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 permuted and then substituted, or was first substituted and then permuted. 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 was transformed into the plaintext matrix M 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 $\mathcal{C}$ 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:

$$\alpha_0 = (1 - \beta^n) \cdot \tan \left( \frac{\alpha}{1 + \beta} \right) \cdot \left( 1 + \frac{1}{\beta} \right)^\beta$$

where $\alpha, \beta$ are control parameters. When $x_n \in (0, 1) \cap \{ \alpha \in (0, 1.4) \cap \beta \in [5, 43) \}$, or $x_n \in (0, 1) \cap \{ \alpha \in (1.4, 1.5) \cap \beta \in [9, 38) \}$, or $x_n \in (0, 1) \cap \{ \alpha \in (1.5, 1.57) \cap \beta \in [3, 15] \}$ 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 $X = 0.x_1 x_2 \bar{L} x_{15} \bar{L}$ is a double-point value, the $n$ bytes decimal random numbers are generated as follows:

$$B_i = \text{mod}(X_{13-n+i}, 256),$$

where $i = 1, 2, \ldots, n$, mod($x, y$) returns the remainder after division, $x_0 = 0, 1, L, 9 \cdot 4 \leq n \leq 13$. 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, L, $M-1$; j=0, 1, L, $N-1$), suppose the secret key $K = (K_1, K_2) = (\alpha_1, \beta_1, x_0; \alpha_2, \beta_2, x_1)$, 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.

![Image encryption scheme](image)

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

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

Step 2 Choose the first sub-key $K_1 = (\alpha_1, \beta_1, x_0)$, 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 $P_1 = p_{nj}, p_{nj+1}, L, p_{nj+n-1}$ as follows:
\[ c_{nj+k} = p_{nj+k} \oplus a_{nj+k} \quad (3) \]

where \( \oplus \) is the XOR operation, and \( k=0, 1, \ldots, n-1 \).

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

\[
\begin{align*}
\alpha_j &= \frac{\sum_{k=0}^{n-1} c_{nj+k} + 10n}{2560n}, \quad \alpha_j > \alpha_0, \sum_{k=0}^{n-1} c_{nj+k} < 10n \\
\alpha_j &= \frac{\sum_{k=0}^{n-1} c_{nj+k}}{2560n}, \quad \alpha_j > \alpha_0, \sum_{k=0}^{n-1} c_{nj+k} \geq 10n \\
\alpha_j &= \frac{\sum_{k=0}^{n-1} c_{nj+k} + 10n}{2560n}, \quad \alpha_j \leq \alpha_0, \sum_{k=0}^{n-1} c_{nj+k} < 10n \\
\alpha_j &= \frac{\sum_{k=0}^{n-1} c_{nj+k}}{2560n}, \quad \alpha_j \leq \alpha_0, \sum_{k=0}^{n-1} c_{nj+k} \geq 10n \\
\beta_j &= \frac{\sum_{k=0}^{n-1} c_{nj+k} + 10n}{256000n}, \quad \beta_j > \beta_0, \sum_{k=0}^{n-1} c_{nj+k} < 10n \\
\beta_j &= \frac{\sum_{k=0}^{n-1} c_{nj+k}}{256000n}, \quad \beta_j > \beta_0, \sum_{k=0}^{n-1} c_{nj+k} \geq 10n \\
\beta_j &= \frac{\sum_{k=0}^{n-1} c_{nj+k} + 10n}{256000n}, \quad \beta_j \leq \beta_0, \sum_{k=0}^{n-1} c_{nj+k} < 10n \\
\beta_j &= \frac{\sum_{k=0}^{n-1} c_{nj+k}}{256000n}, \quad \beta_j \leq \beta_0, \sum_{k=0}^{n-1} c_{nj+k} \geq 10n
\end{align*}
\]

**Step 5** Choose the second sub-key \( K_2 = (\alpha^2, \beta^2, x_0^2) \), and then iterate NCM \( n_2 \) times.

Let \( M' = c_{MN-n}, c_{MN-n+2}, \ldots, c_0 \) and encrypt \( M' \) using the method described in Step 3 and Step 4. Finally, the encrypted matrix \( C \) can be obtained.

**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 \( K = (\alpha^1, \beta^1, x_1^1; \alpha^2, \beta^2, x_0^2) = (1.1, 6.0, 0.5432106789017177; 1.1, 6.001, 0.5432106789017177) \). 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.

![Figure 2. Encryption experimental results](image)

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 256x256 with different values of \( n \) is shown in Table 1. 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 $\left(10^{-15}\right)^3 = 10^{45}$. 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:

\[
H = -\sum_{i} p_i \log_2 p_i
\]

where $p_i$ is the probability of symbol $i$.

<table>
<thead>
<tr>
<th>TABLE I. ENCRYPTION TIME</th>
</tr>
</thead>
<tbody>
<tr>
<td>n</td>
</tr>
<tr>
<td>---------------------------</td>
</tr>
<tr>
<td>Encryption time (S)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TABLE II. INFORMATION ENTROPY</th>
</tr>
</thead>
<tbody>
<tr>
<td>n</td>
</tr>
<tr>
<td>-------------------------------</td>
</tr>
<tr>
<td>Entropy H</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TABLE III. Information entropy with different key</th>
</tr>
</thead>
<tbody>
<tr>
<td>n=4</td>
</tr>
<tr>
<td>a</td>
</tr>
<tr>
<td>-------------------------------------------------</td>
</tr>
<tr>
<td>Entropy H</td>
</tr>
</tbody>
</table>

Figure 3. Grayscale histogram of plain-image and cipher-images
A Novel Image Encryption Scheme based on a Nonlinear Chaotic Map

Figure 4. Distribution of error ciphertext

TABLE IV.
CORRELATION COEFFICIENTS OF TWO HORIZONTALLY ADJACENT PIXELS

<table>
<thead>
<tr>
<th>correlation coefficients</th>
<th>Plain-image</th>
<th>n=4</th>
<th>n=8</th>
<th>n=9</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0.9671</td>
<td>0.0029</td>
<td>-0.00023108</td>
<td>0.0014</td>
</tr>
</tbody>
</table>

Figure 5. Correlations of two horizontally adjacent pixels

\[ H(m) = - \sum_{i=0}^{n-1} P(m_i) \log_2[ P(m_i) ], \tag{6} \]

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, \ldots, m_{2^8-1}\} and P(m_i) = 1/2^8 \quad (i=0, 1, \ldots, 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 key parameters, we will show the distribution of Error Ciphertext \[7\] which means the error number

\[\alpha = 1.0999999999;\]
\[\beta = 6.0010000000001;\]
\[\chi_0^2 = 0.5432106789017176;\]
\[\chi_1^2 = 0.5432106789017178;\]

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:

\[\text{cov}(x, y) = \frac{1}{N} \sum_{i=1}^{N} (x_i - E(x))(y_i - E(y)).\]
\[\gamma_{xy} = \frac{\text{cov}(x, y)}{\sqrt{D(x)D(y)}},\]

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 VI

| CORRELATION COEFFICIENTS OF TWO ADJACENT PIXELS |
|----------------|----------------|
| Horizontal     | Cipher-image   |
| 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 \(n=4, 8, 9\), 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

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.

TABLE VII

<table>
<thead>
<tr>
<th>DIFFERENTIAL ANALYSIS (KA)</th>
</tr>
</thead>
<tbody>
<tr>
<td>n</td>
</tr>
<tr>
<td>---</td>
</tr>
<tr>
<td>4</td>
</tr>
<tr>
<td>5</td>
</tr>
<tr>
<td>6</td>
</tr>
<tr>
<td>7</td>
</tr>
<tr>
<td>8</td>
</tr>
<tr>
<td>9</td>
</tr>
<tr>
<td>10</td>
</tr>
<tr>
<td>11</td>
</tr>
</tbody>
</table>

TABLE VIII

<table>
<thead>
<tr>
<th>DIFFERENTIAL ANALYSIS (KB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>n</td>
</tr>
<tr>
<td>---</td>
</tr>
<tr>
<td>4</td>
</tr>
<tr>
<td>5</td>
</tr>
<tr>
<td>6</td>
</tr>
<tr>
<td>7</td>
</tr>
<tr>
<td>8</td>
</tr>
<tr>
<td>9</td>
</tr>
<tr>
<td>10</td>
</tr>
<tr>
<td>11</td>
</tr>
</tbody>
</table>

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...
According to the two tables, the proposed cryptosystem can achieve a high performance such as NPCR<0.5127% and UACI=0.33033% when \( n \leq 11 \). 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 \( P = p_0, L \cdot p_1, L \cdot p_{MN-1} \) 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.

### ACKNOWLEDGMENT

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 (2008BS01019).

### REFERENCES


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


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.