2008 10th Intl. Conf. on Control, Automation, Robotics and Vision
Hanoi, Vietnam, 17–20 December 2008

A New Pixel-Chaotic-Shuffle Method for Image Encryption

H. H. Nien, S. K. Changchien, and S. Y. Wu
Department of Electrical Engineering
CTU, Changhua 500, Taiwan.
nien@ctu.edu.tw

C. K. Huang
Department of Industrial Education and Technology
NCUE, Changhua 500, Taiwan
ckhuang@cc.ncue.edu.tw

Abstract—**This paper proposes a novel Pixel-Chaotic-Shuffle method for image encryption. Since the dynamic response of chaotic system is highly sensitive to the initial values of a system and to the variation of a parameter, chaotic trajectory is very unpredictable. Therefore we use the chaotic sequences generated by chaotic systems as encryption codes and then implement the digital-color image encryption with high security. The proposed method combined with 4 chaotic systems and pixel shuffle can fully banish the outlines of the original image, disorders the distributive characteristics of RGB levels, and dramatically decreases the probability of exhaustive attacks. Eventually, the statistic methods involving FIPS PUB 140-1, the correlation coefficient *r*, NPCR (Number of Pixel Change Rate), and UACI (Unified Average Changing Intensity) are applied to test on the security analysis and the distribution of distinguished elements of variables of the encrypted image. An empirical example shows that the proposed method has the great encryption performance and achieves the high security.**

Keywords—**Pixel-Chaotic-Shuffle, chaotic system, correlation coefficient *r*, NPCR, UACI.**

I. INTRODUCTION

Since the dynamic response of the chaotic system is sensitively to the initial values and parameters, a great number of researches apply chaotic codes to encrypt images for the purpose of communication security [1-5]. It is a convenient and fast method by conducting a first-order chaotic system to encode a digital-color image [6]. But there was report proposed that the communication security was insufficient [7]. Zhang and He created the encrypting matrix using a first-order chaotic sequence to encrypt the original matrix, and then conducted a second-order sequence to disguise the encrypted matrix with high security [8]. Since the high security is the character of a high-order chaotic system, Zhu et al. proposed a digital-color image encryption based on a third-order chaotic system [9]. They confused the relation between the encryption image and. original image by means of shuffling the position and varying the RGB levels of pixels. Sun and Chen used Lorenz system to produce chaotic sequences, and combined chaotic mapping to encrypt image for promoting encryption security [10]. Sun et al. presented a shuffling method with the third-order Chua system for image space [11]. This method could avoid the localized distribution of grey levels. Kwok and Tang [21] proposed a fast chaos-based image encryption system with stream cipher structure. The major core of the encryption system is a pseudo-random key stream generator based on a cascade of chaotic maps, serving the purpose of sequence generation and random mixing.

However, the small key spaces are the major drawback of those methods with single chaotic system; moreover, the RGB levels are unchanged when only pixel shuffle used. For this reason, this paper conducts chaotic variables with double scroll attractor [13], butterfly attractor [14], spiral attractor [15], and discrete-time [16] to product four encryption-code sets applied on pixel shuffle. Finally, a high communication security with a dramatically large key space and converted RGB-level spectrums are achieved.

II. A NOVEL PIXEL-CHAOTIC-SHUFFLE METHOD

A. Chaotic System

The third-order chaotic systems applied in this paper are shown below:

(1). Hénon map (discrete time) [16]:

$$x(k+1) = a - y^2(k) - bz(k) \quad \text{(1a)}$$

$$y(k+1) = x(k) \quad \text{(1b)}$$

$$z(k+1) = y(k), \quad \text{(1c)}$$

where $a = 1.76$ and b=-0.1.

(2). Lorenz (butterfly attractor) [14]:

$$\dot{x} = -\sigma x + \sigma y \quad \text{(2a)}$$

$$\dot{y} = -xz + \gamma x - y \quad \text{(2b)}$$

$$\dot{z} = xy - bz, \quad \text{(2c)}$$

where $\sigma = 16$, $\gamma = 40$, and $b = -4$.

(3). Chua (double scroll attractor) [13]:

$$\dot{x} = \alpha(y - x - h(x)) \quad \text{(3a)}$$

$$\dot{y} = x - y + z \quad \text{(3b)}$$

$$z = -\beta y - \gamma z \tag{3c}$$

$$h(x) = m_1 x + 0.5(m_0 - m_1)(|x+1| - |x-1|) \quad , \tag{3d}$$

where $\alpha = 10$, $\beta = 14.78$, $\gamma = 0.0385$, $m_0 = -1.27$, and $m_1 = -0.68$.

(4). Rössler (spiral attractor) [15]:

$$x = -(y + z) \tag{4a}$$

$$y = x + ay \tag{4b}$$

$$z = b + z(x - c), \tag{4c}$$

where $a = 0.2$, $b = 0.2$, and $c = 5.7$.

B. Pixel-Chaotic-Shuffle

As the color contrast of the original image's outline becomes more distinct, the characteristic of the RGB levels will not be eliminated when only applied pixel shuffle on the image encryption. For this reason, this paper proposes a novel PCS encryption method. The proposed method can vary the RGB level and position of each pixel simultaneously.

Fig. 1 shows the flowchart of the proposed method. Four chaotic systems are applied to create encryption-code sets individually.

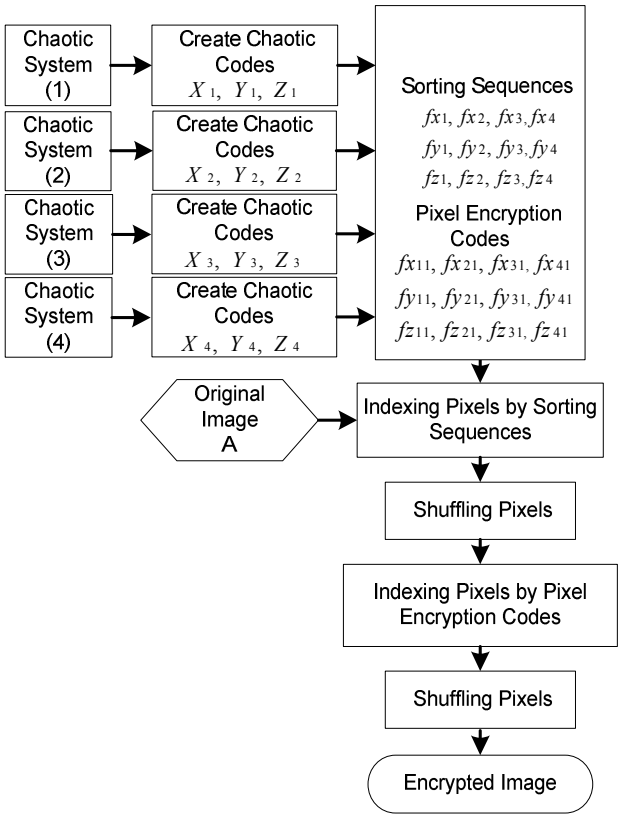

Figure 1. Flowchart of the proposed PCS.

The steps in the PCS can be outlined as follows:

Step 1: Select proper initial values and system parameters to create chaotic variable sets $X_1 \sim X_4$, $Y_1 \sim Y_4$ and $Z_1 \sim Z_4$.

Step 2: Prepare the sorting sequences $fx_1 \sim fx_4$ generated from chaotic variable sets; that are

$$fx1_{C,1} = sort(X1_{C,1}),\ fx2_{C,1} = sort(X2_{C,1})$$
$$fx3_{C,1} = sort(X3_{C,1}),\ fx4_{C,1} = sort(X4_{C,1}),$$

for C=1, 2, 3, …, mn,

where $sort(\bullet)$ is the sequencing index function. Accordingly, we can produce the sorting sequences $fy_1 \sim fy_4$, $fz_1 \sim fz_4$ respectively.

Step 3: Transfer the original image $A_{m \times n}$ to $A_{m*n \times 1}$, that is

$$a_{r_{C,1}} = T_1(\mathrm{A}_{r_{mxn}}),\ \text{for } C\text{=1, 2, 3, …, } mn$$

where A_r is the R-level matrix of original image, and $T_1(\bullet)$ is a transfer function.

Step 4: Conduct the shuffle function $sq(\bullet)$ on pixels of A_r for columns shuffling and indexing. As shown in Fig. 2, we have

$$Ae_1{}^{rb} = sq(A_{rb}, fx_1, fx_2, fx_3, fx_4)$$

Step 5: Shuffle pixels of the original image as follows:

$$Ae_1{}^{rb}{}_{fx1_{C,1},i_1} = A_{rb_{C,i_1}}, \qquad i_1 = 1,\ 2$$
$$Ae_1{}^{rb}{}_{fx2_{C,1},i_2} = A_{rb_{C,i_2}}, \qquad i_2 = 3,\ 4$$
$$Ae_1{}^{rb}{}_{fx3_{C,1},i_3} = A_{rb_{C,i_3}}, \qquad i_3 = 5,\ 6$$
$$Ae_1{}^{rb}{}_{fx4_{C,1},i_4} = A_{rb_{C,i_4}}, \qquad i_4 = 7,\ 8$$

where $A_{rb_{C,i}}$ is the Cth pixel, ith bit of the binary matrix of R level.

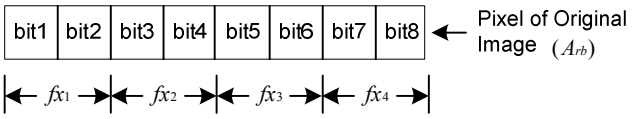

Figure 2. Column shuffling and indexing for each pixel in the same column

Step 6: Shuffle bits within each pixel, as shown in Fig. 3.

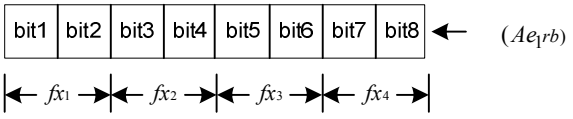

Figure 3. 2-bit shuffling and indexing within a pixel

Step 7: Repeat from Step 1 to Step 6 for the G-level and B-level matrices individually.

III. EXAMPLE

In this paper, a color image "Lena (256x256x3)" is adopted as an example for the proof of the high security of the proposed technique. Fig. 4 shows the original image and its RGB level spectrums. Fig. 5 exhibits the encrypted image and its RGB level spectrums by Zhu et al. [9].

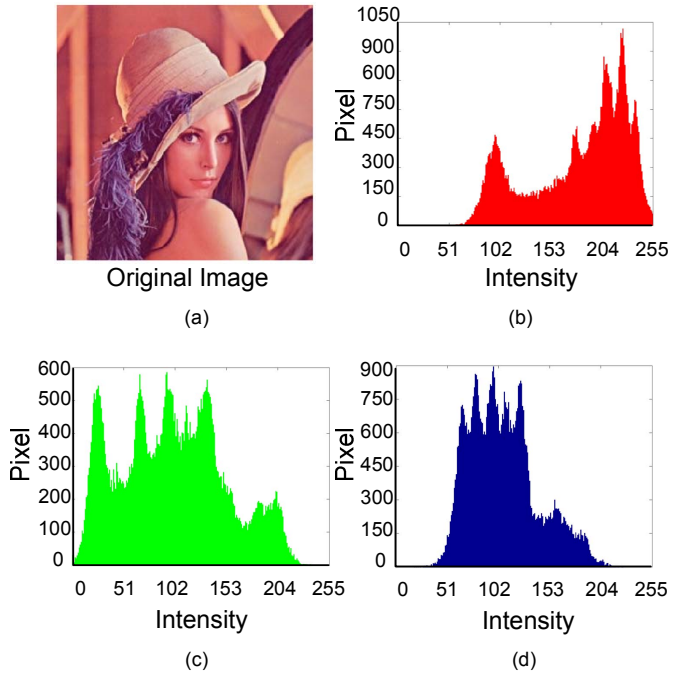

Figure 4. Lena and its RGB-level spectrums.

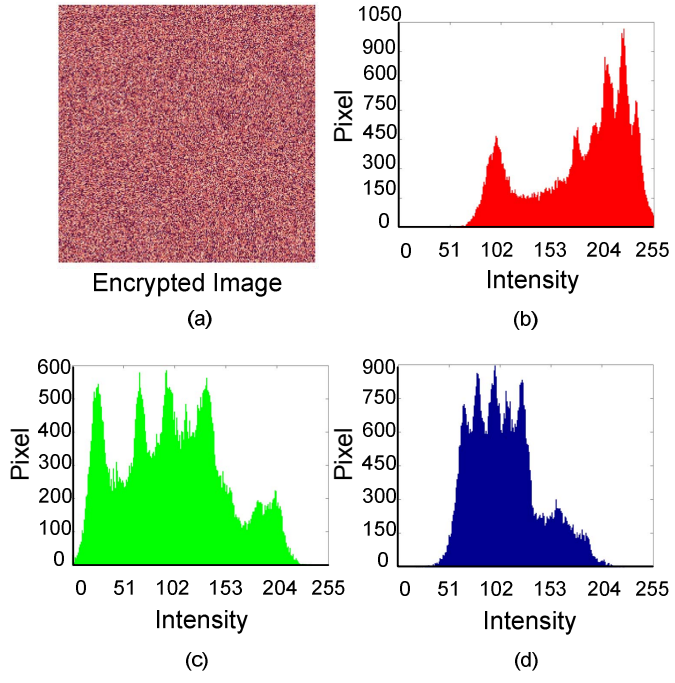

Figure 5. Encrypted Lena using Zhu's technique and its RGB-level spectrums.

Although the encrypted image has lost its outline completely, the RGB levels remain the same. Fig. 6 demonstrates the encrypted Lena using the proposed PCS technique. Not only the Lena's outline but also the RGB levels are changed dramatically.

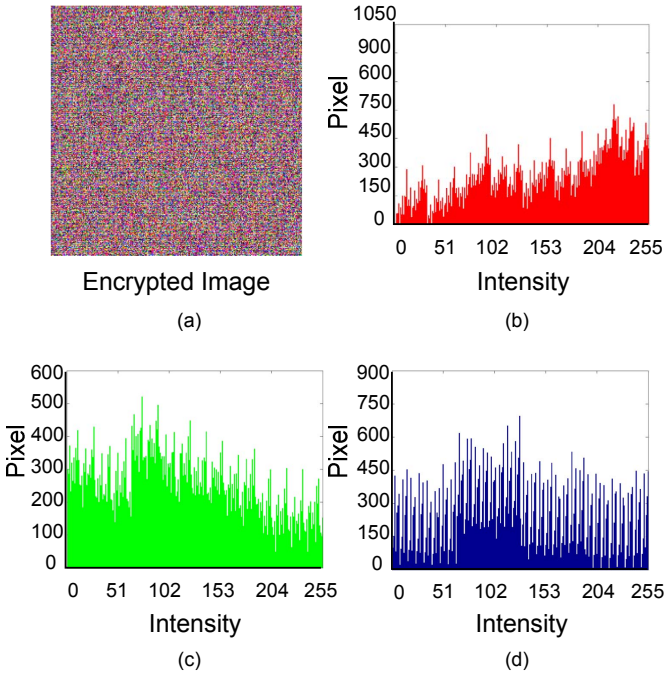

Figure 6. Encrypted Lena using the proposed PCS technique and its RGB-level spectrums.

IV. SECURITY ANALYSIS

Galton mentioned that two random variables x, y (x and y are grey-scale values of two adjacent pixels in the image) are defined as correlated if y changes as x changes, and changes with the same direction as x does. Correlation coefficient is the measure of extent and direction of linear combination of two random variables. If two variables are closely related with stronger association, the correlation coefficient is close to the value 1. On the other hand, if the coefficient is close to 0, two variables are not related and cannot predict each other. The coefficient r can be calculated with the following formula [17]:

$$r = \frac{n(\sum_{i=1}^{n} X_i Y_i) - (\sum_{i=1}^{n} X_i)(\sum_{i=1}^{n} Y_i)}{\sqrt{\left[n(\sum_{i=1}^{n} X_i^2) - (\sum_{i=1}^{n} X_i)^2\right]\left[n(\sum_{i=1}^{n} Y_i^2) - (\sum_{i=1}^{n} Y_i)^2\right]}}, \quad (5)$$

in which, $n(\sum_{i=1}^{n} X_i Y_i) - (\sum_{i=1}^{n} X_i)(\sum_{i=1}^{n} Y_i)$ is called sample covariance, $[n(\sum_{i=1}^{n} X_i^2) - (\sum_{i=1}^{n} X_i)^2]$ and $[n(\sum_{i=1}^{n} Y_i^2) - (\sum_{i=1}^{n} Y_i)^2]$ are the standard deviations of x sample and y sample. According to the prescription of FIPS PUB 140-1 [18], a set of

random numbers needs to satisfy these tests: monobit test, poker test, runs test, and long run test. Table 1 shows the test results and proves that the proposed PCS image encryption passes FIPS PUB 140-1 test.

TABLE I. TEST RESULTS FOR FIPS PUB 140-1.

Monobit Test	OK	$x: 9654 < X = 9995 < 10346$						
	OK	$y: 9654 < X = 9972 < 10346$						
	OK	$z: 9654 < X = 10067 < 10346$						
Poker Test	OK	$x: 1.03 < X = 12.7232 < 57.4$						
	OK	$y: 1.03 < X = 14.1440 < 57.4$						
	OK	$z: 1.03 < X = 13.4400 < 57.4$						
	Length of Run		1	2	3	4	5	6+
	Required Interval		2267 / 2733	1079 / 1421	502 / 748	223 / 402	90 / 223	90 / 223
Runs Test	1 OK	x	2490	1281	663	297	164	136
	OK	y	2462	1255	641	288	168	162
	OK	z	2476	1262	641	319	143	146
	0 OK	x	2535	1274	616	292	165	149
	OK	y	2483	1235	652	302	138	166
	OK	z	2483	1255	604	328	159	159
Long Run Test	1 OK	$x_k: 0$, $y_k: 0$, $z_k: 0$						
	0 OK	$x_k: 0$, $y_k: 0$, $z_k: 0$						

In order to evaluate the variations between the original and encrypted images, we conduct two additional tests: NPCR (Number of Pixel Change Rate) and UACI (Unified Average Changing Intensity). NPCR and UACI are performed as follows:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{N} \times 100\%, \tag{6}$$

$$UACI = \frac{1}{m \times n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \frac{|A(i,j) - A_H(i,j)|}{255} \times 100\%, \tag{7}$$

where $D(i,j) = \begin{cases} 0, & A(i,j) = A_H(i,j) \\ 1, & A(i,j) \neq A_H(i,j) \end{cases}$, A and A_H are RGB-level matrices of the original image and encrypted image respectively. As shown in table 2 and 3, the proposed method has great performances in r, NPCR and UACI tests. The correlation distribution of two horizontally adjacent pixels in the original image and that in the cipher image: the correlation coefficients are 0.9597 and 0.1257, respectively. Similar results for diagonal and vertical axes are obtained. The results reveal that the proposed method dramatically randomized the pixels and varied the grey level of each pixel. Also, the NPCR of PCS encryption being all close to unity are evident that the encryption image has a highly confidential security.

TABLE II. COMPARISONS OF THE CORRELATION COEFFICIENT r.

Axis	Original r	PCS encryption r	Zhu (PS) r
Horizontal	0.9597	0.1257	0.3913
Vertical	0.9792	0.0581	0.3955
Diagonal	0.9570	0.0504	0.3973

TABLE III. RESULTS OF NPCR AND UACI TESTS

Test Method / Image	NPCR (%)			UACI (%)		
	R	G	B	R	G	B
PCS Encryption	99.42	99.60	99.54	27.78	27.66	24.94
Zhu (PS)	99.26	99.45	99.13	21.41	23.42	15.08

V. CONCLUSIONS

This paper introduces a new pixel shuffle technique with multi chaotic systems for the image encryption. Since the chaotic system is highly sensitive to the initial values and parameters of chaotic values, meanwhile, has an enormous key space, the proposed method combined with 4 chaotic systems and pixel shuffle can fully banish the outlines of the original image, disorders the distributive characteristics of RGB levels, and dramatically decreases the probability of exhaustive attacks. We conduct FIPS PUB 140-1, the correlation coefficient r, NPCR, and UACI to test on the security analysis and the distribution of distinguished elements of variables for the encryption image. The adopted example shows the highly confidential encrypted image and demonstrates a good potential in the application of the digital-color image encryption.

REFERENCES

[1] G.R. Chen, Y.B. Mao and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps". Science Direct Chaos, Solitons and Fractals., Vol. 21, pp. 749-761, 2004.

[2] H.H. Nien, C.K. Huang , S.K. Changchien, H.W. Shieh, C.T. Chen, Y.Y. Tuan, " Digital color image encoding and decoding using a novel chaotic random generator", Chaos, Solitons and Fractals 32 (2007) 1070–1080.

[3] L. H. Zhang, X. F. Liao and X. B. Wang, "An image encryption approach based on chaotic maps", Science Direct Chaos, Solitons and Fractals., Vol. 24, pp. 759-765, 2005.

[4] T. Yang, C. W. Wu and L. O. Chua, "Cryptography based on chaotic systems", IEEE Transactions on Circuits and System-I: Fundamental Theory and Applications., Vol. 44, No. 5, pp. 469-472, May 1997.

[5] H. Zhang, X. F. Wang, Z. H. Li, D. H .Liu and Y. C. Lin, "A New Image Encryption Algorithm Based on Chaos System", IEEE International Conference on Robotics, Intelligent Systems and Signal Processing., pp. 778-782, Changsha, China October 2003.

[6] S. S. E. H. Elnashaie and M. E. Abasha, "On the chaotic behaviour of forced fluidized bed catalytic reactors", Elsevier Science Chaos, Solitons and Fractals., Vol. 5, No. 5, pp. 797-831, 1995.

[7] L. Kocarev, "Chaos-based cryptography: a brief overview", IEEE Transactions On Circuits and System-I: Fundamental Theory and Applications., pp. 6-21, 2001.

[8] W. Zhang and R. C. He, "An encryption and hiding algorithm based on Logistic chaotic sequences", China Academic Journal Electronic Publishing House, Journal of Lanzhou Jiaotong University (Natural Sciences)., Vol. 25, No. 4, pp. 80-82, Aug. 2006.

[9] C. X. Zhu, Z. G. Chen and W. W. Ouyang, “A new image encryption algorithm based on general Chen’s chaotic system”, China Academic Journal Electronic Publishing House, J. Cent. Southuniv (Science and Technology)., Vol. 37, No. 6, pp. 1142-1148, Dec. 2006.

[10] Z. J. Sun and Y. Chen, “A new image encryption algorithm based-on Lorenz system”, China Academic Journal Electronic Publishing House, Microprocessors., No. 3, pp. 49-52, June 2007.

[11] Z. J. Sun, Y. Chen, Y. X. Wang and X. F. Liao, “New image encryption algorithm based on Chua’s circuit”, China Academic Journal Electronic Publishing House, Computer Engineering and Design., Vol. 28, No. 14, pp. 3328-3330, July 2007.

[12] H. S. Kwok and Wallace K. S. Tang,"A fast encryption system based on chaotic maps", IEEE Chaos, Solitons and Fractals, Vol.32, pp.1518-1529, 2007

[13] L. O. Chua, “M. Komuro and L. T. Matsumoto, Double scroll family”, IEEE Trans Circ Syst., Vol. 33, pp. 1072-1118, 1986.

[14] E. N, “Lorenz, Deterministic nonperiodic flow”, J. Atmospheric Sci., Vol. 20, pp. 130-141, 1963.

[15] O. E. Rossler, “An equation for continuous chaos”, Physics Letters A., Vol. 57, pp. 397-398, 1976.

[16] G. Grassi and D. A. Miller, “Theory and Experimental Realization of Observer-Based Discrete-Time Hyperchaos Synchronization”, IEEE Transactions on Circuits and System-I: Fundamental Theory and Applications., Vol. 49, No. 3, pp. 373-378, Mar. 2002.

[17] A. G. Bluman,"Elementary statistics. 3rd ed", New York: McGraw-Hill, 1998.

[18] FIPS PUB 140-1, “Security requirement for cryptographic modules”, Federal Information Processing Standards Publication 1994.