Nonlinear Dyn (2014) 75:407–416
DOI 10.1007/s11071-013-0819-6

ORIGINAL PAPER

Using 3-cell chaotic map for image encryption based on biological operations

Morteza SaberiKamarposhti · Dzulkifli Mohammad · Mohd Shafry Mohd Rahim · Mahdi Yaghobi

Received: 27 October 2012 / Accepted: 2 February 2013 / Published online: 15 January 2014

Abstract Recently, image encryption has emerged as an extremely urgent need to provide high protection for secure images against being used without any authorization. In the present paper, the 3-cell chaotic map known as cycling chaos was employed for image encryption based on biological operations. In order to increase security of the proposed method, the 120-bits secret key is used. DNA Sequences and cycling chaos were used to scramble the positions of the image pixels, and then the pixels grey values were modified using a mask DNA generated by cycling chaos. The obtained results demonstrated high security of the proposed method, and it was found acceptably resistant against different well-known attacks.

Keywords Image encryption · Cycling chaos · DNA sequences · Information entropy · Correlation coefficient

M. SaberiKamarposhti (✉) · D. Mohammad ·
M. Shafry Mohd Rahim
Department of Computer Graphics and Multimedia,
Faculty of Computer Science and Information System,
Universiti Teknologi Malaysia, 81300 Skudai, Johor,
Malaysia
e-mail: Morteza.Saberi@iaufb.ac.ir

M. Yaghobi
Department of Electrical Engineering, Faculty of
Engineering, Islamic Azad University, Mashhad Branch,
Mashhad, Iran

1 Introduction

During the last decade, the online accessing, editing, and transferring of digital images became easy, but at the same time, vulnerable. Due to the importance of securing the images against unauthorized distributions and use, image encryption has widely emerged and several encryption methods have been proposed in such a way that the security concerns could be satisfied as far as possible that could be classified as:

1. Spatial domain methods [1–5].
2. Frequency domain methods [6–9].

As it can be seen in Fig. 1, the image encryption methods can be divided into two main groups. Images can be encrypted through several proposed methods. In [10], two chaotic logistic maps and an external secret key of 80-bit were employed. The initial conditions required for the two logistic maps are derived by an external secret key whose bits should be provided with different weights. Further, in the process of this encryption method, eight types of operations have been used for encrypting of an image's pixels, and the logistic map outcome determines which type of operation should be employed for a particular pixel. After encryption of each block of the sixteen pixels, the secret key is modified in order to make the cipher more strong against any attack.

In [11], a random grid is introduced that is a transparency comprising a two-dimensional array of pixels

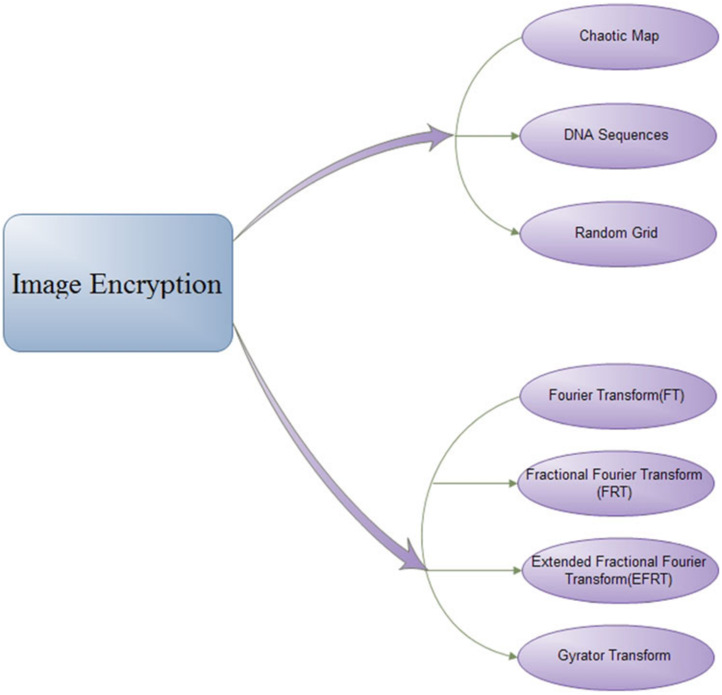


Fig. 1 Image encryption methods

which are either opaque or transparent determined randomly. An algorithm has been proposed employing the random grids for encrypting the color images and secret grey-level images in a way that neither of the two encrypted shares could disclose the information of the image; the secret could be revealed once both shares are superimposed. It is noticeable that the visual system performs the decryption process and there is no need to computation.

In [12], a mix of a one-dimensional chaotic map with a typical coupled map was provided to be used for obtaining a high degree of security for the image encryption with an acceptable speed. Another method for image encryption proposed by [13] is a novel pixel shuffling method. In this method, the chaotic system's output trajectory is not predictable. Thus, based on this unpredictable character, the chaotic sequences that have been generated by the chaotic systems to be used as encryption codes were utilized and then the digital-color image encryption was implemented with a high confidential security. This image encryption method is a combination of pixel shuffling and four different chaotic systems. It is able to banish the original image outlines, dramatically decrease the likelihood of exhaustive attacks, and disorder the RGB levels' distributive characteristics.

In [14], a novel image encryption method has been introduced based on the DNA sequence addition operation and chaos. In this method, a DNA sequence matrix should be firstly obtained through encoding the original image. Then the DNA sequence matrix is divided into equal blocks and using the DNA sequence addition operation, these blocks should be added. Next, using two Logistic maps, the DNA sequence complement operation are performed to the result of the added matrix. At the final step, from the third step, you should decode the DNA sequence matrix, and then you can have an encrypted image.

Based on the discrete fractional random transform and chaotic maps, [15] presented a new double-image encryption algorithm. Using a chaotic map, the random matrices that are employed in this algorithm have been generated. One out of two existing original images is scrambled using the chaotic map of another image, and then it is encoded into a complex matrix phase through the other original image as its amplitude. Afterward, this matrix is encrypted via the discrete fractional random transform. If you can apply the exact keys consisting of the control parameters, the initial values, fractional orders, and the chaotic maps' truncated positions, you can recover the two original images without cross-talk.

In [16], through encoding the original color image that could be changed into three matrices, three DNA sequence matrices have resulted. The Chen's hyperchaotic maps have generated the chaotic sequences that were employed for scrambling the locations of elements from three DNA sequence matrices that have been divided then into some equal blocks. These blocks were added via Chen's hyperchaotic maps and the DNA sequence addition operation. After these processes, if you can decode the DNA sequence matrices and recombine the three channels, you can get the encrypted color image.

In this paper, we use DNA Sequences and Cycling Chaos to propose a secure image encryption method. This paper is organized as shown below. In the first section, Cycling Chaos map will be explained. Then the proposed method is fully discussed. Finally, the proposed method will be tested against several attacks and the experimental results will be illustrated.

2 Related works

Palacios and Juarez have proposed Cycling Chaos [17]. They have supposed a system with N cells that every cell's input dynamic is defined by the equation in K-D as

$$X_{i_{n+1}} = f(X_{i_n}, \lambda_i) \tag{1}$$

that in this system, $x_i = \{x_i, \dots, x_{ik}\} \in R^k$ determines state variable of ith cell and $\lambda_i = \{\lambda_i, \dots, \lambda_{ip}\}$ is a parameter's vector. A network with N cells is modeled by a system as minus equations as

$$X_{i_{n+1}} = f(X_{i_n}, \lambda_i) + \sum_{j \to i} \alpha_{ij} h(X_{i_n}, X_{j_n}) \tag{2}$$

where h is a coupling j cells which are coupled with i cells $(1 \le i \le N)$ and α_{ij} is a determiner coupling durability. Consider that f is independent from i because the cells are supposed to be similar. The same as above, h is an independent form i, j by coupling. Moreover, if we imagine $x = \{x_1, \dots, x_N\}$ as a network state variable, we can write (2) as a simpler form of

$$X_{n+1} = f(X_n, \lambda) \tag{3}$$

Based on what Dellnitz et al. [18] have maintained in their study, we have distinguished between the general symmetric and local symmetric. $L \subset O(k)$ is a group of local or domestic symmetrics, if for all $l \in L$, we have

$$f(lX_i) = lf(X_i) \tag{4}$$

When the local symmetric is generated by f, the general symmetric would be stimulated via a coupling pattern. In fact, $\sigma \in O(N)$ represents a group of general symmetrics in the network if for all $\sigma \in S$ we have

$$F(\sigma X_i) = \sigma F(X_i) \tag{5}$$

Considering coupling h, this possibility is for all local l symmetric to be a symmetric base on network equation (2). Specifically, when we have $l \in L$, the activity of l in each cell is a symmetric, for a coupling we will have:

$$\begin{aligned} h(lX_i, X_j) &= h(X_i, X_j) \\ h(X_i, lX_j) &= lh(X_i, X_j) \end{aligned} \tag{6}$$

Then we call this coupling as "wreath product coupling." To compose a continuous network based on (2), we assume the following wreath product coupling:

$$h(x_i, x_j) = |x_j|^m x_i \tag{7}$$

We have $0 < m < 1$, $\alpha_{ij} = -y$ that $y > 0$, we assume a network by three cells with the following equation:

$$\begin{aligned} x_n &= \lambda_1 x_n - x_n^3 - \gamma |y_n|^m x_n \\ y_n &= \lambda_2 y_n - y_n^3 - \gamma |z_n|^m y_n \\ z_n &= \lambda_3 z_n - z_n^3 - \gamma |x_n|^m z_n \end{aligned} \tag{8}$$

As demonstrated in Fig. 2, this system has three cells. In each moment, one cell exists in chaotic behavior

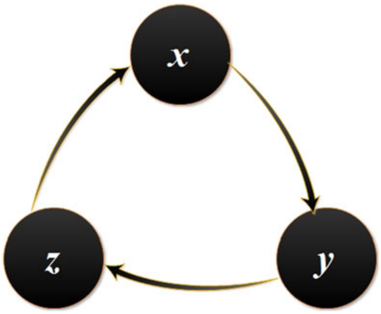


Fig. 2 Turning of chaotic state between 3 cells

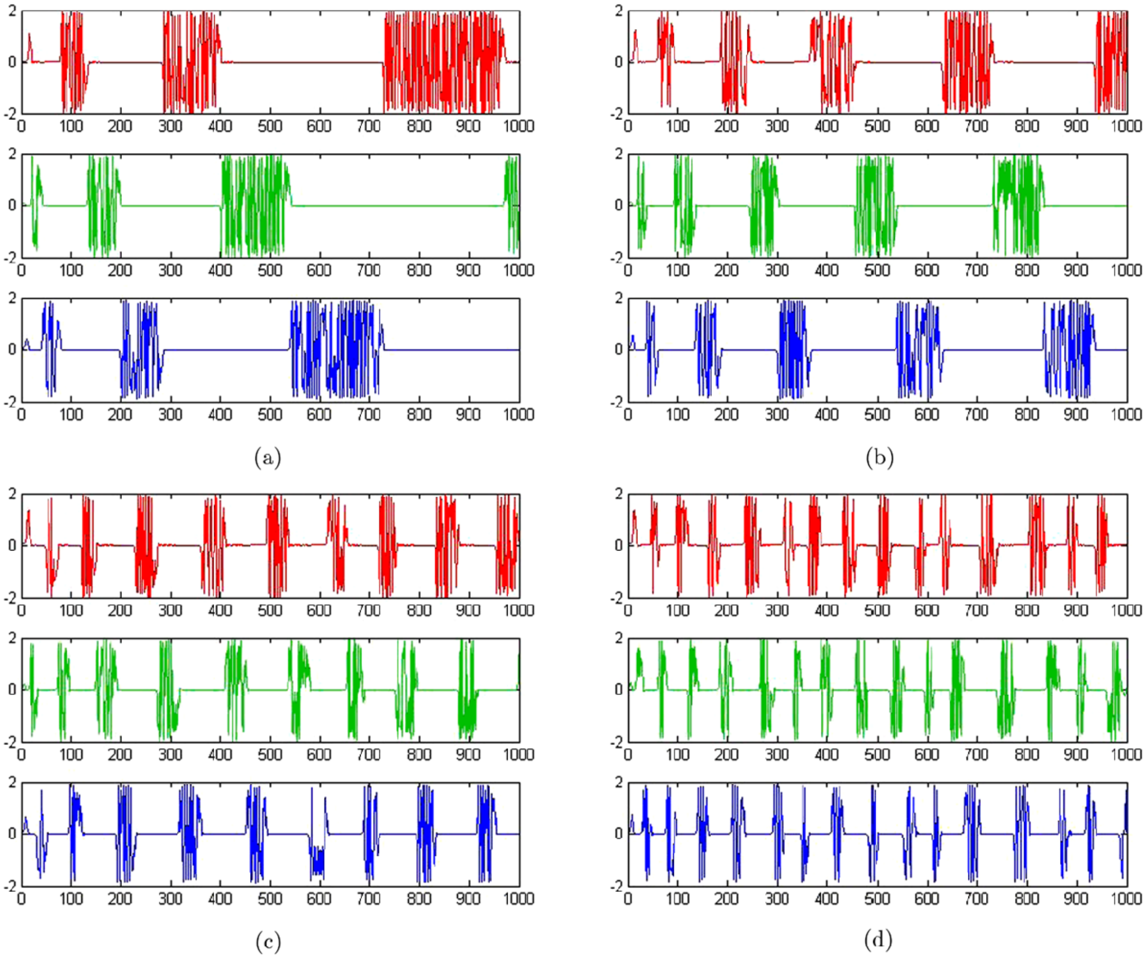


Fig. 3 Cycling chaotic behavior in a network with three discontinuous cells close to each other and with different values of m. $m = 0.2$ (**a**), $m = 0.25$ (**b**), $m = 0.3$ (**c**), $m = 0.35$ (**d**)

and two cells are in a steady state, and this condition will be exchanged between the cells.

Durability of γ coupling and m parameter is of a high significance for initiating the cycling behavior. From Fig. 3, it can be understood that increasing m parameter causes an increase in cycling, velocity in alternative chaotic. In other words, the time will be decreased for every cell in chaotic state.

3 The method

3.1 Secret key

In cycling chaos system, the initial value x_1, y_1, z_1, and m could be considered as the secret keys. In the present paper, for image encryption, a 120-bit (15 characters) secret key is applied. Let k be the secret key, which could be defined as

$$k = k_{120}, k_{119}, k_{118}, \ldots, k_1 \tag{9}$$

Then the initial value could be computed as demonstrated in Table 1.

3.2 DNA operations

A DNA sequence consists of four nucleic acid bases T (thymine), A (adenine), C (cytosine), G (guanine), where A and T are complementary, while G and C are complementary. Because of the fact that 00 and 11 are complementary and 01 and 10 are also complementary, four bases A, G, C, and T could be en-

Table 1 Initialization using secret key

Initial value	Interval	New key
$x_1 = (\frac{\text{sum of } K_1 \text{ bits}}{35} \times 4) - 2$	$-2 < x_1 < 2$	$k = k_{120}, k_{119}, \ldots, k_{86}$
$y_1 = (\frac{\text{Decimal value of } K_2}{2^{35}} \times 4) - 2$	$-2 < y_1 < 2$	$k = k_{85}, k_{84}, \ldots, k_{51}$
$z_1 = (\frac{\text{sum of } K_3 \text{ bits}}{35} \times 4) - 2$	$-2 < z_1 < 2$	$k = k_{50}, k_{49}, \ldots, k_{16}$
$m = (\frac{\text{Decimal value of } K_4}{2^{15}} /5) - 0.1$	$0.1 < m < 0.3$	$k = k_{15}, k_{14}, \ldots, k_1$

Table 2 8 kinds of coding schemes satisfy the Watson–Crick complement rule

Watson–Crick complement 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 3 DNA algebraic operations

(a) Addition					(b) Subtraction				
+	A	C	G	T	−	A	C	G	T
A	A	C	G	T	A	A	C	G	T
C	C	G	T	A	C	C	G	T	A
C	G	T	A	C	C	G	T	A	C
G	T	A	C	G	G	T	A	C	G

coded with these binary codes. Only 8 kinds of the coding schemes satisfy the Watson–Crick complement rule [19, 20] (see Table 2).

Obviously, image pixels are ranged between 0 and 255 grey-level. In the binary form, it has an 8 bit that could be encoded by these four acids. For instance, 141 is shown as 10001101 in binary, and it could be encoded by these acids as "CATG" (i.e., consider A, T, G, and C are 00, 11, 01, and 10, respectively). Two algebraic operations exist on the DNA sequences [19]:

1. Addition.
2. Subtraction.

These operations could be observed in Table 3. It worth noting that in every column or row, the base is unique. It shows that the results of these operations are entirely unique.

3.3 The proposed method

In this section, we describe the method that is proposed in this study. At the first step, the main image should be converted to a DNA image through converting the images pixel values to the binary form and replacing "00" to "A," "11" to "T," "01" to "C," and "10" to "G." After that, using cycling chaos, the obtained image is scrambled and a mask DNA image is produced and then added to the main DNA image using DNA addition operation (modify image). At the final step, the result should be converted into the binary image by replacing "A" to "00," "C" to "01," "G" to "10," and "T" to "11." Figure 4 shows the work flow of the proposed method.

3.3.1 Scrambling procedure

As it was mentioned before, cycling chaos contains three chaotic cells, however, in each situation, one of the cells is chaotic ($-2 <$ value < -0.2 and $0.2 <$ value < 2), and the other two cells are stable ($-0.2 <$ value < 0.2).

Step 1: Define x_{img} as image's rows and y_{img} as image's columns.

Step 2: Generate three chaotic sequences $X = x_0, x_1, \ldots, x_{\text{img}}$, $Y = y_0, y_1, \ldots, y_{\text{img}*4}$, $Z = z_0, z_1, \ldots, z_M$ using cycling chaos and initial values x_0, y_0, z_0, m.

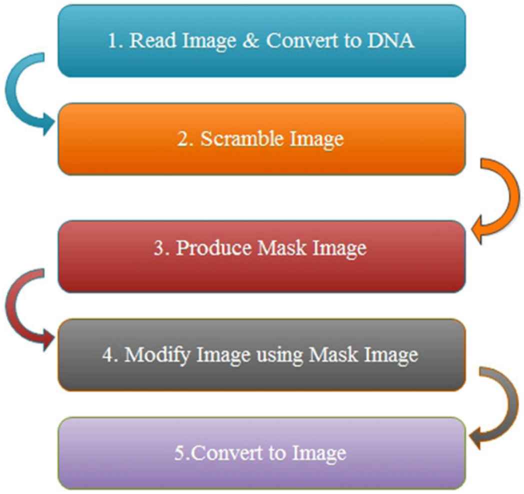

1. Read Image & Convert to DNA
2. Scramble Image
3. Produce Mask Image
4. Modify Image using Mask Image
5.Convert to Image

Fig. 4 The proposed method work-flow

Step 3: Divide image to M equal blocks.
Step 4: Normalize Z matrix between 1 to M and rearrange blocks by new sequences.
Step 5: Reconstruct Y and X to row matrix and column matrix, respectively; and normalize X between 1 to x_{img} and Y between 1 to $y_{\text{img}*4}$. Then calculate $X \times Y$ that each value is an ordered pair (x, y), and then rearrange each blocks pixels via new x and y positions.

3.3.2 *Producing mask DNA image and modify*

In the proposed method, producing mask image is a very simple task. Firstly, generate the chaotic sequences $X = x_0, x_1, \ldots, x_{x_{\text{img}} * y_{\text{img}} * 4}$ by cycling chaos and initial values x_0, y_0, z_0, m. Then generate each pixel value using (10):

$$\mathit{Pixel\ value} = \begin{cases} A & -2 < X \leq -1.1 \\ C & -1.1 < X \leq -0.2 \\ G & 0.2 \leq X < 1.1 \\ T & 1.1 \leq X < 2 \end{cases} \tag{10}$$

After production of the mask image, using the DNA addition operation, it could be added to the main DNA image. The decryption procedure is operated very similar to the encryption one; just it should be noted that DNA Subtraction should be performed instead of the DNA addition.

4 Experimental results

Some numerical experiments were carried out in order to evaluate the robustness of the proposed method against common attacks such as statistical, exhaustive, and cryptanalytic attacks. The experiments are performed using a set of 10 well-known images accessible in the USC-SIPI Image Database (Available online at: http://sipi.usc.edu/database/).

4.1 Key space analysis

To resist the exhaustive attacks, any effectual image encryption method must be provided with a large key space. In the proposed method, the keys have been selected from $2^{120} \simeq 1.329228 \times 10^{36}$ possible keys that is adequately large to be resistive against the exhaustive attacks. Also, the secret key is altered at the time of encryption process, which led to an increase in the key space.

4.2 Statistical analysis

To verify the stability of the proposed method against statistical attacks, the correlation and histogram between adjacent pixels is computed for some common images.

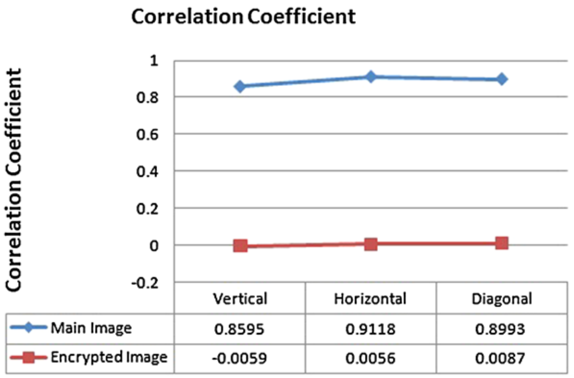
4.2.1 *Correlation coefficient*

Because of the high correlation among adjacent pixels in the original image, the encrypted image should have a low correlation to be able to resist the statistical attacks. 4,096 pairs of the neighboring pixels are chosen in a random way from the encrypted and original images. Then (11) is used for calculating the correlation coefficients. The way the pixels' grey value has been distributed is illustrated in Fig. 5. Also, the vertical, horizontal, and diagonal and the correlation coefficient calculated for the original and encrypted images are presented in Fig. 6.

$$\begin{aligned} E(x) &= \frac{1}{N}\sum_{i=1}^{N} x_i \\ D(x) &= \frac{1}{N}\sum_{i=1}^{N} \left(x_i - E(x_i)\right)^2 \\ \operatorname{cov}(x, y) &= \frac{1}{N}\sum_{i=1}^{N} \left(x_i - E(x_i)\right)^2 \left(y_i - E(y_i)\right)^2 \\ r_{xy} &= \frac{\operatorname{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}} \end{aligned} \tag{11}$$

4.2.2 *Histogram analysis*

The image histogram is a form of graphical representation of the pixels number for each grey-level. In all effective image encryption methods, the encrypted image histogram should be uniformed. It means that it is very probable to occur each grey-level within the encrypted image. Figures 7(a) and 7(b) show the plain image and encrypted image. The histograms of three channels for two images are demonstrated in Figs. 7(c), 7(d), 7(e), 7(f), 7(g), and 7(h).



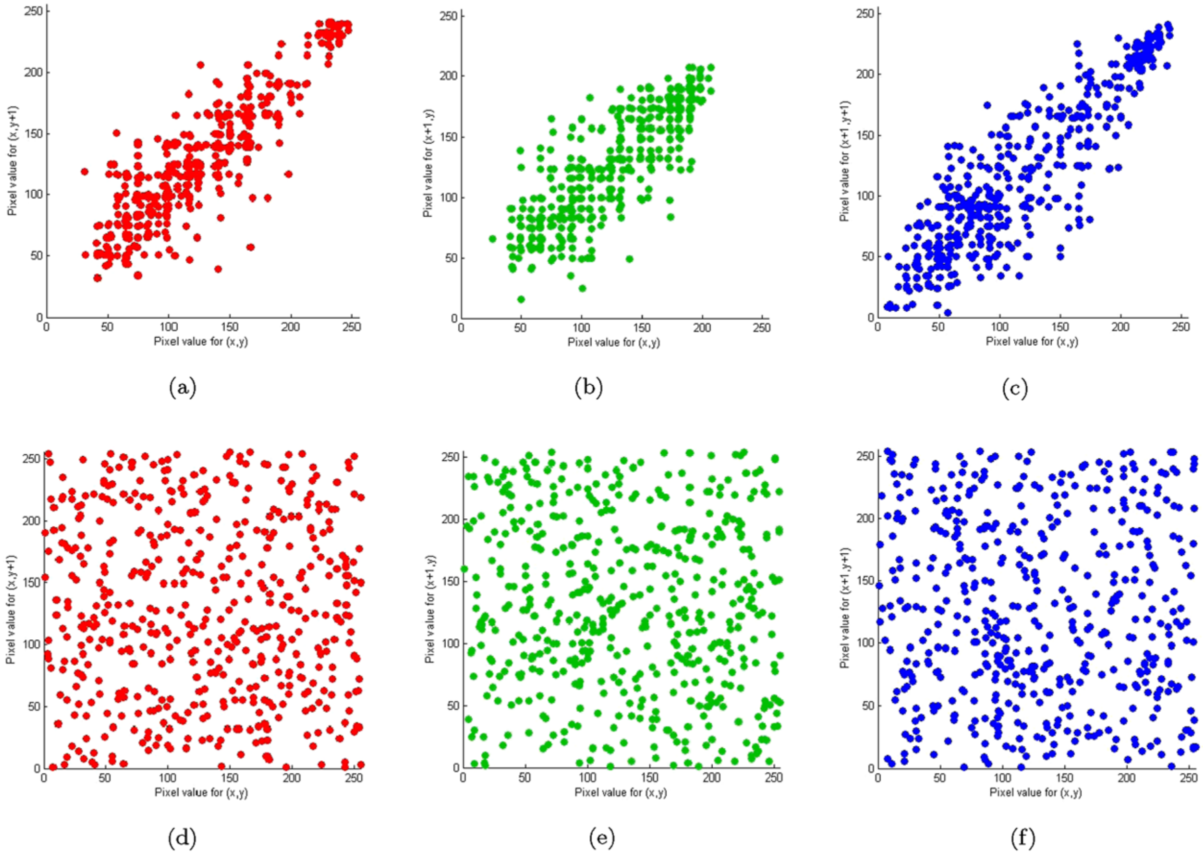
	Vertical	Horizontal	Diagonal
◆ Main Image	0.8595	0.9118	0.8993
■ Encrypted Image	-0.0059	0.0056	0.0087

Fig. 5 Vertical, horizontal, and diagonal correlation coefficient

4.3 Information entropy

The degree of uncertainty could be measured in the system via a parameter known as information entropy [21]. It also could be used to express the uncertainties within the image information. The information entropy is also able to measure the grey values distribution in the image. The greater information entropy is a sign for the fact that the grey values distribution is more uniform. The information entropy is configured by (12).

$$H(S) = \sum_{i=0}^{2N-1} P(s_i)\log\left(\frac{1}{P(s_i)}\right) \qquad (12)$$

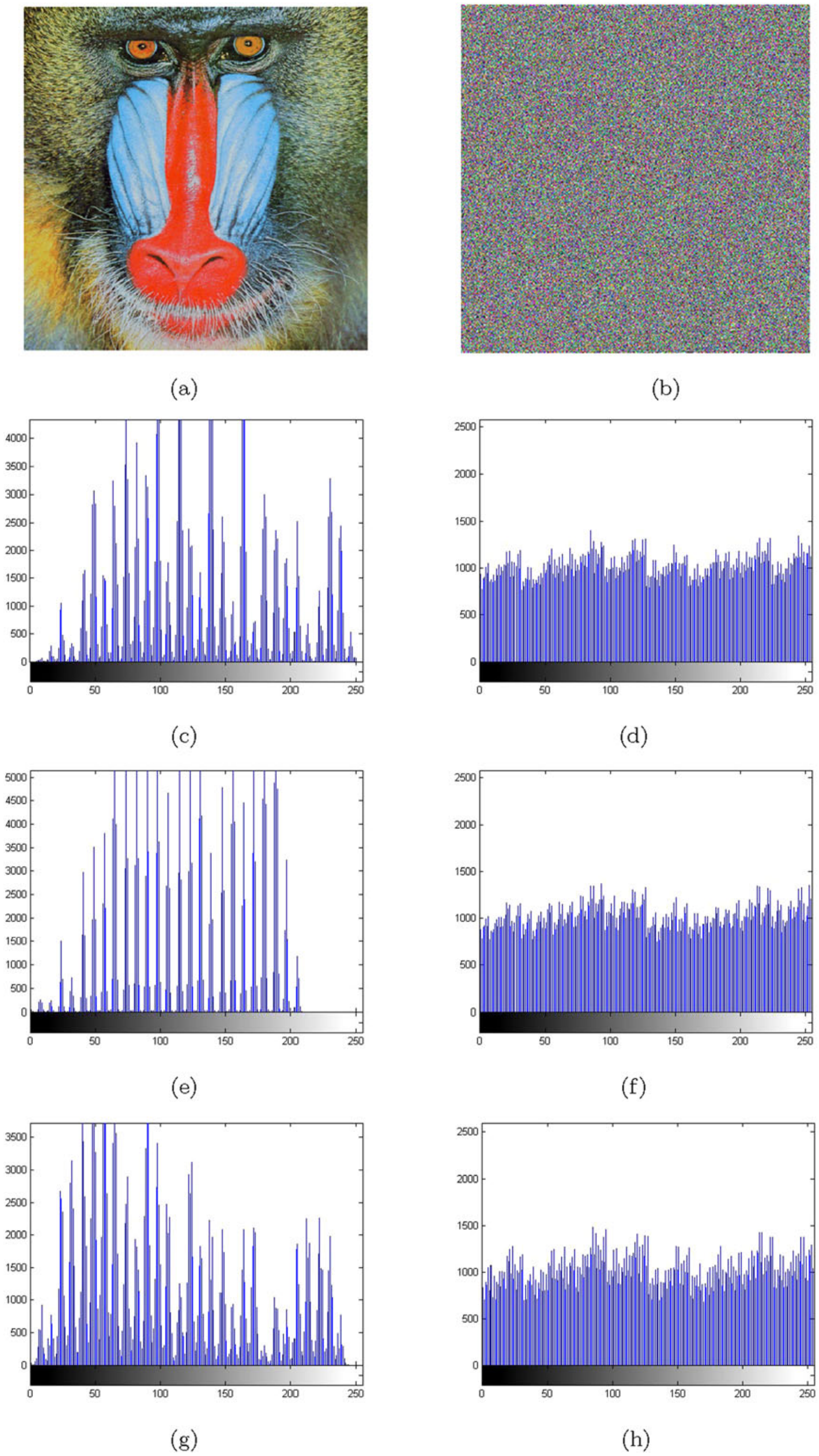


(a) (b) (c)

(d) (e) (f)

Fig. 6 Correlation coefficient between two adjacent pixels in main image and encrypted image

Fig. 7 Main image and encrypted image and their histogram in the *red*, *green*, and *blue* channel (Color figure online)



The perfect value of the information entropy in image is 8. The information entropy computed for the proposed method is 7.9919 that is very competitive when it is compared to the ideal value.

Table 4 NPCR and UACI calculated for 10 test images

Name	Size	*NPCR*	*UACI*
Baboon	512 × 512	99.7091	33.3056
Peppers	512 × 512	99.7065	33.3247
Lena	512 × 512	99.6249	33.2404
Girl	256 × 256	99.6348	33.2656
House	256 × 256	99.6354	33.2546
Tree	256 × 256	99.6512	33.1525
Jelly Bean	256 × 256	99.7172	33.1672
Tiffany	512 × 512	99.6724	33.2675
Splash	512 × 512	99.7599	33.2210
Sailboat	512 × 512	99.7772	33.2061

4.4 Differential attack

In all methods proposed for image encryption, a great difference has occurred between the original image and the encrypted version. For evaluating the effectiveness of changing one pixel of the original image onto that of the encrypted one, the Number of Pixels Change Rate (NPCR) is calculated as follows:

$$NPCR = \frac{\sum_{ij} D(i,j)}{W \times H} \times 100 \tag{13}$$

where W and H stand for the width and height of the encrypted image, respectively, and $D(i,j)$ is

$$D(i,j) = \begin{cases} 0 & \text{if } C(i,j) = \acute{C}(i,j) \\ 1 & \text{if } C(i,j) \neq \acute{C}(i,j) \end{cases} \tag{14}$$

where C and $\acute{C}$ are two images that are encrypted with 1 pixel difference in their original images. Also, Unified Average Changing Intensity (UACI) is calculated for the two encrypted images:

$$UACI = \frac{1}{W \times H}\left[\sum_{ij} \frac{|C(i,j) - \acute{C}(i,j)|}{255}\right] \times 100 \tag{15}$$

The results are tabulated in Table 4 and demonstrate the results obtained from the proposed method.

5 Conclusions

In this paper, using DNA sequences and cycling chaos, a method was proposed for secure image encryption. DNA sequences and cycling chaos have been applied to achieve a high security in image encryption. Employing the cycling chaos for encrypting the images has caused various secure image encryption methods to emerge. The proposed method effectiveness is evaluated on a completely known test image database where the results demonstrate a decrease in the correlation degree between two adjacent pixels and a significant increase in the uncertainty of the system. These features are assessed by correlation coefficient and information entropy. The proposed method robustness against different attacks is tested using UACI and NPCR. The proposed method has been found not only strong against the common attacks, but also simple at the time of implementation. Another important feature of this method is the fact that it does not require much computational effort.

References

1. Ye, G., Wong, K.-W.: An efficient chaotic image encryption algorithm based on a generalized Arnold map. Nonlinear Dyn. **69**, 2079–2087 (2012)
2. Mirzaei, O., Yaghoobi, M., Irani, H.: A new image encryption method: parallel sub-image encryption with hyper chaos. Nonlinear Dyn. **67**, 557–566 (2012)
3. SaberiKamarposhti, M., Yaghoobi, M.: A new approach for image encryption using chaotic logistic map. In: ICACTE, Phuket Thailand, pp. 585–590 (2008)
4. Asadollahi, H., SaberiKamarposhti, M., Moosavian Jandaghi, E.: Image encryption using cellular automata and Arnold cats map. Aust. J. Basic Appl. Sci. **5**(8), 587–593 (2011)
5. Wang, X.-Y., Yang, L., Liu, R., Kadir, A.: A chaotic image encryption algorithm based on perceptron model. Nonlinear Dyn. **62**, 615–621 (2010)
6. Narendra Singh, A.S.: Gyrator transform-based optical image encryption, using chaos. Opt. Lasers Eng. **47**, 55 (2009)
7. Zhou, N., Wang, Y., Gong, L., Chen, X., Yang, Y.: Novel color image encryption algorithm based on the reality preserving fractional Mellin transform. Opt. Laser Technol. **44**, 2270–2281 (2012)
8. Wu, J., Luo, X., Zhou, N.: Four-image encryption method based on spectrum truncation, chaos and the MODFrFT. Opt. Laser Technol. **45**, 571–577 (2013)
9. Liu, Z., Li, S., Liu, W., Wang, Y., Liu, S.: Image encryption algorithm by using fractional Fourier transform and pixel scrambling operation based on double random phase encoding. Opt. Lasers Eng. **51**, 8–14 (2013)
10. Pareek, N.K., Patidar, V., Sud, K.K.: Image encryption using chaotic logistic map. Image Vis. Comput. **24**, 926934 (2006)
11. Shyu, S.J.: Image encryption by random grids. Pattern Recognit. Lett. **40**, 18 (2007)

12. Behnia, S., Akhshani, A., Mahmodi, H., Akhavan, A.: A novel algorithm for image encryption based on mixture of chaotic maps. Chaos Solitons Fractals **35**, 12 (2008)
13. Huang, C.K., Nien, H.H.: Multi chaotic systems based pixel shuffle for image encryption. Opt. Commun. **282**, 5 (2009)
14. Zhang, Q., Guo, L., Wei, X.: Image encryption using DNA addition combining with chaotic maps. Math. Comput. Model. **52**, 2028–2035 (2010)
15. Li, H., Wang, Y.: Double-image encryption based on discrete fractional random transform and chaotic maps. Opt. Lasers Eng. **49**(7), 753–757 (2011)
16. Wei, X., Guo, L., Zhang, Q., Zhang, J., Lian, S.: A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system. J. Syst. Softw. **85**, 290299 (2012)
17. Palacios, A., Juarez, H.: Cryptography with cycling chaos. Europhys. Lett. A **303**, 345–351 (2002)
18. Dellnitz, M., Field, M., Golubitsky, M., Ma, J., Hohmann, A.: Cycling chaos. Int. J. Bifurc. Chaos **5**(4), 1243 (1995)
19. SaberiKamarposhti, M., AlBedawi, I., Mohamad, D.: A new hybrid method for image encryption using DNA sequence and chaotic logistic map. Aust. J. Basic Appl. Sci. **6**(3), 371–380 (2012)
20. SaberiKamarposhti, M., AlBedawi, I., Mohamad, D.: A new algorithm for image encryption using DNA sequence and cycling chaos. Aust. J. Basic Appl. Sci. **6**(3), 381–392 (2012)
21. Shannon, C.E.: Communication theory of secrecy systems. Bell Syst. Tech. J. **28**, 656–715 (1949)