Image Encryption using chaos functions and fractal key

Hooman Kashanian[1], **Masoud Davoudi**[2] **and Hamed Khorramfar**[3]

[1]Electrical and Computer Engineering Faculty, Islamic Azad University, Ferdows, Iran,
[2,3]MSc in Artificial Intelligence, Islamic Azad University of Ferdows,

Abstract
Many image in recent years are transmitted via internet and stored on it. Maintain the confidentiality of these data has become a major issue. So that encryption algorithms permit only authorized users to access data which is a proper solution to this problem. This paper presents a novel scheme for image encryption. At first, a two dimensional logistic mapping is applied to permutaion relations between image pixels. We used a fractal image as an encryption key. Given that the chaotic mapping properties such as extreme sensitivity to initial values, random behavior, non-periodic, certainty and so on, we used theses mappings in order to select fractal key for encryption. Experimental results show that proposed algorithm to encrypt image has many features. Due to features such as large space key, low relations between the pixels of encrypted image, high sensitivity to key and high security, it can effectively protect the encrypted image security.

Keywords:
image encryption, fractal, logistic mapping, Hennon mapping

1. Introduction

Since rapid growth of image transmission on computer networks and Internet, digital image security has been very critical. In order to image transmission, secure and fast algorithms are required for image encryption. Novel encryption schemes has been presented by researchers in recent years. Chaos system like logistic mapping [3] and Lorenz mapping designed for image encryption and researchers presented different encryption schemes based on chaos system [1-4]. Chaos system process has various features like high sensitivity to initial state, certainty, ergodic and etc. chaos sequence which are random sequences are generated by chaos mapping. These structures are very complex and their analysis and prediction is too difficult [5-7]. Wang et al. [8] presented a chaos based encryption algorithm. Teng et al. [9] proposed an encryption algorithm based on parity bit, chaos and self-adaptivity. Chaos mapping networks was employed for random numbers generation [10]. Zhang et al. [11] proposed an image encryption algorithm based on DNA sequence addition operation and two Logistic maps. Wei et al. [12] presented a new color image encryption algorithm based on DNA sequence addition operation and the hyper chaotic system. In [13], a color image encryption algorithm was proposed based on DNA encoding and the Logistic map.
Enayati far et al. [14] were designed an encryption algorithm using a combination of DNA mask and Genetic Algorithm (GA) and used logistic mapping as a key and also initial population generation for genetic algorithm. Enayati far et al. developed their work and proposed a new encryption scheme based on cellular automata and Tinkerbell chaotic mapping. In this scheme all cellular automata rules were employed to generate random numbers [15].

2. Tools and Methods

2.1 Fractal definition

The term “Fractal” was expressed by Mandelbrot in 1967 when he was studying patterns on England coastal line. Many works done by Hausdorff, Serpinski, Lyapunov, coach, Julia and louvi. Fractal geometry is an expression of a repeated pattern in objects and images means that each image or object which has this feature divided into small sections (on the basis of particular relevance), each of these subsections are a small copy of the original shape. Mathematically, Fractals are based on repeated replacements in a recursive mathematical formula which generate fractal geometry and pattern by several repeated times. Fractal have wide variety of usages such as compression (signal, image,…), graphic and computer games design, classification of any phenomenon, simulation, fantasy and artistic creation of two and three dimensional images, numerous applications in medical (blood vessels, airways in lunges, heartbeat, DNA, walking, etc.), meteorology and examine cloud shapes, examine rivers networks and ocean waves, soil mechanics, seismic and so on.

2.2 fractal generation

Each fractal generation methods using several mathematic functions and formulas as a core and initial start point to create fractals. Fractal generation methods are in placed in the following general categories:

Manuscript received October 5, 2016
Manuscript revised October 20, 2016

Repeated conversions via a simple mathematical formula and starting from an initial state, fractals with complex polynomials as a primary function (kernel) which have many usages, (Mandelbrot set, Julia set, etc.), generated fractals by IFS and generated fractals by L-System.
Mandelbrot set is a series of points on complex plane which form a fractal. This set due its beauty and complex structure which is derived only from some simple definitions is also known outside the world of mathematics. Mandelbrot set is consisting of complex "C-values" which the sequence of repeated combination of FC(Z)=Z2+C function with itself do not approach infinity at zero starting point. Figure 1 shows the MATLAB code for Mandelbrot set and its related known form and also set of fractals [16-18].

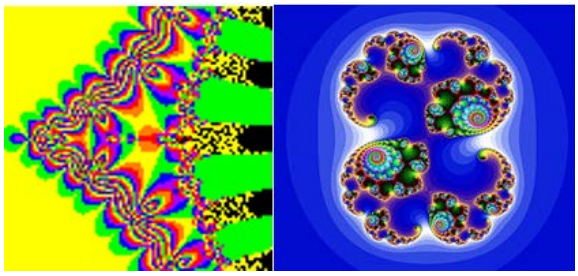

Figure 1: a set of different fractals

2.3 using fractal as a key in encryption

According to encryption procedure, a fractal image can be effectively used as a key in encryption. Breaking this type of key against attacks is very difficult. Generated Fractal image is changed in large amounts when a very small change occurred in one of the parameters of fractal image generation which shows that fractal image is very sensitive to initial values and also have considerable complexity. So fractal image can be used as a secure encryption key. In this paper a color fractal image is used as a key for encryption.

2.4 logistic Mapping

A logistic mapping is a simple chaos function and defied as equation (1).

$$X_{n+1}=RX_n(1 - X_n) \quad (1)$$

The parameter, R, and initial value, x0, are considered as keys which the function has chaotic behavior for 0<xn<1 and 3.57 < R < 4 [14]. Two dimensional logistic mapping are expressed by equations (2) and (3).

$$X_{n+1} = \mu 1 x_n(1 - x_n) + y_1 y_{n2} \quad (2)$$

$$y_{n+1} = \mu 2 x_n(1 - yn) + y2(x_{n2} + x_n y_n) \quad (3)$$

The two dimensional logistic mapping provides more security in system. This system has a chaotic behavior when 2.75< μ1 ≤3.4, 2.7 < μ2 ≤ 3.45, 0.15 < y1 ≤0.21 and 0.13 < y2 ≤ 0.15 and x,y chaos sequences generation occur between (0,1) [19].

2.5 Hennon Mapping

Hennon mapping is a reversible two-dimensional chaotic mapping which was presented by Hennon in 1967. This mapping is introduced as a method to generate pseudo-random sequences. This two-dimensional mapping is defined as follows.

$$\begin{cases} x_{n+1} = 1 + y_n - \alpha x_n^2 \\ y_{n+1} = \beta x_n \end{cases} \quad (4)$$

This mapping is dependent to two parameters, α, β. The Hennon mapping is in the chaotic state When α=1.40 and β=0.2. The Hennon mapping has a strange attractor. Figure 2 shows the space diagram for this mapping when it is in a chaotic state [20].

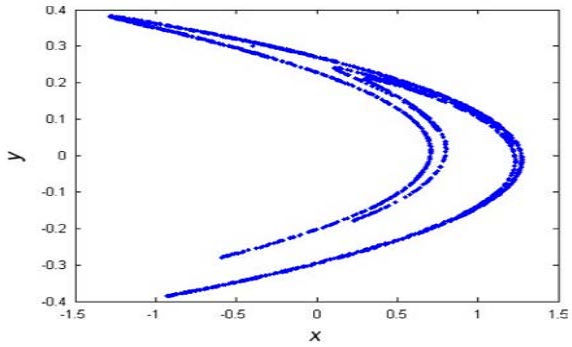

Figure 2: The Hennon attractor

3. Proposed method

The chaos system has various features such a high sensitivity to initial state, certainty, ergodic and etc. chaos sequences which are random sequences are created by chaos mapping. These structures are very complicated and their analysis and prediction are difficult. General encryption based on chaos mapping could be divided into two steps: permutation and diffusion. In practical, researchers often make a combination of permutation and diffusion to get high computational security.
To have a secure and reliable encryption algorithm, x0 and y0 values in equation (4) considered a p 128-bit key which is obtained by equations (5, 6, and 7).

$$K = \{k_1, k_1, k_2, \ldots, k_{16}\} \quad (5)$$

Where Ki shows a group of hexadecimal characters (A-F, 0-9). The initial value of X0 in Hennon mapping is calculated by the following equation:

$$x_0 = \frac{B_1.2^0 + B_2.2^2 + \cdots + B_{127}.2^{126} + B_{128}.2^{127}}{2^{128}} \quad (6)$$

Where Bi is a binary digit (0 or 1). For example if (K1)h="AA", then its decimal value will be (k1)d=170.

Also y0 vlaue in Hennon mapping is obtained by the following equation:

$$y_0 = \frac{B_1.2^0 + B_2.2^1 + \cdots + B_7.2^6 + B_8.2^7}{2^8 - 1} \quad (7)$$

3.1 Encryption

Basic structure of encryption is illustrated in figure 3. The proposed method procedures are as follows:

Step 1: the input is an image called p and has M × N dimension which M and N are rows and columns of the image, respectively. Also a color fractal image with the same size is obtained by the input which is called k.

Step 2: two chaotic sequences, X, Y, under initial values with m × n length are built using two-dimensional logistic mapping.

Step 3: chaos sequences are arranged as follows:

$$\begin{cases} [lx, fx] = sort(x); \\ [ly, fy] = sort(y); \end{cases} \quad (8)$$

Where [.,.]=sort(.) is the list of function sequence, Fx is the new sequence after Ascending sort of x and Lx is index value of Fx. Ly is the same as Lx.

Step 4: select (Lx,Ly) composition in order to change original location of the Original image pixels, P, according to equation (9) for row and equation (10) for columns:

$$P(i,j) \leftrightarrow P(lx(i), ly(j)); \quad (9)$$

$$P(i,j) \leftrightarrow P(ly(i), lx(j)); \quad (10)$$

Where i=1,2, … , M and j=1,2, …, N.

Step 5: we extract pixels' positions of fractal key to do encryption using equation (14).

$$p_1 = \text{fix}(\text{mod}(x_i * 10^4), \text{row\_size}) \quad (11)$$

$$p_2 = \text{fix}(\text{mod}(y_i * 10^4), \text{column\_size})$$

The mod(xi,m) function maps these numbers to integers in the range [0 m]. The row_size and column_size value show the numbers of fractal key rows and columns, respectively. We can get the pixel position in fractal key image selection using Hennon map and equation (11). For example, a pixel addressed by (p1,p2) is identified in fractal key and given that each fractal key is a color image and each of pixel of it have three values as red, blue and green then three pixel values are obtained in the range [0 255] using pixels of image. The output of chaos function is used to determine and select one of the three above values for each pixel in order to do encryption. This is done by the equation (12):

$$T = \text{fix}(\text{mod}(x_i + y_i) * 10^4), 3) \quad (12)$$

Step 6: we will access to one of the red, green or blue components in fractal key using equation (7) and T value. A pixel of fractal key is selected using hyper chaos system and then the XOR operator is used for encryption. The equation (13) shows this procedure:

C(i,j)= Original image(i,j) XOR Fractal_Key(Prow,n ,Pcolumn,n ,T), i=1,2, . . ., M, j=1, 2, . . . , N (13)

The above steps has been provided for image encryption. It is obvious that to decryption the image, these steps must be done inversely.

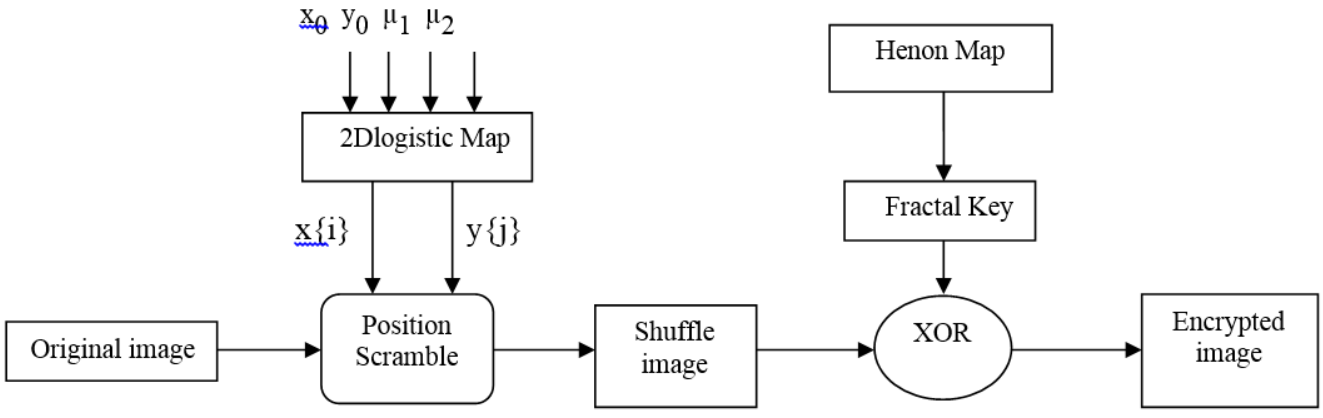

Figure 3: basic encryption structure for proposed method

4. Experimental Results

In this section different experiments that employed to prove proposed algorithm are considered. Different images with 256x256 sizes we used for testing purposes. As a result, the distorted and encrypted images are shown if figure 4.

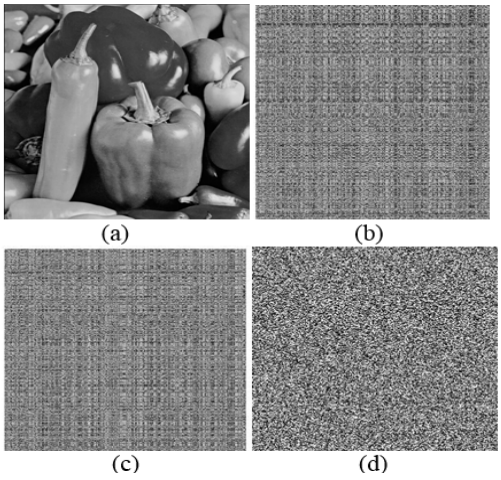

Figure 4: (a) plain image, (b) shuffling image rows, (c) shuffling image columns and (d): encrypted image.

4.1 Histogram Analysis

The Histogram shows the numbers of pixels per each gray level of the image. We used a "Peppers" image with 256x256 size as our testing purposes. The main "Peppers" image and its histogram are depicted in figure 5 and figure 6 shows histogram of the encrypted image. As shown in figure 6, it is observed that the histogram of masked image is a uniform histogram and is completely different to histogram of original image shown in figure 5. For example, distribution of gray values in encrypted image has a very good balance property. Thus the encrypted image does not provide any information about gray values distribution for attacker and as a result, the proposed algorithm can sustain any kind of statistical attack.

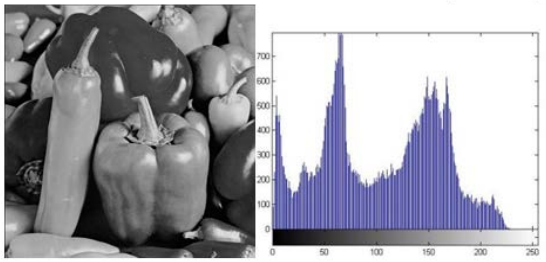

Figure 5: original image and its histogram

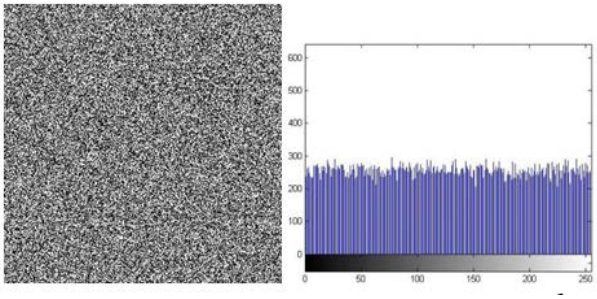

Figure 6: encrypted image and its histogram

4.2 Key Space Analysis

The key space is a set of different keys which could be used in an encryption system. An encryption system must be sensitive to all encryption keys. In this algorithm initial values of two dimensional logistic mapping system can be considered as key. Initial values in Hennon map are obtained by a 128-bit key which has a 2128 space size that is large enough to resist attacks.

4.3 Correlation Coefficient Analysis

It is well known that small correlation coefficient of adjacent pixels has strong ability against statistical attacks. In this section correlation coefficient of two adjacent pixels in original and encrypted images were computed. In order to test the relation between two adjacent pixels, 3000 pairs (horizontal, vertical and diagonal) of adjacent pixels of the original and encrypted images are selected to compute correlation coefficient using the following formula.

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

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \qquad (14)$$

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

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

Where x, y are the gray values of two adjacent pixels in image, cove(x,y), D(x) and E(x) are covariance, variance and mean, respectively. Correlation coefficients are shown in table 1. As seen, the correlation of adjacent pixel is reduced in encrypted image. According to table 1 results, we can see that the Correlation coefficients of encrypted pixels in encrypted image are close to 0. In other words, the proposed image encryption algorithm is more robust against statistical attacks.

Table 1: correlation coefficients of plain image and ciphered image.

Correlation	Vertical	Horizontal	Diagonal
Lena	-0.0103	0.0066	0.0014
Ref. [11]	0.0023	0.0036	0.0039
Ref. [13]	-0.0042	0.0059	0.0180
Ref. [14]	0.0072	0.0058	0.0031
Ref. [15]	0.0021	0.0085	0.0012

4.4 information Entropy

Information entropy can be used as a criteria to obtain a measure of pixels gray levels disturbance. The entropy of an image is calculated as follows:

$$H(m)= \sum_{i=1}^{2^N-1} p(mi) \log_2 \frac{1}{p(mi)} \quad (15)$$

Where p(mi) is the probability of gray level occurrence, mi, and N-1 is the number of gray levels. For example, in a fully uniform image with 256 gray levels which the probability of all pixels are the same, the entropy would have its maximum value, i.e. 8, which means the most irregularities among image pixels. The proximity of the image entropy to 8 means the efficiency of proposed method in image encryption. Table 2 shows the entropy values of different images before and after encryption. Table 3 compares entropy with other encryption algorithms.

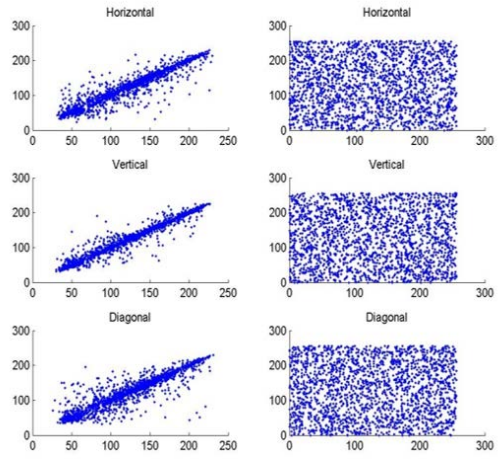

Figure 7: correlation coefficient between original image and encrypted image

Table 2: comparison of entropy values before and after encryption.

Image Name	Value before encryption	Value after encryption
Baboon	7.2925	7.9970
Lena	7.7476	7.9966
Peppers	7.3785	7.9970

Table 2: The information entropy of encrypted image.

Peppers entropies	7.9970
Lena entropies[11]	7.9980
Peppers entropies[13]	7.9894
Peppers entropies[14]	7.9991
Peppers entropies[15]	7.9980

5. Conclusion

In this paper we have used capabilities and features of hyper chaos functions such as sensitivity to initial values, random behavior, non-periodic and certainty which lead to pseudo-random numbers and in order to shuffle the relations between pixels employed two-dimensional logistic mapping. We also used Hennon map to select pixel from fractal key. Using fractal key lead to increased key space and obtain more security and resistance. Experimental results on the basis of test data show that the proposed scheme has complexity in encryption algorithm and high space key.

Reference

[1] Pareek NK, Patidar V, Sun KK. Image encryption using chaotic logistic map. Image Vision Comput 2006;24(9):926–34.

[2] 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 2010;283(17):3259–66.

[3] Kwok HS, Tang KS. A fast image encryption system based on chaotic maps with finite representation. Chaos Soliton Fract 2007;32(4):1518–29.

[4] Behnia S, Akhshani A, Mahmodi H, Akhavan A. A novel algorithm for image encryption based on mixture of chaotic maps. Chaos Soliton Fract 2008;35(2):408–19.

[5] N.K. Pareek, V. Patidar, K.K. Sud, Image encryption using chaotic logistic map, Image Vis. Comput. 24 (9) (2006) 926 - 934.

[6] 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, 2008, pp. 3057 - 3061.

[7] S.G. Lian, A block cipher based on chaotic neural networks, Neurocomputing 72 (2009) 1296- C1301.

[8] X.Y. Wang, J.F. Zhao, H.J. Liu, A new image encryption algorithm based on chaos, Opt. Commun. 285 (5) (2012) 562–566.

[9] L. Teng, X.Y. Wang, A bit-level image encryption algorithm based on spatio-temporal chaotic system and self-adaptive, Opt. Commun. 285 (20) (2012) 4048–4054.

[10] X.Y. Wang, X. Qin, A new pseudo-random number generator based on CML and chaotic iteration, Nonlinear Dyn. 70 (2) (2012) 1589–1592.

[11] Q. Zhang, L. Guo, X. Wei, Image encryption using DNA addition combining with chaotic maps, Math. Comput. Model. 52 (11-12) (2010) 2028–2035.
[12] 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) (2012) 290–299.
[13] L. Liu, Q. Zhang, X. Wei, A RGB image encryption algorithm based on DNA encoding and chaos map, Comput. Electr. Eng. 38 (5) (2012) 1240–1248.
[14] 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 (2014) 83–93.
[15] 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.
[16] S.G. Lian, J.S. Sun, Z.Q. Wang, A block cipher based on a suitable use of the chaotic standard map, Int. J. Chaos Solitons Fractals 26 (2005) 117‑ 129.
[17] Mohammad Ahmad Alia and Azman Bin Samsudin, "New Key Exchange Protocol Based on Mandelbrot and Julia Fractal Sets", IJCSNS International Journal of Computer Science and Network Security, VOL.7 No.2, February 2007.
[18] Huang F, Guan Z-H A modified method of a class of recently presented cryptosystems. Chaos, Solitons & Fractals 2005;23:1893-9.
[19] 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, 2009, pp. 3016_3021
[20] Hongjun Liu, Abdurahman Kadir, "Asymmetric color image encryption scheme using 2D discrete-time map", Signal Processing 113 (2015) 104–112 .