



An Innovative Approach: Image Encryption with Chaotic Maps using DNA Addition Operation

Manisha Raj¹, Shelly Garg²
Indus Institute of Engineering and Technology
Kinana, Haryana, India

Abstract: Encryption technology is an important measure to ensure the security of digital image, this paper's main purpose is to research how to encrypt images by chaos. In this paper, five chaotic maps are compared and noise effects are observed on image. Firstly, we use the image encryption algorithm to convert original image to encrypted image. Now we apply noise on the encrypted image and then decrypt cipher image with noise back to original image. The simulation experimental results show that Cross Chaotic map has got best results. Also, noise has a little effect on original image and can easily be received by the receiver.

General Terms: Chaos theory, chaotic sequences, Correlation coefficient, Secret keys, Grey histogram, Image noise.

Keywords: Image Encryption, Cross Chaotic map, Logistic map, Duffing Map, Gingerbreadman Map, Tinkerbell Map, DNA addition

I. Introduction

Since the computer networks have been widely applied, transmission for digital image over Internet has become more and more popular. However, due to the openness and sharing of networks, make the security of digital image has a serious threat in the process of transmission. Consequently, reliable security in storage and transmission of digital images is needed in many applications, including both public and private services such as medical imaging systems and military information systems.

Chaotic system is a deterministic nonlinear system that has many important properties, such as aperiodic, sensitive dependence on initial conditions and system parameters, density of the set of all periodic points and topological transitivity, etc. It provides a new approach for cryptography and a large number of chaos-based image cryptosystems have been suggested and investigated during the past decade[4-8]. It is neither periodic nor convergent, but significantly sensitive to its initial conditions, so the information encryption technologies which adopt chaotic signals have a broad application future. The basic idea of chaos-based image encryption scheme is implementation both position permutation and grayscale substitution on an image by using chaotic key stream and the security depends on the unpredictability of the pseudorandom key stream. The chaos-based image encryption scheme has the advantages of strong against known/chosen plaintext attack and fast encryption speed. Bimolecular computing has emerged as an interdisciplinary field that draws together molecular biology, chemistry, computer science and mathematics. Our knowledge on DNA nanotechnology and bimolecular computing increases exponentially with every passing year.

II. BASIC THEORY

A. Chaotic Map

In this paper we used five chaotic maps: Logistic map, cross chaotic map, duffing map, tinkerbell map, gingerbread man map.

A.1. 2 D Logistic Map

One of the most known and widely used chaotic systems is the 1 D Logistic map, which is defined as follows,

$$f(x) = \mu x(1-x) \quad x \in (0,1) \quad (1)$$

Where μ is the control parameter. The research result shows that the system is in chaos on condition that $3.569 < \mu < 4.0$. Although Eq. (1.1) is simple, it can embody all the nature of nonlinearity phenomenon. Compared with a complicated chaotic map, the basic Logistic map (1) has a fast iteration speed. Therefore, based on this chaotic map, an image encryption algorithm can have a high efficiency and more fit for practical communication.^[32]

$$\begin{cases} x_{i+1} = \mu_1 x_i(1-x_i) + \gamma_1 y_i^2 \\ y_{i+1} = \mu_2 y_i(1-y_i) + \gamma_2 (x_i^2 + x_i y_i) \end{cases} \quad (2)$$

When

$$2.75 < \mu_1 \leq 3.4, \quad 2.75 < \mu_2 \leq 3.45,$$

$0.15 < \gamma_1 \leq 0.21$, $0.13 < \gamma_2 \leq 0.15$, the system is in chaotic state and can generate two chaotic sequences in the region $(0, 1]$. Here μ_1 , μ_2 , γ_1 , γ_2 are the control parameters of Eq.(1) set $\gamma_1 = 0.17$ and $\gamma_2 = 0.14$. 1 D logistic map can be described as follows

A.2. Cross Chaotic Map

In order to improve security and reduce calculation complexity than logistic map, the cross-chaotic map is defined as following:

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

$$y_{i+1} = \cos(k \cdot \cos^{-1} x_i), x, y \in [1, -1]$$

Where μ and k are the control parameters of the system, respectively. When $\mu=2$ and $k=6$, this system exhibits a great variety of dynamics behavior. [26]

A.3 Duffing Map

The Duffing map (also called as 'Holmes map') is a discrete-time dynamical system. It is an example of a dynamical system that exhibits chaotic behavior. The Duffing map takes a point (x_n, y_n) in the plane and maps it to a new point given by

$$\begin{aligned} x_{n+1} &= y_n \\ y_{n+1} &= -bx_n + ay_n - y_n^3. \end{aligned} \quad (4)$$

The map depends on the two constants a and b . These are usually set to $a = 2.75$ and $b = 0.2$ to produce chaotic behaviour. It is a discrete version of the Duffing equation.

A.4 Tinkerbell Map

The Tinkerbell map is a discrete-time dynamical system given by:

$$\begin{aligned} x_{n+1} &= x_n^2 - y_n^2 + ax_n + by_n \\ y_{n+1} &= 2x_n y_n + cx_n + dy_n \end{aligned} \quad (5)$$

Some commonly used values of a , b , c , and d are

$$a = 0.9, b = -0.6013, c = 2.0, d = 0.50$$

$$a = 0.3, b = 0.6000, c = 2.0, d = 0.27$$

Like all chaotic maps, the Tinkerbell Map has also been shown to have periods; after a certain number of mapping iterations any given point shown in the map to the right will find itself once again at its starting location.

A.3. Gingerbreadman map

In dynamical systems theory, the Gingerbreadman map is a chaotic 2D map. It is given by the transformation:

$$\begin{cases} x_{n+1} = 1 - y_n + |x_n| \\ y_{n+1} = x_n \end{cases} \quad (6)$$

B. Scheme for Encryption and Decryption of Image

B.1 DNA encoding and decoding: The information in DNA is stored as a code made up of four nucleic acid bases: adenine (A), guanine (G), cytosine (C), and thymine (T). DNA bases pair up with each other, A with T and C with G, to form units called base pairs, which are complementary to each other. As in the binary mathematics 0 and 1 are complement, so 00 and 11 are complement, similarly 01 and 10 are complement. In this paper we use 00=A, 01=C, 10=G and 11=T. In the 8 bit grey images each pixel is given by a DNA sequence of length 4. For example: If the first pixel value of the original image is 1 convert it into a binary stream is [10101101], by using abt DNA encoding rule to encode the stream, we can get a n sequence [TTGA]. Whereas use C, A, T, G to denote 00, 10, 11, respectively, and to decode above DNA sequence, can get a binary sequence [10101101].

B.2 Addition and subtraction algebraic operation for DNA sequences: Addition and subtraction operation for DNA sequences are performed according to traditional addition and subtraction in the Z2. For example, $11 + 10 = 01$, $01 - 11 = 10$. We use 00, 01, 10, 11 to denote A, C, G, T respectively. That is $G+T=A$, $A-C=G$

The details of addition and subtraction rule are shown in Table 1 and Table 2 respectively. In other words, the addition algebraic operation table is a double helix structure which has satisfied the Watson-Crick complement regulation. Subtraction is the inverse operation of addition, but whose structure is not double helix structure.

Table 1. Addition Operation

+	A	C	G	T
A	A	C	G	T
C	C	G	T	A
G	G	T	A	C
T	T	A	C	G

Table 2. Subtraction Operation

-	A	C	G	T
A	A	T	G	C
C	C	A	T	G
G	G	C	A	T
T	T	G	C	A

III. THE PROPOSED ENCRYPTION ALGORITHM

In this section, we will study the procedure of the image encryption based on DNA sequence addition operation in detail. Firstly we have to produce the secret keys using the original image and secondly, divide the original image into blocks and add these blocks by using DNA sequence addition operation and carry out DNA sequence complement operation. At last, decode the scramble DNA matrix to binary matrix by using the rule of A = 00, T = 01, C = 10, G = 11, and then reconstruct it to a image matrix.

A. Generation of secret sequences

For the generation of the secret sequences, a input of 8 bit grey image A as the original image, $A = A(a_{ij})$, $i = 1, 2, \dots, m$, $j = 1, 2, \dots, n$. Here, a_{ij} is the pixel value of image, (i, j) is the position of image, and (m, n) is the size of image. Using following formulas to calculate k_1 and k_2 .

$$k_1 = \frac{1}{256} \bmod \left(\sum_{i=1}^m \sum_{j=1}^n a_{ij}, 256 \right) \quad (7)$$

$$k_2 = \frac{1}{256} \bmod \left(\sum_{i=m/2}^m \sum_{j=1}^n a_{ij}, 256 \right) \quad (8)$$

Choose two initial values x_1, y_1 and four system control parameters $\mu_1, \mu_2, \mu_3, \mu_4$. Now calculate x_0, y_0 using the following pseudo code:

```

x0 = x1 + k1
if x0 > 1 then
x0 = mod(x0, 1)
else
x0 = x0
end

```

B. Algorithm Principle

This algorithm can be divided into following steps:

Step1: Convert the original image (m, n) matrix into binary matrix $(m, nx8)$ then use DNA encoded rule to obtain a matrix K of size $(m, nx4)$;

Step 2: Divide K into small blocks called cells $k\{i,j\}$, $i=1,2,\dots, m/4$, $j=1,2,\dots,n$. size of each cell is 4×4 ;

Step 3: Generate two chaotic sequences $X = \{x_0, x_1, \dots, x_{m/4}\}$, $Y = \{y_0, y_1, \dots, y_n\}$, using chaotic maps and initial values x_0, y_0 and control parameters of equations;

Step 4: Reconstruct X and Y to row matrix and column matrix respectively. Do multiply operation on X and Y, we get a matrix k' then convert it to binary matrix using Eq (9). Using DNA encoded matrix rule we got a DNA encoded matrix k' . Divide

matrix k' into small cells $k'\{i,j\}$ of size 4×4 ;

Step 5: Add $k\{i,j\}$ and $k'\{i,j\}$ according to DNA addition rule shown previously to obtain added cells as $B\{i,j\}$;

Step 6: Recombine these small cells $B\{i,j\}$, we will get a new matrix C;

Step 7: Again two chaotic sequences Z1 and Z2 are generated whose lengths are m and $nx4$. Reconstruct Z1 and Z2 to two matrices Z1 $(m, 1)$ and Z2 $(1, nx4)$. Do multiply operation, we get Z matrix whose size is $(m, nx4)$;

Step 8: Map the value of Z into $(0, 1)$ by $\bmod(Z, 1)$. Gets binary sequence matrix using following threshold function:

$$f(x) = \begin{cases} 0, & 0 < Z(i, j) \leq 0.5 \\ 1, & 0.5 < Z(i, j) \leq 1 \end{cases} \quad (9)$$

Step 9: If $Z(i,j) = 1$, $C(i,j)$ is complemented, otherwise it is unchanged. Here, we get a complemented matrix P;

Step 10: carry out inverse process of step 1 for matrix P, we will obtain the real matrix D. here D is our encrypted image; Decryption can be done by moving from step 10 to step 1, except addition operation is replaced by subtraction operation. Receiver obtains secret keys from sender.

IV. EXPERIMENT RESULT

In this paper we used standard 256×256 grey image Lena as the original image, use Matlab 7.0.1 to simulate experiment. Set $x_1 = 0.89$, $y_1 = 0.29$. In case of logistic map we have 6 secret keys $x(0) = 0.89$, $y(0) = 0.29$, $\mu_1 = 3.4$, $\mu_2 = 2.784$, $\mu_3 = 3.7092$, $\mu_4 = 3.7109$. Cross chaotic map also has 6 secret keys $\mu_1 = 2$, $\mu_2 = 1.9$, $x(0) = 0.7199$, $y(0) = 0.7654$, $k_1 = 6$, and $k_2 = 5$.

In case of Duffing map, four secret keys $x(0) = 0.89$, $y(0) = 0.29$, $a = 2.75$, $b = 0.2$. Tinkerbell map has six secret keys $x(1) = 0.72$, $y(1) = 0.64$, $a = 0.9$, $b = 0.6013$, $c = 2$, $d = 0.5$. The Gingerbreadman map has 2 secret keys $x_1 = 0.7298$ and $y_1 = 0.7654$. Figure 1(a) shows the original image, the encrypted image of cross chaotic map, logistic map, duffing, tinkerbell, and gingerbreadman map are shown in figure 1(b), (c), (d), (e), (f) respectively and figure 1(g) shows decrypted image. Here, the cross chaotic map shows the best encryption effect on image.

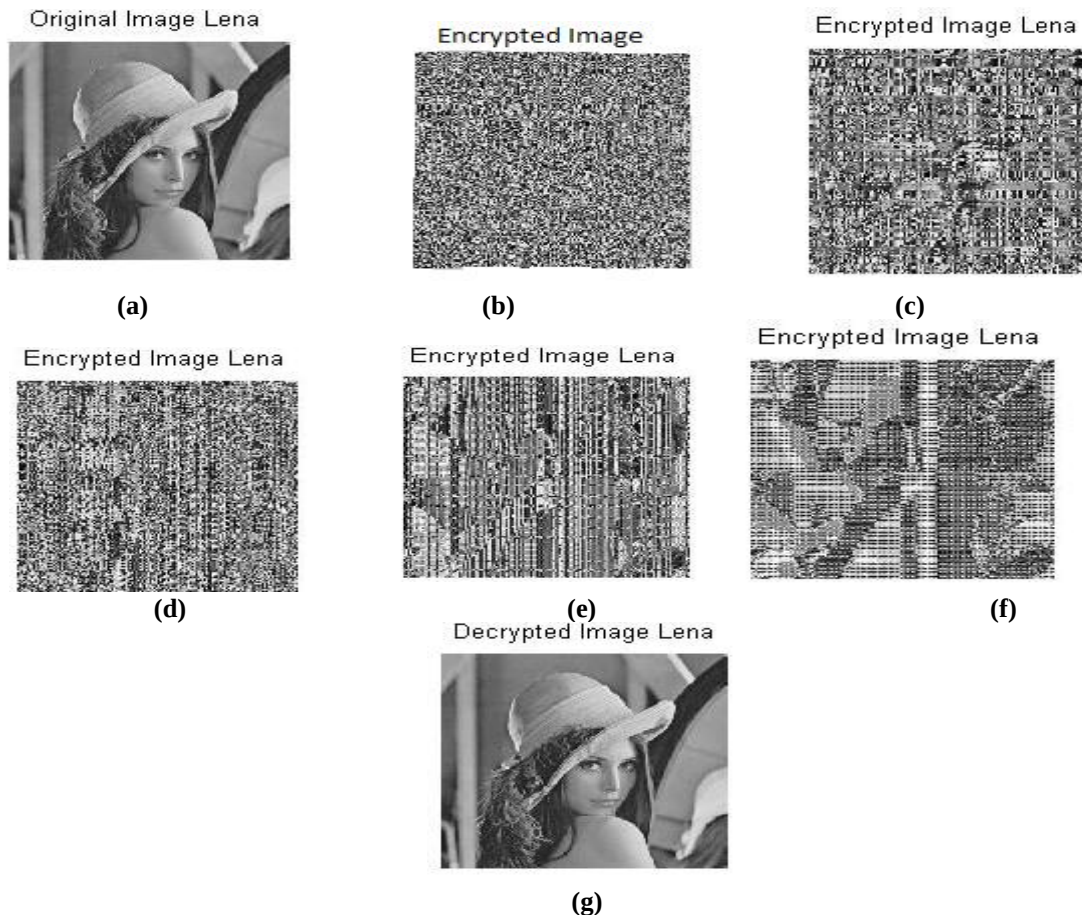


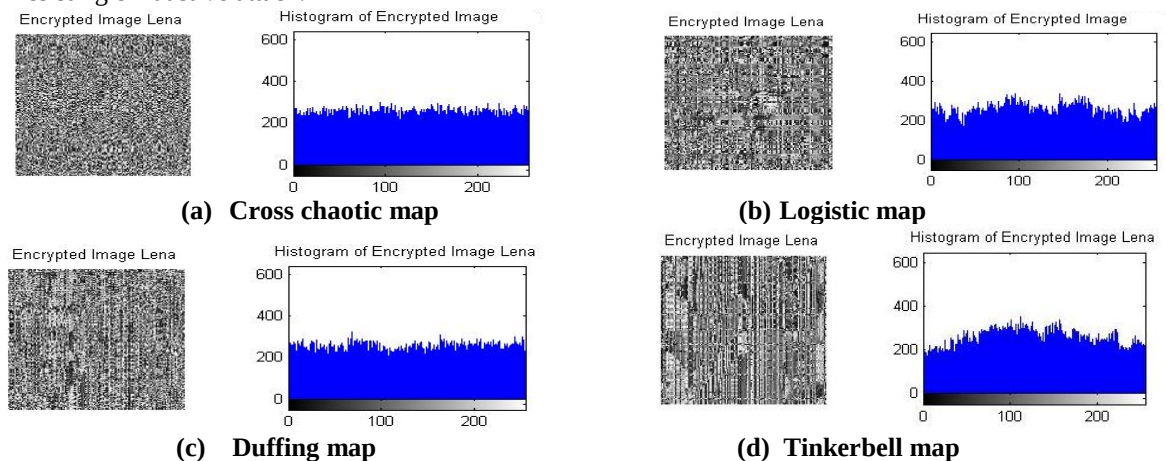
Figure 1: (a) the original image (b) Encrypted image (cross chaotic map) (c) logistic map (d) duffing map (e) Tinkerbell map (f) Gingerbreadman map (g) Decrypted image

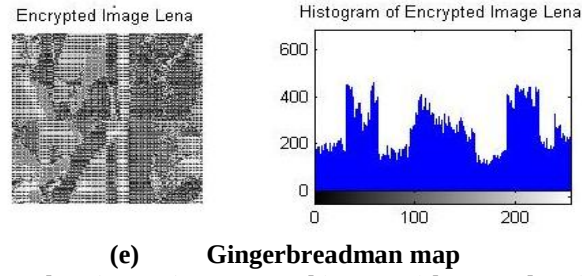
V. THE SECURITY AND ANALYSIS

A good encryption algorithm should resist all kinds of known attacks, such as exhaustive attack, statistical attack and differential attack, etc. In this section, we will discuss the security analysis on the proposed encryption scheme

A. Ability of resisting exhaustive attack

A.1 Key sensitivity analysis: Chaotic maps are highly sensitive to initial condition and system control parameters. If there is a minute change, then decrypted image will no longer be similar to original image. Some secret key tests are shown here. Figure 2 (a), (b), (c), shows the decrypted image and corresponding histogram with wrong secret key. Here the correct key is $x(0)=0.7199$ and the incorrect key is $x'(0)=0.71990000000001$. We can see that the histogram of the decrypted images are fairly uniform and the decrypted images are different from the original image. The sensitivity of the other parameters (secret keys) is also same, we have not shown it. Based on the above argument, our algorithms are sensitivity to the secret key which demonstrates it has ability of resisting exhaustive attack.





(e) Gingerbreadman map
Figure 2 sensitivity to secret key (0.7199), Decrypted image with secret key (0.719900000000001) and corresponding histogram (a) cross chaotic map (b) logistic map (c) Duffing map (d) Tinkerbell map (e) Gingerbreadman map

B. Ability of resisting statistical attack

B.1 Histogram analysis: Histogram shows the number of pixels for any grey value in the image. Considering the statistical analysis of the original image and the encrypted image. Figure 3 (a), (b), (c), and (d), show the grey-scale histograms of the original image and the encrypted images (of Duffing, Tinkerbell, and Gingerbreadman map) respectively. Comparing all the histograms we find that pixel grey values of the original image are concentrated on some values, but the histogram of the encrypted images is very uniform, and that the encrypted images transmitted do not provide any suspicion to the attacker, which can strongly resist statistical attacks. Grey histogram of cross chaotic map shows the best results.

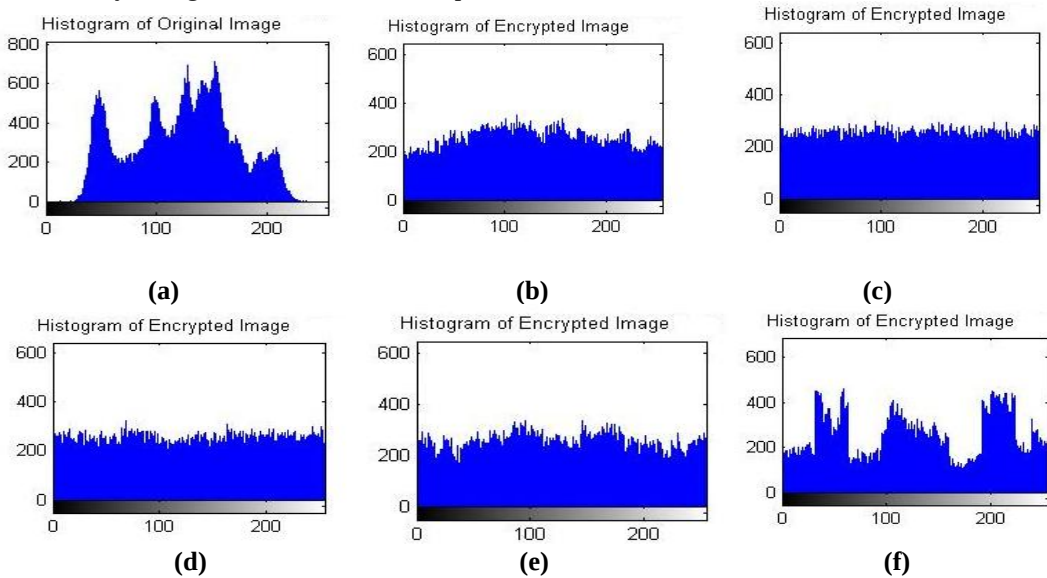


Figure 3- The grey histogram of the original image and the encrypted image. (a) shows grey histogram of original image and (b), (c), (d), (e), (f) shows grey histogram of encrypted image of cross chaotic map, logistic map, Duffing map, Tinkerbell map, Gingerbreadman map respectively.

B.2 Correlation coefficient analysis: In this section the horizontal, vertical and diagonal correlation coefficient of pixels studied. To do this we choose 2000 pair of adjacent pixels (horizontal, vertical, and diagonal) from original image and encrypted image. To test the correlation between two adjacent pixels in plain image and encrypted image, we can use formula of correlation coefficient are:-

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

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

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

$$\gamma(x, y) = \frac{cov(x, y)}{\sqrt{D(x)} \cdot \sqrt{D(y)}}$$

Where x and y are grey value of two adjacent pixels in the image, $cov(x, y)$ is covariance, $D(x)$ is variance, $E(x)$ is mean. Figure 4 (a), (b), (c), (d), and (e) shows the correlation of two horizontally adjacent pixels of original image and encrypted images of logistic, cross chaotic, Duffing map, Tinkerbell map, Gingerbreadman map respectively. Here, we can see the correlation between the adjacent pixels is greatly reduced. Detailed analysis is shown in Table 3, 4, 5, and 6. From the results of Table 3 to 6, we find that the correlation coefficient of the adjacent pixels in encrypted image is very small. It can clearly be seen our algorithm can destroy the relativity effectively; the proposed image encryption algorithm has strong ability of resisting statistical attack.

Table 3-Cross Chaotic Map

Direction	Original image	Encrypted image
Horizontal	0.9484	-0.0576
Vertical	0.9910	0.0190
Diagonal	0.8885	-0.0117

Table 4-Logistic Map

Direction	Original image	Encrypted image
Horizontal	0.9484	0.0273
Vertical	0.9910	-0.0225
Diagonal	0.8885	-0.0229

Table 5-Duffing Map

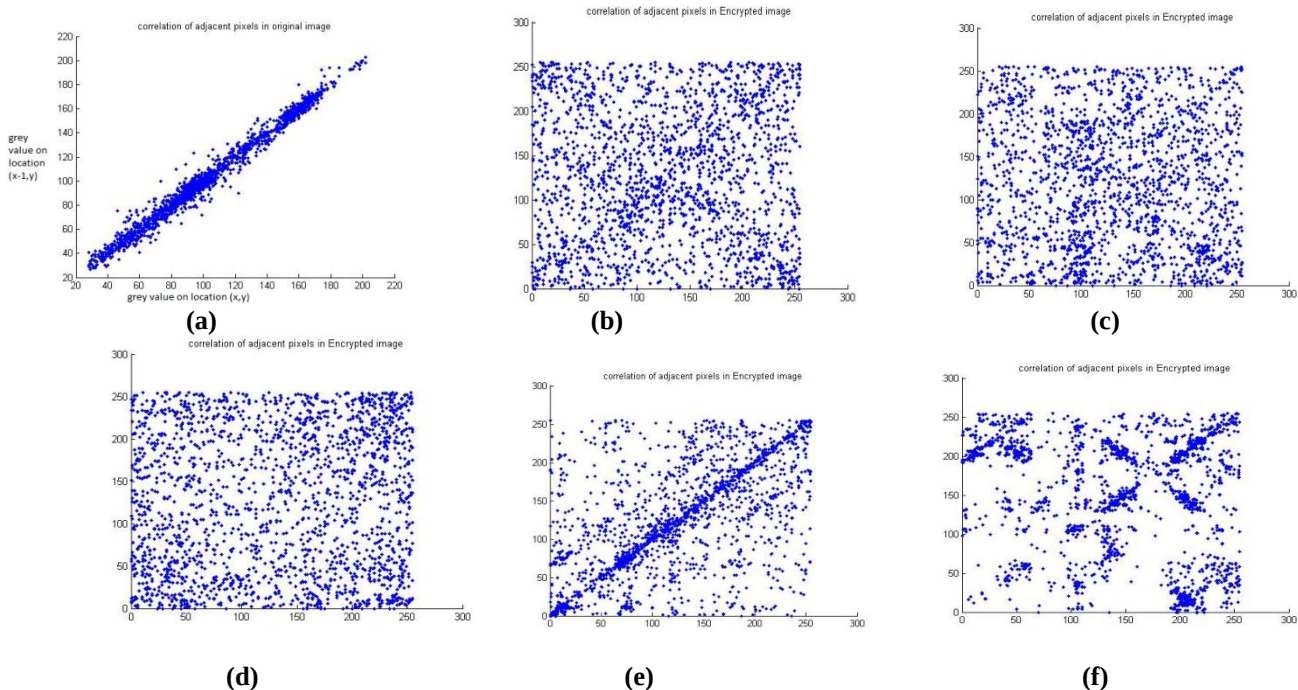
Direction	Original image	Encrypted image
Horizontal	0.9484	0.0091
Vertical	0.9910	0.0893
Diagonal	0.8885	0.0055

Table 6- Tinkerbell Map

Direction	Original image	Encrypted image
Horizontal	0.9484	-0.0065
Vertical	0.9910	0.5910
Diagonal	0.8885	-0.0460

Table 7-Gingerbreadman Map

Direction	Original image	Encrypted image
Horizontal	0.9484	0.4140
Vertical	0.9910	-0.1804
Diagonal	0.8885	-0.0329

TABLE 3, 4, 5, 6, 7 shows correlation coefficient of two adjacent pixels**Figure 4: correlations of two vertically adjacent pixels in (a) original image and in encrypted images of (b) cross chaotic map (c) logistic map (d) Duffing map, (e) Tinkerbell map, (f) Gingerbreadman maps****C. Ability of resisting differential attack**

As we know, in order to avoid the known-plaintext attack and the chosen-plaintext attack, a good encryption algorithm should have the desirable property which spreads the influence of a single plaintext bits over as much of the ciphertext as possible so as to hide the statistical structure of the plaintext. This means the small difference of the plaintext should be diffused to the whole ciphertext. Attackers often make a slight change for the original image, and use the proposed algorithm to encrypt for the original image before and after changing, through comparing two encrypted image to find out the relationship between the original image and the encrypted image. It is called differential attack. NPCR and UACI are the two criterion that examine the effect of changing the just one pixel in the original image. The number of pixels change rate (NPCR) is the pixel change rate at the encrypted image for changing a pixel at the original image and unified average changing intensity (UACI) is the mean of these changes. These two measures are defined as:

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

$$UACI = \frac{1}{W \times H} \left[\sum_{i,j} \frac{|E1(i,j) - E2(i,j)|}{255} \right] \times 100\%$$

Where E1 and E2 denote two encrypted images, respectively, W and H are the width and height of image, and the grayscale values of the pixels at grid (i, j) of E1 and E2 are labeled as E1(i, j) or E2(i, j), respectively.

The results are obtained by simulation for all four maps and are shown in Table 6. These results show that cross chaotic map has strongest ability of resisting differential attack.

Table 8. Ability to resist Differential attack

	Cross chaotic	Logistic	Duffing	Tinkerbell	Gingerbreadman
NPCR	99.9969	99.9969	99.9969	99.9969	99.9969
UACI	0.0018	0.0019	0.0021	0.0019	0.0019

VI. CONCLUSION

In this paper, we proposed a new image encryption algorithm based on DNA sequence addition. From above discussing, the pixel grey values of the original image are scrambled by DNA sequence addition operation and DNA complement operation completely. Through the experiment result and security analysis, we find that our algorithm has better encryption effect, larger secret key space and high sensitive to the secret key. We have compared five different chaotic maps: Logistic Map, Cross Chaotic Map, Duffing map, Tinkerbell map, Gingerbreadman map. Through the simulation results, histogram analysis and correlation analysis we have found out that Cross Chaotic Map, showed best results than other chaotic maps. It is sensitive to the secret keys, it has larger key space, and it gives best encrypted image. All these features show that our algorithm is very suitable for image encryption. We have also shown the effect of various noises on the image. Although the quality of image degrades due to the effect of noise but not to an extent that image cannot be recognized.

VII. FUTURE SCOPE

This paper mainly focused on comparison of chaotic maps and noise effects. Further research can be done on the following points:

- Noise effects can be removed by using suitable noise filtering scheme.
- Blurring effects can be deblurred from the image using suitable algorithms.

REFERENCES

- [1] Chen Wei, Zhangxin, "Image Encryption Algorithm Based on Henon Chaotic System", 2009 IEEE
- [2] Dong enzeng, Chen zengqiang, Yuan zhuzhi, Chen zaiping, A Chaotic Image Encryption Algorithm with The Key Mixing Proportion Factor, 2008 International Conference on Information Management, Innovation Management and Industrial Engineering, 2008, 169-174.
- [3] Hasan S. M. Al-Khaffaf, Abdullah Z. Talib, Rosalina Abdul Salam, "Removing Salt-and-Pepper Noise from Binary Images of Engineering Drawings", IEEE 2008
- [4] International conference on DNA computing and molecular programming Feb, 2009
- [5] Jun Peng, Shangzhu Jin, Yongguo Liu etc., A Novel Scheme for image Encryption Based on Piecewise Linear Chaotic Map, Cybernetics and Intelligent Systems, 2008, 1012-1016.
- [6] Ling Wang, Quen Ye Yaoqiang, Yongxing zou, Bo Zang, "An Image Encryption Scheme based on cross chaotic map" 2008 IEEE
- [7] Peng Fei, Shui Sheng Qiu, Long Min, "An Image Encryption Algorithm based on Mixed Chaotic Dynamics Systems and external keys, 2005 IEEE"
- [8] Rafael Gonzalez, Richard Woods, Steven Eddins, "Digital Image Processing using Matlab" Prentice Hall Publication 2003
- [9] Raymond H. Chan, Chung-Wa Ho, and Mila Nikolova, "Salt-and-Pepper Noise Removal by Median-type Noise Detectors and Detail-preserving Regularization", July 30, 2004
- [10] Robert L. Devaney, A First Course in Chaotic Dynamical Systems, Perseus Books Publishing, L.L.C.
- [11] Qiang Zhang, Ling Guo, Xianglian Xue, Xiaopeng Wei, An Image Encryption Algorithm Based on DNA Sequence Addition Operation, 2009 IEEE
- [12] Qian Wang, Qiang Zhang, Changjun Zhou, "A Multilevel Image Encryption Algorithm Based on Chaos and DNA Coding", 2009 IEEE.