Multimed Tools Appl (2016) 75:11433–11446
DOI 10.1007/s11042-015-2861-5

A novel block chaotic encryption scheme for remote sensing image

Guodong Ye[1] · **Xiaoling Huang**[1]

Received: 28 January 2015 / Revised: 17 June 2015 / Accepted: 3 August 2015 /
Published online: 20 August 2015

Abstract An image encryption scheme is proposed using block cipher for remote sensing image in this paper. Remote sensing image means the detection of earth surface including mainly the land, ocean, and atmosphere from satellite. Due to the huge data in normal remote sensing image with security communication requirement, block encryption is adopted for fast implementation, which can effectively resist chosen and known plaintext attacks. Actually, it is a integer factorization problem in mathematics science. The factorization method is not secret but can be open. Some control parameters are produced from the plain-image of which shows that the new scheme can resist well the known-plaintext and chosen-plaintext attacks. Here, The Lorenz system in three-dimension is used for big key space. Classical encryption architecture, i.e., permutation and diffusion, is adopted for high security. All experimental results and security analyses show the efficiency of the proposed method. Therefore, it is suitable for secure communication of big remote sensing image.

Keywords Image encryption · Block cipher · Lorenz chaotic system · Remote sensing image

1 Introduction

Because of special characteristics [12, 27] such as ergodicity, sensitive dependence on initial conditions, random-like behavior, and mixing effect, chaotic system has been found very useful in the field of image encryption. As early as year 1989, Matthews [19] proposed a new image encryption based on chaotic system using logistic map. Since then, the application of chaos in image has attracted more and more researchers' attention. In [18], the authors used a coupled chaotic system called CCS-PRBG to generate bitstream. This system

✉ Guodong Ye
guodongye@hotmail.com

[1] College of Science, Guangdong Ocean University, Zhanjiang, 524088, Guangdong, China

has perfect cryptographic properties, and can be employed to construct stream cipher with high security. A new cryptosystem based on hyper chaos, P-Box, and S-Box was suggested by Hermassi et al. [9]. They made an improvement for classical algorithm, and then showed a better performance of confusion and key sensitivity. Normally, image encryption algorithm includes two stages [3], i.e., permutation and diffusion. This kind of cryptosystems have been adopted in most image encryption algorithms [4–6, 10, 23, 25, 26]. In particular, the appearance of high-dimensional chaotic systems, for example, standard map [13], have solved partially the low security problem existed in low-dimensional systems such as Logistic map.

However, some image encryption algorithms have been found in low security level. For example, Li et al. [15] re-evaluated the security to [2] and found that the scheme is not sensitive enough to the changes of plaintext. Gao et al. [8] proposed an image encryption algorithm in which the cipher-image is obtained just by doing XOR operation between the plain-image and the chaotic sequence after pixel permutation. It was broken successfully by [16] due to key-dependency. Arroyo et al. [1] performed cryptanalysis on a family of self-synchronizing chaotic image encryption algorithms. Unfortunately, the cryptosystem studied in [14] can be analyzed successfully.

By studying the weakness existed in image encryption algorithms, two common drawbacks are summarized as: (1) keystream is used to do modular operation or XOR function with the plain-image directly, (2) permutation and diffusion functions are implemented separately. In this paper, we analyze the property of remote sensing image, and propose a novel block encryption scheme. Double diffusions in forward and backward directions [28] are performed in the first and the last blocks. Compared with pixel-by-pixel encryption method, our scheme can save much time by blocking. Some control parameters are also added in proposed algorithm to enlarge the key space given by Lorenz chaotic system.

The rest of this paper is organized as follows. In Section 2, remote sensing image, Lorenz system, and blocking method are introduced in the first place. Then, the circular function and diffusion process are also described. We also give the encryption steps with help of block diagram in this section. Simulation results are reported in Section 3 to show the efficiency of our proposed method. Section 4 evaluates the security level including the key space, sensitivity on initial conditions and plain-image, statistical analysis, and information entropy analysis. Finally, Section 5 is a conclusion of the whole manuscript.

2 Encryption scheme for remote sensing image

2.1 Remote sensing image

Remote sensing can be seen as a technology to collect information about an object or phenomenon at certain height by satellite. It does not make physical contact directly with the object but only observation in a distance. More important, the develop of remote sensing makes it possible to collect data in dangerous environment or inaccessible areas such as crater. Commonly, remote sensing consists of land remote sensing, ocean remote sensing, and atmosphere. However, because of long distance of monitoring and precise requirement, the data collected by remote sensing will be very huge. As a result, more time cost should be spent to deal with remote sensing data. Considering the security communication of remote sensing image between satellite in the air and receiver on the ground, a block chaotic encryption scheme is suggested in this manuscript to supply a protection. There are many applications of remote sensing image such as inland water [22], and ocean colour [24].

2.2 Lorenz system and blocking method

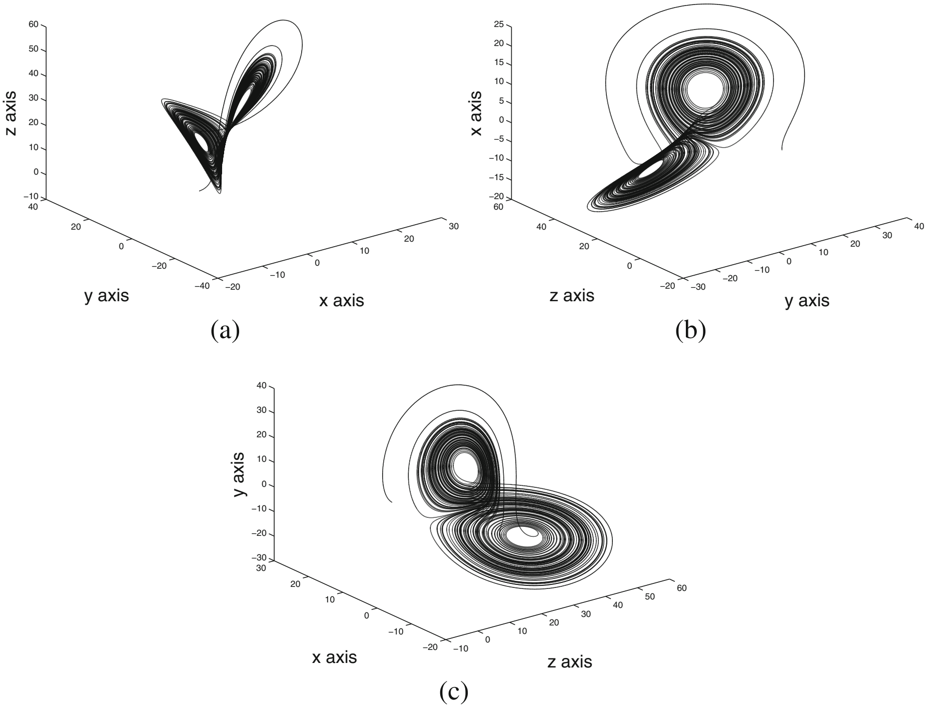
The chaotic Lorenz system [11, 17] can be described as (1).

$$\begin{cases} dx/dt = a(y-x) \\ dy/dt = cx - y - xz \\ dz/dt = xy - bz \end{cases} \tag{1}$$

Here, if $a = 10$, $b = 8/3$, $c = 28$ are set, Lorenz system will exhibit chaotic behavior as plotted in Fig. 1. To solve Lorenz system, classical Runge-Kutta method is usually taken.

Without loss of generality, suppose that the plain-image of remote sensing is denoted as A, which has size of $M \times N$ and is decomposed into $p \times q$ sub-blocks. Each block is in size $m \times n$, i.e., $p \times m = M$, $q \times n = N$. In general, M should be divisible by p while N should be divisible by q. If this is not satisfied, we can change again the values p and q. Here, p and q can be open and are considered as control parameters. Before using the chaotic sequence generated from Lorenz system, some former iterated values should be thrown away for high randomness. Assume $\{x_0, y_0, z_0, x_1, y_1, z_1, \cdots\}$ be the chaotic sequence. With new control parameters r_2, r_3 and r_4, we can get set $S = \{s_1, s_2, s_3, \cdots\} = \{x_{r_2+1}, y_{r_3+1}, z_{r_4+1}, x_{r_2+2}, y_{r_3+2}, z_{r_4+2}, \cdots\}$.

To make keystream be dependent on the plain-image, we design three control parameters w_1, w_2, and w_3, i.e., $w_1 = \Sigma A$, $w_2 = \overleftarrow{w_1}$, $w_3 = (w_1 + w_2)/2$. Here, $\overleftarrow{a}$ denotes inverse order of a, for example, $w = 3241$ while $\overleftarrow{w} = 1423$. Then, initial conditions of Lorenz system are updated as: $x_0 = x_0 + w_1 \times 10^{-14}$, $y_0 = y_0 + w_2 \times 10^{-14}$, $z_0 = z_0 + w_3 \times$



(a)

(b)

(c)

Fig. 1 Chaotic phenomenon of Lorenz system: **a** x-y-z, **b** y-z-x, **c** z-x-y

10^{-14}. As a result, the proposed encryption algorithm can resist the known-plaintext and chosen-plaintext attacks.

2.3 Block circular permutation

To save much time spent on position relocation and sorting function for chaotic sequence, a fast permutation operation by circular function is suggested. Before applying it, we preprocess chaotic sequence using following (2) and (3) to let values fall into [0, p] (for column circulation) and [0, q] (for row circulation) respectively.

$$\alpha_i = [s_i \times 10^{14}]\, mod\ p,\ i = 1, 2, \cdots, p. \tag{2}$$

$$\beta_j = [s_{j+p} \times 10^{14}]\, mod\ q,\ j = 1, 2, \cdots, q. \tag{3}$$

Here, $[x]$ rounds x to the nearest integer towards minus infinity, mod means the remainder after division. $s_i = S_{r_1+i}$ is the chaotic value extracted from S with control parameter r_1. Then we use $\{\alpha_i\}_{i=1}^{p}$ and $\{\beta_j\}_{j=1}^{q}$ to do column circular and row circular accordingly.

For row cyclic shift in blocks, we cycle sub-blocks to the right by α_1 blocks in first row, the second row by α_2 blocks to the right until the last row. The same is to column case, we move the j-th column down by β_j blocks to the bottom($j = 1, 2, \cdots, q$). As a result, we can finish permutation operation in blocks in a fast way thanks to smaller numbers of blocks compared with pixel numbers.

2.4 Block diffusion operation

Many permutation-only image encryption methods have been cryptanalyzed [15, 16] successfully. To enhance the security level, it is necessary to continue the diffusion operation. Suppose the permuted image above is denoted in block as $P_{i,j}(i = 1, 2, \cdots, p, j = 1, 2, \cdots, q)$. In the first step, we pick out the first block $P_{1,1}$ for diffusion by arranging it into vector $u1$ with size $1 \times mn$. From set S obtained by above updated initial keys, a sequence with length $1 \times MN$ can be got and is arranged into a diffusion matrix F of $M \times N$. Then we do a processing for it by (4).

$$F(i, j) = [F(i, j) \times 10^{14}]\, mod\ 256,\ i = 1, 2, \cdots, M,\ j = 1, 2, \cdots, N. \tag{4}$$

Similarly, matrix F is divided into blocks like the same way for the plain-image. Then we pick out first block $F_{1,1}$ and convert it into vector $v1$ in size of $1 \times mn$. To achieve the goal that any change to one pixel in the plain-image can cause a big difference in the cipher-image, the following double diffusions (5) and (6) are performed to the first block.

$$\begin{cases} c_i &= c_{i-1} \dot{+} u1_i \dot{+} v1_i,\ i = 1, 2, 3, \cdots, mn. \\ c_0 &= constant \end{cases} \tag{5}$$

$$\begin{cases} p'_j &= p'_{j+1} \dot{+} c_j \dot{+} v1_j,\ j = mn-1, \cdots, 2, 1. \\ p'_{mn} &= c_{mn} \end{cases} \tag{6}$$

Here, $\dot{+}$ denotes the modular operation under gray level 256.

Then, we obtain pixel p'_j and update all pixels for block $P_{1,1}$. Next, we do the forward diffusion for all blocks $P_{i,j}$ using (7). For simplicity of expression, we mark down the former updated block P into rectangular matrix $Q_{m \times pqn}$ using program fragment 1 before applying diffusion (7).

Program fragment 1

```
$Q = zeros(m, pqn);$
$for\ i = 1 : p$
$Q(:, (i-1)n+1 : in) = P((i-1)m+1 : im, :);$
$end$
```

$$\begin{cases} Q1_i = Q1_{i-1} + Q_i + F_i,\ i = 1, 2, 3, \cdots, pq. \\ Q1_0 = constant \end{cases} \tag{7}$$

Where, $Q_i (i = 1, 2, \cdots, pq)$ of size $m \times n$ is the i-th block in Q, F_i is the i-th block diffusion matrix from F just as the same way to get Q_i. Then arrange the last block of $Q1$ into vector $q2$, and perform double diffusions using (8) and (9).

$$\begin{cases} \overline{c}_i &= \overline{c}_{i-1} + q2_i + v2_i,\ i = 1, 2, 3, \cdots, mn. \\ \overline{c}_0 &= constant \end{cases} \tag{8}$$

$$\begin{cases} \overline{p}'_j &= \overline{p}'_{j+1} + \overline{c}_j + v2_j,\ j = mn-1, \cdots, 2, 1. \\ \overline{p}'_{mn} &= \overline{c}_{mn} \end{cases} \tag{9}$$

Where vector $v2$ is the chaotic sequence from last block $F_{p\times q}$ just the same as $v1$, $\overline{c}_i$ and $\overline{p}'_i$ is the i-th pixel of the cipher-image. Then, update the last block of $Q1$ with $\overline{p}'_j$, and obtain image matrix $\overline{P}'$.

Using (10), we perform backward diffusion by blocks, and obtain the cipher-image $EQ_{M\times N}$ from $Q2$ using program fragment 2.

$$\begin{cases} Q2_j &= Q2_{j+1} + \overline{P}'_j + F_j,\ j = pq-1, \cdots, 2, 1. \\ Q2_{pq} &= \overline{P}'_{pq} \end{cases} \tag{10}$$

Program fragment 2

```
$EQ = zeros(M, N);$
$for\ i = 1 : p$
$EQ((i-1)m+1 : im, :) = Q2(:, (i-1)n+1 : in);$
$end$
```

2.5 Encryption steps

The encryption process is illustrated in the block diagram as shown in Fig. 2. Details are listed in the following algorithm: Encryption process.

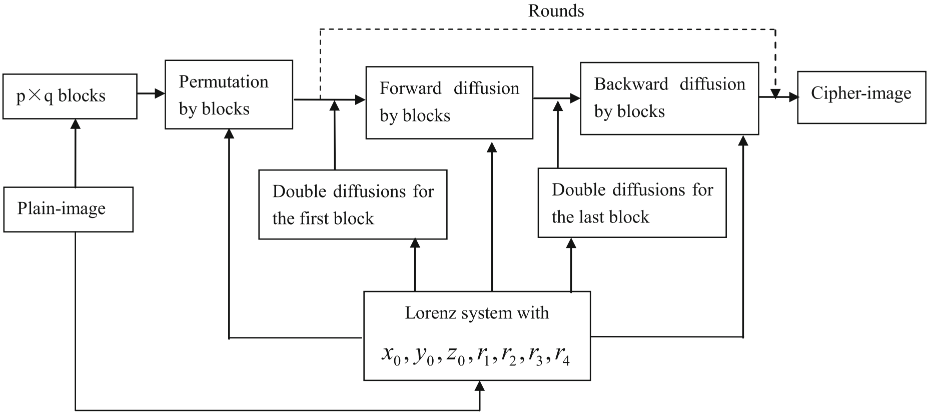

Rounds
p×q blocks
Permutation by blocks
Forward diffusion by blocks
Backward diffusion by blocks
Cipher-image
Plain-image
Double diffusions for the first block
Double diffusions for the last block
Lorenz system with
$x_0, y_0, z_0, r_1, r_2, r_3, r_4$

Fig. 2 Block diagram of the proposed method

Algorithm 1 Encryption process

```
Input: Plain-image $A$, open parameters $a$, $b$, $c$, $r_1$, $r_2$, $r_3$, $r_4$, and keys $x_0$, $y_0$, $z_0$.
Output: Cipher-image $EQ$.
Compute image size $M \times N$, and block numbers $p \times q$.
Get chaotic matrix $F$ for diffusion, and chaotic sequences $\alpha$, $\beta$ for permutation from Lorenz system.
Implement block permutation to $A$ and obtain image $P$.
Perform double diffusions to the first block $P_{1,1}$ in $P$, and get an updated image $Q$.
Apply forward block diffusion to $Q$ and get $Q1$.
Perform double diffusions for the last block in $Q1$ and get another updated image $\overline{P}'$.
Apply backward diffusion to $\overline{P}'$ by blocks and obtain $Q2$.
Rearrange $Q2$ into cipher-image $EQ$ of size $M \times N$.
```

2.6 Decryption process

Because of symmetry, decryption process can be carried out reversely if we have the correct keys x_0, y_0, z_0 and the control parameters $r_i (i = 1, 2, 3, 4)$. The reversion of function (10) is shown in (11).

$$\begin{cases} \overline{P}'_j &= Q2_j - Q2_{j+1} - F_j, \;\; j = pq - 1, \cdots, 2, 1. \\ \overline{P}'_{pq} &= Q2_{pq} \end{cases} \tag{11}$$

Equations (12) and (13) are the inverse processes of operations (9) and (8) respectively.

$$\begin{cases} \overline{c}_j &= \overline{p}'_j - \overline{p}'_{j+1} - v2_j, \;\; j = mn - 1, \cdots, 2, 1. \\ \overline{c}_{mn} &= \overline{p}'_{mn} \end{cases} \tag{12}$$

$$\begin{cases} q2_i &= \overline{c}_i - \overline{c}_{i-1} - v2_i, \;\; i = 1, 2, 3, \cdots, mn. \\ \overline{c}_0 &= constant \end{cases} \tag{13}$$

The same can be done to (7), (6), (5) and obtain (14), (15), (16), respectively. Finally, we can recover the plain-image from the cipher-image.

$$\begin{cases} Q_i &= Q1_i - Q1_{i-1} - F_i, \ i = 1, 2, 3, \cdots, pq. \\ Q1_0 &= constant \end{cases} \tag{14}$$

$$\begin{cases} c_j &= p'_j - p'_{j+1} - v1_j, \ \ j = mn - 1, \cdots, 2, 1. \\ c_{mn} &= p'_{mn} \end{cases} \tag{15}$$

$$\begin{cases} u1_i &= c_i - c_{i-1} - v1_i, \ i = 1, 2, 3, \cdots, mn. \\ c_0 &= constant \end{cases} \tag{16}$$

3 Simulation

In this section, simulation is implemented to the proposed encryption scheme using gray plain-image Coastal city of size 512 × 512 (see Fig. 3a) from google image database. All experiments are test by Matlab r2011b on a Lenovo Win7 PC with an Intel(R) Core(TM) i3-2350M, 2.30 GHz CPU. Figure 3b shows the cipher-image with two rounds of iteration. Here,initial conditions are set to be $a = 10$, $b = 8/3$, $c = 28$, $x_0 = 2.155$, $y_0 = 3.022$, $z_0 = -9.811$ in system (1) with random control parameters $r_1 = 10$, $r_2 = 40$, $r_3 = 38$, $r_4 = 45$. According to the size of the plain-image and integer factorization, 8×16 blocks are divided. From Fig. 3b, we can not found any information related to the plain-image because there is no connection between them.

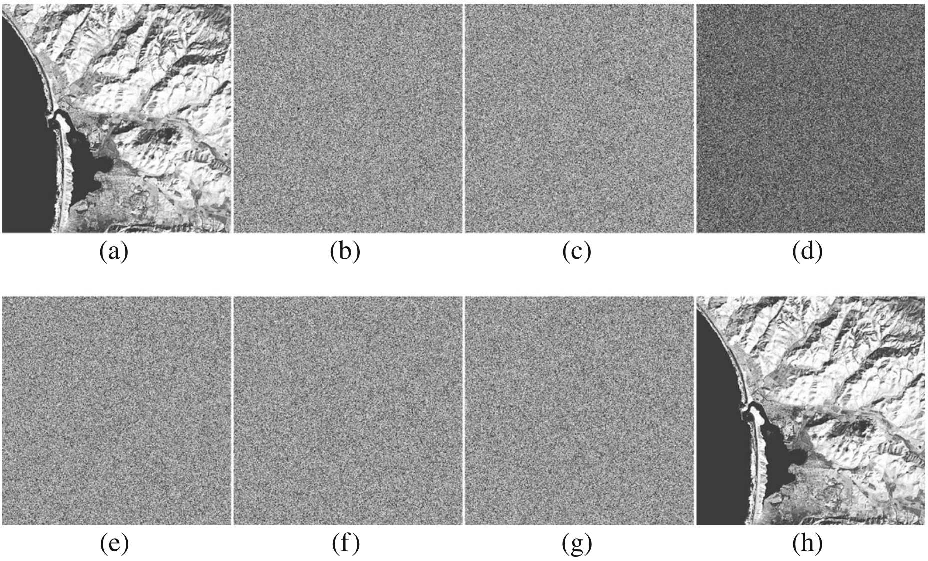


Fig. 3 Coastal city: **a** plain-image, **b** cipher-image, **c** cipher-image using $y_0 + 10^{-14}$, **d** difference between (**b**) and (**c**), **e** decrypted image using $x_0 + 10^{-14}$, **f** decrypted image using $y_0 + 10^{-14}$, **g** decrypted image using $z_0 + 10^{-14}$, **h** correct decrypted image

Table 1 UACI and NPCR values for different images

Image	Cameraman	Baboon	Lena	Boat
UACI	33.368	33.473	33.441	33.432
NPCR	99.582	99.618	99.602	99.613

4 Security analyses

In the proposed cryptosystem, the block permutation approach is suggested together with double diffusions. The security analyses of our method are evaluated as below.

4.1 Key space analysis

The number of possible combinations of keys is an important index to evaluate whether the proposed algorithm can resist the brute-force attack. The key of our approach is composed of initial conditions x_0, y_0, z_0 in the Lorenz system, and control parameters r_1, r_2, r_3, and r_4. Thus, the key space is large enough to resist brute-force attack.

4.2 Sensitivity analysis

On the one hand, the cipher-image should be sensitive to the initial conditions. Figure 3c shows the cipher-image just with 10^{-14} difference in key y_0. The difference between Fig. 3b and c is plotted in Fig. 3d. We cannot recover the plain-image even if there is any change for example 10^{-14} in keys as shown in Fig. 3e, f, and g. Of course the plain-image can be obtained with correct keys as shown in Fig. 3h. Therefore, the proposed method is very sensitive to every key.

On the other hand, a good image encryption algorithm should also satisfy the requirement that any tiny change in the plain-image even just one-bit can lead to a totally different cipher-image. The number of pixels change rate (i.e., NPCR) and the unified average changing intensity (i.e., UACI) defined in (17) and (18) [26] are commonly used to test the sensitivity. Table 1 lists the results for different images. Furthermore, Table 2 gives the corresponding values by changing different pixel positions in Lena image of size 256 × 256. These values justify that our algorithm can resist differential attacks including chosen-plaintext and known-plaintext attacks.

$$NPCR = \frac{\sum_{ij} D(i,j)}{M \times N} \times 100\ \% \tag{17}$$

$$UACI = \frac{1}{M \times N}\left[\sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255}\right] \times 100\ \% \tag{18}$$

where $D(i,j) = 0$ if $C_1(i,j) = C_2(i,j)$; otherwise, $D(i,j) = 1$.

Table 2 UACI and NPCR values at different positions

Lena image	(1,1)	(53,241)	(222,34)	(256,256)
UACI	33.587	33.516	33.459	33.672
NPCR	99.561	99.654	99.614	99.588

Table 3 Correlation coefficients for Lena image

Direction	plain-image	cipher-image
Diagonal	0.951	−0.099
Horizontal	0.951	0.061
Vertical	0.962	−0.008

4.3 Statistical analysis

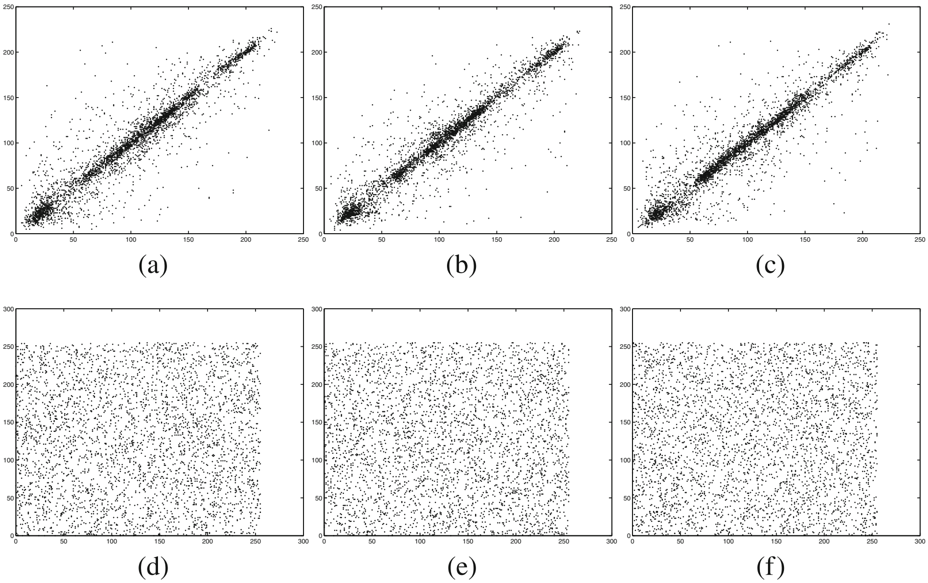
(1) Correlation coefficients

For a meaningful plain-image, the correlation coefficients between two adjacent pixels are usually high. Any ideal image encryption scheme should have the ability to reduce them to near zeros [20]. In our test, 2500 pairs of adjacent pixels are randomly selected along the vertical, horizontal and diagonal directions in Lena image and its cipher-image. Using (19), the results are given in Table 3. So, we can see that the correlation coefficients of adjacent pixels in the cipher-image are greatly reduced by using the proposed method. Meanwhile, Fig. 4 plots the correlation coefficients for Barb image.

$$r_{xy} = \frac{cov(x, y)}{\sqrt{D(x)D(y)}} \tag{19}$$

where $cov(x, y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y))$, $D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2$, $E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i$, x_i and y_i represent the gray values of two adjacent pixels in the image.

(2) Histogram



(a) (b) (c)

(d) (e) (f)

Fig. 4 Correlation coefficients in the plain-image: **a** diagonal direction, **c** vertical direction, **e** horizontal direction; Cipher-image: **b** diagonal direction, **d** vertical direction, **f** horizontal direction

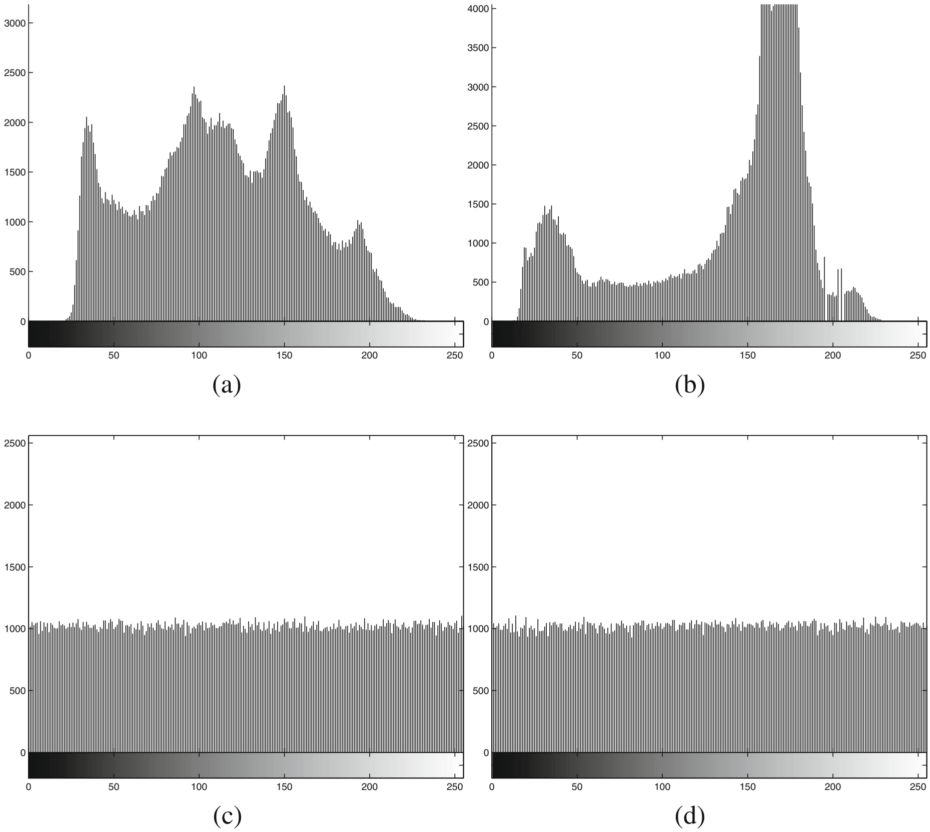


Fig. 5 Histogram test:**a** plain-image Barb, **b** plain-image Boat, **c** cipher-image of (**a**), **d** cipher-image of (**b**)

If the histogram of the cipher-image is relatively uniformed, i.e., the gray values are distributed evenly, statistical attacks will be more difficult. Figure 5a and b show the histograms of the plain-images Barb and Boat while Fig. 5c and d are the histograms of the corresponding cipher-images respectively. Because the histograms of the cipher-image are uniformed compared with those of the plain-image, we can conclude that the proposed chaotic encryption algorithm possesses high security against statistical attacks.

Table 4 Entropy information for different images

Image	Lena	Barb	Cameraman	Boat	Baboon
Plain-image	7.568	7.466	7.010	7.124	7.358
Cipher-image	7.990	7.991	7.989	7.992	7.991

Table 5 Speed performance

Image size	Ref. [10]	Ref. [5]	Ref. [7]	Ours
256 × 256	0.351 s	0.710 s	0.105 s	0.055 s
512 × 512	1.599 s	2.293 s	0.452 s	0.203 s
1024 × 1024	6.490 s	8.689 s	1.802 s	0.741 s

4.4 Information entropy analysis

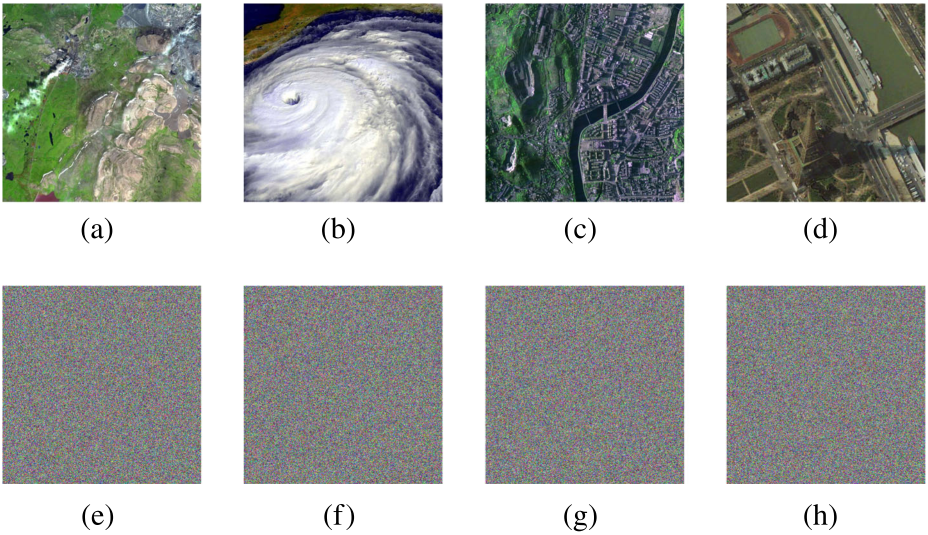
Equation (20) is commonly employed to calculate the information entropy for message or image.

$$H(s) = \sum_{i=0}^{2^n-1} p(s_i)log_2\frac{1}{p(s_i)} \tag{20}$$

Here, s is the information source, $p(s_i)$ represents the probability of occurrence of symbol s_i. The theoretical value of an image with random pixel values is 8 [21]. Table 4 lists the values of information entropy for different cipher-images. As a result, our method can show high degree of randomness.

4.5 Speed analysis

Block permutation plus block diffusion approach is suggested in this paper, of which can be implemented in a fast way. Table 5 shows the comparisons with three existed methods [5, 10] and [7]. Therefore, we can see the high efficiency of the proposed method.



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

(e) (f) (g) (h)

Fig. 6 Other remote sensing tests: plain-images: **a** test one, **b** test two, **c** test three, **d** test four; cipher-images: **e** test one, **f** test two, **g** test three, **h** test four

4.6 Applications to other remote sensing images

In this section, four other colour remote sensing images from google image database are randomly selected to do the experiments. Figure 6e, f, g, and h show the cipher results for plain-images of size 512 × 512 in Fig. 6a, b, c, and d respectively. Therefore, the proposed algorithm can be applied to any other remote sensing images.

5 Conclusion

A novel block-based image encryption algorithm has been proposed for remote sensing image in this paper. To overcome the drawbacks such as small key space and weak security in one-dimensional chaotic maps, chaotic Lorenz system is employed to enhance the security. Furthermore, the keystream is generated dependent on the plain-image. The values of UACI and NPCR show that any tiny change in the plain-image will lead to a significantly difference in the cipher-image. As a result, the proposed method can resist known-plaintext and chosen-plaintext attacks. Additionally, due to the block method adopted in the proposed cryptosystem, it is specially suitable to big size remote sensing image, and can achieve high security for image encryption. Speed tests also explain that our method is efficient than some existed encryption algorithms.

Acknowledgment The authors would like to thank the editors and two anonymous reviewers for their positive comments and valuable suggestions. The work described in this paper was fully supported by the National Natural Science Foundation of China (No.11301091), the Project of Enhancing School With Innovation of Guangdong Ocean University of China (No.Q14217), and the Science & Technology Planning Project of Zhanjiang City of China (No.2015B01051, No.2015B01098).

References

1. Arroyo D, Alvarez G, Amig JM, Li S (2011) Cryptanalysis of a family of self-synchronizing chaotic stream ciphers. Commun Nonlinear Sci Numer Simul 16:805–813
2. Behnia S, Akhshania A, Akhavanb A, Mahmodi H (2008) Chaotic cryptographic scheme based on composition maps. Int J Bifurcation Chaos 18:251–261
3. Chen GR, Mao YB, Chui CK (2004) A symmetric image encryption scheme based on 3D chaotic cat maps, Chaos. Solions and Fractals 21:749–761
4. Chen JX, Zhu ZL, Fu C, Yu H, Zhang LB (2015) A fast chaos-based image encryption scheme with a dynamic state variables selection mechanism. Commun Nonlinear Sci Numer Simul 20:846–860
5. Eslami Z, Bakhshandeh A (2013) An improvement over an image encryption method based on total shuffling. Opt Commun 286:51–55
6. Fouda JSAE, Effa JY, Ali M (2014) Highly secured chaotic block cipher for fast image encryption. Appl Soft Comput 25:435–444
7. Gao TG, Chen ZQ (2008) Image encryption based on a new total shuffling algorithm, Chaos. Solitons Fractals 38:213–220
8. Gao HJ, Zhang YS, Liang SY, Li DQ (2005) A new chaotic algorithm for image encryption, Chaos. Solitons Fractals 29:393–399
9. Hermassi H, Rhouma R, Belghith S (2013) Improvement of an image encryption algorithm based on hyper-chaos. Telecommun Syst 52:539–549
10. Huang XL (2012) Image encryption algorithm using chaotic Chebyshev generator. Nonlinear Dyn 67:2411–2417
11. Huang CK, Nien HH (2009) Multi chaotic systems based pixel shuffle for image encryption. Opt Commun 282:2123–2127
12. Huang XL, Ye GD (2014) An image encryption algorithm based on hyper-chaos and DNA sequence. Multimedia Tools and Appl 72:57–70

13. Kumar A, Ghose MK (2011) Extended substitution-diffusion based image cipher using chaotic standard map. Commun Nonlinear Sci Numer Simul 16:372–382
14. Kurian AP, Puthusserypady S (2008) Self-synchronizing chaotic stream ciphers. Signal Process 88:2442–2452
15. Li SJ, Li CQ, Chen GR, Bourbakis NG, Lo KT (2008) A general quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks. Signal Process Image Commun 23:212–223
16. Li CQ, Lo KT (2011) Optimal quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks. Signal Process 91:949–954
17. Lorenz EN (1963) Deterministic nonperiodic flow. J Atmos Sci 20:130–148
18. Li SJ, Mou XQ, Cai YL (2001) Pseudo-random bit generatorg based on couple chaotic systems and its applications in stream-cipher cryptography. Lect Notes Comput Sci 2247:316–329
19. Matthews R (1989) On the derivation of a chaotic encryption algorithm. Cryptologia 4:29–42
20. Mandal MK, Kar M, Singh SK, Barnwal VK (2014) Symmetric key image encryption using chaotic Rossler system. Secur and Commun Netw 7:2145–2152
21. Mirzaei O, Yaghoobi M, Irani H (2012) A new image encryption method: parallel sub-image encryption with hyper chaos. Nonlinear Dyn 67:557–566
22. Palmer SCJ, Kutser T, Hunter PD (2015) Remote sensing of inland waters: Challenges, progress and future directions. Remote Sens Environ 157:1–8
23. Pareek NK, Patidar V, Sud KK (2006) Image encryption using chaotic logistic map. Image Vis Comput 24:926–34
24. Ruddick K, Neukermans G, Vanhellemont Q, Jolivet D (2014) Challenges and opportunities for geostationary ocean colour remote sensing of regional seas: A review of recent results. Remote Sens Environ 146:63–76
25. Seyedzadeh SM, Mirzakuchaki S (2012) A fast color image encryption algorithm based on coupled two-dimensional piecewise chaotic map. Signal Process 9:1202–1215
26. Tong XJ (2012) The novel bilateral-diffusion image encryption algorithm with dynamical compound chaos. J Syst Softw 85:850–858
27. Wang XY, Xu DH (2014) Image encryption using genetic operators and intertwining logistic map. Nonlinear Dyn 78:2975–2984
28. Ye RS (2011) A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism. Opt Commun 284:5290–5298

Guodong Ye was born in China. He received the Master degree in Mathematics in 2006. Currently, he is an associate professor in College of Science at Guangdong Ocean University of China, and pursuing the PhD degree in department of Electronic Engineering at City University of Hong Kong. His areas of interests are cryptography, image quality assessment, and compressive sensing.

Xiaoling Huang was born in China. She received the Master degree in Mathematics in 2008 at Shantou University of China, and then joined in College of Science at Guangdong Ocean University. She is currently a lecturer in Mathematics. The interesting areas include Mathematical model, cryptography, image processing, and information coding.