ICIC Express Letters
Volume **10**, Number **5**, May **2016**

 ISSN 1881-803X
pp. **1121–1127**

IMAGE ENCRYPTION: IMPROVED GENERALIZED DISCRETE ARNOLD TRANSFORMATION AND NONLINEAR CHAOTIC MAP

Ye Tian[1,2], Zhimao Lu[1,3] and Xueyao Gao[4]

[1]College of Information and Communication Engineering
Harbin Engineering University
No. 145, Nantong Street, Nangang District, Harbin 150001, P. R. China
hsdtianye@126.com

[2]Key Laboratory of Photonic and Electronic Bandgap Materials, Ministry of Education
School of Physics and Electronic Engineering
Harbin Normal University
No. 1, Shida Road, Hulan District, Harbin 150025, P. R. China

[3]Faculty of Electronic Information and Electrical Engineering
Dalian University of Technology
No. 2, Linggong Road, Ganjingzi District, Dalian 116024, P. R. China
lzm@dlut.edu.cn

[4]School of Computer Science and Technology
Harbin University of Science and Technology
No. 52, Xuefu Road, Nangang District, Harbin 150080, P. R. China
gaoxueyao@hotmail.com

Received November 2015; accepted February 2016

Abstract. *The development of computer networks makes image files transportation via network become more and more convenient. However, the security of most existing image encryption methods requires to be further improved. In this paper, we present an Image Encryption algorithm combining an Improved generalized discrete Arnold transformation and a Nonlinear Chaotic map (IEIANC). It adopts the scrambling and diffusion encryption framework. First, it designs an extra 256-bit key to make the key space large enough. Next, it utilizes an improved generalized discrete Arnold transformation to scramble image pixels, and divides the scrambled image into several blocks. Finally, it applies a nonlinear chaotic map to diffuse these blocks. The experimental results show the effectiveness of the proposed algorithm.*
Keywords: Image encryption, Discrete Arnold transformation, Nonlinear chaotic map

1. **Introduction.** The fast development of computer and network technologies has greatly changed people's communications ways [1]. Transmission over the Internet for digital multimedia content becomes more and more frequent; yet the sharing and openness of the network seriously threaten the security of the transmitted multimedia information. Thus, people have to pay more attention to the security of multimedia information. Among various image information protection methods, image encryption technique is one of the most common and efficient methods. However, due to the high correlation among pixels, special storage format and bulky data capacity in an image, many traditional block ciphers such as Advanced Encryption Standard (AES), Data Encryption Standard (DES) and International Data Encryption Algorithm (IDEA) are not suitable for image encryption [2]. During the past few years, many studies discovered that an image encryption scheme combining the permutation and diffusion stages was available to overcome the above shortcomings. For example, Chen et al. [3] proposed a confusion-diffusion architecture based image encryption scheme that employed a 3D cat map to shuffle the locations of pixels and used another chaotic map to confuse the relationship between the plain-image

and cipher-image. Zhu et al. [4] presented an image cryptosystem employing an Arnold cat map for bit-level permutation and a logistic map for diffusion. In the cryptosystem, when a bit in one pixel was exchanged with a bit in another pixel, the information in these two pixels was exchanged and their values were changed. Zhu et al. [5] also proposed an image encryption scheme applying a generalized Arnold map to performing a bit-level permutation procedure and affine cipher to execute a diffusion procedure. Although most of the above proposed combined methods could obtain good encryption effect, they adopted a one-dimensional chaos system, e.g., logistic map, or a high dimensional chaos map to perform the diffusion process. These chaotic systems still have many irritating weaknesses, such as small key space and weak security. In this paper, we adopt the permutation-diffusion framework and present an Image Encryption algorithm combining an Improved discrete Arnold transformation and a Nonlinear Chaotic map (IEIANC). IEIANC designs a 256-bit key to make the key space large enough, and uses the improved discrete Arnold transformation to scramble an image and nonlinear chaotic map to diffuse an image. The experimental results show the validity of the proposed image encryption algorithm. The rest of the paper is organized as follows. In Section 2, the chaotic system is introduced. The proposed image encryption scheme is presented in Section 3. The security analysis and evaluation are presented in Section 4, and Section 5 concludes this paper.

2. **Chaotic System.**

2.1. **L-T cascade transformation.**

The L-T cascade transformation that is the cascade of a Logistic map and a Tent map can be written as [6],

$$w_{n+1} = 1 - p\left|vw_n(1-w_n) - (1/p)\right|, \tag{1}$$

where, $p \in [0,2]$, $v \in [0,4]$ are system initial values, $w \in [0,1]$ is an initial value.

2.2. **Improved generalized two-dimensional Arnold transformation.**

Generalized two-dimensional Arnold transformation [5] is a one-to-one map of two-dimensional area-preserving. Since it is unavailable for zero vector and cannot resist differential attack, many nonlinear variables are introduced in this paper to improve it.

Generalized two-dimensional Arnold transformation can be written as,

$$\begin{aligned} x_{n+1} &= (ax_n + by_n) \bmod N, \\ y_{n+1} &= (cx_n + dy_n) \bmod N, \end{aligned} \tag{2}$$

where a, b, c, d are positive integers. Improved generalized two-dimensional Arnold transformation expression can be written as [7],

$$\begin{aligned} x_{n+1} &= (x_n + hy_n) \bmod N, \\ y_{n+1} &= (gx_n + (hg+1)y_n + ef(x_{n+1})) \bmod N, \end{aligned} \tag{3}$$

where, e, g and h are positive integers, and $f(x_{n+1})$ that can take the form, $f(x_{n+1}) = (x_{n+1})^r + d$, $r \in \{2,3,\ldots,7\}$, $d \in \{1,2,\ldots,255\}$, is a nonlinear function.

The corresponding inverse transformation expression can be written as,

$$\begin{aligned} x_n &= \left(\begin{vmatrix} x_{n+1} & h \\ y_{n+1} - ef(x_{n+1}) & hg-1 \end{vmatrix} \right) \bmod N, \\ y_n &= \left(\begin{vmatrix} 1 & x_{n+1} \\ g & y_{n+1} - ef(x_{n+1}) \end{vmatrix} \right) \bmod N, \end{aligned} \tag{4}$$

where, e, g and h are positive integers, and $f(x_{n+1})$ that can take the form, $f(x_{n+1}) = (x_{n+1})^r + d$, $r \in \{2,3,\ldots,7\}$, $d \in \{1,2,\ldots,255\}$, is a nonlinear function.

2.3. **Nonlinear chaotic map.** In this section, we will introduce another chaotic map, nonlinear chaotic map, the definition of which can be written as [8],

$$\begin{aligned} x_{n+1} &= [u \times \mu_1 \times (1 - x_n)^2 \times y_n + z_n] \bmod 1, \\ y_{n+1} &= [u \times \mu_2 \times x_{n+1} + (1 + (y_n)^2) \times z_n] \bmod 1, \\ z_{n+1} &= [u \times \mu_3 \times \sin(x_{n+1}) \times z_n + y_{n+1}] \bmod 1, \end{aligned} \tag{5}$$

where, $0 < u < 3.999$, $|\mu_1| > 29.5$, $|\mu_2| > 31.3$, $|\mu_3| > 25.1$, mod 1 refers to selecting the fraction part, i.e., $x \bmod 1 = x - \lfloor x \rfloor$.

3. Description of the Proposed Image Encryption Algorithm.

3.1. **Encryption process.** Without loss of generality, assume that the plaintext P is a grayscale image sizing of $M \times N$. The detailed encryption process of IEIANC can be described as the following.

(1) Use a 256-bits binary number to represent a key, and divide it into $k_1, k_2, \ldots, k_{32}$ with each k_i $(i = 1, 2, 3, \ldots, 32)$ representing an integer ranging of $[0, 255]$. The initial state of each variable of the encryption system can take the following forms,

$$key = [k_1, k_2, \ldots, k_{32}], \tag{6}$$

$$xork = k_1 \oplus k_2 \oplus \cdots \oplus k_{32}, \tag{7}$$

$$avi = \left\lfloor \sum_{x \in [1,M], y \in [1,N]} P(x, y)/(M \times N) \right\rfloor, \tag{8}$$

$$avk = 2 \times \left(\left\lfloor \sum_{i=1}^{32} k_i/32 \right\rfloor \bmod 3 + 1 \right), \tag{9}$$

$$w_0 = (k_1 + k_3 + k_5 + k_7 + xork + avi)/2^{12} + 0.2, \tag{10}$$

$$p = (k_2 + k_4 + k_6 + k_8 + xork + avi)/2^{12} + 1.7, \tag{11}$$

$$v = (k_9 + k_{11} + k_{13} + k_{15} + xork + avi)/2^{12} + 3.7, \tag{12}$$

$$e = 1, \tag{13}$$

$$r = 3, \tag{14}$$

$$d = \left(xork + \sum_{x \in [1,M], y \in [1,N]} P(x, y) \right) \bmod 256, \tag{15}$$

$$u = (k_{10} + k_{12} + k_{14} + k_{16} + xork + avi)/2^{12} + 3.7, \tag{16}$$

$$\mu_1 = (k_{17} + k_{18} + k_{19} + k_{20} + xork + avi)/2^{12} + 30, \tag{17}$$

$$\mu_2 = (k_{19} + k_{20} + k_{21} + k_{22} + xork + avi)/2^{12} + 32, \tag{18}$$

$$\mu_3 = (k_{21} + k_{22} + k_{23} + k_{24} + xork + avi)/2^{12} + 26, \tag{19}$$

$$x_0 = (k_{25} + k_{26} + k_{27} + k_{28} + xork + avi)/2^{12} + 0.2, \tag{20}$$

$$y_0 = (k_{27} + k_{28} + k_{29} + k_{30} + xork + avi)/2^{12} + 0.2, \tag{21}$$

$$z_0 = (k_{29} + k_{30} + k_{31} + k_{32} + xork + avi)/2^{12} + 0.2, \tag{22}$$

where, w_0, e, r, d, x_0, y_0 and z_0 are initial values of the L-T cascade map and improved generalized two-dimensional Arnold transformation, p, v, u, μ_1, μ_2 and μ_3 are initial control parameters of the L-T cascade map and nonlinear chaotic map.

(2) Substitute the initial values w_0 and control parameters p into Equation (1) to iterate $1000 + 2average\_k$ times. To avoid the transient effects, we discard the iteration values before 1000 times such that the results are more random, and substitute the remaining $2average\_k$ iteration values into Equation (23).

$$s = \left\lfloor w_i \times 10^2 \right\rfloor \bmod 10 + 1 \qquad i = 1, 2, 3, \ldots, 2average\_k. \tag{23}$$

(3) Substitute s into Equations (24) and (25) to obtain h and g.

$$h = s_i \qquad i = 1, 3, 5, \ldots, 2average - 1, \tag{24}$$

$$g = s_i \qquad i = 2, 4, 6, \ldots, 2average. \tag{25}$$

(4) Substitute h, g, e, r, d into Equation (4) to gain a scrambled image, denoted by P'.

(5) Decompose P' into $m \times n$ sub-blocks scaled as $M/m \times N/n$, denote each sub-block by A_i, $i \in [1, m \times n]$, and convert A_i to a one-dimensional vector B_i (from left to right, and top to bottom).

(6) Set $j \leftarrow 1$, and substitute initial values x_0, y_0, z_0, and control parameters u, μ_1, μ_2, μ_3 into Equation (5) to iterate. Discard the former 1000 iteration values and continue to iterate 15000 times with the 1001st value being the initial value to obtain the real value sequences x_i, y_i, z_i, $i = 1, 2, 3, \ldots$.

(7) Substitute x_i into Equation (26).

$$X_j = \lfloor x_i \times 10^2 \rfloor \bmod (M/m \times N/n) + 1. \tag{26}$$

(8) Define an array (denoted by S) of length $M/m \times N/n$. If X_i has appeared in S or $X_i = i$, abandon X_i; otherwise, deposit X_i into S. When the array is filled in, the S-box is generated, i.e., $S = \{s_1, s_2, s_3, \ldots, s_{M/m \times N/n}\}$.

(9) Use $S = \{s_1, s_2, s_3, \ldots, s_{M/m \times N/n}\}$ to scramble sequence B_j to obtain C_j.

(10) Substitute y_i, z_i into Equations (27) and (28).

$$Y_j = \lfloor y_i \times 10^3 \rfloor \bmod 256 \qquad i = 1, 2, \ldots, M/m \times N/n, \tag{27}$$

$$Z_j = \lfloor z_i \times 10^3 \rfloor \bmod 256 \qquad i = 1, 2, \ldots, M/m \times N/n. \tag{28}$$

(11) Use the following two equations to encrypt,

$$D_j(i) = ((C_j(i) \oplus Y_j(i) + Z_j(i)) \bmod 256) \oplus avi \qquad i = 1, \tag{29}$$

$$D_j(i) = ((C_j(i) \oplus Y_j(i) + Z_j(i)) \bmod 256) \oplus D_j(i-1) \qquad i = 2, 3, \ldots, M/m \times N/n, \tag{30}$$

where $\oplus$ represents XOR operation, $D_j(i)$ denotes the i-th pixel of the j-th block cipher. Note: avi that is the average pixel value of a plaintext image will be used to encrypt the 1-st pixel of the corresponding ciphertext image in this paper.

(12) Let $j \leftarrow j + 1$, and repeat Steps (6)-(11) until $j = m \times n$, where x_0, y_0, z_0 respectively represent the last three pixels of the former ciphertext image. Output the ciphertext D when all pixels are encrypted.

(13) If a higher security is required, begin at the ciphertext of the last four pixels and from back to front, return to Steps (6)-(12).

3.2. **Decryption process.** The decryption process and encryption process are opposite, i.e., reverse Steps (2)-(7). In this way, the ciphertext image can be restored.

4. Experimental Results and Performance Analysis.

4.1. **Experimental results.** To verify the effectiveness of IEIANC, we adopt three famous indexes, Number of Pixels Change Rate (NPCR), Unified Average Changing Intensity (UACI) [9] and information entropy [10], to evaluate the encryption effect of IEIANC and compare it with the algorithms proposed in [11-18] because IEIANC has the same encryption stages as the literature except for the chaotic maps. A 256×256 Lena grayscale picture shown in Figure 1(a) is used as the plaintext. We will operate only one encryption round with $M = 256$, $N = 256$, $m = 32$, $n = 32$ and use the following encryption key, 100 130 63 112 23 18 114 30 156 120 127 100 27 190 11 119 26 19 110 57 149 124 23 168 101 30 141 65 12 64 91 116 (32 decimal numbers, each number can be written in an 8-bit binary number, a total of 256 bits). The encrypted image is shown in Figure 1(b).

(a) Original image (b) Encrypted image

FIGURE 1. Original image and its encrypted image

4.2. **Differential attack test.** NPCR and UACI are adopted to analyze encryption effects, and the ideal values of NPCR and UACI are 100% and 33.333% respectively. Suppose two ciphertext images C_1, C_2, the corresponding plaintext images are the same except for only one pixel. Use Equations (31) and (32) to calculate NPCR and UACI [9],

$$\text{NPCR} = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} D(i,j) \times 100\%, \tag{31}$$

$$\text{UACI} = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{|C_1(i,j) - C_2(i,j)|}{255} \times 100\%, \tag{32}$$

where, M and N respectively represent the width and height of the image, $C_1(i,j)$ and $C_2(i,j)$ respectively denote the pixels at position (i,j) of two ciphertext images which originate from the plaintext and the one pixel changed plaintext. If $C_1(i,j) \neq C_2(i,j)$, then $D(i,j) = 1$; otherwise, $D(i,j) = 0$.

TABLE 1. NPCR and UACI of ciphertext of Lena

Image	Lena	Ref. [11]	Ref. [12]	Ref. [13]	Ref. [14]	IEIANC
NPCR	0.9963	0.9962	0.9961	0.9961	0.9958	0.9963
UACI	0.3351	0.3346	0.3346	0.3346	0.3341	0.3351

Table 1 depicts the NPCR and UACI of the ciphertext of Lena obtained by different algorithms. The results show that IEIANC is sensitive to the plaintext, and has a high capability of resisting the differential attack.

4.3. **Entropy analysis.** In this paper, the information entropy reflecting the randomness of the occurrence of the pixel gray values in the encryption results is used. Denote by m the information source, and use Equation (33) to calculate the entropy [10],

$$H(m) = \sum_{i=0}^{2^n-1} p(m_i) \log_2 \frac{1}{p(m_i)}. \tag{33}$$

Here, $p(m_i)$ represents the probability of the occurrence of pixel gray value m_i. According to Equation (33), if the information entropy $H(m) = 8$, the information is then completely random, and the disorder of the information is the strongest, that is, the information entropy of the ciphertext should be close to 8.

TABLE 2. Information entropy of Lena ciphertext

Methods	Ref. [15]	Ref. [16]	Ref. [17]	Ref. [18]	IEIANC
Entropy	7.9971	7.9965	7.9968	7.9966	7.9974

Table 2 depicts the information entropy of ciphertext of Lena obtained by different algorithms. We can make the observation that the encryption effect of IEIANC is better since its information entropy is closer to 8.

5. **Conclusion and Looking.** A block encryption algorithm combining an improved generalized two-dimensional Arnold map and a nonlinear chaotic map is proposed in this paper. Its image encryption process consists of two stages: scrambling and diffusion. In the scrambling stage, it divides an image into several sub-blocks that are respectively scrambled by an improved generalized two-dimensional Arnold map; as a result, it disturbs the correlation among adjacent pixels. Furthermore, by introducing the nonlinear variable, the improved Arnold map becomes a non-quasi-affine transformation that can resist differential attack. Meanwhile, the usage of the Arnold map significantly expands the scrambling period, which further breaks the correlation among adjacent pixels. In the diffusion stage, A nonlinear chaotic map is applied to diffuse the sub-blocks to enhance the proposed algorithm's ability of resisting chosen plaintext and known plaintext attacks. The results via simulation show the effectiveness of the proposed encryption algorithm. In the future, the feasibility of combining chaotic encryption system and DNA rules to further enhance the security of image encryption will be investigated.

Acknowledgment. This work is partially supported by the National Natural Science Foundation of China (Nos: 60603092, 60975042, and 61502124). The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers, which help to improve the presentation.

REFERENCES

[1] G. Ye, A novel logistic-based image encryption scheme, *ICIC Express Letters*, vol.4, no.3(B), pp.979-984, 2010.
[2] X. Huang, A novel high-diemension chaos-based block image encryption algorithm, *ICIC Express Letters*, vol.6, no.12, pp.3171-3176, 2012.
[3] G. Chen, Y. Mao and 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.
[4] Z. L. Zhu, W. Zhang, K. W. Wong and H. Yu, A chaos-based symmetric image encryption scheme using a bit-level permutation, *Information Sciences – An International Journal*, vol.181, no.6, pp.1171-1186, 2011.
[5] H. Zhu, C. Zhao, X. Zhang and L. Yang, An image encryption scheme using generalized Arnold map and affine cipher, *Optik – International Journal for Light and Electron Optics*, vol.125, no.22, pp.6672-6677, 2014.
[6] G. Y. Wang and F. Yuan, Cascade chaos and its dynamic characteristics, *Acta Physica Sinica*, vol.62, no.2, p.20, 2013.
[7] C. M. Wu, An improved discrete Arnold transform and its application in image scrambling and encryption, *Acta Physica Sinica*, vol.63, no.9, p.20, 2014.
[8] I. S. Sam, P. Devaraj and R. S. Bhuvaneswaran, An efficient quasigroup based image encryption using modified nonlinear chaotic maps, *Sensing and Imaging*, vol.15, no.1, 2014.
[9] C. X. Zhu, A novel image encryption scheme based on improved hyperchaotic sequences, *Optics Communications*, vol.285, no.1, pp.29-37, 2012.
[10] Y. Wang, K. W. Wong, X. F. Liao and G. R. Chen, A new chaos-based fast image encryption algorithm, *Applied Soft Computing*, vol.11, no.1, pp.514-522, 2011.
[11] G. D. Ye and K. W. Wong, An efficient chaotic image encryption algorithm based on a generalized Arnold map, *Nonlinear Dynamics*, vol.69, no.4, pp.2079-2087, 2012.
[12] H. Hermassi, R. Rhouma and S. Belghith, Improvement of an image encryption algorithm based on hyper-chaos, *Telecommunication Systems*, vol.52, no.2, pp.539-549, 2013.

[13] Y. Wang, K. W. Wong, X. Liao, T. Xiang and G. Chen, A chaos-based image encryption algorithm with variable control parameters, *Chaos, Solitons and Fractals*, vol.41, no.4, pp.1773-1783, 2009.
[14] X. Y. Wang and X. M. Bao, A novel block cryptosystem based on the coupled chaotic map lattice, *Nonlinear Dynamics*, vol.72, no.4, pp.707-715, 2013.
[15] X. Y. Wang, L. T. Liu and Y. Q. Zhang, A novel chaotic block image encryption algorithm based on dynamic random growth technique, *Optics and Lasers in Engineering*, vol.66, pp.10-18, 2015.
[16] F. Sun, Z. Lv and S. Liu, A new cryptosystem based on spatial chaotic system, *Optics Communications*, vol.283, no.10, pp.2066-2073, 2010.
[17] S. Behnia, A. Akhshani, H. Mahmodi and A. Akhavan, A novel algorithm for image encryption based on mixture of chaotic maps, *Chaos Solitons and Fractals*, vol.35, no.2, pp.408-419, 2008.
[18] Q. Zhou and X. F. Liao, Collision-based flexible image encryption algorithm, *Journal of Systems and Software*, vol.85, no.2, pp.400-407, 2012.