the output encrypted images of the above two stages is merge by using the X-OR operation to generate the final encrypted image with high security attributes. Experimental results of the proposed method of encrypt images show that it has many effective features such as low relations between the pixels of encrypted image, large space key and high sensitivity to key in addition to high security. Therefore, it can be effectively protecting the security of encrypted images.

Keywords: Image Encryption, Fractal Geometry, Chaotic Map, Logistic Mapping, Image Decryption.

تشفير الصور بالاعتماد على الهندسة الكسرية والخرائط الفوضوية

جمال مصطفى التويجري

جامعة ديالى- كلية العلوم - قسم علوم الحاسوب

الخلاصة

أصبح أمن البيانات قضية مهمة حرجة في الوقت الحاضر. يجب إخفاء البيانات الحساسة عن المستخدمين غير المصرح لهم. في السنوات الأخيرة، يتم تخزين أنواع مختلفة من الصور ونقلها عن طريق الإنترنت. هذا يجعل الحفاظ على سرية وسلامة وصحة الصور مسالة مهمة كبيرة. وقد تم اقتراح العديد من التقنيات لتشفير الصور ونقلها بشكل آمن. واحدة من المفاتيح الفعالة لتشفير الصورة هو استخدام الهندسة الكسرية بسبب طبيعتها العشوائية والفوضوية. هذا البحث يقدم تقنية مقترحة لتشفير الصور استنادا إلى الهندسة كسورية والخرائط الفوضوية. وتشمل الطريقة المقترحة تشفير صورة ملونة على ثلاث مراحل. في المرحلة الأولى، يتم تشفير الصورة المدخلة الواضحة باستخدام مفاهيم الهندسة الكسرية. في المرحلة الثانية، يتم تشفير نفس الصورة باستخدام وظائف رسم الخرائط اللوجستية ذات البعد الواحد لتوليد صورة عشوائية بالاعتماد على الطبيعة العشوائية للدوال اللوجستية. وأخيرا، في المرحلة الثالثة، يتم دمج الصور المشفرة الناتج من المرحلتين المذكورة أعلاه باستخدام عملية-X ORلتوليد الصورة المشفرة النهائية ذات السمات الأمنية العالية. وتظهر النتائج التجريبية للطريقة المقترحة لتشفير الصور أن لديها العديد من الميزات الفعالة مثل انخفاض العلاقات بين بكسل الصورة المشفرة، مفتاح مساحة كبيرة، حساسية عالية للمفتاح بالإضافة إلى أمنية عالية. لذلك فان الطريقة المقترحة تكون فعالة في حماية أمن الصور المشفرة.

الكلمات المفتاحية: تشفير الصور، الهندسة الكسرية، الخرائط الفوضوية، فك تشفير الصورة

Introduction

Duo to the rapid growth of image transmission over a communication channel, computer networks and Internet, the security of digital image become critical issue. To prevent secret information from being detected to unauthorized and illegal users and for secure and fast transmission, effective algorithms are required for image encryption. In recent years, many encryptions schemes and techniques based on chaos system such as logistic mapping for image encryption has been presented by scientific researchers [1-5]. Chaos system process has several effective features such as certainty, high sensitivity to initial state, etc. The chaos sequence is random sequences and generated by chaos mapping. The structures of chaos sequence and chaos mapping are very complex in addition, their analysis and their prediction is difficult [5-9]. The first used of fractals for text encryption were presented in [10] by Jhansi et al. where they used self-symmetric property of Sierpinsky fractal. On the other hand, using fractals for image encryption was proposed at first time in [11] where the fractal key is specified by a selected square fractal key matrix. In [12], Zhang et al. present an algorithm for image encryption based on DNA sequence of addition operation and two Logistic maps. Enayati far et al. [3] proposed a new developed encryption scheme. The schemes based on Tinkerbell chaotic mapping and cellular automata. This scheme employed all cellular automata rules to generate random numbers. In [6], Teng et al. present a new encryption algorithm based on chaos, parity bit and self-adaptively. Wei et al. [7] proposed a new algorithm for color image encryption. This algorithm based on DNA sequence addition operation in addition to the hyper chaotic system. X.Y. Wang and X. Qin [8] present chaos-mapping networks used for random numbers generation based on CML. In [9], L. Liu et al. present a color images encryption algorithm based on DNA encoding technique and logistic map. Wang et al. [5] developed a chaos based encryption algorithm. In [4], Enayati far et al. used a combination of DNA mask technique and Genetic Algorithm to design an encryption algorithm. They employed a logistic mapping as a key and in addition the initial population generation for genetic algorithm.

Fractal Concepts

“Fractal” is a term expressed at first time in 1967 by Mandelbrot during his study of the patterns of England coastal line. Many researches have been done by several researchers in the field of Fractal geometry such as Serpinski, coach, Hausdorff, Lyapunov, louvi and Julia. Fractal geometry is a term used for repeated pattern of images and objects, which means that each one of these images or object has this feature can be divided into small sections and each subsection is represented as a small copy of the primary shape of these images and objects [10]. In formal mathematical definition of fractal, we can say that the repeated replacements of a recursive mathematical formula are the base of Fractals, these repeated replacements are generating fractal geometry and pattern by many repeated times. Fractal is used in variety aspects of computer science for example graphic and computer games design, compression of signal or image, classification of any phenomenon, fantasy and artistic, simulation, creation of three or two-dimensional images, several applications in medical such as blood vessels, DNA, heartbeat, etc and so on [11,13].

1.Generation of Fractal

There are many methods of fractal generation, each method using various formulas and mathematical functions as an initial start point and as core for create fractals. The methods of fractal generation in placed can be categorizing as follows: Repeated conversions by a mathematical formula as well as starting from specific initial state, as Julia set, Mandelbrot set, etc., the fractals that are generated by IFS and the fractals that generated by LSystem [11,14]. Figure 1 shows a set of different fractals. Mandelbrot set is consisting of a sequence of points on complex plane that form the fractal. This set has a complex structure and is derived from simple definitions is also recognized outside the field of mathematics. The Mandelbrot set is comprising a complex “C-values” which is represent sequence of repeated integration of the function

$F_c(Z) = Z^2 + C$ with itself and this will not approach infinity when the starting point is zero. The mandelbulb fractals are generated using the following iteration in the equation (1) [11,15]:

$Z_{i+1} = Z_i^n + C$,   i = 0, 1, 2, …(1)

Where n ≥ 3, z_0: the initial point, z_i:iteration, z_i ∈C, C is a vector in 3D space.

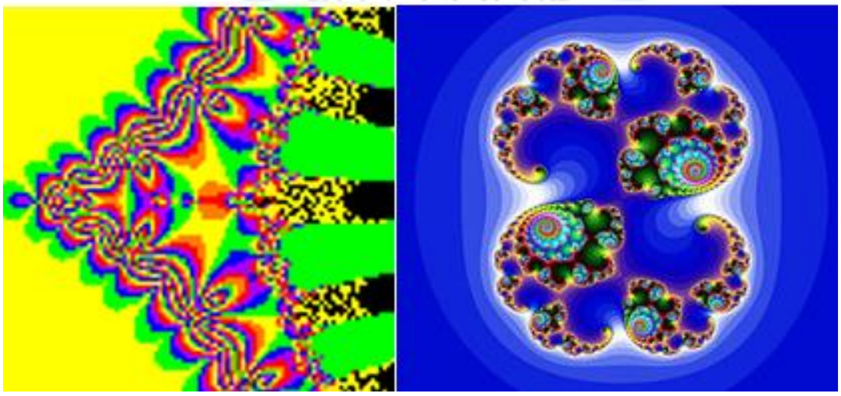


Figure 1: a set of different fractals

The Use of Fractal as a Key in Encryption

The fractal image can be used as a key of encryption in efficient manner according to encryption process. In addition, attempting to break this key by attacks is extremely difficult. The fractal image is considerably complex and highly sensitive to initial values. This can be shown when very large amount of change is taking place in the generated Fractal image when a very small amount of change is occurred in any one of the main parameters that are used for fractal image generation. Therefore, according to these robust specifications, the fractal image nowadays is used as a secure and effective encryption key [16].

Chaotic System (Logistic mapping)

The chaos system has several strong features such as certainty and high sensitivity to initial state, in addition to the random sequences feature of chaos sequences, which are created by chaos mapping. These features make the structures are complicated and their prediction and analysis as a result is more difficult. A logistic mapping considered as a simple chaos function and defined as shown in equation (2).

$$x_{n+1} = Rx_n(1 - x_n) \ldots (2)$$

Where x_0 the initial value and R is the control parameter, are considered as the keys where the function has chaotic behavior for $0<x_n<1$ and $3.57 < R < 4$ [17]. On the other side, the two-dimensional logistic map gives the system more security and expressed by the following two equations, (3) and (4) [18]:

$$X_{n+1} = \mu_1 x_n(1 - x_n) + y_1 y_{n^2} \ldots (3)$$

$$Y_{n+1} = \mu_2 x_n(1 - y_n) + y_2(x_{n^2} + x_n y_n) \ldots (4)$$

The two-dimensional logistic mapping system has a chaotic behavior where x, y generation chaos sequences occur between (0,1), in addition to, $2.75< \mu_1 \leq 3.4$, $2.7 < \mu_2 \leq 3.45$, $0.15 < y_1 \leq 0.21$ and $0.13 < y_2 \leq 0.15$ [19].

Error and Statistical Test

Error and statistical test are the essential measures to test the image quality and their performance [20,21]. In the following are the important and effective test that have been done in order to prove the robust and efficient of the proposed method.

1. Error Tests

These types of tests are very important and efficient and are successfully passed as shown in table 1. The error tests include the following tests [20,21] :

1.1 Mean Square Error (MSE test)

This test is the cumulative squared error between two digital images. The mean-squared-error (MSE) the most widely used and the simplest, full-reference for image quality measurement. It can be used to check the avalanche effect by using the following equation [20,21].:

$$MSE = \frac{1}{M*N} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} [C_1(i,j) - C_2(i,j)]^2 \ldots(5)$$

Where $C_1$and C_2 be the two cipher images and the encrypted image and i and j are represent the position of pixel of the $M * N$ image. MSE is equal to zero when $C_1(i,j) = C_2(i,j)$

1.2 Mean Absolute Error Test (MAE test)

MAE is used to obtain the average of absolute difference between two images: the reference image and the test image. It is carried out by using equation (5) [20,21]:

$$MAE = \frac{1}{M*P} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} |C_1(i,j) - C_2(i,j)| \ldots(6)$$

Where $C_1$and C_2 be the two cipher images and the encrypted image and i and j are represent the position of pixel of the $M *P$ image

1.3 Peak Signal-to-Noise Ratio *Test (PSNR Test)*

The PSNR test is evaluated in decibels. It is inversely proportional of the Mean Squared Error (MSE). It is performed by the equation (6) [20,21]:

$$PSNR = 10 * Log(\frac{(255)^2}{\frac{\sum_{i=1}^{x} \sum_{j=1}^{y} (A_{i,j} - B_{i,j})^2}{x*y}} \ldots(7)$$

Where the denominator is the mean squared error (MSE)

1.4 Unified Average Changing Intensity Test (UACI Test)

The UACI test determines the ratio of the changes between two cipher-images and the scale of UACI is [0, 1] in addition the preferred value is near to zero. It is given by the equation (7) [20,21]:

$UACI = \frac{1}{W* H}\left[\sum_{IJ}\frac{C_1(i,j)-C_2(i,j)}{255}\right] * 100\%$...(8)

Where $C_1$and C_2 be the two cipher images and the encrypted image and i and j are represent the position of pixel of the $W * H$ image

1.5 Number of Pixel Change Rate Test (NPCR test)

The NPCR test determines the number of the pixels that their values change during the encryption operation. The scale of the NPCR is [0, 1] where the value 1 shows that all pixels in image1 are different from the pixels in image2, while the value 0 shows that there is no change in the pixels of imge1 and image2. It is performed by the equation (8) [20,21]:

$NPCR = \frac{\sum_{i,j}^{N,M} D(i,j)}{W*H}$…(9)

The grey-scale values of the pixels at grid (i,j) in two ciphered images C1 and C2 denoted by C1(i,j) and C2(i,j), respectively, then D(i,j) is determined by C1(i,j) and C2(i,j), namely, if C1(i,j) = C2(i,j) then D(i,j) = 1; otherwise, D(i,j) = 0, W and H are the width and height of C1 or C2. The NPCR measures the percentage of different pixel numbers between these two images.

2. Statistical Test

The result of the tests that have been obtained from this type of tests show they are successfully passed with high performance as shown in table 2. The tests are include the following [20,21].

2.1 Correlation Test

Correlation test is the quality analysis that is used to measure the similarity between the plain image and the encrypted image. The correlation can be calculated from equation (10 – 14). The best desire value of the correlation test is near the zero. The correlation coefficient of two adjacent pixels calculated using the following equations (10 – 14) [20,21]:

$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i$... (10)

$D(x) = \frac{1}{N}\sum_{i=1}^{N} (x_i - Ex_i)^2$ …(11)

$D(y) = \frac{1}{N}\sum_{i=1}^{N}(y_i - Ey_i)^2$…(12)

$Cov(x, y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - Ex_i)(y_i - Ey_i)$…(13)

$r_{xy} = \frac{Cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}$ …(14)

Where r_{xy} is correlation coefficient and *Cov* is covariance at pixels x and y, where x and y are the gray-scale values of two pixels in the same place in the plaintext and ciphertext images. $D(x)$ is variance at pixel value x in the plaintext image, $D(y)$ is variance at pixel value y in the plaintext image, *E* is the expected value operator and *N* is the total number of pixels for *N* × *N* matrix.

2.2 Entropy Test

The Entropy is the average of information (or the expected value) that can be extracted from the image. It expressed by equation (15) [20,21].

$H(\mathrm{S}) = \sum_{i=0}^{N-1} P(S_i)Log_2P(S_i)$…(15)

Where $P(S_i)$ represents the probability of symbol S_i and the entropy is expressed in bits, S = $\{S_1, S_2, \dots, S_{256}\}$

Proposed method

The proposed method, which is used in this research, consists of three main stages, where in stage one the selected image is encrypted by using the fractal image. In the second stage, the same image is encrypted by using the logistic map function. In the final stage the two encrypted images, which are the output of stage one and stage two are merged using the X-OR operation to produce hybrid encrypted image with efficient and high-level security. The hybrid algorithm is as below:

Proposed algorithm: Encryption algorithm by using permutation between columns and rows.

Input: color image

Output: Encrypted image

Step1: Image pre-processing

Step2: Image encryption by using fractal geometry (permutation between columns and rows)

Step3: Image encryption by using logistic map (permutation between columns and rows)

Step4: Merge the output of step2 with the output of step3 by using the X-OR operation

Figures 2 shows the general overview of proposed method and figure 3 shows the details of steps of each stage. The steps of the three stages are illustrated as follows.

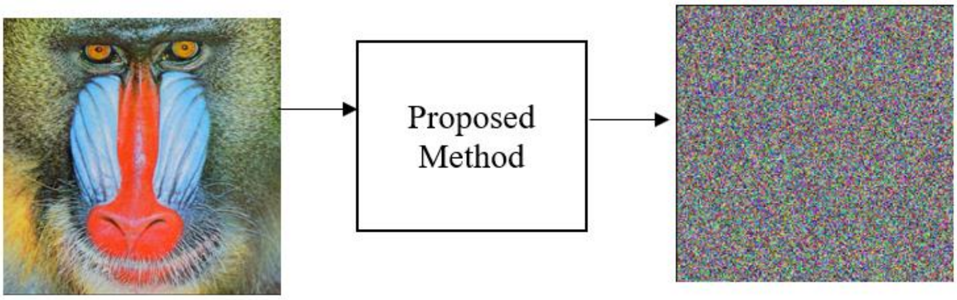


Figure 2: General over view of proposed method

1- Color image pre-processing

The first step of proposed method is the color image pre-processing where the color image is the input for this step and the image splits into its three primary color components red, green and blue (RGB). The primary colors RGB are used to encrypt the images and to generate encrypt chaotic images by using the following algorithm.

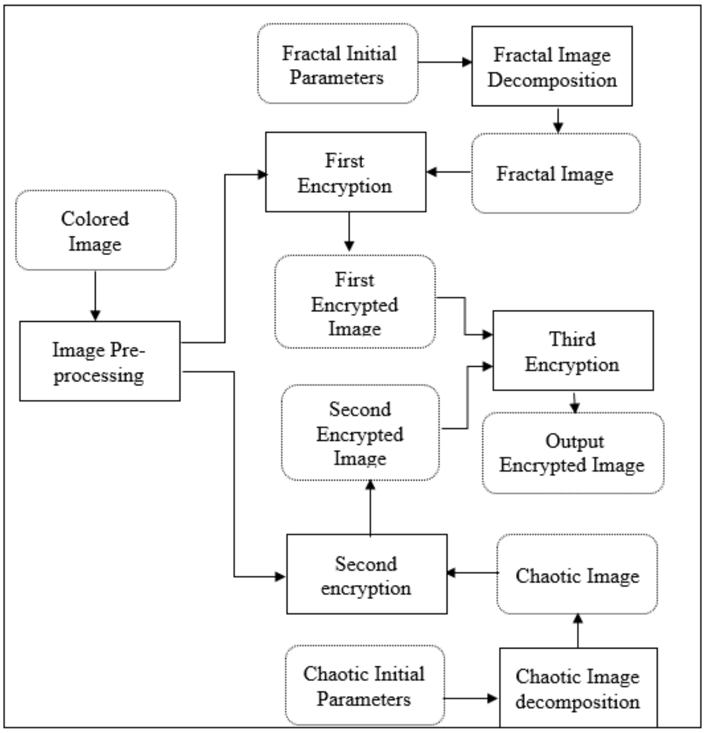


Figure 3: The framework of proposed method

Algorithm: Image pre-processing

Input: Color image

Output: Encrypted image

Step1: Generate 255 real numbers between 0 and 1.

Step2: An ascending order is making to these numbers to determine the location of rows of image matrix in which they will be exchange with the columns.

Step3: Generate another 255 real numbers between 0 and 1.

Step4: An ascending order is making to these numbers to determine the location of columns of image matrix in which they will be exchange with the rows.

Step5: An exchanging between rows and columns of the matrix of explicit image is carrying out.

2. Fractal image decomposition

In this step, the images were generated depending on fractal image corresponding to the output encrypted images of the previous step in section 6.1 and have the same size of these chaotic images.

3. First encryption stage

In this step, the encrypted chaotic images which are generated in section 6.1 are merging with the image that is generated from previous step in section 6.2 by using X-OR operation to produce the first encrypted image.

4. Chaotic image decomposition

In this step, chaotic images were generated, each image corresponding to the primary color components RGB depending on logistic map functions of section 4. The output is a chaotic image.

5. Second encryption stage

In this step the X-OR operation is used to merge the encrypt chaotic images which are generated in section 6.1 with the images that is produce from previous step in section 6.4 and the output will be the second encrypted image.

6. Third encryption stage

In this step the X-OR operation is used one more time to merge the first encrypted image which is produced from the first encryption stage in section 6.3 and the second encrypted image which is produced from the second encryption stage in section. 6.5, the output is the final encrypted image**.**

Experimental Test Results

Experiments have been performed using five common images: Lena, Baboon, Girl, Cameraman and Peppers to test the proposed algorithm by implementing the important and effective tests which are illustrated in section 5. Table 1 below shows the result of error test metrics for five encrypted images by using the proposed algorithm where it was calculate each of MSE, MAE, PSNR, UACI and NPCR for the plain images and the encrypted images. The obtained results are accepted and excellent compared to the standard measurements. The result of error metrics tests were as following:

MSE: it ranges between 8153.087 and 11168.606.

MAE: it ranges between 74.65647 and 86.29682

PSNR: it ranges between 7.6508 and 29.4266.

UACI: it ranges between 8.9226 and 33.7096.

NPCR: it ranges between 0.371805 and 0.414021.

Table 1: Error Tests

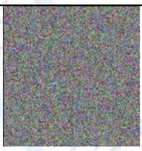
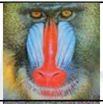
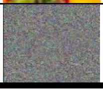
	Original Image	Encryption	Error Metrics				
			Mean Squared Error (MSE)	Mean Absolute Error (MAE)	Peak Signal-To-Noise Ratio (PSNR)	Unified Average Changing Intensity Test (UACI)	Number of Pixel Change Rate Test (NPCR)
1			8925.257	77.56219	8.6245	30.2977	0.400288
2			8333.303	75.33214	29.4266	8.9226	0.371805
3			8153.087	74.65647	9.0175	29.1626	0.396728
4			9528.290	79.98141	8.3406	31.2427	0.398254
5			11168.606	86.29682	7.6508	33.7096	0.414021

Table 2 shows the result of statistical test metrics for the same five encrypted images by using the proposed algorithm where it calculates the Correlation Coefficient Calculator (Vertical, Horizontal) and Entropy for the plain and the encrypted images. The obtained results were accepted and excellent compared to the standard measurements. The result of statistical test are as following:

Table 2: Statistical Tests

No	Type image		Statistical Test		
			Correlation Coefficient Calculator		Entropy
			Vertical (X,Y) (X+1,Y)	Horizontal (X,Y)(X,Y+1)	
1	A		0.99412841	0.99704394	7.250863706
	B		0.60178564	0.59739189	7.990496044
2	A		0.98634734	0.979271502	7.6188031
	B		0.60286101	0.597215659	7.99133704
3	A		0.99647456	0.9970874495	7.25623237
	B		0.598269408	0.5973296354	7.98978039
4	A		0.9775444	0.985247109	7.0097162
	B		0.60327349	0.6005226175	7.9911764
5	A		0.99822015	0.9984534758	7.2308664
	B		0.59612133	0.595648784	7.99011

Correlation Coefficient Calculator: Entropy (range)

Vertical (range)

0.998220159739353 - 0.596121335001296

7.00971628334551 - 7.99133704467341

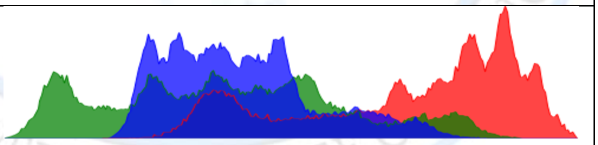
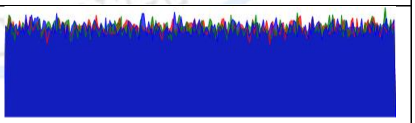
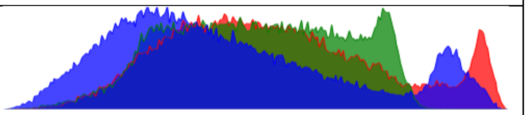
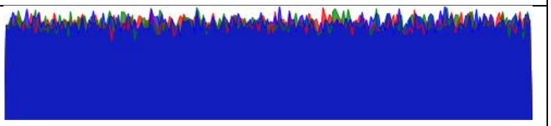
Horizontal (range)

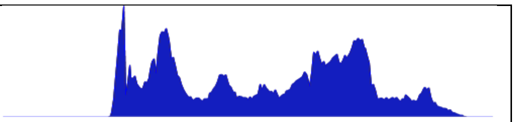
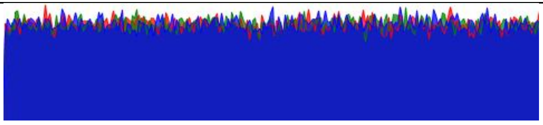
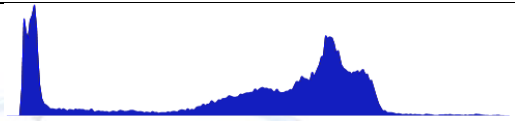
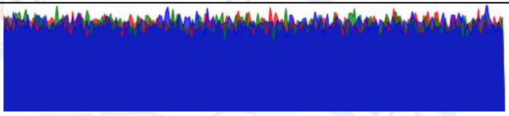
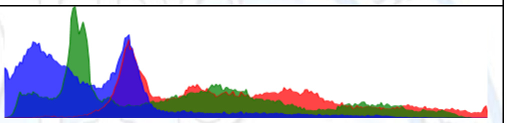
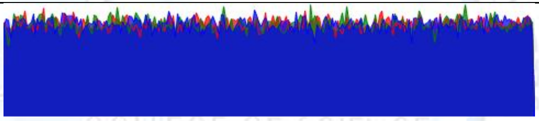
0.9984534758735380 - 0.595648784082349

Histogram Test

Table 3 includes the histogram test for the five images, which are adopted. The results before and after encryption gave an excellent distribution of histogram in term of frequency as shown in the table. The histogram measures for encrypted image when use the proposed method shows flat histogram without peak, which means that the encrypted image features were hidden and their analysis is very difficult.

Table 3: Histogram Tests

No	Type image		Statistical Test
			Histogram
1	A		
	B		
2	A		
	B		

3	A		
	B		
4	A		
	B		
5	A		
	B		

Conclusion

In this paper, the proposed method has been applied for five images and such conclusions have been obtained. First, the proposed method passed all tests with high level of success. Secondly, the proposed method achieved a high level of security in comparison with the old encryption methods. In addition, the use of a hybrid algorithm of fractional geometry and chaotic map functions gave high efficiency results. A comparison has been done between the results obtained from the proposed algorithm and the results of a set of algorithms, which are mentioned in the related work in section 1, it has been shown that the proposed algorithm gave better and good results than the rest of other algorithms.

References

1. Houman K., Masoud D. and Hamed K. Image Encryption Using Chaos Functions and Fractal Key. International Journal of Advanced Biotechnology and Research, Vol-7, Special Issue-Number4, pp1075-1082, 2016.
2. Jamal Mustaf Al-Tuwaijari. Multi-Cipher Technique Based on RNA and Chebyschev Map. Iraqi Journal of Information Technology, Vol.7th No.1st, 2015.
3. R. Enayatifar, H.J. Sadaei, A.H. Abdullah , M. Lee, I.F. Isnin, “A Novel Chaotic Based Image Encryption Using a Hybrid Model of Deoxyribonucleic Acid and Cellular Automata”, Opt. Lasers Eng. 71(2015) 33–41, 2015
4. R. Enayatifar, A.H. Abdullah, I.F. Isnin, “Chaos-Based Image Encryption Using a Hybrid Genetic Algorithm and a DNA Sequence”, Opt.Lasers Eng.56, 83– 93, 2014. X.Y. Wang, J.F. Zhao, H.J. Liu, A New Image Encryption Algorithm Based on Chaos, Opt. Commun. 285 (5), 562–566, 2012.
5. L. Teng, X.Y. Wang, A Bit-Level Image Encryption Algorithm Based on Spatiotemporal Chaotic System and Self-Adaptive, Opt. Commun. 285 (20), 4048–4054, 2012.
6. X. Wei, L. Guo, Q. Zhang, J. Zhang, S.Lian, A Novel Color Image Encryption Algorithm Based on DNA Sequence Operation and Hyper-Chaotic System, J. Syst.Softw. 85 (2), 290–299, 2012.
7. X.Y. Wang, X. Qin, A New Pseudo-Random Number Generator Based on CML and Chaotic Iteration, Nonlinear Dyn. 70 (2), 1589–1592, 2012.
8. L. Liu, Q. Zhang, X. Wei, A RGB Image Encryption Algorithm Based on DNA Encoding and Chaos Map, Comput. Electr. Eng. 38 (5), 1240–1248, 2012.
9. P. Jhansi Rani, Durga Bhavani, Symmetric Encryption Using Sierpinsky Fractal Geometry, International Conference on Information Processing, ICIP, 2011Proceedings, Springer-Verlag Berlin Heidelberg, pp. 240-245, 2011.
10. G. B. Huntress, Encryption Using Fractal Key, United States Patent 6782101, 2004.
11. Q. Zhang, L. Guo, X. Wei, Image Encryption Using DNA Addition Combining With Chaotic Maps, Math. Comput. Model. 52 (11-12) 2028–2035, (2010).

12. Akhshani A, Behnia S, Akhavan A, Abu Hassan H, Hassan Z. A novel Scheme For Image Encryption Based on 2D Piecewise Chaotic Maps. Opt Commun 283(17): 3259–66, 2010.

13. H.J. Liu, Z.L. Zhu, H.Y. Jiang, B.L. Wang, "A Novel Image Encryption Algorithm Based on Improved 3D Chaotic Cat Map", in: The 9th International Conference For Young Computer Scientists, pp. 3016_3021, 2009.

14. S.G. Lian, A Block Cipher Based on Chaotic Neural Networks, Neurocomputing 72, 1296–C1301, 2009.

15. C. Fu, Z.L. Zhu, A Chaotic Image Encryption Scheme Based on Circular Bit Shift Method, in: The 9th International Conference for Young Computer Scientists, pp. 3057–3061, 2008.

16. Kwok HS, Tang KS. A Fast Image Encryption System Based on Chaotic Maps With Finite Representation. Chaos SolitonFract ;32(4):1518–29, 2007.

17. Pareek NK, Patidar V, Sun KK. Image Encryption Using Chaotic Logistic Map. Image Vision Comput ;24(9):926–34, 2006.

18. N.K. Pareek, V. Patidar, K.K. Sud, Image Encryption Using Chaotic Logistic Map, Image Vis. Comput. 24 (9), 926–934,2006.

19. A. M. Eskicioglu and P. S. Fisher, "Image Quality Measures and Their Performance," in IEEE Transactions on Communications, vol. 43, no. 12, pp. 2959-2965, Dec 1995.

20. T. Veldhuizen. "Measures of Image Quality,"

21. http://homepages.inf.ed.ac.uk/rbf/CVonline/LOCAL_COPIES/VELDHUIZEN/node18.html. 2010.