I.J. Image, Graphics and Signal Processing, **2010, 1, 61-68**
Published Online November 2010 in MECS (http://www.mecs-press.org/)

A Novel Image Encryption Scheme based on a Nonlinear Chaotic Map

Shujiang Xu* and Yinglong Wang
Shandong Provincial Key Laboratory of computer Network,
Shandong Computer Science Center, Jinan, PR China
Email: {xushj, wangyl}@keylab.net

Yucui Guo and Cong Wang
Beijing University of Posts and Telecommunications, Beijing, PR China
Email: {ycguo, wangc}@bupt.edu.cn

Abstract—**Only by means of XOR operation, a novel image encryption scheme is proposed based on a nonlinear chaotic map (NCM). There are two rounds in the proposed image encryption scheme. In each round of the scheme, the pixel gray values are modified from the first pixel to the last pixel firstly, and then the modified image is encrypted from the last pixel to the first pixel in the inverse order. In order to accelerate the encryption speed, every time NCM is iterated, *n* (*n*>3) bytes random numbers which are used to mask the plain-image can be gained. And to enhance the security, a small perturbation will be given to the parameters of the NCM based on the last obtained *n* bytes modified elements before next iteration. Experimental results and theory analysis show that the algorithm has a high security performance and a good efficiency.**

Index Terms—**chaos; chaotic cryptosystem; image encryption**

I. Introduction

With the rapid development of multimedia technology and Internet, digital images and other multimedia are more commonly and frequently transmitted in the public communication network. Therefore, the security of image data attracts more and more attention, and image encryption technology becomes an important issue of cryptography. Image data have strong correlations among adjacent pixels. Statistical analysis on large amounts of images shows that averagely adjacent 8 to 16 pixels are correlative in horizontal, vertical, and diagonal directions for both natural and computer-graphical images [1]. Moreover, due to some intrinsic features of images, such as bulk data capacity and high redundancy, encryption of images is different from that of texts [2]. Therefore, conventional cipher algorithms such as DES, IDEA etc. are not suitable for image encryption. The chaos-based cryptography has suggested a new and efficient way to develop fast and secure image encryption algorithms.

Matthews first proposed the chaos-based encryption scheme in 1989 [3], and Fridrich first adopted chaotic map into image encryption in 1997 [4]. Since then, many chaos-based image encryption algorithms have been designed to realize secure communications [1, 4-12], but it is pointed out that most of them are flawed by lack of robustness and security [10-14].

In [6, 7], a type of chaotic encryption scheme which was based on circular bit shift and XOR operations was proposed. In this type algorithm, the plaintext block was permuted by a circular bit shift approach and then encrypted by the XOR operation. However, it was shown that there are some defects with this type algorithm in [11-13]: 1) Low sensitivity of encryption to plaintexts. 2) Not secure against the chosen plaintext attack. In [13], the type algorithm was cryptanalysis by chosen plaintext attack and improved to avoid chosen plaintext attack, but the first defect exists in the improved scheme yet. It is necessary to note that the improved scheme also has low sensitivity to small changes of the plaintext. If a plaintext byte is changed, only the ciphertext bytes behind the corresponding ciphertext byte are changed, i.e., it has no effect to the ciphertext bytes before the corresponding ciphertext byte.

Based on a permutation approach and the XOR operation, a type of chaotic image encryption algorithm was proposed in [1, 15-19]. In this type encryption scheme, the plain-image was first permutated and then substituted, or was first substituted and then permutated. It has been pointed out that the type algorithm also has the two defects which are described in the above paragraph [20].

In [21, 22], a type of image encryption scheme which employs an image total shuffling matrix to shuffle the positions of image pixels was present. In the schemes, the image was shuffled based on a total image shuffling matrix generated by a chaotic map, and then the shuffled image was encrypt based on XOR operation by another chaotic map. Unfortunately, the two defects were founded in the type of algorithm, too [14]. Though the ciphertext feedback method was adopted in [22], the encryption scheme still has low sensitivity to small changes of the plaintexts.

A new class of chaos-based image encryption schemes was proposed [23-25]. In this class of algorithms, the plain-image $P_{m\times n}$ was transformed into the plaintext matrix $M_{(mn)\times 1}$ firstly, and then this matrix was encrypted using results of iteration of chaotic maps to obtain a new modified message matrix M. Finally, the whole process was repeated for the new *M* from the last element to the first one, and new matrix *C* was the output as the ciphertext. To enhance the security, a small perturbation was given to the parameters of chaotic maps based on the last obtained encrypted element.

In this class of schemes and most other classes of chaos-based encryption algorithms, each time a one-dimensional chaotic map is iterated, only a single byte random number can be generated. To accelerate the encryption speed and to enhance the security, an improved image encryption scheme is proposed by means of three other measures in this paper. First, there are two rounds in the proposed scheme. Second, every time NCM is iterated, *n* (*n*>3) bytes random numbers can be gained so as to accelerate the encryption speed. Finally, a piecewise linear function is used, which can make sure that the perturbation isn't too small. Based on the last obtained *n* bytes modified elements, only the parameters of the NCM are perturbed before next iteration. So the state transfer function not only depends on the secret key, but also depends on the output ciphertext. Therefore, the proposed scheme can resist chosen plaintext effectively.

The rest of the paper is organized as follows: Sec. 2 gives a brief introduction of the nonlinear chaotic map. A chaos-based image encryption scheme is proposed in Sec. 3. Sec. 4 shows the simulation result. The security analysis is given in Sec. 5. Finally, Sec. 6 concludes the work.

II. THE NONLINEAR CHAOTIC MAP

Chaos, which has many good properties, such as the ergodicity, sensitive dependence on initial conditions and random-like behaviors, is an aperiodic dynamics process, seeming disorderly and unsystematic [26]. In fact, the properties just suit to the diffusion and confusion process in cryptography [1, 8].

One-dimensional chaotic system which has the advantages of high-level efficiency and is implicit [27], such as Logistic map, is being widely used now. But their weaknesses, such as small key space and weak security, are also known to us obviously [28]. With more than one control parameters and initial conditions, high dimensional chaotic systems are most complex and have a big key space. However, complex calculations make the encryption algorithm too slow.

To overcome these drawbacks, a nonlinear chaotic map (NCM) [29] is adopted in this paper:

$$x_{n+1} = \left(1-\beta^{-4}\right)\cdot \operatorname{ctan}\left(\frac{\alpha}{1+\beta}\right)\cdot\left(1+\frac{1}{\beta}\right)^{\beta} \cdot \tan\left(\alpha x_n\right)\cdot\left(1-x_n\right)^{\beta} \tag{1}$$

where α , β are control parameters. When $x_n \in (0,1)$, $\alpha \in (0,\ 1.4)$, $\beta \in [5,\ 43]$, or $x_n \in (0,1)$, $\alpha \in (1.4,\ 1.5]$, $\beta \in [9,\ 38]$, or $x_n \in (0,1)$, $\alpha \in (1.5,\ 1.57]$, $\beta \in [3,\ 15]$, NCM performs chaotic phenomena. It is shown that the system NCM is a chaotic system with good properties of balanced 0–1 ratio, zero co-correlation and ideal nonlinearity, while maintaining acceptable efficiency in [30].

In order to get a faster encryption speed, every time NCM is iterated, *n* bytes random numbers can be gained In this paper. Suppose that $x = 0.x_1x_2 \cdots x_{15} \cdots$ is a double-point value, the *n* bytes decimal random numbers are generated as follows:

$$B_i = \operatorname{mod}(x_{13-n+i}x_{14-n+i}x_{15-n+i}, 256)\,, \tag{2}$$

where $i = 1, 2, \cdots, n$, mod(*x*, *y*) returns the remainder after division, $x_k = 0, 1, \cdots, 9$, $4 \le n \le 13$. If *n*=4, for example, four bytes random numbers B_1=mod(x_{10} x_{11} x_{12}, 256), B_2=mod(x_{11} x_{12} x_{13}, 256), B_3=mod(x_{12} x_{13} x_{14}, 256) and B_4= mod(x_{13} x_{14} x_{15}, 256) will be gained.

III. THE PROPOSED IMAGE ENCRYPTION SCHEME

Given an image plaintext p_{ij} (*i*=0, 1, $\cdots$, *M*-1; *j*=0, 1, $\cdots$, *N*-1), suppose the secret key $K = K(K_1; K_2) = (\alpha^1, \beta^1, x_0^1; \alpha^2, \beta^2, x_0^2)$, where the sub-key K_1, K_2 include the control parameters and the initial conditions of the NCM. The proposed scheme which is shown in Figure 1 is described below.

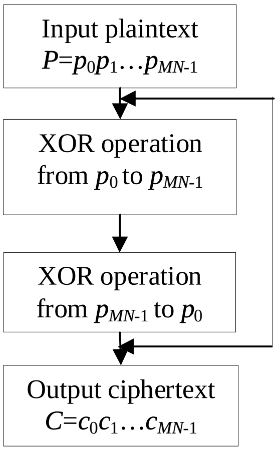

Input plaintext
$P=p_0p_1\ldots p_{MN-1}$
XOR operation from p_0 to p_{MN-1}
XOR operation from p_{MN-1} to p_0
Output ciphertext
$C=c_0c_1\ldots c_{MN-1}$

Figure 1. Encryption scheme, *m*=2.

Step 1 Arrange the plain-image p_{ij} (*i*=0, 1, $\cdots$, *M*-1; *j*=0, 1, $\cdots$, *N*-1) by the order from left to right and then top to bottom, and a plaintext matrix $P = p_0$, $p_1, \cdots, p_{MN-1}$ can be obtained.

Step 2 Choose the first sub-key $K_1 = (\alpha^1, \beta^1, x_0^1)$, and then iterate NCM (1) n_1 times to avoid the transient effect.

Step 3 Iterate NCM once, *n* bytes random numbers can be gained by Eq. (2), and then encrypt the message block $P_j = p_{nj}, p_{nj+1}, \cdots, p_{nj+n-1}$ as follows:

$$c_{nj+k}=p_{nj+k}\oplus a_{nj+k}\tag{3}$$

where ⊕ is the XOR operation, and k=0, 1, L , $n-1$.

Step 4 If all the plaintext has already been encrypted, then the encrypted message matrix $M=c_0, c_1,$ L $, c_{MN-1}$ is obtained, and turn to Step 5. Otherwise, $\alpha_{j+1}=g(\alpha_j, c_{nj}, c_{nj+1}, \mathrm{L}, c_{nj+n-1})$, $\beta_{j+1}=h(\beta_j,$ $c_{nj}, c_{nj+1}, \mathrm{L}, c_{nj+n-1})$, where g and h are piecewise linear function in Eq. (4) and Eq. (5), then let j=j+1 and turn to Step 3.

$$\alpha_{j+1}=g(\alpha_j, c_{nj}, c_{nj+1}, \mathrm{L}, c_{nj+n-1})=$$
$$\begin{cases}\alpha_j-\dfrac{\sum_{k=0}^{n-1}c_{nj+k}+10n}{2560n}, & \alpha_j>\alpha_0, \sum_{k=0}^{n-1}c_{nj+k}<10n\\ \alpha_j-\dfrac{\sum_{k=0}^{n-1}c_{nj+k}}{2560n}, & \alpha_j>\alpha_0, \sum_{k=0}^{n-1}c_{nj+k}\geq 10n\\ \alpha_j+\dfrac{\sum_{k=0}^{n-1}c_{nj+k}+10n}{2560n}, & \alpha_j\leq\alpha_0, \sum_{k=0}^{n-1}c_{nj+k}<10n\\ \alpha_j+\dfrac{\sum_{k=0}^{n-1}c_{nj+k}}{2560n}, & \alpha_j\leq\alpha_0, \sum_{k=0}^{n-1}c_{nj+k}\geq 10n\end{cases}\tag{4}$$

$$\beta_{j+1}=h(\beta_j, c_{nj}, c_{nj+1}, \mathrm{L}, c_{nj+n-1})=$$
$$\begin{cases}\beta_j-\dfrac{\sum_{k=0}^{n-1}c_{nj+k}+10n}{256000n}, & \beta_j>\beta_0, \sum_{k=0}^{n-1}c_{nj+k}<10n\\ \beta_j-\dfrac{\sum_{k=0}^{n-1}c_{nj+k}}{256000n}, & \beta_j>\beta_0, \sum_{k=0}^{n-1}c_{nj+k}\geq 10n\\ \beta_j+\dfrac{\sum_{k=0}^{n-1}c_{nj+k}+10n}{256000n}, & \beta_j\leq\beta_0, \sum_{k=0}^{n-1}c_{nj+k}<10n\\ \beta_j+\dfrac{\sum_{k=0}^{n-1}c_{nj+k}}{256000n}, & \beta_j\leq\beta_0, \sum_{k=0}^{n-1}c_{nj+k}\geq 10n\end{cases}\tag{5}$$

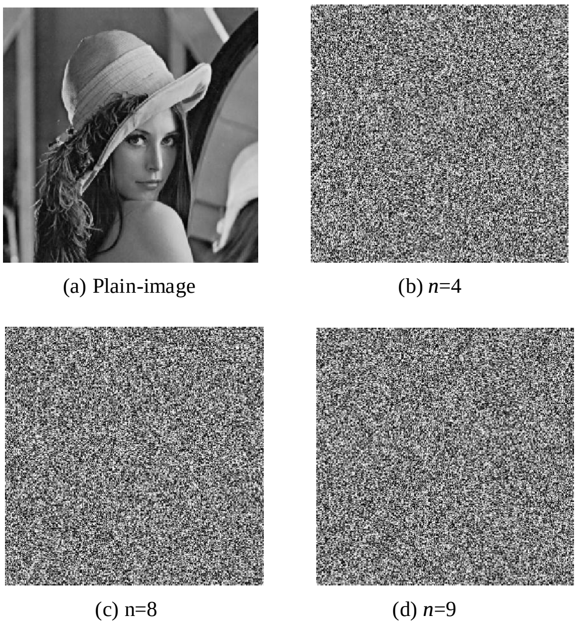
Step 5 Choose the second sub-key $K_2=(\alpha^2, \beta^2, x_0^2)$, and then iterate NCM n_2 times. Let $M'=c_{MN-1}, c_{MN-2}, \mathrm{L}, c_0$, and encrypt M' using the method described in Step 3 and Step 4. Finally, the encrypted matrix C can be obtained.

Step 6 Do step 2-5 for the matrix C again, and the final ciphertext can be gained. Rearrange the ciphertext into the cipher-image, and the encryption process is finished.

In this scheme, suppose that m=mod(MN, n). If m>0, we can only generate m random numbers in the last block, or let p_k=0 (k=MN, L , MN+n-m-1) and MN=MN+n -m. The decryption process is almost the same as the encryption one. We only need to do the XOR operation by the second sub-key K_2 from the last byte to the first byte for the ciphertext matrix C to obtain the modified message matrix M first, and then do the XOR operation for matrix M from the first byte to the last byte by the first sub-key K_1. Do the above process again, and finally the plaintext matrix P can be recovered.

IV. EXPERIMENTAL RESULTS

The experimental results are shown in this section. Take a 256 grey-scale BMP plain-image of size 256×256 for example. The secret key is chosen as K= $(\alpha^1,$ $\beta^1, x_0^1; \alpha^2, \beta^2, x_0^2)$ =(1.1, 6.0, 0.5432106789017177; 1.1, 6.001, 0.5432106789017177). Figure 2 shows the experimental results of the proposed scheme. Figure 2(a) is the plain-image Lena.bmp. Figure 2(b), (c) and (d) are the corresponding encrypted images when n=4, 8 and 9. From Figure 2(b), (c) and (d), we can see that the encrypted images are rough-and-tumble and unknowable, so the diffusion and confusion properties are confirmed.



(a) Plain-image (b) n=4

(c) n=8 (d) n=9

Figure 2. Encryption experimental results

All the simulation experiments are implemented using Visual C++ 6.0 and running in a personal computer with Pentium (R) D CPU 2.80 GHz 2.79 GHz, 1.00 GB memory, 160 GB hard-disk capacities. The time used in encryption on 256 grey-scale BMP images of size 256×256 with different values of n is shown in Table I. It is shown that the proposed algorithm is fast enough for practical transmission of image files over public communication network. For different practical demands of encryption speed, we can choose a suitable value of *n*.

V. SECURITY ANALYSIS

To show the satisfactory security of the proposed scheme, some security analyses on the proposed encryption scheme, including the most important ones like key space analysis, information entropy, correlation analysis of two adjacent pixels and differential analysis, are shown in this section.

A. *Key space analysis*

The key space of a good encryption scheme should be large enough to make brute-force attacks infeasible. Two groups of secret keys, including the initial values and the control parameters of the NCM, are employed in our encryption algorithm. Suppose that the precision is 10^{-15}, the key space size of the proposed scheme is $((10^{15})^3)^2=10^{90}$. Therefore, the key space is large enough to resist all kinds of brute-force attacks.

B. *Information entropy*

It is well known that the information entropy is defined to express the degree of uncertainties in the system. The information entropy is defined as follows:

TABLE I.
ENCRYPTION TIME

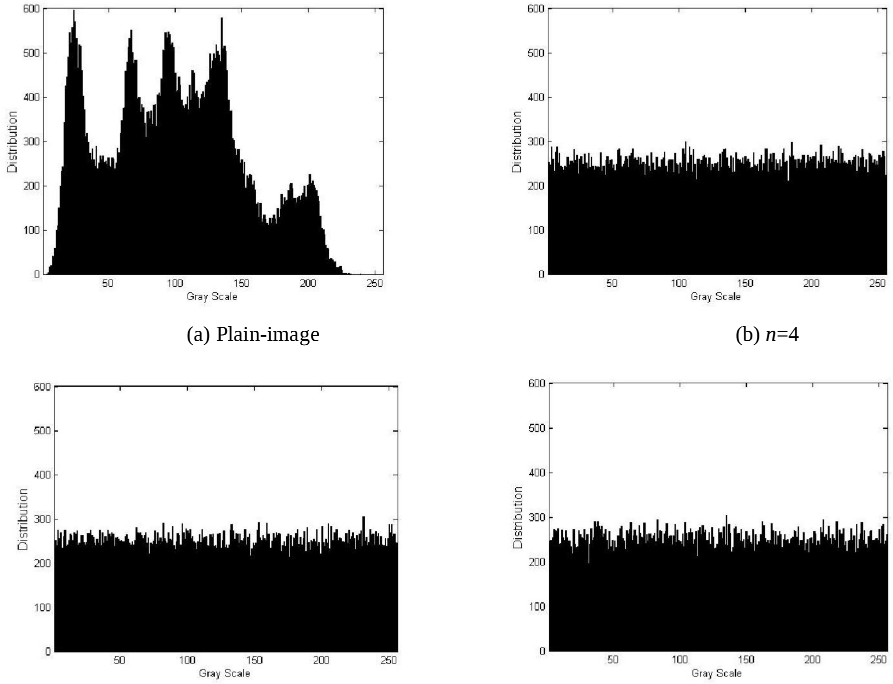
n	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**
Encryption time (S)	0.12669	0.10246	0.086579	0.075185	0.066874	0.061955	0.055768	0.051060

TABLE II.
INFORMATION ENTROPY

n	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**
Entropy *H*	7.9974	7.99701	7.99707	7.99686	7.99756	7.99675	7.99722	7.99708

TABLE III.
Information entropy with different key

	n=4	a	b	c	d
Entropy *H*	7.9974	7.9972	7.99717	7.99708	7.99706



(a) Plain-image

(b) *n*=4

(c) *n*=8

(d) *n*=9

Figure 3. Grayscale histogram of plain-image and cipher-images

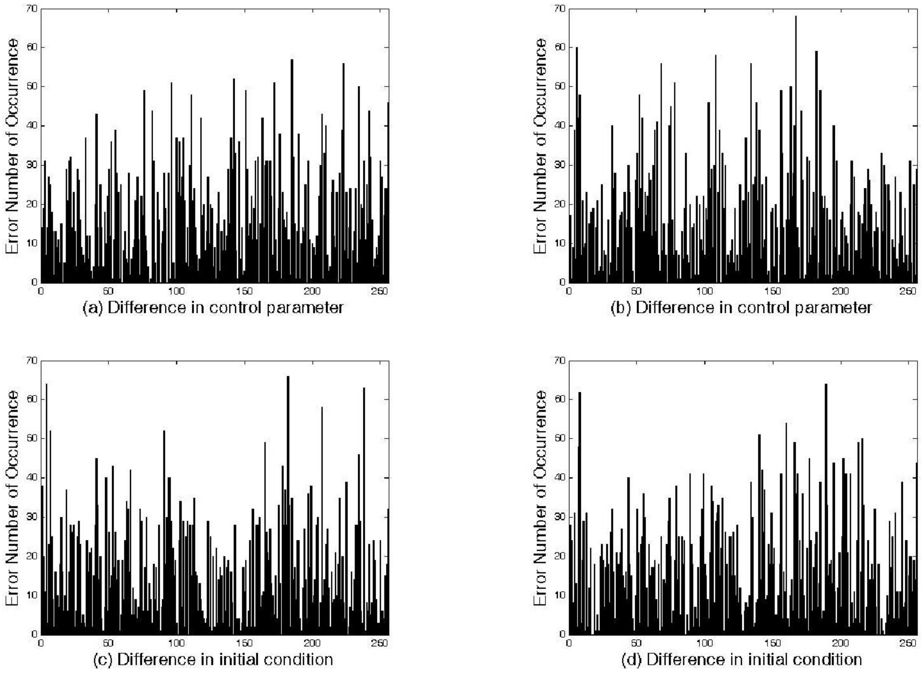
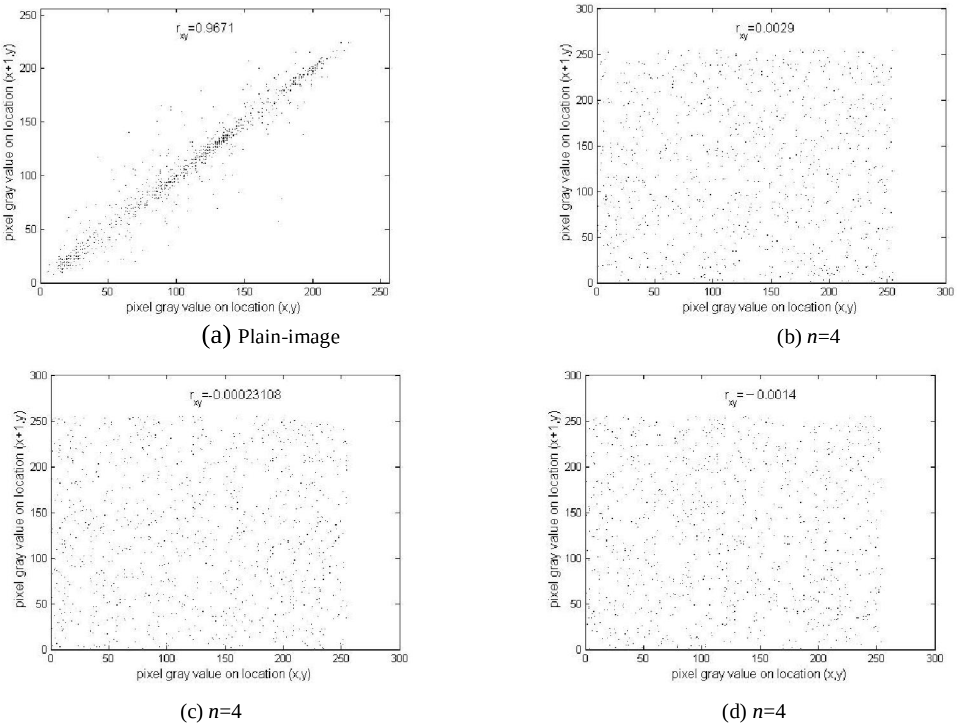


Figure 4. Distribution of error ciphertext

TABLE IV.
CORRELATION COEFFICIENTS OF TWO HORIZONTALLY ADJACENT PIXELS

	Plain-image	*n*=4	*n*=8	*n*=9
correlation coefficients	0.9671	0.0029	-0.00023108	−0.0014



(a) Plain-image (b) *n*=4

(c) *n*=4 (d) *n*=4

Figure 5. Correlations of two horizontally adjacent pixels

$$H(m) = -\sum_{i=0}^{2^N-1} P(m_i)\log_2[P(m_i)], \qquad (6)$$

where $P(m_i)$ is the emergence probability of m_i. If every symbol has an equal probability, i.e.,

$m = \{m_0, m_1, \mathrm{L}\ , \ m_{2^8-1}\}$ and $P(m_i) = 1/2^8$ (i=0, 1, L , 255), then the entropy is $H(m)$=8, which corresponds to a random source. Usually, the practical information entropy is less diverse than the ideal one. The information entropy is respectively shown in Table II, which is very close to the ideal one, by different *n*.

C. Statistical analysis

a) Gray-scale histograms

Considering the statistical analysis of the plain-image and its encrypted images, the grey-scale histograms of them are shown in Figure 3. From Figure 3(b), (c) and (d), we can see that the grayscale distribution of encrypted image has good balance property, which is strongly against known plaintext attacks.

In order to show the small perturbations of unknown key parameters, we will show the distribution of Error Ciphertext [7] which means the error number occurrences between the encryption system in the above section and the incryption system with small perturbations of unknown keys listed as follows:

(a) $\alpha^1 = 1.0999999999$;

(b) $\beta^2 = 6.0010000000001$;

(c) $x_0^1 = 0.5432106789017176$;

(d) $x_0^2 = 0.5432106789017178$;

the others are the same as those in Sec. IV. The distribution of Error map is shown in Figure 4, respectively. And the information entropy of them is respectively shown in Table III. It is shown that even a small variation of system parameters may result in the wrong encryption maps. Therefore, it is really hard to reveal the original cryptosystem.

b) Correlation analysis

To test the correlation between two adjacent pixels in plain-image and cipher-image, the following procedure was carried out [2]. First, select 1000 pairs of two adjacent (in horizontal, vertical, and diagonal direction) pixels from an image randomly. Then, calculate the correlation coefficient of each pair by using the following formulas:

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

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

where *x* and *y* are grey-scale values of two adjacent pixels in the image. In numerical computation, the following discrete formulas are used:

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

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

TABLE V.
CORRELATION COEFFICIENTS OF TWO ADJACENT PIXELS

	Plain-image	**Cipher-image**
Horizontal	0.9671	0.0029
Vertical	0.9339	0.0096
Diagonal	0.9066	0.0054

Figure 5 shows the correlation distribution of two horizontally adjacent pixels in the plain-image and that in the cipher-image when *n*=4, 8, and 9, and the correlation coefficients are shown in Tab. IV. It is shown that the correlation coefficients of two horizontally adjacent pixels in the plain-image and that of the cipher-image are far apart. Similar results for vertical and diagonal directions are obtained, which are shown in Table V when *n*=2. These correlation analyses prove that the chaotic encryption algorithm satisfies zero co-correlation.

D. Differential analysis

TABLE VI.
DIFFERENTIAL ANALYSIS (*KA*)

n	NPCR(%)	UACI(%)
4	0.492859	0.331024
5	0.497437	0.330658
6	0.497437	0.330826
7	0.500449	0.331451
8	0.497437	0.330856
9	0.492859	0.330795
10	0.492859	0.330627
11	0.503540	0.331329

TABLE VII.
Differential analysis (*KB*)

n	NPCR(%)	UACI(%)
4	0.512695	0.330750
5	0.502014	0.330338
6	0.508118	0.330826
7	0.486755	0.330994
8	0.495911	0.331116
9	0.506592	0.330597
10	0.492859	0.330765
11	0.497437	0.331238

To test the influence of one-pixel change on the whole image encrypted by the proposed algorithm, two common measures, NPCR and UACI [2], were used. NPCR means the change rate of the number of pixels of ciphered image while one pixel of plain-image is changed. UACI which is the unified average changing intensity, measures the average intensity of the differences between the plain-image and ciphered image.

Denote two cipher-images, whose corresponding plain-images have only one-pixel difference, by C_1 and C_2, respectively. Label the grey-scale values of the pixels at grid (i, j) of C_1 and C_2 by $C_1(i, j)$ and $C_2(i, j)$, respectively. Define a bipolar array, *D*, with the same size as image C_1 or C_2. Then, $D(i, j)$ is determined by

$C_1(i, j)$ and $C_2(i, j)$, namely, if $C_1(i, j)=C_2(i, j)$ then $D(i, j)=1$; otherwise, $D(i, j)=0$. To resist differential attack, the NPCR value should be small enough, and the UACI value should be large enough for an ideal cipher system.

Tests have been performed on the proposed scheme, about the one-pixel change influence on a 256 grey-scale image of size 256×256. With two different keys, *KA* and *KB* the results are shown in Table VI and Table VII. According to the two tables, the proposed cryptosystem can achieve a high performance such as NPCR<0.5127% and UACI>0.33033% when $n \le 11$. Therefore, the proposed algorithm can resist differential attacks.

VI. CONCLUSION

Only by the XOR operation, a novel image encryption scheme based on NCM is proposed in this paper. Every time the NCM is iterated, *n* (*n*>3) bytes random numbers can be gained so as to improve the encryption speed, and before next time iteration, a small perturbation will be given to the parameters of NCM based on the last obtained *n* bytes message. In each round of the proposed scheme which includes two rounds, the message $P = \; p_0, \mathrm{L}\, , p_j, \mathrm{L}\; p_{MN-1}$ is modified in the ascending order of *j* firstly, and then the modified message is encrypted in the descending order of *j*. Simulation results show that the new cryptosystem is fast, which makes the transmission of large multi-media files over public data communication network more practical. Theoretical analysis indicates that the proposed chaos-based image encryption scheme can achieve a high performance and is secure against known/chosen plaintext attack and all kinds of brute-force attacks.

ACKONOWLEDGMENT

This work is supported by the Natural Science Foundation of China (No. 60973146 and No. 61070163), the Natural Science Foundation of Shandong Province, China (ZR2009GM036), the Foundation for Study Encouragement to Middle-aged and Young Scientists of Shandong Province, China (No. 2008BS01019).

REFERENCES

[1] Z. H. Guan, F. Huang and W. Guan, "Chaos-based image encryption algorithm," *Phys. Lett. A*, vol. 346, no. 1-3, pp. 153-157, 2005.

[2] G. Y. Chen, Y. B. Mao, C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," *Chaos, Solitons and Fractals*, vol. 21, no.3, pp. 749-761, 2004.

[3] R. Matthews, "On the derivation of a 'chaotic' encryption algorithm," *Cryptologia*, vol. 13, no. 1, pp. 29-42, 1989.

[4] J. Fridrich, "Image encryption based on chaotic maps," *The 1997 IEEE International Conference on Systems, Man, and Cybernetics*, Hyatt Orlando, Florida, USA, vol. 2, pp. 1105-1110, October 12-15, 1997.

[5] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," *Int. J. Bifurcat Chaos*, vol. 8, no. 6, pp. 1259-1284, 1998.

[6] T. Xiang, X. F. Liao, G. P. Tang, Y. K. Chen, and W. Wong, "A novel block cryptosystem based on iterating a chaotic map," *Phys. Lett. A*, vol. 349, no. 1-4, pp. 109-115, 2006.

[7] W. W. Yu and J. D. Cao, "Cryptography based on delayed chaotic neural networks," *Phys. Lett. A*, vol. 356, no. 4-5, pp. 333-338, 2006.

[8] T. G. Gao and Z. Q. Chen, "Image encryption based on a new total shuffling algorithm," *Chaos, Solitons and Fractals*, vol. 38, no.1, pp. 213-220, 2008.

[9] T. G. Gao and Z. Q. Chen, "A new image encryption algorithm based on hyper-chaos," *Phys. Lett. A*, vol. 372, no. 4, pp. 394-399, 2008.

[10] G. Alvarez, F. Montoya, M. Romera, and G Pastor, "Cryptanalysis of an ergodic chaotic cipher," *Phys. Lett. A*, vol. 311, no. 2-3, pp. 172-179, 2003.

[11] C. Q. Li, S. J. Li, G. Alvarez, G. R. Chen, and K. T. Lo, "Cryptanalysis of two chaotic encryption schemes based on circular bit shift and XOR operations," *Phys Lett A*, Vol. 369, no. 1-2, pp. 23-30, 2007.

[12] S. J. Xu and J. Z. Wang, "An improved block cryptosystem based on iterating chaotic map," *Acta Phys. Sin.*, vol. 57, no. 1, pp. 37-41, 2008.

[13] Y. Wang, X. F. Liao, T. Xiang, K. W. Wong and D. G. Yang, "Cryptanalysis and improvement on a block cryptosystem based on iteration a chaotic map," *Phys. Lett. A*, vol. 363, no. 4, pp. 277-281, 2007.

[14] D. Arroyo, C. Q. Li, S. J. Li, G. Alvarez and W. A. Halang, "Cryptanalysis of an image encryption scheme based on a new total shuffling algorithm," *Chaos, Solitons and Fractals*, vol. 41, no. 5, 2613-2616, 2009.

[15] A. Akhshani, H. Mahmodi and A.Akhavan, "A Novel Block Cipher Based on Hierarchy of One-Dimensional Composition Chaotic Maps," *IEEE Int. Conf. on Image Processing*, Atlanta, GA, USA, pp. 1993-1996, Oct. 2006.

[16] H. P. Xiao and G. J. Zhang, "An Image Encryption Scheme Based on Chaotic Systems," *the Fifth Int. Conf. on Machine Learning and Cybernetics*, Dalian, China, vol. 5, pp. 2707-271, Aug. 2006.

[17] C. Fu, Z. C. Zhang and Y.Y. Cao, "An Improved Image Encryption Algorithm Based on Chaotic Maps," *thr Third Int. Conf. on Natural Comput*. Haikou, Hainan, China, vol. 3, pp. 189-193, Aug. 2007.

[18] Y. Y. Cao and C. Fu, "An image encryption scheme based on high dimension chaos system," *International Conference on Intelligent Computation Technology and Automation*, Changsha, Hunan, China, vol. 1, pp. 104-108, October 20-22, 2008.

[19] H. Y. Jiang and C. Fu, "An Image Encryption Scheme Based on Lorenz Chaos System", *Fourth International Conference on Natural Computation,* Jinan, China, vol. 4, pp. 600-604, October 18-20, 2008.

[20] S. J Xu, J. Z. Wang and S. X. Yang, "An improved image encryption algorithm based on chaotic maps," *Chin. Phys. B*, vol. 17, no. 11, pp. 4027-4032, 2008.

[21] T. G. Gao and Z. Q. Chen, "Image encryption based on a new total shuffling algorithm," *Chaos, Solitons and Fractals*, vol. 38, no.1, pp. 213-220, 2008.

[22] T. G. Gao and Z. Q. Chen, "A new image encryption algorithm based on hyper-chaos," *Phys. Lett. A*, vol. 372, no. 4, pp. 394-399, 2008.

[23] S. Behnia, A. Akhshani, S. Ahadpour, H. Mahmodi, and A. Akhavand, "A fast chaotic encryption scheme based on

piecewise nonlinear chaotic maps," *Phys. Let. A*, vol. 366, no. 4-5, pp. 391-396, 2007.

[24] S. Behnia, A. Akhshani, H. Mahmodi, and A. Akhavand, "A novel algorithm for image encryption based on mixture of chaotic maps," *Chaos, Solitons and Fractals*, vol. 35, no. 2, pp. 408-419, 2008.

[25] F. Y. Sun, S. T. Liu, Z. Q. Li, Z. W. Lu, "A novel image encryption scheme based on spatial chaos map," *Chaos, Solitons and Fractals*, vol. 38, no. 3, pp. 631-640, 2008.

[26] X. Y. Wang, *Chaos in complex nonlinear system*, Beijing: Publishing House of Electronics Industry, 2003.

[27] S. S. E. H. Elnashaie, Abasha ME, "On the chaotic behaviour of forced fluidized bed catalytic reactors," *Chaos, Solitons and Fractals*, vol. 5, no. 5, pp. 797-831, 1995.

[28] L.Kocarev, "Chaos-based cryptography: a brief overview," *IEEE Circuits and Systems Magazine*, vol. 1, no. 3, pp. 6-21, 2001.

[29] M. I. Sobhy, A. R. Shehata, "Methods of attacking chaotic encryption and countermeasures," *IEEE Acoust Speech Signal Process*, Salt Lake City, UT, USA, vol. 2, pp. 1001-4, 2001.

[30] H. J. Gao, Y. S. Zhang, S. Y. liang and D. Q. Li, "A new chaotic algorithm for image encryption," *Chaos, Solitons and Fractals*, Vol. 29, no. 2, pp. 393-399, 2006.

Shujiang Xu received the Science degree in mathematics and applied mathematics from Shandong Normal University, Jinan, P.R. China, in 2003 and the M.S. degrees in applied mathematics in computer symbolic computing from Beijing University of Posts and Telecommunications, Beijing, P.R. China, in 2006.

Since 2006, he has been a Research Assistant in Shandong Provincial Key Laboratory of computer Network, Shandong Computer Science Center, Jinan, PR China. Her research interests include chaotic systems, trust management, computer symbolic computing and cryptanalysis.

Yinglong Wang received the Engineer M.S. degree in industrial automation from Shandong University of Technology, Jinan, P.R. China, in 1995 and the Ph. D. degree in communication and information systems from Shandong University, Jinan, P.R. China, in 2005.

Since 1996, he has been a Researcher in Shandong Provincial Key Laboratory of computer Network, Shandong Computer Science Center, Jinan, PR China. His research interests include information security, wireless network, and cloud computing.

Yucui Guo received the Science degree in mathematics from Jilin University, Changchun, P.R. China, in 1982 and the M.S. of Technology in Academe of Railroad Science, Beijing, PR China, in 1988 and Ph.D. degree in Beijing Institute of Technology, Beijing, P.R. China, in 1997.

She worked at Shenyang Institute of Technology as a teacher from 1982 to 1985 and at Beijing automobile Institute as a Design Engineer from 1988 to 1994.

Since Eight 1997, she has been with the School of Science, Beijing University of Telecommunications and Posts, where she is currently a Professor. Her current research interests lie in the areas of Applying Mathematics and Information Security, Trust Management. She is the author of books titled Introduction of Nonlinear Partial Differential Equations and Mathematical Methods in Physics Science (Tsinghua University Press, 2008 & 2005). She is now presiding over a Project of National Natural Science Foundation of China--Research on Autonomic Trust Management for Fundamental Software Platform.