I. J. Computer Network and Information Security, 2015, 5, 25-33
Published Online April 2015 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2015.05.04

An Image Encryption Scheme Based on Hybrid Orbit of Hyper-chaotic Systems

Junming Ma and Ruisong Ye*
Department of Mathematics, Shantou University Shantou, Guangdong, 515063, P. R. China
* Corresponding author, Email: rsye@stu.edu.cn

***Abstract*—**This paper puts forward a novel image encryption scheme based on ordinary differential equation system. Firstly, a hyper-chaotic differential equation system is used to generate two hyper-chaotic orbit sequences. Introducing the idea of hybrid orbit, two orbits are mixed to generate a hybrid hyper-chaotic sequence which is used to be the initial chaotic key stream. Secondly, the final encryption key stream is generated through two rounds of diffusion operation which is related to the initial chaotic key stream and plain-image. Therefore, the algorithm's key stream not only depends on the cipher keys but also depends on plain-image. Last but not least, the security and performance analysis have been performed, including key space analysis, histogram analysis, correlation analysis, information entropy analysis, peak signal-to-noise ratio analysis, key sensitivity analysis, differential analysis etc. All the experimental results show that the proposed image encryption scheme is secure and suitable for practical image and video encryption.

***Index Terms*—**Hyper-chaotic system, hybrid hyper-chaotic sequence, image encryption, diffusion operation.

I. Introduction

With the rapid developments of multimedia processing and network techniques in the last decades, digital multimedia data like images, videos, audios is being stored on different media, increasingly shared and communicated over the Internet and wireless networks. Protection of digital information against illegal usage becomes extremely urgent. Image encryption is a direct and efficient way to protect image information from unauthorized eavesdropping. Digital images possess some intrinsic features, such as bulk data capacity, high correlation among adjacent pixels, and human visual properties. As a consequence, traditional encryption algorithms, such as DES, RSA [1], are thereby not suitable for practical digital image encryption due to the weakness of low-level efficiency while encrypting images.

Chaotic system has been popularized in most aspects of science, such as mathematics, physics, biology, computer, finance and even arts. In particular chaotic system has been successfully introduced to modern cryptography thanks to its fantastic features, such as topological transitivity, orbit inscrutability, sensitivity to initial conditions and control parameters, pseudo-randomness, etc. which meet the fundamental requirements such as mixing and diffusion in the sense of cryptography. These properties make chaotic system a potential candidate for constructing cryptosystems [2-15]. As a consequence, many chaos-based image cryptosystems have been proposed. However, most of the existing chaos-based image cryptosystems adopted low dimensional chaotic systems with permutation-diffusion architecture. The permutation–diffusion chaos-based image encryption scheme is firstly proposed by Fridrich in 1998 [2]. The proposed architecture is usually composed of two processes: chaotic confusion of pixel positions by permutation process and diffusion of pixel gray values by diffusion process, where the former permutes the plain-image pixel positions governed by a 2D chaotic map, while the latter changes the pixel gray values sequentially controlled by a 1D chaotic map, so that a tiny change for one pixel can spread out to almost all pixels in the whole image. The Fridrich architecture has become the most popular structure adopted in a great number of chaos-based image encryption algorithms subsequently proposed [2-8, 10-11]. However, some image encryption schemes based on low dimensional chaotic systems with permutation–diffusion architecture are broken recently [16-20]. The common drawbacks of permutation–diffusion based image encryption algorithms are outlined as follows. Firstly the key stream in the diffusion step only depends on the cipher key. The key streams used to encrypt different plain-images are the same if the cipher key keeps unchanged. The attacker can obtain the key stream by known-plaintext attack and chosen-plaintext attack. Secondly the two processes will become independent if the plain-image is a homogeneous one with identical pixel gray value [21]. Thirdly the cryptosystems based on low dimensional chaotic systems have some weakness, such as small key space, short periodicity and weak security. Such a kind of encryption algorithms can be generally attacked by the following steps: (i) a homogeneous image with identical pixel gray values is adopted to eliminate the confusion effect; (ii) the key-stream of the diffusion process is obtained via known-plaintext or chosen plaintext attacks; (iii) the remaining cipher-image can be regarded as the output of a kind of permutation-only cipher, which has been shown insecure and can be cryptanalyzed by known-plaintext or chosen plaintext attacks [22, 23].

Copyright © 2015 MECS

It has been pointed out that the permutation process is not necessary in an image encryption scheme. Usually, omitting the permutation process will improve the executing time and make the proposed scheme more simple and easy to implement. For example, the two stages of permutation and diffusion were combined and were executing at the same time at the pixel level or bit level [7]. Regarding the security issue, hyper-chaotic systems can be employed to improve the security of the cryptosystem proposed [7, 24]. Higher dimensional chaotic systems with higher dimensional attractors shall have good chaotic features. The adopting of higher dimensional chaotic systems which own more than one positive Lyapunov exponents clearly improves the security of encryption scheme by generating more complex dynamical behavior or high randomness. It is more difficult to predict the chaotic sequences generated by higher dimensional chaotic systems. Therefore, some high dimensional chaotic systems are used in image encryption.

In this paper, we propose an image encryption scheme based on hybrid orbit of hyper-chaotic system and diffusion-only mechanism. As far as we know, image encryption scheme based on hybrid orbit of hyper-chaotic system only with diffusion operation has not been reported. The adopting of hybrid orbit of hyper-chaotic system can enlarge the key space efficiently and therefore enhance the security. Given two sets of initial states, the fourth order Ronge-Kutta method is used to generate two orbits of the hyper-chaotic system consisting of four ordinary differential equations. Tent map is applied to generate one pseudo-random sequence to determine the hybrid orbit points from which of the two yielded orbits. Based on the improved hyper-chaotic sequences derived by the hybrid orbit, we design an image encryption scheme with plain-image dependent key stream. The proposed scheme applies different key streams when encrypting different plain-images (even with the same hybrid hyper-chaotic sequences). To make the proposed scheme resist differential analysis attack, we perform one diffusion process with two rounds of diffusion operation which depends on both the cipher keys and the plain-image. The diffusion process can modify the pixel values and break the correlations between adjacent pixels of an image simultaneously. The security and performance analysis of the proposed image encryption are carried out using the histograms, correlation coefficients, information entropy, key sensitivity analysis, differential analysis, key space analysis, etc. All the experimental results show that the proposed image encryption scheme is highly secure and excellent performance, which makes it suitable for practical application.

The rest of the paper is organized as follows. In Section II, we briefly introduce the hyper-chaotic system and discuss its chaotic natures. The improved hybrid sequence from hyper-chaotic sequences is outlined as well. Section III devotes to designing the image encryption scheme. One diffusion function is presented to encrypt images. In Section IV, we present the results of security and performance analysis of the proposed image encryption scheme using the histograms, correlation coefficients, information entropy, key sensitivity analysis, differential analysis, key space analysis, encryption rate analysis, etc. Section V concludes the paper.

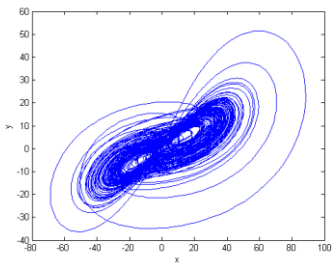
II. The Hyper-Chaotic System and Its Hybrid Orbits

A. The hyper-chaotic system

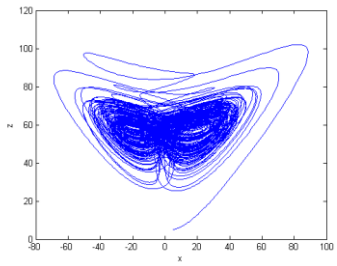
The notation of hyper-chaotic system is firstly put forward by Rössler in 1979 [25]. Hyper-chaotic system is a high order ordinary differential equation, which is widely applied in cryptography and circuit design. Hyper-chaotic system presents more than one positive Lyapunov exponents and therefore generates more complex dynamical behavior or high randomness. The hyper-chaotic sequences generated surely improve the security of encryption scheme. In this paper, a hyper-chaotic system is used in key scheming and modeled by

$$\begin{cases} \dot{x} = a(y-x) + yz, \\ \dot{y} = cx - y - xz + w, \\ \dot{z} = xy - bz, \\ \dot{w} = dw - xz, \end{cases} \tag{1}$$

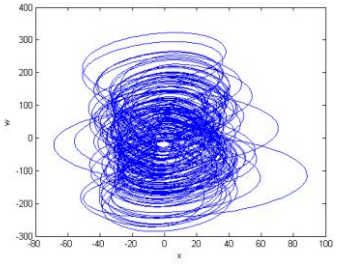
where a, b, c and d are system parameters. When $a = 35, b = 8/3, c = 55, d = 1.3$, the Lyapunov exponents of system (1) are $\lambda_1 = 1.4164$, $\lambda_2 = 0.5318$, $\lambda_3 = 0$, $\lambda_4 = -39.1015$, implying that system (1) exhibits a hyper-chaotic behavior. For the initial condition (x_0, y_0, z_0, w_0), one can obtain four hyper-chaotic sequences $\{x_i, y_i, z_i, w_i : i = 1, 2, 3, \cdots\}$ by the fourth order Runge–Kutta algorithm. These hyper-chaotic sequences are non-periodicity and very sensitive dependence on initial conditions (x_0, y_0, z_0, w_0). Setting the initial conditions $(x_0 = 5, y_0 = 10, z_0 = 5, w_0 = 10)$ and integration step h=0.001, we solve system (1) and get the first 5000 real values of each sequence. The corresponding sequence pairs are depicted in Figure 1.



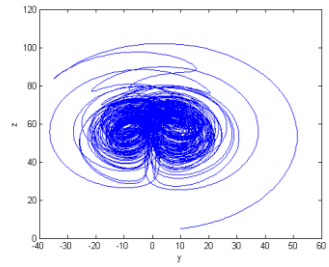
(a) $x - y$ projection



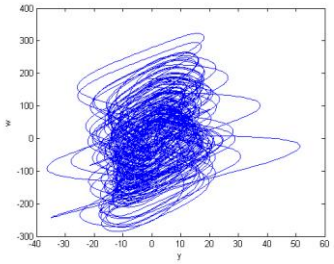
(b) $x-z$ projection



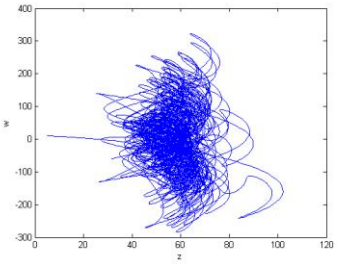
(c) $x-w$ projection



(d) $y-z$ projection



(e) $y-w$ projection



(f) $z-w$ projection

Fig.1. The phase diagrams of hyper-chaotic sequence pairs.

B. Generation of hyper-chaotic sequences

Assume that we need one hyper-chaotic sequence with length L. Set the initial condition to be $(x_0^1, y_0^1, z_0^1, w_0^1)$ one can solve system (1) by the fourth order Runge–Kutta algorithm to obtain four hyper-chaotic sequences $\{x_i,\ y_i,\ z_i,\ w_i :\ i=1,\ 2,\ 3,\cdots, L/4\}$. Then we process the four hyper-chaotic sequences to be four 8-bit gray value sequences by

$$s_i^* = \mathrm{mod}(|\ fix(s_i\ -\ fix(s_i))\times 10^{14}\ |,\ 256) \tag{2}$$

where $fix(x)$ rounds the elements of x to the nearest integers towards zero, $\mathrm{mod}(x, y)$ represents the remainder of x divided by y. We then get four hyper-chaotic sequences $\{xs_i^1, ys_i^1, zs_i^1, ws_i^1, i=1,...,L/4\}$. We integrate the four sequences to be one mixed sequence $S^1=\{k_i^1, i=1,...,L\}$ by

$$\begin{aligned} &k_{4i-3}^1 = xs_i^1, k_{4i-2}^1 = ys_i^1, k_{4i-1}^1 = zs_i^1, \\ &k_{4i}^1 = ws_i^1, i=1,2,...,L/4. \end{aligned} \tag{3}$$

Set the initial condition to be $(x_0^2, y_0^2, z_0^2, w_0^2)$ different from $(x_0^1, y_0^1, z_0^1, w_0^1)$, one can similarly obtain another integrated sequence $S^2=\{k_i^2, i=1,...,L\}$.

C. Generation of hybrid hyper-chaotic sequences

The tent map is used to generate one random sequence $\{t_n, n=1,...,L\}$ which is quantized to be one two-value sequence $\{l_n, n=1,...,L\}$. l_n is used to determine $k_n^{l_n}$ to form one hybrid sequence $\{k_n^{l_n}, n=1,2,\cdots,L\}$. The chaotic tent map is defined by

$$t_{i+1} = \begin{cases} \dfrac{t_i}{q}, & 0<t_i<q \\ \dfrac{1-t_i}{1-q}, & q<t_i<1 \end{cases}, t_i \in [0,1], i=1,2,\ldots,n, \tag{4}$$

where q is the control parameter, t_i is the state variable, t_0 is the initial value. The tent map shows good chaotic nature, including ergodicity, pseudo-randomness, high sensitivity to control parameters and initial values, etc. Set the control parameter and initial value $q=0.3,\ t_0=0.4$, we iterate the system (4) to get chaotic sequence $\{t_n, n=1,...,L\}$, and yield the choice sequence by

$$l_i = floor(t_i\times 2)+1, i=1,2,\ldots,L. \tag{5}$$

To improve the computation efficiency, we introduce two counter variables $T(1), T(2)$, which are used to count the number of points selected from the k th hyper-chaotic sequence S^k. $T(1), T(2)$ are initialized to be zero. As the k th hyper-chaotic sequence S^k is chosen, $T(k)$ is increased by 1. When the hybrid hyper-chaotic sequence with length L is finally generated, $\sum_{i=1}^{2} T(i) = L$. We denote

the hybrid hyper-chaotic sequence with length L to be $\{mk_i, i=1,...,L\}$ yielded by

$$mk_i = k^{l_i}_{T(l_i)}, i=1,2,...,L. \quad (6)$$

III. The Proposed Image Encryption Scheme

We assume that the plain-image is a 8-bit gray-scale image of size $L=M\times N$, it is an integer matrix of M rows and N columns, in which the values range from 0 to 255. The 2D pixel gray value matrix can be convert to a 1D vector $P=\{p_1, p_2,..., p_L\}$, where p_i denotes the gray level of the image pixel in the row $floor(i/N)$ and column $mod(i,N)$, where $floor(x)$ rounds x to the nearest integer less than or equal to x. The hyper-chaotic system (1) is used to generate the initial chaotic key stream. The image encryption scheme is based on the final secret key stream which is not only related on the original chaotic key stream but also the plain-image. The image encryption scheme includes generating initial chaotic key stream and two rounds of diffusion operation.

A. The generation of initial chaotic key stream

Step 1. Input the initial conditions $(x^1_0, y^1_0, z^1_0, w^1_0)$ and $(x^2_0, y^2_0, z^2_0, w^2_0)$, set the step h, and integer $N_0 > 500$, the control parameter and initial condition q, t_0, integer $C_0 \in [0,255]$.

Step 2. Solve the hyper-chaotic system (1) with the initial conditions $(x^1_0, y^1_0, z^1_0, w^1_0)$ and $(x^2_0, y^2_0, z^2_0, w^2_0)$ respectively. Discard the first N_0-1 points of the orbits to overcome the transient effect. Set the N_0 th points $(x^1_{N_0}, y^1_{N_0}, z^1_{N_0}, w^1_{N_0})$ and $(x^2_{N_0}, y^2_{N_0}, z^2_{N_0}, w^2_{N_0})$ to the new initial conditions.

Step 3. Iterate the tent map (4) for N_0+L times, and discard the first N_0 transient points and preserve the remainder which is still denoted as $\{t_i, i=1,...,L\}$, and then generate the two-value orbit choice sequence $Ln=(l_1,l_2,...,l_L)$.

Step 4. To reduce the workload, we count the number of 1 and 2 in $Ln=(l_1,l_2,...,l_L)$. It is then easy to calculate needed orbit point numbers T_1 and T_2 of the two hyper-chaotic orbit derived from the new initial conditions $(x^1_{N_0}, y^1_{N_0}, z^1_{N_0}, w^1_{N_0})$ and $(x^2_{N_0}, y^2_{N_0}, z^2_{N_0}, w^2_{N_0})$. We note that T_1 and T_2 should satisfy $4\times(T_1+T_2)\geq L$ and can be calculated by

$$T_j = ceil(sum(Ln == j)/4),\ j=1,2,$$

where $sum(x==y)$ denotes the total number of $x(i)=y(i), i=1,2,\cdots,L$, $ceil(x)$ rounds x to the nearest integer greater than or equal to x.

Step 5. Solve the system (1) by initial condition $(x^1_{N_0}, y^1_{N_0}, z^1_{N_0}, w^1_{N_0})$ and step h and get four hyper-chaotic sequences $\{x^1_i, y^1_i, z^1_i, w^1_i, i=N_0+1,..., N_0+T(1)\}$. We then generate the first improved hyper-chaotic sequence $\{k^1_i, i=1,...,4T_1\}$ by (2) and (3). Similarly the second improved hyper-chaotic sequence $\{k^2_i, i=1,...,4T_2\}$ is either generated with initial condition $(x^2_{N_0}, y^2_{N_0}, z^2_{N_0}, w^2_{N_0})$ and step h.

Step 6. Combine the improved hyper-chaotic sequences $\{k^1_i, i=1,...,4T_1\}$ and $\{k^1_i, i=1,...,4T_2\}$ to be one hybrid initial key stream $\{mk_i\}, i=1,...,L$ by (6).

B. Two rounds of diffusion operation

Assume that the 2D gray value matrix of the plain-image is converted to be one vector $P=\{p_1, p_2,..., p_L\}$, and $C=\{c_1, c_2,..., c_L\}$ denotes the corresponding vector of the cipher-image. One diffusion process is outlined as follows.

Step 1. Set $i=1$.

Step 2. Compute the first pixel gray value of the cipher-image by using the first pixel gray value of the plain-image, the integer C_0 and the first initial key stream element mk_1 by

$$c_1 = bitxor(p_1, bitxor(\mathrm{mod}(C_0+mk_1, 256), mk_1)),$$

where $bitxor(x,y)$ returns the result after bitwise XOR operation.

Step 3. Let $i=i+1$, and calculate the next pixel gray value of the cipher-image by using c_{i-1}, the i th pixel gray value of the plain-image and the i th initial key stream element mk_i by

$$c_i = bitxor(p_i, bitxor(\mathrm{mod}(c_{i-1}+mk_i, 256), mk_{i-1}))$$

Step 4. Return to Step 3 until $i=L$, and finally we get the cipher-image vector $C=\{c_1, c_2,..., c_L\}$ after one round of diffusion.

Step 5. Set $i=1$.

Step 6. Utilized the first pixel gray value c_1, the last one c_L, and mk_1 to get c_1 by

$$c_1 = bitxor(c_1, bitxor(\mathrm{mod}(c_L+mk_1, 256), mk_1))$$

Step 7. Let $i=i+1$, then calculate c_i by

$$c_i = bitxor(c_i, bitxor(\mathrm{mod}(c_{i-1}+mk_i, 256), mk_{i-1}))$$

Step 8. Return to Step 7 until $i=L$. The finally yielded vector $C=\{c_1, c_2,..., c_L\}$ is the resulted cipher-image after two rounds of diffusion operation.

Copyright © 2015 MECS

IV. Security and Performance Analysis

According to the basic principle of cryptology [1], an ideal encryption cryptosystem requires sensitivity to cipher keys, i.e., the cipher-text should have close correlation with the keys. Furthermore, an ideal encryption scheme should have a large key space to make brute-force attack infeasible; it should also well resist various kinds of attacks like statistical attack, differential attack, etc. Some security analysis will be performed on the proposed image encryption scheme, including the most important ones like key sensitivity test, key space analysis, statistical analysis, and differential attack analysis. The plain-image is 256 gray-scale and of size 256×256 (including Lena, Boat, Cameraman). In the simulation experiment, we set two initial conditions

$$(x_0^1=5, y_0^1=10, z_0^1=5, w_0^1=10),$$
$$(x_0^2=10, y_0^2=5, z_0^2=10, w_0^2=5),$$

and step $h=0.001$, $N_0=1000$, $C_0=3$, $q=0.3$, $t_0=0.4$. All the analysis shows that the proposed image encryption scheme is highly secure thanks to its high sensitivity of the control parameters and initial conditions of the considered chaotic systems, large key space, and satisfactory diffusion mechanism.

A. Key space analysis

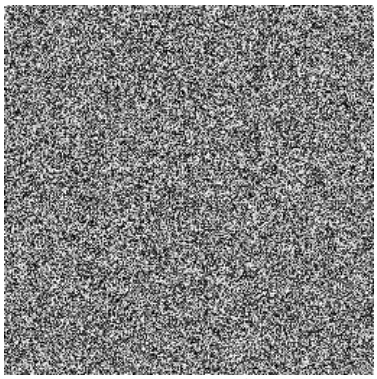
Key space consists of all the possible cipher keys. A good image encryption scheme needs to contain sufficiently large key space for compensating the degradation dynamics in PC. It should be also large enough to effectively resist brute-force attack and prevent invaders decrypting original data even after they invest large amounts of time and resources. We can just set the two initial conditions $(x_0^1, y_0^1, z_0^1, w_0^1)$, $\left(x_0^2, y_0^2, z_0^2, w_0^2\right)$ of the hyper-chaotic system, the initial condition t_0 and the control parameter q of chaotic tent map to be the cipher keys. If they are represented as floating number with precision 10^{-14}, then the number of x_0^1 is 10^{14}, Therefore the total cipher keys will be as many as $(10^{14})^{10}\approx 2^{465}$, which is large enough to make brute-force attack infeasible.

B. Statistical analysis

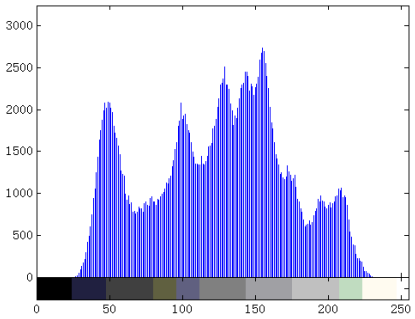
Shannon pointed out in his masterpiece [26] the possibility to solve many kinds of ciphers by statistical analysis. Therefore, passing the statistical analysis on cipher-image is of crucial importance for a cryptosystem. Indeed, an ideal cryptosystem should be robust against any statistical attack. In order to prove the security of the proposed encryption scheme, the following statistical tests are performed.

(i) Histogram analysis. We encrypt the plain-image Lena (Figure 2(a)) and get the cipher-image Figure 2(b). We also plot the histograms of plain-image and cipher-image as shown in Figures 2(c)-(d). Figure 2(d) shows that the histograms of cipher-image is fairly uniform and significantly different from the histogram of the original plain-image Figure 2(c). Hence it does not provide any useful information for the opponents to perform any statistical analysis attack on the encrypted image.

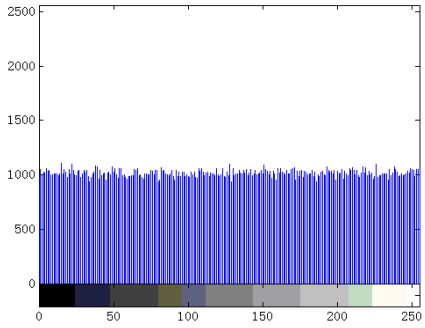
(a) plain-image Lena



(b) cipher-image of Lena



(c) Histogram of Lena



(d) histogram of cihoer-image of Lena

Fig. 2. The histogram analysis result.

(ii) Correlation analysis of adjacent pixels. To test the correlation between two adjacent pixels, the following performances are carried out. First, we select 1000 pairs of two adjacent pixels randomly from coefficient of the selected pairs using the following formulae:

$$Cr = \frac{\operatorname{cov}(x,y)}{\sqrt{D(x)D(y)}},$$

$$\operatorname{cov}(x,y) = \frac{1}{T}\sum_{i=1}^{T}\big(x_i - E(x)\big)\big(y_i - E(y)\big),$$

$$E(x) = \frac{1}{T}\sum_{i=1}^{T} x_i, D(x) = \frac{1}{T}\sum_{i=1}^{T}\big(x_i - E(x)\big)^2,$$

where x, y are the gray-scale values of two adjacent pixels in the image and T is the total pairs of pixels randomly selected from the image. The correlations of two adjacent pixels in the plain-image and in the cipher-image are shown in Table 1. It is clear from Table 1 that the proposed image encryption technique significantly reduces the correlation between the adjacent pixels of the plain-image.

Table 1. Correlation between adjacent pixels of plain-image and cipher-image.

	horizontal	vertical	diagonal
Plain-image Lena	0.9446	0.9718	0.9206
Cipher-image of Lena	0.0003	0.0005	-0.0060
Plain-image Boat	0.9233	0.9409	0.8815
Cipher-image of Boat	0.0145	-0.0124	-0.0118
Plain-image Cameraman	0.9415	0.9626	0.9167
Cipher-image of Cameraman	0.0762	0.0163	-0.0494

(iii) Correlation between plain-images and cipher-images. We have also analyzed the correlation between plain-image and cipher-image by computing the two-dimensional correlation coefficients between of plain-image and cipher-image. The 2D-correlation coefficients are calculated by

$$C_{AB} = \frac{\frac{1}{H\times W}\sum_{i=1}^{H}\sum_{j=1}^{W}(A_{i,j} - \bar{A})(B_{i,j} - \bar{B})}{\sqrt{\left(\frac{1}{H\times W}\sum_{i=1}^{H}\sum_{j=1}^{W}(A_{i,j} - \bar{A})^2\right)\left(\frac{1}{H\times W}\sum_{i=1}^{H}\sum_{j=1}^{W}(B_{i,j} - \bar{B})^2\right)}},$$

$$\bar{A} = \frac{1}{H\times W}\sum_{i=1}^{H}\sum_{j=1}^{W}A_{i,j}, \quad \bar{B} = \frac{1}{H\times W}\sum_{i=1}^{H}\sum_{j=1}^{W}B_{i,j},$$

where A represents one of the red, green and blue channel of the plain image, B represents one of the red, green and blue channel of the cipher image, $\bar{A}$ and $\bar{B}$ are the mean values of the elements of 2D matrices A and B respectively; M and N are respectively the height and width of the plain/cipher image. We have computed the correlation coefficients for the pair of plain-image Lena and its corresponding cipher-image. The results are shown in Table 2. One can see from the results that the correlation coefficients between plain-image and cipher-image are very small (or practically zero), hence the cipher-image owns the characteristics of a random image.

Table 2. Correlation between plain-image and cipher image.

Image	Encryption CC	entropy	PSNR	Decryption CC
Lena	-0.003545	7.9972	9.3566	1.0
Boat	-0.002246	7.9970	9.3530	1.0
Cameraman	0.000475	7.9971	8.3771	1.0

(iv) Information entropy analysis. Information entropy is a measure of the uncertainty associated with a random variable and can be also a measure of disorder and randomness. It quantifies the amount of information contained in data, usually in bits/symbol. Two extremely cases are: a long sequence of repeating characters and a truly random sequence. The former has entropy of 0 since every character is predictable, and the latter has maximum entropy since there is no way to predict the next character in the sequence. Regarding image, it can be used to measure the uniformity of image histograms. The entropy $H(m)$ of a message source m can be measured by

$$H(m) = -\sum_{i=0}^{L-1} p(m_i)\log(p(m_i)) \text{ (bits)},$$

where L is the total number of symbols m, $p(m_i)$ represents the probability of occurrence of symbol m_i and log denotes the base 2 logarithm so that the entropy is expressed in bits. For a random source emitting 256 symbols, its entropy is $H(m) = 8$ bits. For a 8-bit gray image, the information entropy is given as

$$H(m) = \sum_{i=0}^{2^8-1} P(I_i)\log_2\frac{1}{P(I_i)} \text{ (bits).}$$

We have calculated the information entropies for plain-images and their corresponding cipher-images. The results are shown in Table 2. The value of information entropy for the cipher-image produced by the proposed image encryption scheme is very-very close to the expected value of truly random image, i.e., 8bits. Hence the proposed encryption scheme is extremely robust against entropy attacks.

(v) Peak signal-to-noise ratio analysis. Another parameter to describe the encryption quality is the peak signal-to-noise ratio (PSNR). This term is described based on that the mean squared error (MSE) is calculated. This criterion provides the error between input image and output image. The MSE value is

$$MSE = \left\{ \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \left[I_O(i,j) - I_E(i,j) \right]^2 \right\}^{1/2},$$

where $I_O(i,j)$ is the pixel value of plain-image, $I_E(i,j)$ is the pixel value of cipher-image. Thus the PSNR is described by

$$PSNR = 20 \log \left[\frac{I_{\max}}{MSE} \right]$$

where $I_{\max}$ is the maximum of pixel value of the image. The PSNR should be a low value, which corresponds to great difference between the original image and the encrypted image. To determine the encryption quality, the PSNR is computed for the encryption of Lena, Boat and Cameraman. In Table 2, the PSNR values are shown in the fourth column. The results show that these PSNR values are all very low. Therefore, the encryption quality is good in sense of PSNR.

C. Sensitivity Analysis

To test the sensitivity of cipher keys and plain-image, two measures NPCR (net pixel change rate) and UACI (unified average changing intensity) are usually used. NPCR measures the percentage of different pixel numbers between the two encrypted images. UACI measures the average intensity of difference between the two encrypted images. They can be calculated by the following formulae:

$$\mathrm{NPCR} = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\%,$$

$$\mathrm{UACI} = \frac{1}{M \times N} \left[\sum_{i,j} \frac{|c_1(i,j) - c_2(i,j)|}{255} \right] \times 100\%$$

where c_1 and c_2 are the two cipher-images and $D(i,j)$ is defined by

$$D(i,j) = \begin{cases} 1, & c_1(i,j) \neq c_2(i,j), \\ 0, & \text{otherwise.} \end{cases}$$

The NPCR for two random images, which is an expected estimate for an ideal image cryptosystem, is given by $\mathrm{NPCR}_{Expected} = (1 - 2^{-L}) \times 100\%$, where L is the number of bits used to represent all the gray values of the considered image. For a 8-bit gray scale image L, hence $\mathrm{NPCR}_{Expected} = 99.6094\%$.

The UACI for two random images, which is an expected estimate for an ideal image cryptosystem, is given by $\mathrm{UACI}_{Expected} = \frac{1}{2^{2L}} \cdot \frac{\sum_{i=1}^{2^L - 1} i(i+1)}{2^L - 1} \times 100\%$. For a 8-bit gray image, $\mathrm{UACI}_{Expected} = 33.4635\%$.

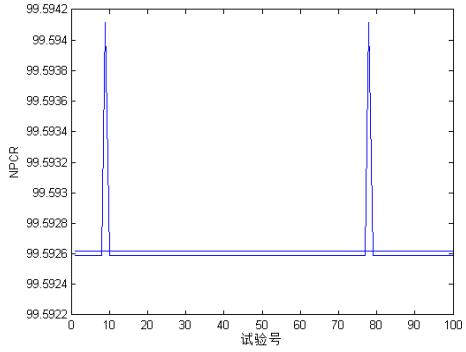
(i) Key sensitivity analysis. A good image encryption scheme should be extremely sensitive to cipher keys, which is an essential feature for any good cryptosystem in the sense that it can effectively prevent invaders decrypting original data even after they invest large amounts of time and resources. Assume that we want to verify the sensitivity of cipher key K, we encrypt the plain-image $A = (A(i,j))_{M \times N}$ with K and $K + \Delta K$ respectively while keeping the other keys unchanged, the corresponding encrypted images are A_1, A_2 respectively, where ΔK is the perturbing value. We then calculate the corresponding NPCR,UACI,CC and PSNR. We set the perturbing value to be 10^{-10} and get the results shown in Table 3. All the experimental results show that the cipher keys are all strongly sensitive.

Table 3. Key sensitivity analysis

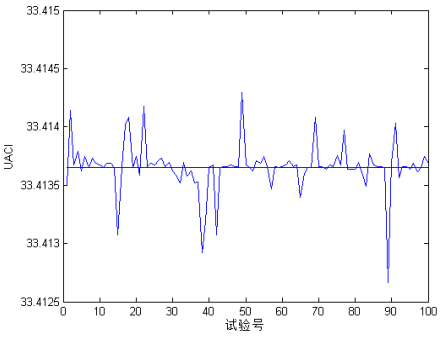
Perturbing value	NPCR	UACI	CC	PSNR
$\Delta x = 10^{-10}$	99.6338	33.6484	-0.0071	7.7203
$\Delta y = 10^{-10}$	99.5880	33.3717	0.0047	7.7648
$\Delta z = 10^{-10}$	99.6017	33.3773	0.0057	7.7687
$\Delta w = 10^{-10}$	99.6124	33.3265	0.0084	7.7757
$\Delta a = 10^{-10}$	99.5956	33.4732	0.0013	7.7355
$\Delta t_0 = 10^{-10}$	99.6124	33.4483	0.0047	7.7498

(ii) Plain-image sensitivity analysis. The differential cryptanalysis of a block cipher is the study of how differences in a plaintext can affect the resultant differences in the ciphertext with the same cipher key. It

is usually done by implementing the chosen plaintext attack but now there are extensions which use known plaintext as well as ciphertext attacks also. As for image cryptosystems, attackers may generally make a slight change (e.g., modify only one pixel) of the plain-image, and compare the two cipher-images (obtained by applying the same cipher key on two plain-images having one pixel difference only) to find out some meaningful relationships between the plain-image and the cipher-image. If a meaningful relationship between plain-image and cipher-image can be found in such analysis, which may further facilitate the opponents to determine the cipher key. If one minor change in the plain-image will cause significant, random and unpredictable changes in the cipher-image, then the encryption scheme will resist differential attack efficiently. To test the robustness of image cryptosystems against the differential cryptanalysis, We have performed the differential analysis by calculating NPCR and UACI on plain-image Lena. The analysis has been done by randomly choosing 100 pixels (one at a time, including the very first and very last pixels) in each plain-image and changing their all three color values by one unit. The average values of NPCR and UACI thus obtained for all three images are given in Figure 3. It is clear that the NPCR and UACI values are very close to the expected values, thus the proposed image encryption technique shows extreme sensitivity on the plaintext and hence not vulnerable to the differential attacks. The average of the 100 NPCR values is 99.5926% and the average of UACI is 33.4136%, they are both highly close to their expectation values 99.6094% and 33.4635% respectively.



(a) 100 NPCR values



(b) 100 UACI values

Fig. 3. The differential analysis.

D. Resistance to known-plaintext and chosen-plaintext attacks

It follows from the encryption scheme that mk_i is related to the initial cipher keys of the hyper-chaotic system, and c_i depends on the pixel gray values of the plain-image. Hence, the pixel gray values of the plain-image are employed to change the final encryption keys except for the first pixel in the first round of diffusion operation. Hence, the final encryption keys depend on not only the initial state value of the hyper-chaotic system, but also the plain-image. When different plain-images are encrypted, the corresponding key stream is not the same. The attacker cannot obtain useful information by encrypting some special images since the resultant information is related to those chosen-images. Therefore, the attacks proposed in Refs. [16–20] become ineffective on this new scheme. The proposed scheme can well resist the known-plaintext and the chosen-plaintext attacks.

V. Conclusions

In this paper, a novel plain-image dependent encryption scheme based on hybrid orbit of hyper-chaotic system is proposed. Two hyper-chaotic sequences are generate from one hyper-chaotic system and then are improved and integrated into one hybrid sequence to achieve better randomness and security for image encryption. One diffusion procedure with two rounds of diffusion operations are performed, which makes the key stream depend on both the initial hybrid hyper-chaotic sequence and plain-image. Therefore, the key stream in the encryption process depends on both the initial keys and the plain-image and the cipher-image can resist the known-plaintext and chosen-plaintext attacks efficiently. The key space is large enough to resist brute-force attacks as well. All the performance analysis shows that the scheme can well prevent the image from statistical attacking and that the scheme possesses high key sensitivity and gets a good ability to resist differential attack. With high-level security, it can be used in internet applications, such as network security and secure image communications.

Acknowledgment

This research is supported by National Natural Science Foundation of China (No. 11071152 & No. 11271238).

References

[1] B. Schiener, Applied Cryptography: Protocols, Algorithms and Source Code in C, John Wiley and sons, New York, 1996.

[2] F. Huang, Z.-H. Guan, A modified method of a class of recently presented cryptosystems, Chaos, Solitons and Fractals, 23(2005), 1893–1899.

[3] G. J. Zhang, Q. Liu, A novel image encryption method based on total shuffling scheme, Optics Communications, 284(2011), 2775–2780.

[4] R. Ye, A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism, Optics Communications, 284(2011), 5290–5298.
[5] N. K. Pareek, V. Patidar, K. K. Sud, Image encryption using chaotic logistic map, Image and Vision Computing, 24(2006), 926-934.
[6] N. Masuda, K. Aihara, Cryptosystems with discretized chaotic maps, IEEE Trans. Circuits Syst. I, 49(2002), 28–40.
[7] H. Liu, X. Wang, Color image encryption using spatial bit-level permutation and high-dimension chaotic system, Optics Communications, 284(2011), 3895–3903.
[8] S. Behnia, A. Akhshani, S. Ahadpour, H. Mahmodi, A. Akhavan, A fast chaotic encryption scheme based on piecewise nonlinear chaotic maps, Phys. Lett. A, 366(2007), 391–396.
[9] R. Ye, H. Huang, Application of the Chaotic Ergodicity of Standard Map in Image Encryption and Watermarking, I. J. Image, Graphics and Signal Processing, 1(2010), 19–29.
[10] S. Lian, J. Sun, Z. Wang, A block cipher based on a suitable use of the chaotic standard map, Chaos, Solitons and Fractals, 26 (2005), 117–129.
[11] V. Patidar, N. K. Pareek, K. K. Sud, A new substitution–diffusion based image cipher using chaotic standard and logistic maps, Communications in Nonlinear Science and Numerical Simulation, 14 (2009), 3056–3075.
[12] N. Masuda, K. Aihara, Cryptosystems with discretized chaotic maps, IEEE Trans. Circuits Syst. I, 49(2002), 28–40.
[13] R. Ye, W. Guo, An image encryption scheme based on chaotic system with changeable parameters, I.J.Computer Network and Information Security, 6:4(2014), 37-45.
[14] S. Lian, J. Sun, Z. Wang, A block cipher based on a suitable use of the chaotic standard map, Chaos, Solitons and Fractals, 26 (2005), 117–129.
[15] L. Kocarev, Chaos-based cryptography: a brief overview, IEEE Circuits and Systems Magazine, 1(2001), 6–21.
[16] G. Alvarez, S. Li, Breaking an encryption scheme based on chaotic baker map, Physics Letters A, 352(2006), 78–82.
[17] D. Xiao, X. Liao, P. Wei, Analysis and improvement of a chaos-based image encryption algorithm, Chaos, Solitons and Fractals, 40 (2009), 2191–2199.
[18] J. M. Liu, Q. Qu, Cryptanalysis of a substitution-diffusion based on cipher using chaotic standard and logistic map, in: Third International Symposium on Information Processing, 2010, pp.67-69.
[19] R. Rhouma, E. Solak, S. Belghith, Cryptanalysis of a new substitution-diffusion based image cipher, Communications in Nonlinear Science and Numerical Simulation, 15 (2010), 1887–1892.
[20] X. Wang, G. He, Crytanalysis on a novel image encruption method based on tatal shuffling scheme[J]. Optics Communications, 284 (2011) , 5804-5807
[21] Y. Wang, K.W. Wong, X. F. Liao, T. Xiang, G. R. Chen, A chaos-based image encryption algorithm with variable control parameters. Chaos, Solitons and Fractals, 41(2009), 1773–1783.
[22] S. J. Li, C. Q. Li, G. R. Chen, N. G. Bourbakis, K. T. Lo, A general quantitative cryptanalysis of permutation-only multimedia ciphers against plain-image attacks. Signal Process. Image Commun, 23(2009), 212–223.
[23] C. Q. Li, S. J. Li, G. R. Chen, G. Chen, L. Hu, Cryptanalysis of a new signal security system for multimedia data transmission. EURASIP J. Appl. Signal Process., 8(2005), 1277–1288.
[24] C. Zhu, A novel image encryption scheme based on improved hyper chaotic sequences, Optics Communications, 285 (2012), 29-37.
[25] O.E. Rössler. An equation for hyper chaos. Physics Letters A, 1979, 71(2-3): 155–157.
[26] C.E.Shannon. Communication Theory of Secrecy Systems. Bell System Technical Journal, 1949, 28(4): 656-715.

Authors' Profiles

Junming Ma, master degree candidate at department of mathematics in Shantou University.

Ruisong Ye, born in 1968 and received the B.S. degree in Computational Mathematics in 1990 from Shanghai University of Science and Technology, Shanghai, China and the Ph. D. degree in Computational Mathematics in 1995 from Shanghai University, Shanghai, China. He is a professor at Department of Mathematics in Shantou University, Shantou, Guangdong, China since 2003. His research interest includes bifurcation theory and its numerical computation, fractal geometry and its application in computer science, chaotic dynamical system and its application in computer science, specifically the applications of fractal chaotic dynamical systems in information security, such as, digital image encryption, digital image hiding, digital image watermarking, digital image sharing.

How to cite this paper: Junming Ma, Ruisong Ye,"An Image Encryption Scheme Based on Hybrid Orbit of Hyper-chaotic Systems", IJCNIS, vol.7, no.5, pp.25-33, 2015.DOI: 10.5815/ijcnis.2015.05.04

Copyright © 2015 MECS