Image Encryption using Chaotic Maps and DNA Addition Operation and Noise Effects on it

Kuldeep Singh
ITM University
School of Engineering & Technology
Department of EECE, Gurgaon, Haryana

Komalpreet Kaur
Assistant Professor
ITM University, School of Engineering & Technology
Department of EECE, Gurgaon, Haryana

ABSTRACT
In this paper, four 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 shows 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, chaotic Map Logistic Map, Cross Chaotic Map, Henon Map, Ikeda Map, DNA addition

1. INTRODUCTION
Today, due to advances in communication technology, illegal data access has become more easy and prevalent in wireless and general communication networks. Hence, data security has become very critical and important issue. Most of the information transmitted on internet belongs to digital images. However, the image information, which is different from text message, has larger scale of data, higher redundancy and stronger correlation between pixels. Therefore, reliable security in storage and transmission of digital images is needed in many applications, including both public and private services such as Patient data, medical imaging systems and military information systems.

Chaos is a kind of d random-like process which occurred in nonlinear dynamic systems. 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. At present, chaotic securer communication systems have been developed to certain, while extending the chaotic security communication systems to Internet and multimedia security is becoming a hot research spot.

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.

2. OVERVIEW
2.1 Chaotic map
In this paper, we used four chaotic maps: Logistic map, cross chaotic map, henon map, and Ikeda map.

2.1.1 2 D logistic map
$$\begin{cases} x_{i+1} = \mu_1 x_i (1 - x_i) + \gamma_1 y_i^{\,2}; \\ y_{i+1} = \mu_2 y_i (1 - y_i) + \gamma_2 (x_i^{\,2} + x_i y_i); \end{cases} \quad (1)$$

Where,

$2.75 < \mu_1 \le 3.4, 2.75 < \mu_2 \le 3.45,$
$0.15 < \gamma_1 \le 021, 0.13 < \gamma_2 \le 015$

The above equation (1) is chaotic and this will generate two chaotic sequences in the region (0, 1]. Here $\mu_1 \mu_2 \gamma_1 \gamma_2$ are the control parameters of Eq.(1) set γ_1=0.17 and γ_2=0.14.

1 D logistic map can be described as follows:

$$x_{i+1} = \mu x_i (1 - x_i) \quad (2)$$

Where $\mu \in [0,4]$, $x_i \in (0,1)$, ..i=0, 1, 2……the system is under chaotic state when 3.56994< $\mu \le 4$.

2.1.2 Cross chaotic map
In order to improve security and reduce calculation complexity, the cross chaotic map is defined as following:

$$\begin{cases} x_{i+1} = 1 - \mu y_i^{\,2}; \\ y_{i+1} = \cos(k \cos^{-1} x_i); \end{cases} , x, y \in [-1,1] \quad (3)$$

Where μ and k are control parameters of the system. The system will show the chaotic behaviour when $\mu = 2$ and k=6.

2.1.3 Henon map

Henon chaotic map is first discovered in 1978, which is described as following:

$$\begin{cases} x_{i+1} = 1 - ax_i^2 + y_i; \\ y_{i+1} = bx_i; \end{cases} \quad (4)$$

The system has two control parameters a and b and the system will show chaotic behavior when a=0.3 and b=1.4.

2.1.4 Ikeda map

In mathematics, an Ikeda map is a discrete-time dynamical system given by (5) and (6).

$$\begin{cases} x_{n+1} = 1 + u[x_n \cos t_n - y_n \sin t_n]; \\ y_{n+1} = u[x_n \sin t_n + y_n \cos t_n]; \end{cases} \quad (5)$$

Where u is an equation parameter and

$$0.4 - \frac{6}{(1 + x_n^2 + y_n^2)} \quad (6)$$

This map has a chaotic behavior for u in [0.5, 0.95]

2.2 DNA encryption

2.2.1 Logic for DNA encoding and decoding

The information in DNA is stored as a code made up of four chemical 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 complement 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: 4th pixel value is 173, then its binary form is [10101101] and by using above rule we get DNA sequence as [TTGA].

2.2.2 Logic for addition and subtraction of DNA sequences

DNA computing is becoming a very important field of research as year's passes. Addition and subtraction operation for DNA sequences are performed according to traditional addition and subtraction. 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.

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

3. ALGORITHM USED

In this sub section encryption algorithm is described in detail. Firstly we have to produce the secret keys using the original image and then follow the algorithm steps for encryption of image.

3.1 Generation of secret keys

To generate the secret key, Input a 8 bit grey image A as the original image, A = A(a_{ij}), i = 1,2, ... , m, j = 1,2, . .. , 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.

$$k_1 = \frac{1}{256} \bmod(\sum_{i=1}^{\frac{m}{2}} \sum_{j=1}^{n} a_{ij}, 256); \quad (7)$$

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

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:

$x_0 = x_1 + k_1$
if $x_0 > 1$ then
$x_0 = \bmod(x_0,1)$
else
$x_0 = x_0$
end

3.2 Algorithm for image encryption

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,…., m/4, j=1,2,…..,n. size of each cell is 4 x 4;

Step 3: Generate two chaotic sequences X= { x_0, x_1, ….., $x_{m/4}$}. Y= {y_0, y_1,……..,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 x 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 mod (Z, 1). Gets binary sequence matrix using following threshold function:

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

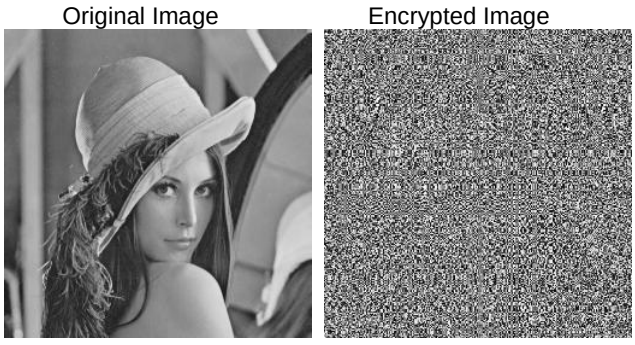
Step 9: If Z(i,j) = 1, C(i,j) is complemented, otherwise it is unchanged. Here, we get a complemented matrix P;

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.

4. RESULTS AND ANALYSIS

In this paper we used standard 256 x 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, μ_1 =3.4, μ_2 =2.784, μ_3 =3.7092, and μ_4 =3.7109. Cross chaotic map also has 6 secret keys μ_1 =2, μ_2 =1.9, x(0)=0.7199, y(0)=0.7654, k_1=6, and k_2=5. Ikeda map has 3 secret keys x(0)=0.7298, y(0)=0.7654, and u=0.8999. Henon map has 4 secret keys x(0)=0.7298, y(0)=0.7654, a=1.4, and b=0.3. Figure 1(a) shows the original image, the encrypted image with logistic, cross chaotic, ikeda, and henon map are shown in figure 1(b), (c), (d), (e) respectively and figure 1(f) shows decrypted image. Here, cross chaotic map shows the best encryption effect on image.



(a) **(b)**

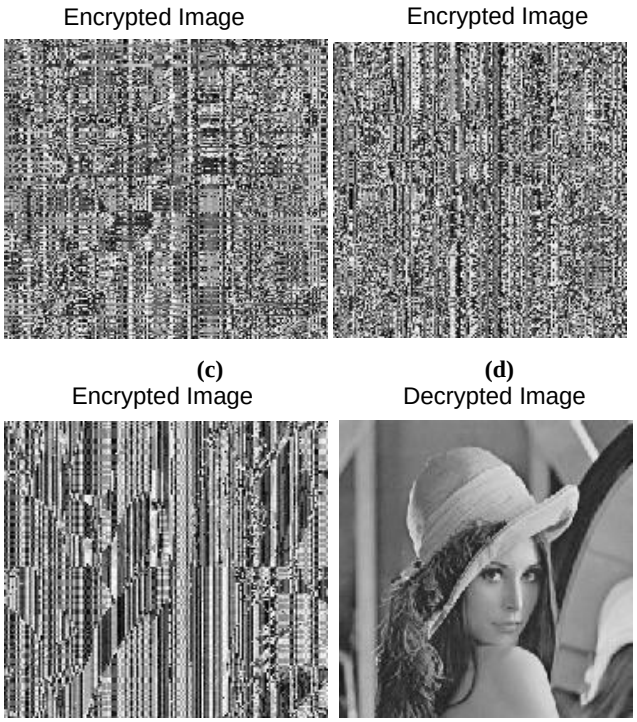
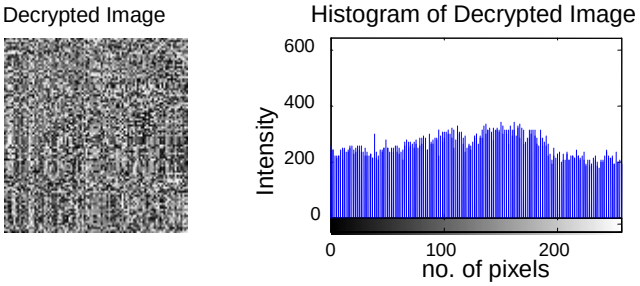


Figure 1(a) the original image (b) Encrypted image (cross chaotic map) (c) Ikeda map (d) Henon map (e) Logistic map (f) Decrypted image

4.1 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), and (d) 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, cross chaotic map is sensitivity to the secret key which demonstrates it has ability of resisting exhaustive attack.



(a)

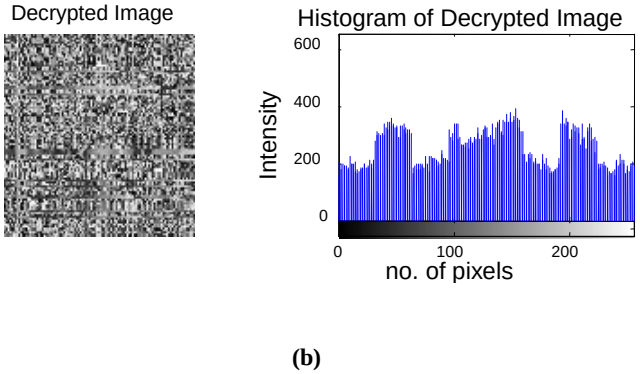
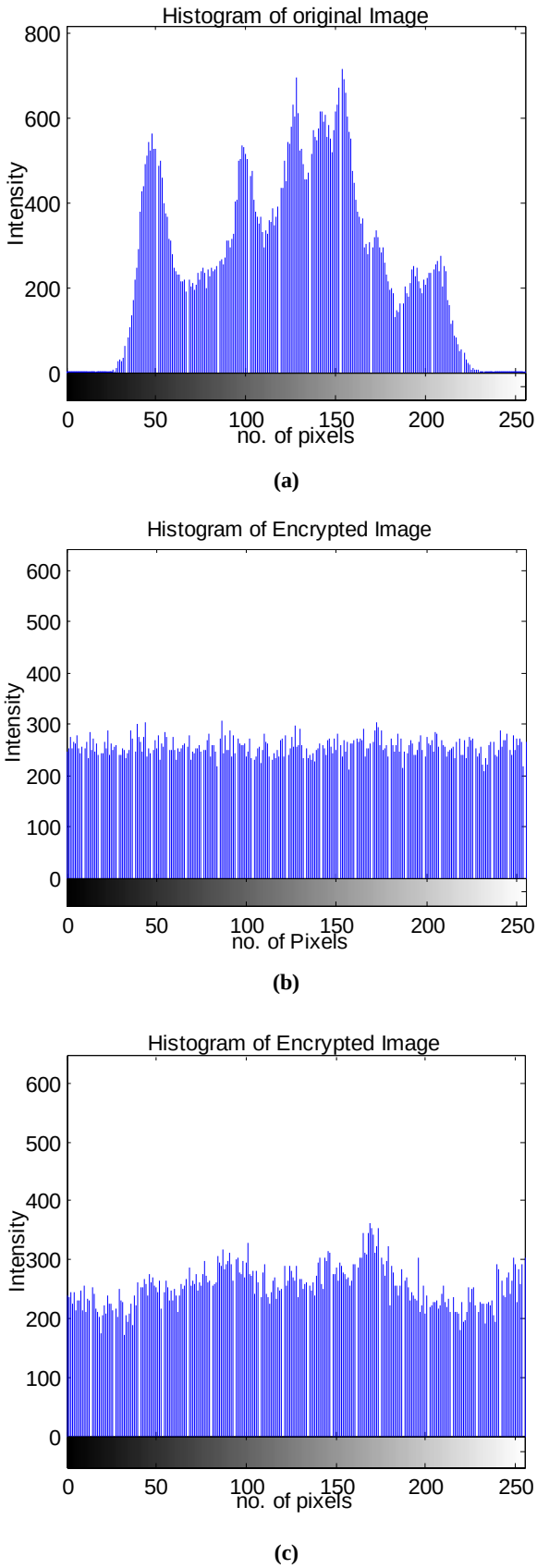
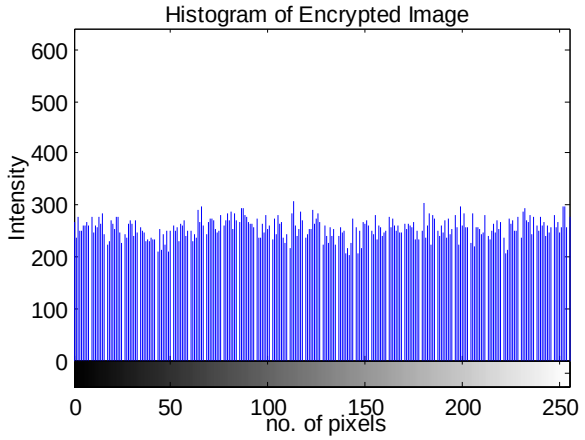


Figure 2 sensitivity to secret key (0.7199), Decrypted image with secret key (0.71990000000001) and corresponding histogram (a) Cross chaotic map (b) Ikeda map (c) Henon map and (d) Logistic map

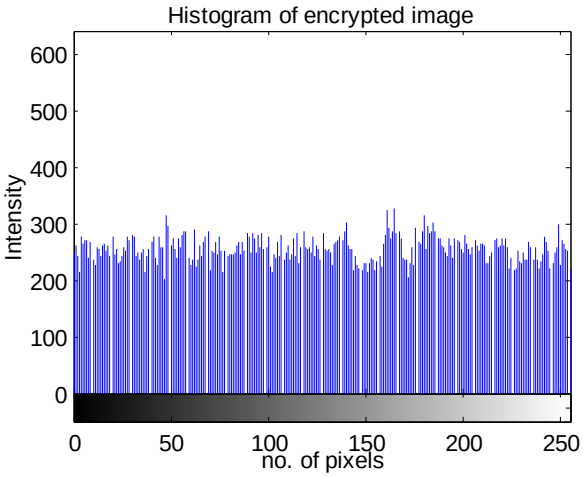
4.2 Grey histogram analysis

Figure 3 (a), (b), (c), (d), and (e) show the grey-scale histograms of the original image and the encrypted images(logistic, cross chaotic, ikeda, and henon 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, which makes statistical attacks difficult. Grey histogram of cross chaotic map shows the best results.





(d)



(e)

Figure 3 (a) shows grey histogram of original image (b), (c), (d), (e) shows grey histogram of encrypted images cross chaotic, Ikeda, Henon, Logistic map respectively and (f) shows grey histogram of Decrypted image

4.3 Correlation coefficient analysis

As we know that correlation between the adjacent pixels in a plain image is very high. Therefore it is one of the most important attack method used by the attackers. An efficient scheme can reduce the correlation between the adjacent pixels. To do this we choose 2000 pair of adjacent pixels (horizontal, vertical, and diagonal) from original image and encrypted image. Some formulas of correlation coefficient are:-

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

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

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

$$r_{x,y} = \frac{\mathrm{cov}(x, y)}{\sqrt{D(x)} \times \sqrt{D(y)}} \tag{13}$$

Where x and yare 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 (logistic, cross chaotic, ikeda, and henon) 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. Therefore cross chaotic map correlation analysis shows that it has strongest ability of resisting statistical attack than other three maps.

Table 3. Cross chaotic map

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

Table 4. Ikeda map

Model	Original image	Encrypted image
Horizontal	0.9484	-0.0562
Vertical	0.9910	0.2024
Diagonal	0.8885	-0.0340

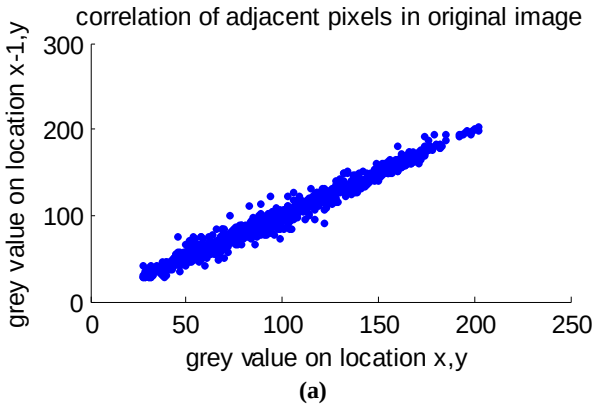
Table 5. Henon map

Model	Original image	Encrypted image
Horizontal	0.9484	-0.0134
Vertical	0.9910	0.6949
Diagonal	0.8885	0.0068

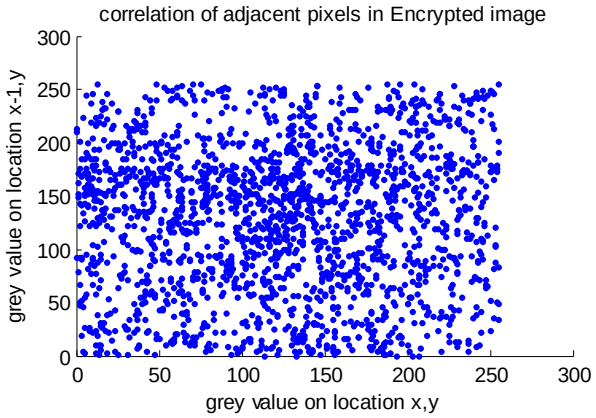
Table 6. Logistic map

Model	Original image	Encrypted image
Horizontal	0.9440	0.0273
Vertical	0.9910	-0.0225
Diagonal	0.8768	0.0229

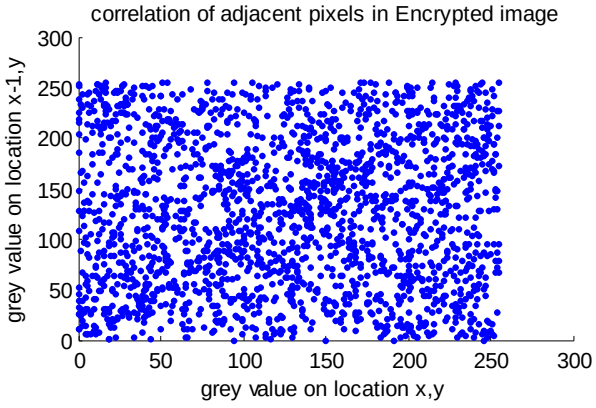
TABLE III, IV, V, VI shows correlation coefficient of two adjacent pixels



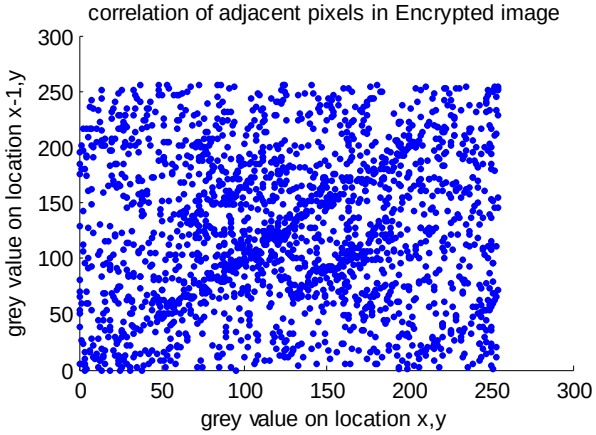
(a)



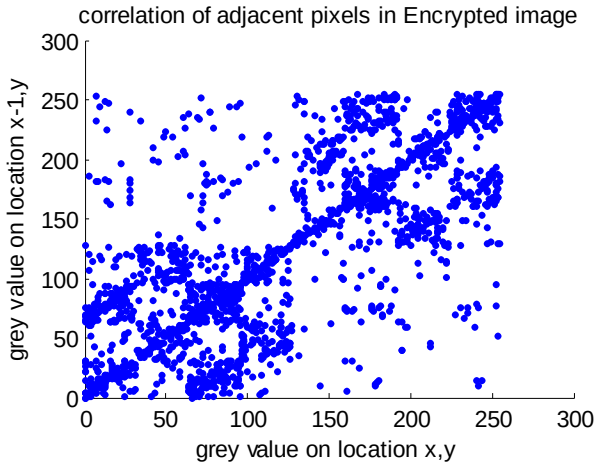
(b)



(c)



(d



(e)

Figure 4 correlations of two vertically adjacent pixels in (a) original image and in encrypted images of (b) cross chaotic (c) Ikeda (d) Henon (e) Logistic map

4.4 Differential attack

Attackers often make a slight change for the original image, and use the proposed scheme 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. To evaluate the influence of one-pixel change on the whole encrypted image, two common measures are used, i.e., number of pixels change rate (NPCR) and unified average changing intensity (UACI). These two measures are defined as:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\% \qquad (14)$$

$$UACI = \frac{1}{W \times H}\left[\sum_{i,j} \frac{|E_1(i,j) - E_2(i,j)}{255}\right] \times 100\% \qquad (15)$$

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 $E_1(i, j)$ or $E_2(i, j)$, respectively.

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

Table 7. Ability to resist Differential attack

	Corss chaotic	Ikeda	Henon	Logistic
NPCR	99.9969	99.9969	99.9969	99.9969
UACI	0.0018	0.0027	0.0022	0.0019

5. NOISE EFFECTS

For cross chaotic map:

5.1 Gaussian noise

Gaussian noise is statistical noise that has its probability density function equal to that of the normal distribution, which is also known as the Gaussian distribution. In other words, the values that the noise can take on are Gaussian-distributed. Figure 5(a) shows the effect of Gaussian noise on the image.

5.2 Salt and pepper noise

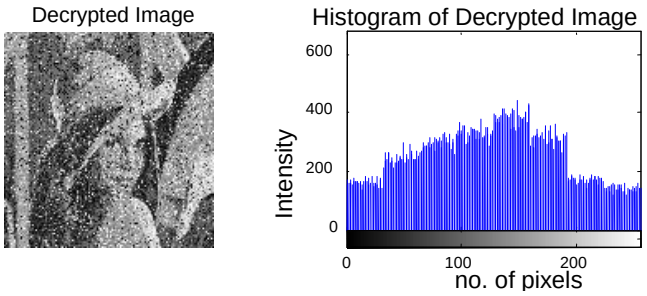
An image containing salt-and-pepper noise will have dark pixels in bright regions and bright pixels in dark regions. This type of noise can be caused by dead pixels. Figure 5(b) shows the effect of Salt and pepper noise on the image.

5.3 Poisson noise

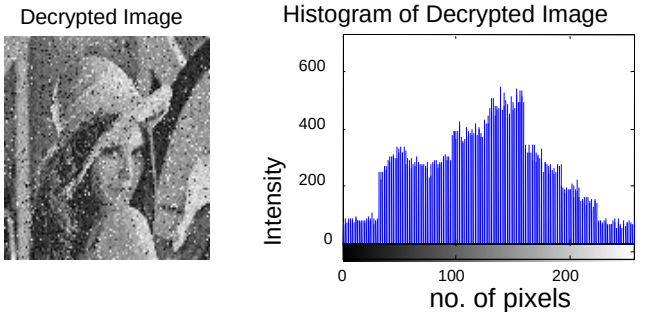
The dominant noise in the lighter parts of an image from an image sensor is typically that caused by statistical quantum fluctuations, that is, variation in the number of photons sensed at a given exposure level. Figure 5(c) shows the effect of Poisson noise on the image.

5.4 Speckle noise

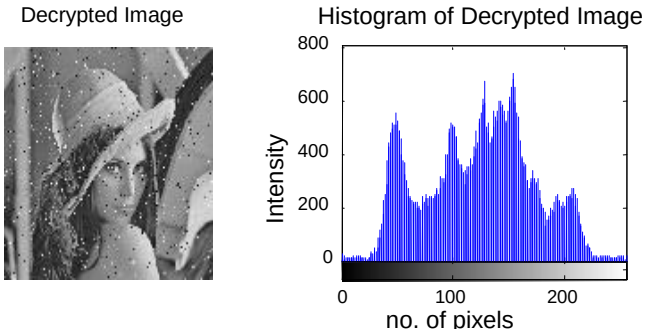
Speckle noise is a granular noise that inherently exists in and degrades the quality of the images. . Figure 5(d) shows the effect of Speckle noise on the image.



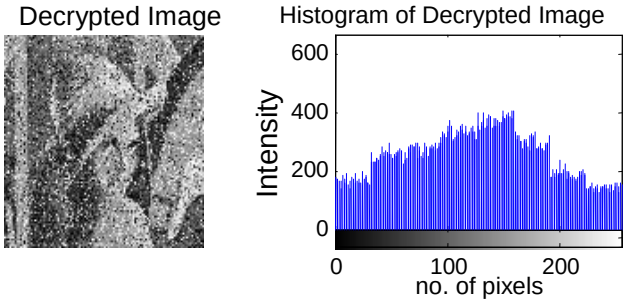
(a)



(b)



(c)



(d)

Figure 5 (a) shows the Gaussian noise (b) Salt & Pepper noise (c) Poisson noise (d) Speckle noise in decrypted image

The histogram analysis of noise images shows that Salt & pepper was least affected by noise whereas Speckle noise was largely affected by noise.

6. CONCLUSION

In this paper we have compared four different chaotic maps Cross chaotic, Logistic, Ikeda and Henon map. Through the simulation results, histogram analysis and correlation analysis we have found out that cross chaotic map showed best results than other three chaotic maps. It is sensitive to the secret keys, it has larger key space, and it gives best encrypted image. This shows that cross chaotic map is best suitable for the image encryption. Also, cross chaotic map resist most of the known attacks such as statistical attack, differential attack and exhaustive attack. 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 extend that image can not be recognized.

7. FUTURE SCOPE

This paper mainly focused on comparison of chaotc 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.

8. 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] Robart 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.

[13] Xiaogang Jia, "Image Encryption Using Ikeda map", 2010 International conference on intelligent computing and cognitive infomatics.