An image encryption based on DNA coding and 2DLogistic chaotic map

FAYZA ELAMRAWY, MAHA SHARKAS, ABDEL MONEM NASSER

Arab Academy for Science & Technology

Abu Kir, Alexandria

EGYPT

engfayzaelamrawy@gmail.com, mshsarkas@aast.edu, monem_1954@aast.edu
Fayza Elamrawy, Maha Sharkas, Abdel Monem Nasser

Abstract— **A novel image encryption algorithm based on DNA coding and the Two-dimensional logistic chaotic map is presented in this paper. The proposed encryption algorithm consists of three parts, DNA coding, permutation, and diffusion. First, the image is encoded by DNA coding, then, the DNA coded image is permutated by using the 2D logistic chaotic map. Finally, the image is diffused by using the 2Dlogistic chaotic map to get the encrypted images. Simulation results show that the proposed algorithm provides good encryption effect, high performance and high sensitivity.**

Index Terms-- **Image encryption, DNA operation. 2D logistic chaotic map.**

1. Introduction

Due to high redundancy, large data capacity, and high correlation among pixels in images file [1 &2] the traditional encryption methods like IDEA, AES, and DES are found not suitable to image encryption. Chaos seems to be a good candidate due to its ergodicity and complex dynamics [3]. An image encryption based on row-column, masking and main diffusion processes with hyper chaos is presented in [4]. The initial conditions of the hyper chaotic system are generated using a 256-bit long external secret key. An image encryption scheme based on two processes; key stream generation process and one-round diffusion process is presented in [3]. A new chaotic algorithm with nonlinearity and coupled structure based on a coupled two-dimensional piecewise nonlinear chaotic map is suggested. Other image encryption schemes based on self-adaptive wave transmission and DNA sequences are presented in [5 & 6]. DNA based methods include DNA encoding and DNA computing which include some biological operations and algebra operations on a DNA sequence, such as the complementary rule of bases [6], DNA addition, DNA subtraction [7], and DNA exclusive OR (XOR) operation [8]. The idea of combining chaos and DNA computing in image cryptosystems is proposed in [8] where a color image encryption method based on DNA operations and chaotic maps is presented. A masking matrix is generated using a 1D chaotic system which is added to the DNA encoded plain-image and the intermediate result is complemented with the help of a complement matrix generated through two 1D chaotic maps and finally the result is permuted using a 2D chaotic map. Liu H, Wang X, Kadir [7] had employed the MD5 hash to produce initial conditions of the chaotic maps where each image pixel is encoded to four nucleotides by DNA coding, then, the complementary rule is used to transform each nucleotide into their base pair. Meanwhile, some cryptanalysis work demonstrated that some image encryption methods are insecure against various conventional attacks, especially on chosen-plaintext attack. Especially when the key stream used to encrypt different plain-images are the same. In other words, the keys are independent of the plain images.. An image encryption algorithms using DNA operations where a low-dimensional Logistic map is chosen to produce the chaotic sequence is presented by Zhang et al in [6]. Later, authors in [10] modified their work and suggested an invertible method for color image encryption by modifying the DNA addition in [6].

In this paper an image encryption algorithm is suggested and is implemented by transforming the original image into other formats—DNA sequence and 2D Logistics -image. Through encoding, the original image is transformed into DNA sequence; and through encoding and random segmentation, the original image is transformed into ‘2D Logistics-image'. Substitution and permutation are then imposed on the two formats of the image respectively to achieve a nice encryption result. There are three highlights in the proposed scheme. The first one is chaotic-random substitution strategy imposed on the image in the DNA sequence format. The second one is the construction of the 2D Logistics -image. The third one is the usage of 2D Logistics-chaotic system to generate the random sequence for deciding the complementary DNA nucleoside in the substitution period and for randomly constructing the 2D Logistics-image.

2. Background

A DNA molecule is made up from four nucleic acid bases namely; adenine (A), cytosine (C), guanine (G) and thymine (T). A and T are complements and C and G are complements. Because 0 and 1 are complementary in the binary processing, so 00 and 11 are complementary and 01 and 10 are also complimentary. The four bases A, C, G, and T are used to encode 00, 01, 10 and 11. Only 8 kinds of coding schemes satisfy the Watson-Crick complement rule [6] and are listed in Table I. If four nucleic acid bases A, C, G, and T, are used to denote the binary values of 00, 01, 10 and 11 respectively, each 8-bit pixel value of the image can be expressed as a DNA sequence whose length is 4. For example, if the gray value of the original image pixel is 199 then, its binary value is “11,000,111”. We can produce a DNA sequence “TACT” using the DNA encoding rule 1 to encode the stream. Inversely, we can get the pixel value by decoding the nucleotide string. For example, “GCAT” is considered as “01,101,100”. By rule 8, its decimal value is 108. Obviously, it is also a simple method of encryption.

2.1 Algebraic operation for DNA sequences

Some biology and algebraic operations based on the DNA sequence are employed in [6], such as the addition, subtraction, and XOR operations. These operations are performed according to traditional addition, subtraction, and XOR in binary arithmatics. Some examples are given here where 10 + 11 = 01, 01–11 = 10, and $01 \oplus 11 = 10$. Corresponding to 8 states of DNA encoding schemes, there also exist 8 kinds of DNA addition rules, 8 kinds of DNA subtraction rules, and 8 kinds of DNA XOR rules. In this paper, rule 2 is adopted as shown in Table I. In other words, A, C, G, T are used to denote 00,10, 01, 11, respectively. The details of XOR operation rules are illustrated in Tables II.

TABLE I:. 8 Kinds of coding schemes satisfy the Watson-crick complement rule

Rule	1	2	3	4	5	6	7	8
A	00	00	01	01	10	10	11	11
C	01	10	00	11	00	11	01	10
G	10	01	11	00	11	00	10	01
T	11	11	10	10	01	01	00	00

TABLE II: XOR operation for DNA sequences

XOR	A=00	G=01	C=10	T=11
A=00	A	G	C	T
G=01	G	A	T	C
C=10	C	T	A	G
T=11	T	C	G	A

2.2 The Two-Dimensional Logistic Map

The two-dimensional logistic map is researched for its complicated behaviors in relation to the evolution of basins and attractors. This two-dimensional logistic map can be discretely defined in Eq. (1), where r is the system parameter and (x_i, y_i) is the pair-wise point at the i^{th} iteration

Two-dimensional logistic map:

$$x_{i+1} = r(3y_i + 1)x_i(1 - x_i)$$

$$y_{i+1} = r(3x_i + 1)y_i(1 - y_i) \qquad (1)$$

The two-dimensional logistic map defined in equation (1) has higher complexity compared to the conventional logistic map, that is, the one-dimensional logistic map defined in equation (2), where r is the parameter controlling the chaotic behaviors.

The one dimensional logistic map is defined in equation (2)

$$x_{i+1} = rx_{i+1}(1 - x_i) \qquad (2)$$

3. The Proposed Model

Although the two-dimensional logistic map has various behaviors according to different system parameters, we concentrate on the parameter interval r ∈ [1.1; 1.19], where the system is chaotic. The image encryption algorithm consists of DNA sequence generation, Logistic Permutation and Diffusion created for image ciphering. If K denotes the cipher key, A is the original image, and E and D are encryption and decryption function respectively, then Encryption and decryption operations are expressed using equations 3 and 4.

$$C=E(A, K) \tag{3}$$

$$A=D(C, K) \tag{4}$$

3.1 Image encryption

The structure of the proposed image encryption algorithm is shown in Fig. 1. The input image is grayscale of dimension 256 × 256. The proposed encryption algorithm is composed of three parts, DNA coding, permutation, and diffusion. First, the image is converted into binary sequences, then, the binary sequences are converted using DNA coding to get the DNA sequences matrix. Secondly, DNA matrices of the image are permutated under the 2 D Logistics system. Finally, the permutated 2 D Logistic-image is transformed by diffusion to get the encrypted image.

3.2 Logistic Permutation

Logistic permutation generates a random cipher text permutation matrix for an image permutation matrix based on certain initial conditions using 2D logistic map. Considering the size of the original image A to be M×N, a sequence of pairwise x and y can be generated using Equation (5). If Xseq and Yseq represents x and y coordinate sequence respectively then

$$x_{seq} = \{x_{1,}x_{2,} \dots \dots \dots, x_{MN}\}$$

$$y_{seq} = \{y_{1,}y_{2,} \dots \dots \dots, y_{MN}\} \tag{5}$$

On rearranging the above elements, we obtain a matrix of size M×N for X and Y respectively. Thus r^{th} row of X can be used to form a bijective mapping $e_{\pi x}$ and c^{th} column of Y have a bijective mapping $e_{\pi y}$ .Thus X sorted and Y sorted can be expressed using Equation (6)

$$x^{sorted}_{r,i} = x_{r,e_{\pi x}}\ (i)$$

$$y^{sorted}_{i,c} = x_{r,e_{\pi y}}\ (i), c \tag{6}$$

3.3 Logistic Diffusion

In order to achieve good diffusion properties, we apply the logistic diffusion for every H×H image block named A_b within the original image A over the finite field GF=2^8 where GF has to be an integer number. H is the block size variable determined by the plaintext image format, and M_d is the maximum distance separation matrix found from H×H random permutation matrices defined in equation (7) where H=4. If the plaintext image A is either grayscale or color mage pixel, the image block A_b has size 4×4; else if the plaintext image is a binary image, then A_b is of size 32×32 in bits equivalent to 4×4 image block in bytes. If a plaintext image A has size M × N indivisible by H, we only apply this process with respect to the region M×N = floor (size (W)/H) ×H. Since the 2D logistic diffusion process is applied to every H×H image blocks in the plaintext image per cipher iteration, any one-pixel change in plaintext image then causes a change for H×H pixels in each round. Therefore, the least number of cipher iterations to have M×N changing pixels is calculated by Equation (8). After some iterations, any slight change in a plaintext image leads to significant changes in cipher text C_b and thus attains the diffusion properties where C_b is equal to

$$C_b = (M_d\ \times A_b\ \times M_d\ ) \tag{7}$$

$$iteration_{min} = log_{(HxH)}\ MxN$$
$$= ceil\left(\frac{log_{2\ MxN}}{2log_{2\ H}}\right) \tag{8}$$

3.4 Encryption

The encryption process is illustrated in the following steps

Step 1. Input an image A (M, N), as the original image, where M and N are rows and columns of the image.

Step 2. Convert image A into binary matrix A.

Step 3. Carry out DNA encoding operation according to the four-bit planes, then we get four coding matrices all of their sizes are (M×N).

Step 4. Formulate the 2D Logistic-image with the binary sequence according to the method proposed in section II (B), the random sizes of every piece are generated through the iteration of the 2D Logistic chaotic system.

Step 5. Permute the 2D Logistic image.

Step6. Diffuse the 2 D Logistic image into ordinary image form

A block diagram of the system is shown in figure.1.

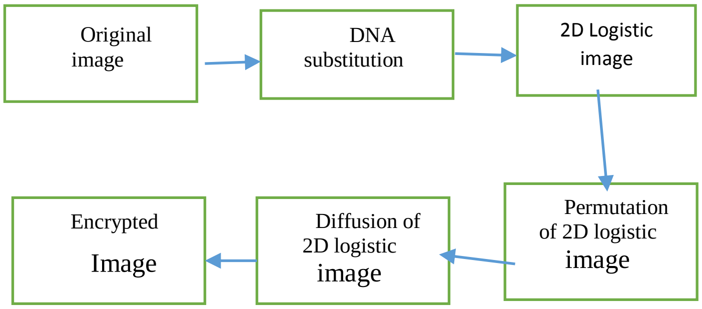
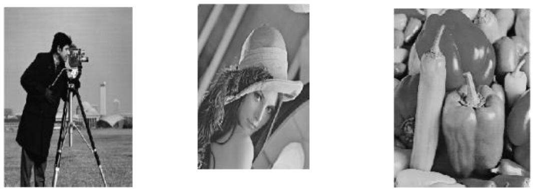

Original image
DNA substitution
2D Logistic image
Permutation of 2D logistic image
Diffusion of 2D logistic image
Encrypted Image

Figure 1. Block diagram of the proposed scheme

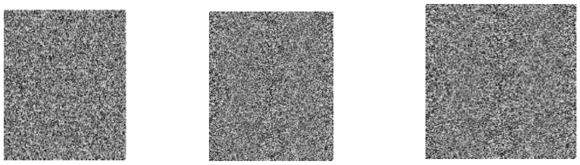
4. Results and Discussion

To demonstrate the security and efficiency of our algorithm, we use the standard 256 x256 gray image cameraman as the original image. Matlab 2016 is used to simulate the suggested algorithm. Figure 2.a, b and c show the original images, while the encrypted images are shown in Figure 3.a,b and c. The decrypted images are shown in figure 4.a, b and c. Lena and peppers images are also evaluated.



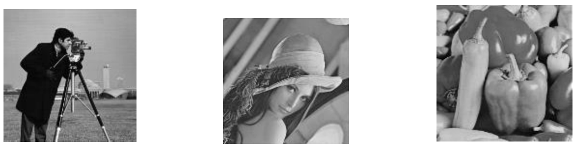
(a) cameraman (b)Lena (c)peppers

Figure 2.The Original images



(a) cameraman (b)Lena (c)peppers

Figure 3. The Encrypted image



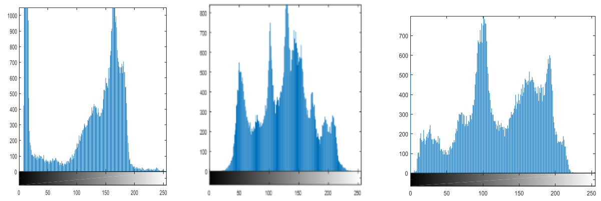
(a) cameraman (b)Lena (c)peppers

Figure 4. Decrypted image

The cipher image generated by the algorithm must not show any predictable statistical relation to the original image in order to prevent the attacker to use that information to decipher the information being transmitted. Statistical attacks include histogram analysis and correlation coefficient analysis. Also, the entropy, mean squared error MSE and Peak signal-to-noise ratio PSNR are calculated to evaluate the obtained results.

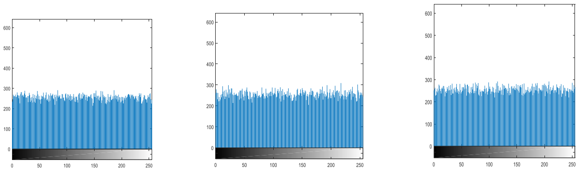
4.1 Histogram Analysis

An image histogram is a valuable tool employed to view the intensity profile of an image. Three 256 Grey-level images of size 256 × 256 are selected that have different contents, and their histograms are calculated. A good encryption algorithm is the one which generates a cipher image whose histogram is uniform and completely different from that of the original image. Thus it will be difficult for attackers to identify the pixels from the encrypted image having similar nature to that of the original image. The histogram for the original and encryption image has been shown in figures 5 and 6.



(a) Cameraman (b)Lena (c)peppers

Figure 5. Histogram of original image



(a) Cameraman (b)Lena (c)peppers

Figure 6. Histogram of the encrypted image.

4.2 Correlation coefficient analysis

A secure encryption scheme should remove correlation of adjacent image pixels to improve resistance against statistical analysis. The correlation coefficients of each pair were calculated using the following formulas:

$$r_{xy} = \frac{cov(x,y)}{} \tag{9}$$

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

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

$$cov(x) = \frac{1}{N} \sum_{i=1}^{N} (x_i - E(x))\, (y_i - E(y) \qquad (12)$$

Where x and y are grey-scale values of two adjacent pixels in the image. N is the total number of duplets (x, y) obtained from the image. Correlation coefficients of cameraman, Lena and peppers in the horizontal, vertical and diagonal positions are reported in Table III with reference to the plain image.

TABLE III: Correlations Coefficients of images

Image	Original image			Cipher image		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Cameraman	0.9439	0.9630	0.9161	-0.0040	-0.00049	0.0015
Lena	0.9348	0.9151	0.8408	0.0015	-0.0037	0.0079
Peppers	0.9230	0.9225	0.8551	-0.0028	0.0031	0.0026

The correlation between various pairs of plain/cipher images has also been analyzed by computing the 2D Correlation Coefficients (CC). The CC is calculated in equation (13). The correlation coefficients are given in table IV.

$$cc = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} (A_{ij} - A)(B_{ij} - B)}{\sqrt{\sum_{i=1}^{M} \sum_{j=1}^{N} \left((A_{ij} - A)\right)^2 \;\; \sum_{i=1}^{M} \sum_{j=1}^{N} \left((B_{ij} - B)^2 (B_{ij} - B)\right)}} \qquad (13)$$

TABLE IV: Correlation Coefficient between Original And Cipher Images

Image	Correlation coefficients
Cameraman	-0.0013
Lena	0.0076
Peppers	0.0013

4.3 MSE and peak PSNR ratio analysis

As a general requirement for the image encryption algorithms, the cipher-image should be significantly different than the original one. Such difference can be measured by means of two criteria namely, the Mean Square Error (MSE) and Peak Signal-to-Noise Ratio (PSNR) between the plain-images and the cipher-images. PSNR is most easily defined via the MSE. Given an M × N input image A and its encrypted-image B, MSE and PSNR are given in equations 14 and 15. The MSE and PSNR results are shown in Table V

$$\text{MSE}=\frac{1}{M\ X\ N} \sum_{i=1}^{M} \quad \sum_{j=1}^{N} \left(A(i,j) - B(i,j)\right)^2 \qquad (14)$$

$$\text{PSNR}=20 \log[\text{M}\times\text{N}]/\text{MSE} \qquad (15)$$

TABLE V: MSE and PSNR OF the used images

Image	MSE	PSNR
Cameraman	9391	8.4377
Lena	7542.2	9.3898
Peppers	8298.3	8.9749

4.4 Information entropy

In information theory (the mathematical theory of data communication and storage founded in 1949 by Shannon), entropy is a measure of the uncertainty in a random variable and is given in equation 16. The entropy results are shown in Table VI

$$H(m) = \sum_{i=0}^{2^n} p(mi) log_2 \frac{1}{p(mi)} \qquad (16)$$

TABLE VI: Information Entropy Of Image

Image	Original image entropy	Encryption image entropy
Cameraman	7.0097	7.9972
Lena	7.3846	7.9972
Peppers	7.5327	7.9970

The performance of the proposed image encryption system and other methods based on the correlation coefficients are compared in Table VII. These results reveal the fact that our algorithm yields better security performance in comparison with the results obtained by other algorithms.

TABLEVII: Comparison Results

	Original image			Encryption image		
Lena	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Ours	*0.9348*	*0.9151*	*0.8408*	*0.0015*	*-0.0037*	*0.0079*
Zhang's[10]	0.9821	0.9912	0.9431	0.0012	0.0156	0.1326
Lin's [11]	0.9217	0.9711	0.9227	0.0242	0.0194	0.0243
Ye's [12]	0.9833	0.9626	0.9514	0.0770	−0.0724	−0.0615
Huang's [13]	0.9457	0.9291	0.9859	−0.0974	−0.0707	0.0484
Ye's [14]	0.9690	0.9637	0.9492	−0.0134	0.0012	0.0398
Qiang Zhang,[15]	0.9432	0.9688	0.9148	0.1366	0.0166	0.0021

5. CONCLUSION

This paper presents a novel image encryption algorithm based on DNA sequence operations and 2D Logistic map. Our method can be easily implemented and is computationally simple to achieve high-security level, high speed, and high sensitivity. Moreover, it can be applied to encrypt images. In order to increase the security of the proposed algorithm, a 256 bit-long secret key is employed to produce the initial conditions of the 2D Logistic map. The entropy test indicates that information leakage is negligible. The encrypted image histogram is uniform and the analysis of its correlation coefficient values indicates that the adjacent pixels are nearly unrelated. The individual correlation coefficient values are smaller compared with the available literature.

REFERENCES

[1] Benyamin Norouzi1 & Sattar Mirzakuchaki, "An image encryption algorithm based on DNA sequence operations and cellular neural network," Multimed Tools Appl (2017)

[2] Mazloom S, Eftekhari-Moghadam, "Color image encryption based on the coupled nonlinear chaotic map," Journal of Chaos, Solitons and Fractals, 2009.

[3] Seyedzadeh SM, Mirzakuchaki, "A fast color image encryption algorithm based on coupled two dimensional piecewise chaotic map.,"J Signal Process 92:1202–1215, May 2012

[4] Norouzi B,Mirzakuchaki, "A fast color image encryption algorithm based on hyper-chaotic systems," .Nonlinear Dynamics 78:995–1015, 2014.

[5] Liao X, Lai S, Zhou Q, "A novel image encryption algorithm based on self-adaptive wave transmission," J Signal Process 90:2714–2722, 2010.

[6] Zhang Q, Guo L, Wei X, "Image encryption using DNA addition combining with chaotic maps," Math Comput Model 52:2028–2035, 2010

[7] Liu H, Wang X, Kadir A, "Image encryption using DNA complementary rule and chaotic maps,". Appl Soft Comput 12:1457–1466, 2012.

[8] Zhang Q, Wang Q, Wei X, "A novel image encryption scheme based on DNA coding and multi chaotic maps," Adv Sci Lett 3:447–451, 2010.

[9] Jain A, Rajpal N, "A robust image encryption algorithm resistant to attacks using DNA and chaotic logistic maps.," Multimed Tools Appl. doi:10.1007/s11042-015-2515-7, 2015.

[10] Liu L, Zhang Q, Wei X, "A RGB image encryption algorithm based on DNA encoding and chaos map," Comput Electr Eng 38:1240–1248, 2012.

[11] Zhang Q, Guo L, Wei X, "A novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system," Optik Int J Light Electron Opt 124:3596–3600, 2013.

[12] Lin T, Xingyuan W, "A bit-level image encryption algorithm based on spatiotemporal chaotic system and self-adaptive," Opt Commun, 2012.

[13] Ye G, Wong K-W, "An efficient chaotic image encryption algorithm based on a generalized Arnold map," Nonlinear Dyn 69:2079–2087, 2012

[14] Huang X, "Image encryption algorithm using chaotic Chebyshev generator," Nonlinear Dyn 67:2411–2417, 2012.

[15] Ye G, "Image scrambling encryption algorithm of pixel bit based on chaos map," Pattern Recogn Lett 31:347–354.

[16] Qiang Zhang, Xianglian Xue, and XiaopengWei, "A Novel Image Encryption Algorithm Based on DNA Subsequence Operation," The Scientific World Journal Volume 2012, 10.1100/2012/286741.