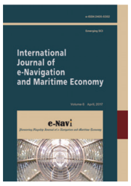
Available online at www.sciencedirect.com
ScienceDirect



Original article

A Novel Image Encryption Scheme Based on Clifford Attractor and Noisy Logistic Map for Secure Transferring Images in Navy[☆]

Mohadeseh KANAFCHIAN [a], Behrouz FATHI-VAJARGAH [b*]

[a] Dep. of Mathematics, University of Guilan, Rasht, Iran, m.kanafchiyan@gmail.com

[b*] Dep. of Statistics, University of Guilan, Rasht, Iran, fathi@guilan.ac.ir, Corresponding Author

Abstract

Cryptography is a science to maintain the security of the message by changing data or information into a different form, so the message cannot be recognized. Today, many algorithms have been proposed for image encryption, but the chaotic encryption methods have a good combination of speed and high security. In recent years, the chaos based cryptographic algorithms have suggested some new and efficient ways to develop secure image encryption techniques. The chaos-based encryption schemes are composed of two steps: chaotic confusion and pixel diffusion. In the chaotic confusion stage, a combination of the chaotic maps is used to realize the confusion of all pixels.

In this paper, we first give a brief introduction into chaotic image encryption and then we investigate some important properties and behaviour of the logistic map. The logistic map, aperiodic trajectory, or random-like fluctuation, could not be obtained with some choice of initial condition. Therefore, a noisy logistic map with an additive system noise is introduced. The proposed scheme is based on the extended map of the Clifford strange attractor, where each dimension has a specific role in the encryption process. Two dimensions are used for pixel permutation and the third dimension is used for pixel diffusion. In order to optimize the Clifford encryption system we increase the space key by using the noisy logistic map and a novel encryption scheme based on the Clifford attractor and the noisy logistic map for secure transfer images is proposed. This algorithm consists of two parts: the noisy logistic map shuffle of the pixel position and the pixel value. We use times for shuffling the pixel position and value then we generate the new pixel position and value by the Clifford system. To illustrate the efficiency of the proposed scheme, various types of security analysis are tested. It can be concluded that the proposed image encryption system is a suitable choice for practical applications.

Keywords: Image encryption, Chaos, Noisy logistic map, Clifford attractor, Image security analysis

☆

[☆] This is a revised version presented at the 4th Ai-MAST held at Mokpo, Korea, December 12-15, 2016.

1. Introduction

An increasing amount of information is being transmitted over the Internet, including not only text but also audio, image, and other multimedia files.

Protection of digital information against illegal access and distribution has become extremely important. Therefore, techniques are required to provide security functionalities like privacy, integrity, or authentication especially suited for these data types of multimedia. A few applications of these techniques for providing privacy and confidentiality of visual data are in the areas of telemedicine, video conferencing, images, military surveillance and etc. Navy cryptology includes analyzing electronic communications, cracking enemy codes, jamming enemy radar signals, deciphering foreign languages and maintaining the equipment needed to produce top-secret intelligence. Cryptology at sea was proven decisive during World War II, beginning with the battle at Midway and the breaking of the Japanese naval code “JN25.” naval cryptology played a vital role in meeting national and tactical intelligence requirements. Image encryption is different from text, some algorithms such as DES, IDEA, AES and most other methods are not suitable for image encryption.

According to Kocarev et al. (2011) and Sprott (1993), chaos theory is a field of study in mathematics that studies the behaviour of dynamical systems that are highly sensitive to initial conditions. Image encryption for wavelet-base images has been started recently and lots of research is being performed.

Most research in this area insists that the data compression and encryption should be combined or performed simultaneously and only part of image data should be encrypted because of the cost such as processing time, power, etc (Wu and Moo 1999, Alattar et al., 1999, Seo et al., 2013, Park et al., 2005, Pommer et al., 2001).

Because this article focuses on the chaos-based image encryption, only the research related to this area is reviewed.

Matthews (1989) firstly used chaos to encrypt information and produced the key stream based on logistic map.

Baptista (1991) published a paper about chaotic encryption algorithm. 2D or higher dimensional chaotic maps are usually employed for image encryption.

Friedrich (1998) has suggested that an image encryption system need to be repeated in two steps: diffusion and confusion.

Giesl (2009) proposed an image encryption system using strange attractor.

Today, because of the properties of chaotic systems, such as sensitive to initial conditions and control parameters, pseudo randomness and ergodicity, chaos becomes popular in image encryption (Hua et al., 2015, Kocarev et al., 2011, Patidar et al., 2010, Wang et al., 2012, Yen et al., 2000).

The rest of the paper is arranged as follows: section 2 describes the 1D noisy logistic map, Section 3 constructs a new image encryption algorithm based on Clifford attractor and noisy logistic map.

The experimental results, analysis and comparison of the proposed image encryption system are shown in section 4, and finally section 5 concludes the paper.

2. Noisy logistic map

There are two main types of random noise used to extend the deterministic model to the stochastic model in the analysis of initial value sensitivity: observation noise and system noise.

In the case of the observation noise, or measurement noise, observables are given as the sum of stochastic noise and the unobservable generated from the deterministic model.

In contrast, with the system noise, or dynamic noise, observables are generated directly from a nonlinear autoregressive model. In practice, it is often convenient to introduce the system noise in the additive manner. Theoretically, system noise can allows it to have a unique stationary distribution. Note that for the example of the logistic map, aperiodic trajectory, or random-like fluctuation, could not be obtained with some choice of initial condition with measure zero.

In general, the deterministic systems can have an infinite number of stationary distributions. However, typically, the presence of additive noise can exclude all degenerate marginal distributions. Furthermore, additive system noise is convenient to generalize the use of the Lyapunov exponents, originally defined in the deterministic system as a measure of sensitive dependence, to the case of a stochastic system.

One of the most studied examples of a one-dimensional system capable including chaos is the logistic map (Arrowsmith and Place, 1992, p.244).

$$x_{n+1} = r\,x_n\left(1 - x_n\right) \tag{1}$$

where r is the control parameter. Control parameter r has a crucial role in behavior of the map and we can recognize the qualitative changes in the dynamics of map by varying the value r. It is now widely understood that complex behavior in nature may have a simple underlying cause. Several examples of low-dimensional nonlinear maps have been extensively studied.

On the other hand, many familiar processes are known to have regular periodic solutions.

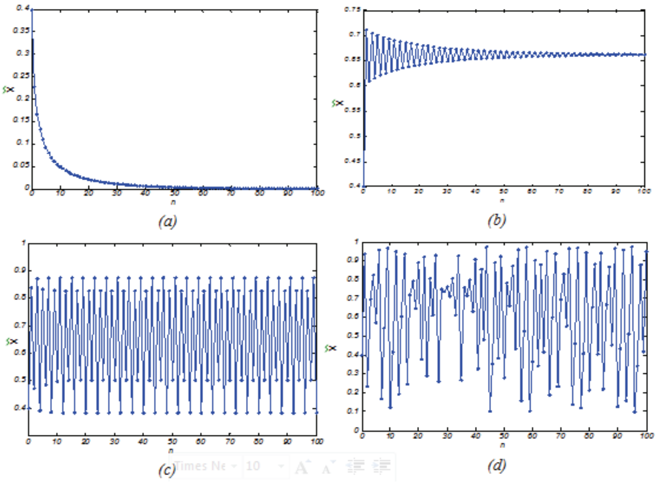

(a) (b) (c) (d)

Figure 1: 100 points of logistic map with $x_0 = 0.4$ and different values of r (a) $r = 0.95$, (b) $r = 2.95$, (c) $r = 3.5$, (d) $r = 3.9$.

Upon repeated iteration, the solution will be one of the following cases, depending upon the initial condition and its value: (1) it will converge to a stable fixed point (a point attractor), (2) it will converge to a periodic series of distinct values (a limit cycle), (3) it will yield a non-periodic series of values within some bounded range of X (a chaotic strange attractor), or (4) it will diverge (attract to infinity).

A feature of a chaotic system is sensitivity to initial conditions. If two trajectories which start off close to each other deviate more and more as the time increases time, the system is said to be chaotic.

The rate at which nearby trajectories deviate from each other with time is characterized by a quantity called the Lyapunov exponent. The Lyapunov exponent for the discrete chaos system can be described as below

$$h = \lim_{n\to\infty}\frac{1}{n}\ln\left|f'(x)\right| \tag{2}$$

where the parameter n is the length of the sequence and f is the chaos map. If $h > 0$, it means that the chaos system is currently chaotic with the certain condition. If $h \le 0$, the chaos system is not chaotic under current condition.

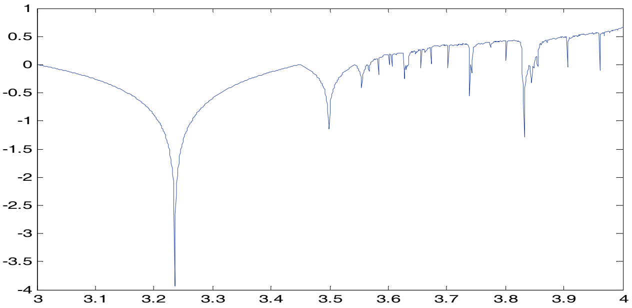


Figure 2: Lyapunov exponent for logistic map

For this case, the stable solutions are all in the range of $3.5 \le r \le 4$, and it is only within this range that the logistic equation represents a candidate model for a real physical process.

A noisy logistic map with an additive system noise given by (Meyers 2009, p. 432)

$$x_{n+1} = r\,x_n\left(1 - x_n\right) + \sigma\left(x_{n-1}\right)\varepsilon_n \tag{3}$$

where ε_n are independent, identically distributed random variables with the uniform distribution on $\left(\frac{-1}{2}, \frac{1}{2}\right)$ and $\sigma\left(x_{n-1}\right) = 0.5\min\left(x_n, 1 - x_n\right)$. Note that the conditional heteroskedasticity function $\sigma(x)$ here ensures that the process x_n is restricted to the unit interval $[0,1]$.

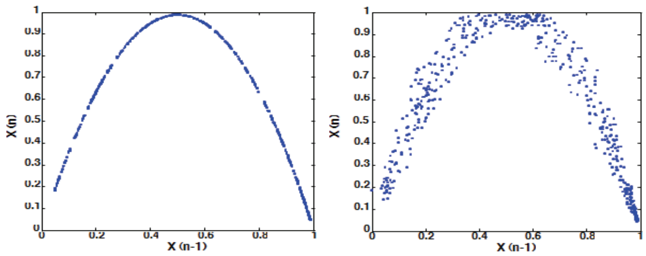


Figure 3: (a) Logistic map and, (b) Noisy logistic map with $x_0 = 0.4$, $r = 3.95$

The following figures show 100 points of the noisy logistic map with $x_0 = 0.4$ and different values of r.

It can be seen that the noisy logistic map has no period 2 and 4.

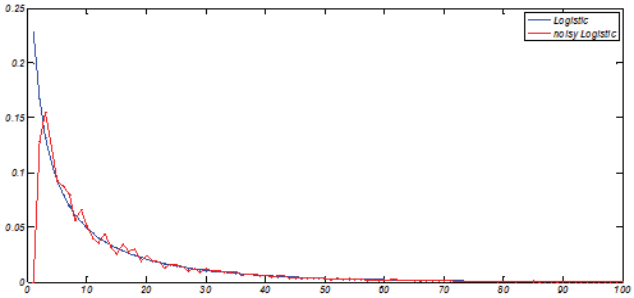


Figure 4: 100 points of noisy logistic map with $r = 0.95$

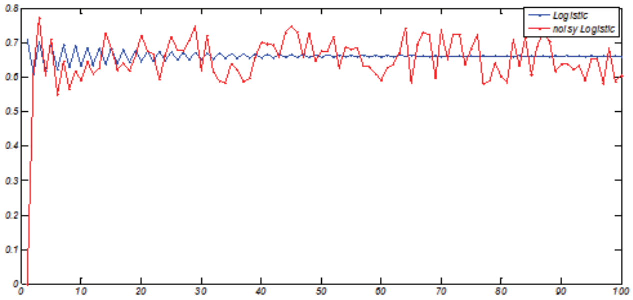


Figure 5: 100 points of noisy logistic map with $r = 2.95$

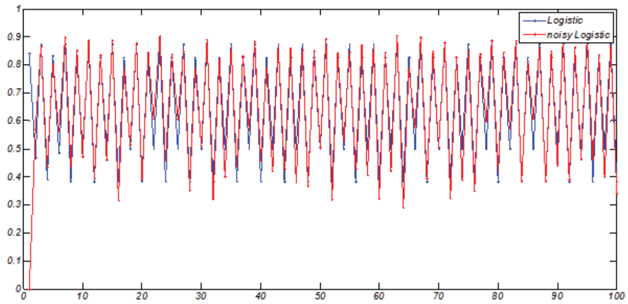


Figure 6: 100 points of noisy logistic map with $r = 2.95$

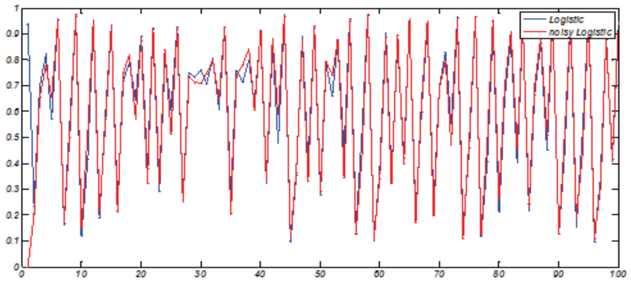


Figure 7: 100 points of noisy logistic map with $r = 3.9$

3. Methodology

According to Pickover (1988) and Sprott (1993), strange attractors are complicated sets with a fractal structure to which chaotic dynamical systems evolve after enough long time. These attractors can be generated in several ways. In general, a map is said to be dissipative if it does not preserve phase space volumes on each iterate.

Therefore, the bounded region on the phase place will certainly shrink for the reason that map can be iterated and this is associated with the presence of an attractor within that region.

The proposed image encryption is a modification of the one suggested by Giesl (2009, p.20). This algorithm does not create any encryption key, but uses an attractor map for pixel permutation and diffusion directly. Parameters of the attractor map play the role of encryption keys here and key space is very large due to their non-integer character.

According to Giesl (2009, p.20) and Zelinka et al. (2010, p.330), chaos-based encryption has been done by means of the so called Clifford system (attractor)

$$\begin{aligned} x_{n+1} &= \sin(ay_n) + c\cos(ax_n) \\ y_{n+1} &= \sin(bx_n) + d\cos(by_n) \\ z_{n+1} &= \sin(ey_n) + f\cos(ez_n) \end{aligned} \tag{4}$$

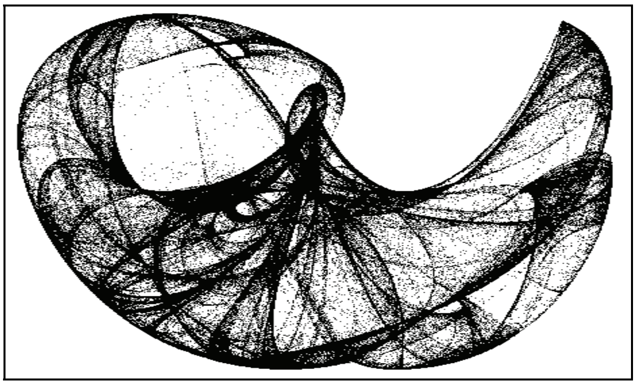


Figure 8: Clifford attractor based on Equ. (4)

Implementation of image encryption is in two steps: the first step is image scrambling so that the position of the pixels in the image is changed and the second step is pixel substitution. An image can be described by the position and the pixel value. This method can change the position and value of the image pixel and it converts the image from a plain digital image into a noise-polluted image.

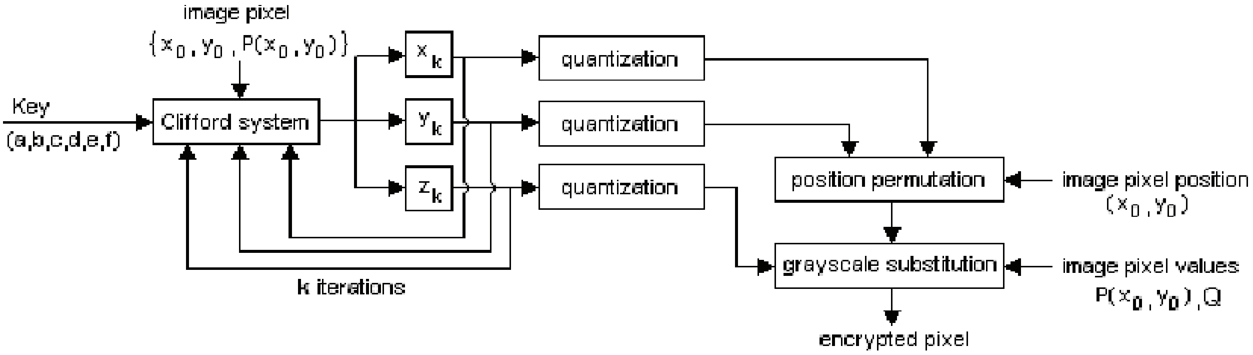


Figure 9: Flowchart of encryption process

Source: Giesl (2009), p.21.

Pixel substitution is implemented by XOR or other operation with other sequence or matrix to change plain image pixel value. The main parameters of the Clifford attractor are keys for the process of encryption. Pixel of image is used as the initial value of Clifford system. Equation (4) is 3D extension which can be used for encryption of coordinates (pixel position) and the value of each pixel. New positions and modification value are gained after iterations and quantization. These positions are then used for pixel permutation and the modification value is XOR operated with original pixel value and the value of the previous pixel and encrypted pixel is gained this way (Giesl, 2009). According to Figure 9, the previous algorithm was changed as follows:

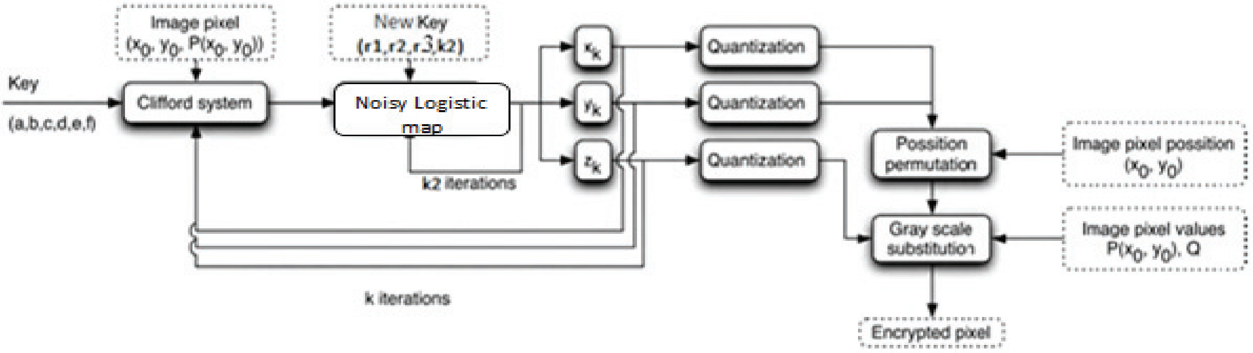


Figure 10: Flowchart of the proposed encryption

In the new algorithm, first coordinates (x_0, y_0) and value $P(x_0, y_0)$ of pixels were put into a Clifford system. Next noisy logistic map iterate k_2 times with r_1, r_2, r_3 parameters.

After the quantization step, the positions and modification value are gained. Encryption system contains 7 steps. Detailed as follows:

Step 1. Key generation: Select parameters a, b, c, d, e and f of Clifford attractor and r_1, r_2, r_3, k_2 of the noisy Logistic map.

Step 2. Image conversion matrix: Converts the tested image to a matrix. For grayscale image, the dimension of matrix is $[n \times m]$. n is the height of the image while m is the width. A color image can be converted into grayscale image.

Step 3. Initial selection: as with the initial process of encryption, select a pixel position (x_0, y_0) and a pixel value $z_0 = P(x_0, y_0)$.

Step 4. New Clifford system: perform the noisy logistic map and Clifford stranger to disorder the position and value pixel of the image.

Generate the random number $\varepsilon \sim U\left(\frac{-1}{2}, \frac{1}{2}\right)$.

Put x_0, y_0 and $z_0 = P(x_0, y_0)$ into the noisy Logistic map with k_2 iterations.

$$x_0 = r_1 \; x_0(1 - x_0) + 0.5 \min(x_0, 1 - x_0)\varepsilon$$
$$y_0 = r_1 \; y_0(1 - y_0) + 0.5 \min(y_0, 1 - y_0)\varepsilon$$
$$z_0 = r_1 \; z_0(1 - z_0) + 0.5 \min(z_0, 1 - z_0)\varepsilon$$

Then Clifford attractor is used to shuffle pixel position and pixel value. The obtained x_0, y_0, z_0 are the initial values for Clifford equation.

$$x_k = \sin(a y_0) + c\ \cos(a x_0)$$
$$y_k = \sin(b x_0) + d\ \cos(b y_0)$$
$$z_k = \sin(e y_0) + f\ \cos(e z_0)$$

Set $x_0 = x_k$, $y_0 = y_k$, $z_0 = z_k$ and iterate the above equation k times. The original pixel at coordinates (x_0, y_0) is swapped with the pixel at coordinates (x_k, y_k).

Step 5. Reshaping matrices: Convert 2D matrices x, y, z into 1D matrices.

Step6. Quantization: For the obtained vectors in step 5, determine minimum and maximum value of vectors. Then the range is divided between the minimum and maximum values.

Step7. Changing values of the pixels: Pixel value at coordinates (x_k, y_k) is modified by XOR operation of value z_k and then XOR operated with the value of the previous processed pixel Q. This process must be done for every pixel in the image.

$$P(x_0, y_0) \leftrightarrow P(x_k, y_k) \oplus z_k \oplus Q$$

4. Simulation results and statistical analysis

The following tests are realized by MATLAB software on Intel Core (TM) i7, 2.2 GHz PC.

4.1. Key space analysis

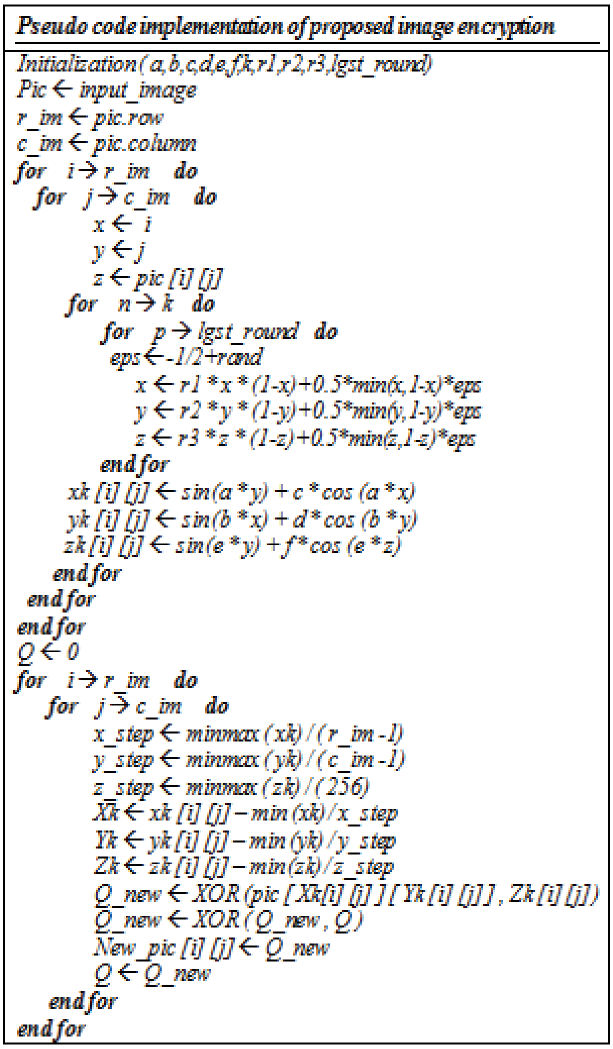
A good encryption algorithm should have large key space to prevent brute-force attacks which is defined to exhaust all the possible keys until the correct one. The size of key space for the proposed system is larger than Clifford system$\left(2^{318}\right)$.

4.2. Encryption and histogram test

Some experimental results are given in this section to demonstrate the efficiency of our scheme. The plain images are with the size 256×256.

As we can see, the pixel distribution of the cipher images is fairly uniform, which can greatly reduce the correlation between the pixel values.

Both kinds of pictures show that the picture is really well encrypted.



```
Pseudo code implementation of proposed image encryption
Initialization( a,b,c,d,e,f,k,r1,r2,r3,lgst_round)
Pic ← input_image
r_im ← pic.row
c_im ← pic.column
for  i → r_im  do
  for  j → c_im  do
        x ← i
        y ← j
        z ← pic [i] [j]
     for  n → k  do
        for  p → lgst_round  do
         eps ← -1/2+rand
            x ← r1 * x * (1-x)+0.5*min(x, 1-x)*eps
            y ← r2 * y * (1-y)+0.5*min(y, 1-y)*eps
            z ← r3 * z * (1-z)+0.5*min(z,1-z)*eps
        end for
     xk [i] [j] ← sin(a * y) + c * cos (a * x)
     yk [i] [j] ← sin(b * x) + d * cos (b * y)
     zk [i] [j] ← sin(e * y) + f * cos (e * z)
    end for
  end for
end for
Q ← 0
for  i → r_im  do
   for  j → c_im  do
        x_step ← minmax (xk) / (r_im -1)
        y_step ← minmax (yk) / (c_im -1)
        z_step ← minmax (zk) / (256)
        Xk ← xk [i] [j] – min (xk) / x_step
        Yk ← yk [i] [j] – min (yk) / y_step
        Zk ← zk [i] [j] – min(zk) / z_step
        Q_new ← XOR (pic [ Xk[i] [j] ] [ Yk [i] [j] ] , Zk [i] [j])
        Q_new ← XOR ( Q_new , Q )
        New_pic [i] [j] ← Q_new
        Q ← Q_new
   end for
end for
```

a = -1.85, b=1.48, c = -1.55, d = -1.87, e= -4.32,

f =0.63, $r_1 = 4, r_2 = 4, r_3 = 3.95, k_2 = 5$

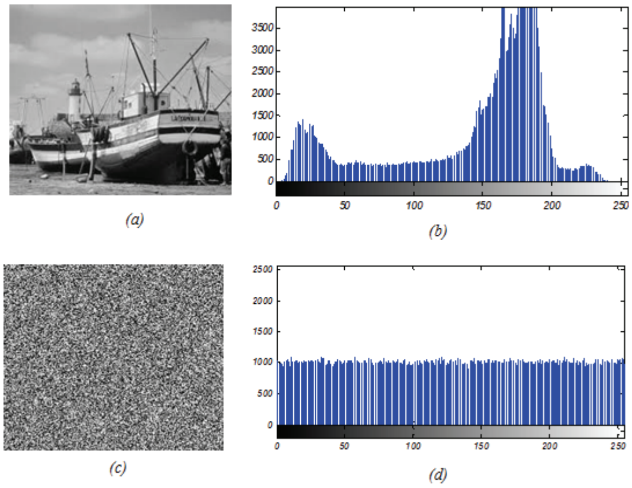


Figure 11: (a) Plain image, (b) Histogram of plain image, (c) Cipher image by the proposed encryption system, (d) Histogram of cipher image by the proposed encryption system

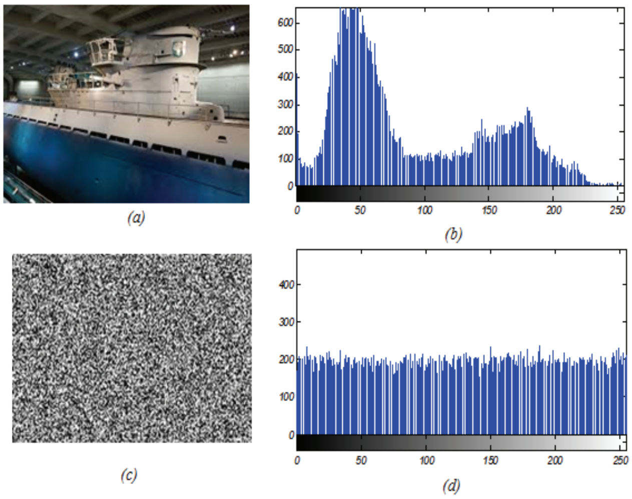


Figure 12: (a) Plain image, (b) Histogram of plain image, (c) Cipher image by the proposed encryption system, (d) Histogram of cipher image by the proposed encryption system

4.3. Chi-square test

The uniformity is justified by chi-square test, which is described by the following expression:

$$\chi^2 = \sum_{k=1}^{256} \frac{(O_k - E_k)^2}{E_k} \qquad (5)$$

O_k = The observed frequencies of each gray level(0-255)

E_k = The expected frequencies of each gray level(0-255)

Assume significant level of 0.05, $\chi^2(255,0.05)=291$. If $\chi^2_{test} < \chi^2(255,0.05)$ then the distribution of the encrypted histogram is uniform. Following table shows chi-square values of different cipher images.

Table 1: Chi-square test for cipher images

Image	size	Chi-square	
		χ^2_{test}	H_0
Monalisa	128×128	255.312500	Accepted
Elaine	225×225	225.934834	Accepted
Lena	256×256	246.804687	Accepted
Cameraman	256×256	231.992187	Accepted
Puppy	256×256	223.817510	Accepted
Moon surface	256×256	240.930373	Accepted
Boat	256×256	220.0175781	Accepted
Mandrill	256×256	259.980901	Accepted
Barbara	256×256	248.382812	Accepted

4.4. Analysis for correlation of adjacent pixels

Correlation analysis of adjacent pixels is an important way to test the gray value relationship between adjacent pixels in cipher image. Adjacent pixels in plain image have high correlation and in ciphered image should have low correlation. We calculate the correlation coefficient of a plain and encrypted image $r_{P,C}$ by using the following formulas:

$$E(P)=\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}P(i,j)}{M.N},\ E(C)=\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}C(i,j)}{M.N} \qquad (6)$$

$$D(P)=\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}\left[P(i,j)-E(P)\right]^2}{M.N} \qquad (7)$$

$$\operatorname{cov}(P,C)=\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}\left[P(i,j)-E(P)\right]\left[C(i,j)-E(C)\right]}{M.N}$$

$$r_{P,C}=\frac{\operatorname{cov}(P,C)}{\sqrt{D(P)}\sqrt{D(C)}} \qquad (8)$$

In these formulas $P(i,j)$ and $C(i,j)$ are gray values of the plain pixel and the encrypted one. $E(P), E(C)$, $D(P)$ and $D(C)$ are mathematical expectation of plain pixels $P(i,j)$, mathematical expectation of cipher pixels $C(i,j)$, variance of plain pixels $P(i,j)$ and variance of cipher pixels $C(i,j)$, respectively. In order to test the correlation of adjacent pixels in the cipher image which is encrypted according to the proposed scheme, a test is designed.

2000 pixels are chosen randomly from Boat image, and their correlation distribution of gray value is plotted.

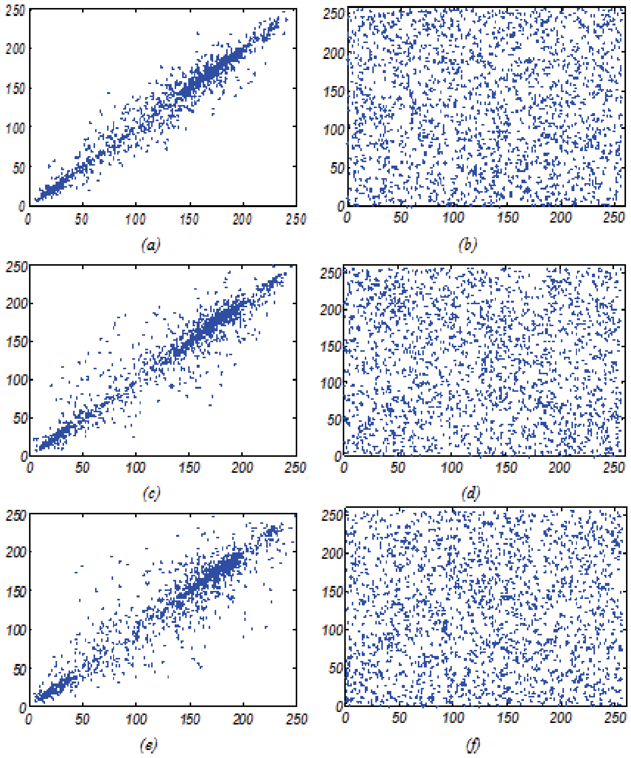


Figure 13: Distribution of correlation coefficients: (a) distribution of the horizontal correlation coefficients of adjacent pixels of plain image, (b) distribution of the horizontal correlation coefficients of adjacent pixels of cipher image, (c) distribution of the vertical correlation coefficients of adjacent pixels of plain image, (d) distribution of the vertical correlation coefficients of adjacent pixels of cipher image , (e) distribution of the diagonal correlation coefficients of adjacent pixels of plain, (f) distribution of the diagonal correlation coefficients of adjacent pixels of cipher image

The correlation coefficients of the adjacent pixels in horizontal, vertical and in diagonal are listed in Table 2.

Table 2: Comparison of correlation coefficient of the cipher images in five algorithms

	Correlation		
Method	**Horizontal**	**Vertical**	**Diagonal**
Plain image	0.964433	0.983118	0.949929
Proposed system	-0.006112	-5.40233×10^{-5}	-0.001815
Clifford system	-0.022289	-0.002046	-0.000317
Yue et.al.(2014)	0.005336	-0.002761	0.001662
Wan and Lie (2012)	0.02046	0.01748	0.002317
Fu et.al.(2011)	0.0368	-0.0392	0.0068

4.5. Analysis for correlation of plain image and cipher image

We analyzed the correlation between various pairs of plain image and cipher image. Table 3 shows the results of the correlation coefficient between the plain image and corresponding cipher image.

Table 3: Comparison of correlation coefficient of the plain and cipher images by using two methods

Image	**Correlation coefficient**	
	Proposed system	**Clifford system**
Lena	-0.000549	0.000809
Puppy	-0.001600	0.002807
Mona_lisa	0.000195	-0.007508
Moon surface	0.002943	0.004224
Boat	0.001781	-0.001809
Mandrill	0.000679	0.000911
Barbara	-0.001112	0.001239

The correlation coefficient value ranges from −1 to +1. The correlation coefficients measured by using the proposed encryption system are very close to 0. Therefore, the cipher and plain images are significantly different.

4.6. Information entropy analysis

Image information entropy can measure the distribution of image gray values. Image entropy is defined as

$$H = -\sum_{i=1}^{256} p_i \log p_i \tag{9}$$

where p_i represents the probability of occurrence of each pixel and log denotes the base 2 logarithm. The ideal value of the cipher information entropy is 8. Table 4 and Table 5 demonstrate that the entropy of cipher images is very close to the ideal value by using the proposed method.

Table 4: Comparison of entropy test for the cipher images

Image	**Entropy**		
	plain image	**Proposed system**	**Clifford system**
Lena	7.597635	7.999320	7.998972
puppy	7.453406	7.998325	7.998300
Mona_lisa	7.345221	7.988825	7.9882351
Moon surface	6.709312	7.997903	7.997010
Boat	7.215447	7.999393	7.999248
Mandrill	7.284855	7.999399	7.999411
Barbara	7.632119	7.999317	7.999282

Table 5: Comparison of the cipher image entropy by using five algorithms

Image	Proposed system	Clifford system	Yue et.al. (2014)	Wan and Lie (2012)	Fu et.al. (2011)
Lena	7.999320	7.99897	7.9971	7.999	7.9880

Table 6: Entropy test of proposed algorithm for different cipher images

Image	Entropy test			
	Global entropy	Actual block entropy	Theoretical block entropy	
			$\alpha = 0.01$	$\alpha = 0.05$
			7.16276745	7.16634107
Lena	7.999320	7.17251101	Pass	Pass
puppy	7.998325	7.17786312	Pass	Pass
Mona_lisa	7.988825	7.17543120	Pass	Pass
Mandrill	7.999399	7.17805673	Pass	Pass
Moon surface	7.997903	7.17219417	Pass	Pass
Boat	7.999393	7.17503241	Pass	Pass
Barbara	7.999317	7.17552748	Pass	Pass

In the above block entropy test (Wu et.al. 2011) 100 non-overlapped blocks of the size 16×16 are randomly selected from each cipher image. The information entropy of each block is recorded via Eq. (9) and the average entropy is calculated.

4.7. Sensitivity analysis

A good encryption algorithm should be sensitive to the plain image and the secret keys.

4.7.1. Plain image sensitivity

For calculation of the number of pixel change rate (NPCR) and unified average changing intensity (UACI), let us assume two cipher images C_1 and C_2 whose corresponding plain images have only one-pixel difference. NPCR and UACl are defined through the following formula as:

$$NPCR = \frac{\sum_i \sum_j D(i,j)}{T} \times 100 \tag{10}$$

$$UACI = \left[\sum_i \sum_j \frac{\left| C_1(i,j) - C_2(i,j) \right|}{L.T} \right] \times 100 \tag{11}$$

The symbols T and L denote the number of pixels in the cipher image and the largest allowed pixel intensity, respectively. $D(i,j)$ is defined as:

$$D(i,j) = \begin{cases} 0 & C_1(i,j) = C_2(i,j) \\ 1 & C_1(i,j) \neq C_2(i,j) \end{cases} \tag{12}$$

Table 7 shows the real values of NCPR and UACI of cipher images by changing a pixel of the plain image.

Table 7: Comparison of NPCR and UACI of cipher image by changing a pixel of plain image

Image	method	NPCR%	UACI%
Lena	**Proposed system**	99.623107	33.463145
	Clifford system	99.622414	33.472513
	Huaet.al (2015)	99.60	99.66
	Yen and Gua (2000)	99.61	33.48

4.7.2. Key sensitivity

A 128×128 gray Boat image is encrypted by using a = -1.85, b=1.48, c = -1.55, d = -1.87, e= -4.32, f =0.63, $r_1 = 4, r_2 = 4, r_3 = 3.95$ as the first set of key. The key is changed slightly to be used to encrypt the same plain image. Slightly different kinds of key are listed below.

1. a= -1.8500001, b=1.48, c = -1.55, d = -1.87, e= -4.32, f =0.63, $r_1 = 4, r_2 = 4, r_3 = 3.95$

2. a= -1.85, b=1.4800001, c = -1.55, d = -1.87, e= -4.32, f =0.63, $r_1 = 4, r_2 = 4, r_3 = 3.95$

3. a= -1.85, b=1.48, c = -1.5500001, d = -1.87, e= -4.32, f =0.63, $r_1 = 4, r_2 = 4, r_3 = 3.95$

4. a= -1.85, b=1.48, c = -1.55, d = -1.8700001, e= -4.32, f =0.63, $r_1 = 4, r_2 = 4, r_3 = 3.95$

5. a= -1.85, b=1.48, c = -1.55, d = -1.87, e= -4.3199999, f =0.63, $r_1 = 4, r_2 = 4, r_3 = 3.95$

6. a= -1.85, b=1.48, c = -1.55, d = -1.87, e= -4.32, f =0.6300001, $r_1 = 4, r_2 = 4, r_3 = 3.95$

7. a= -1.85, b=1.48,c= -1.55, d= -1.87, e= -4.32, f=0.63, $r_1 = 4.0000001, r_2 = 4, r_3 = 3.95$

8. a= -1.85, b=1.48, c= -1.55, d= -1.87, e= -4.32, f=0.63, $r_1 = 4, r_2 = 3.9999999, r_3 = 3.95$

9. a= -1.85, b=1.48, c = -1.55, d = -1.87, e= -4.32, f =0.63, $r_1 = 4, r_2 = 4, r_3 = 3.9500001$

Table 8 shows the NPCR and UACI between the cipher images with the correct key and slightly different keys mentioned above.

The cipher images with the correct and slightly different keys are compared pixel-by-pixel.

This table shows that more than 99.60 % pixels in the cipher image change their gray rate when one of the keys just changes 10^{-6}. If a slightly modified key is used to decrypt the cipher image, the decryption fails completely.

Table 8: NPCR and UACI between the cipher image with key a = -1.85, b=1.48, c = -1.55, d = -1.87, e= -4.32, f =0.63, $r_1 = 4,\ r_2 = 4,\ r_3 = 3.95$ and other cipher images with slightly different keys

kinds of modified key	NPCR %	UACI%
(1)	99.609375	33.592696
(2)	99.633789	33.157360
(3)	99.682617	33.522015
(4)	99.621582	33.578503
(5)	99.615478	33.558229
(6)	99.627685	33.343601
(7)	99.511718	33.441856
(8)	99.652099	33.585659
(9)	99.670410	33.661726

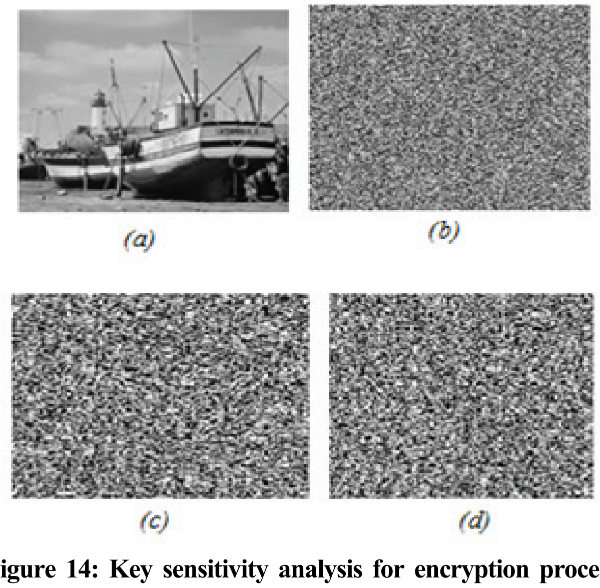


Figure 14: Key sensitivity analysis for encryption process for CT scan of brain Image (a) Plain Image (b) Cipher image with correct key (c) Cipher image by changing parameter b, b=1.4800001 (d) Cipher image by changing parameter $r_3 = 3.9500001$.

Comparison of NPCR and UACI for five cipher images by using proposed and Clifford systems is listed in Table 9.

Table 9: Comparison of NPCR and UACI between cipher image with key a = -1.85, b=1.48, c = -1.55, d = -1.87, e= -4.32, f =0.63, $r_1 = 4, r_2 = 4, r_3 = 3.95$ and other cipher images by changing parameter b, b=1.4800001

Image	Proposed system		Clifford system	
	NPCR%	UACI%	NPCR %	UACI%
Lena	99.613952	33.464651	99.599711	33.402580
Puppy	99.630522	33.470107	99.623159	33.488289
Mandrill	99.613621	33.477241	99.606999	33.518280
Elaine	99.587530	33.284322	99.613497	33.452525
Barbara	99.609075	33.515951	99.607467	33.476234

5. Conclusions

The reported paper aimed at developing a secure algorithm for image encryption. A computer simulation is used to evaluate and compare the encrypted images by the proposed algorithm with other methods. The results of computer simulation show good results in the proposed method by using the noisy Logistic map to achieve the improvements of the Clifford system.

These comparisons were based on chi-square test of histogram, correlation coefficients of pixels, NPCR, entropy test, UACI, key space and sensitivity analysis.

In ideal condition, there should not be any relation between the pixels of the encrypted image. As shown in Figure 13, Table2 and Table3, the absolute value of correlation coefficient of the proposed system is less than image encryption algorithms by Yue et al. (2014), Wan and Lie (2012) and Fu et al. (2011).

The results of statistical tests provided sufficient evidence for the superiority of the proposed chaotic image encryption system over other algorithms.

Submitted : Jan. 4, 2017

Accepted : April 15, 2017

There is no conflict of interest for all authors.

References

Alattar, A. M. et al., (1999), *Improved Selective Encryption Techniques for Secure Transmission of MPEG Video Bit-streams*, ICIP'99.

Arrowsmith, D. and Place, C. M. (1992), *Dynamical Systems: Differential Equations, Maps, and Chaotic Behaviour*, New York, Chapman & Hall.

Baptista, M. S. (1991), Cryptography with chaos, *Physics Letters A*, 240, pp. 50–54.

Fu, C., Lin, B., Miao, Y., Liu, X. and Chen, J. (2011), A novel chaos-based bit-level permutation scheme for digital image encryption, *Optics Commun*, 284, pp. 5415–5423.

Fridrich, J. (1998), Symmetric ciphers based on two-dimensional chaotic maps, *Int. J. Bifurcation and Chaos*, vol. 8, no. 6, pp. 1259–1284.

Giesl. J. and Vlcek. K. (2009), Image encryption based on strange attractors*, ICGST-GVIP Journal*, Vol .9, Issue (II), pp. 19-26.

Hua, Z., Zhou, Y., Pun, C. M. and Chen, C. L. P. (2015), 2D Sine logistic modulation map for image encryption, *Inf. Sci.,* 297, pp. 80-94.

Kocarev, L. and Lian, S. (2011), *Chaos-Based Cryptography, Theory, Algorithms and Applications*, New York, Springer.

Matthews, R. (1989), On the derivation of a chaotic encryption algorithm*, Cryptology*, 8, pp. 29–41.

Meyers R. A. (2009), *Complex Systems in Finance and Econometrics*, New York, Springer.

Patidar, V., Pareek, N. K., Purohit, G. and Sud, K. (2010), Modified substitution-diffusion image cipher using chaotic standard and logistic maps, *Commun. Nonlinear Sci. Number Simul.*, 15, pp. 2894-2906.

Pickover, C. (1988), A note on rendering 3-D strange attractors, *Computers & Graphics*, Vol. 12, pp. 263-267.

Park, S. H., Choi, H. J., Seo, Y. H. and Kim, D. W. (2005), Ciphering scheme and hardware implementation for MPEG-based image/video security, *Journal of the Institute of Electronics and Information Engineers* , Vol. 42, No. 2, pp. 27-36.

Pommer, A. and Uhl, A. (2001), Wavelet Packet Methods for Multimedia Compression and Encryption*, IEEE Pacific Rim Conf. On Communications, Computers, and Signal Processing*, pp. 1-4.

Sprott, J. C. (1993), How common is chaos?, *Physics Letters A*, 173, pp. 21-24.

Sprott, J. C. (1993), *Strange attractors: Creating Patterns in Chaos*, M&T Books.

Seo, Y. H., Choi, E. S. and Kim, D. W. (2013), Efficient encryption technique of image using packetized discrete wavelet transform, *Journal of Korea Institute of Information and Communication Engineering*, Vol.17, No. 3, pp. 603-611.

Wang, X. Y. and Gua, K. (2014), A new image alternate encryption algorithm based on chaotic map, *Nonlinear Dyn.*, 67, pp. 1943-1950.

Wang, X. and Lie, Y. (2012), A novel chaotic image encryption algorithm based on water wave motion and water drop diffusion models, *Optics communications*, 282, 4033-4042.

Wu, Y., Noonan, J. P. and Agaian, S. (2011), Shannon entropy based randomness measurement and test for image encryption, *Information Sciences*, pp. 1-23.

Wu, X. and Moo, P. W.(1999), Joint image/video compression and encryption via high-order conditional entropy coding of wavelet coefficients, *Int'l Conference on Multimedia Computing and Systems*, pp. 908-912.

Yen, J. C. and Guo, J. I. (2000), A new chaotic key-based design for image encryption and decryption, ISCAS, *IEEE International Symposium on Circuits and Systems*, May 28-31, Geneva, Switzerland, IV, pp. 49-52.

Yue, W., Yicong, Z., Joseph, P. et al. (2014), Design of image cipher using Latin squares, *Information Sciences*, 264, 317-339.

Zelinka, I., Celikovsky, S., Richter, H. and Chen, G. (2010), *Evolutionary Algorithms and Chaotic Systems*, Springer-Verlag Berlin Heidelberg.