Fast Adaptive Image Encryption using Chaos by Dynamic State Variables Selection

Daniel Roohbakhsh
Department of Electrical Engineering, Mashhad Branch Islamic Azad University, Mashhad, Iran
IT Specialist, Social Security Organization, Mashhad, Iran

Mahdi Yaghoobi
Department of Electrical Engineering, Mashhad Branch Islamic Azad University, Mashhad, Iran

ABSTRACT
A new image encryption scheme based on high dimensional compound chaotic systems is proposed in this paper. Common chaotic image encryption, will perform encryption algorithm on pixels one by one which make the process slower, in this paper we called logistic map to choose and encrypt appropriate number of pixels makes the algorithm swifter and much more reliable by enlarging the key length.

Keywords
Encrypting, Information, Security, Hyper chaos

1. INTRODUCTION
With the dramatic development of communication technologies, digital image application and exchange across Internet have become much more prevalent than the past. Cryptographic approaches are therefore critical for secure image transmission and storage over public networks. However, traditional encryption algorithms are typically designed for textual information and have been found not suitable for image encryption due to some intrinsic features of images such as high pixel correlation and redundancy [1]. Since 1990s, many researchers have noticed that the fundamental features of chaotic systems such as ergodicity, mixing property, unpredictability, sensitivity to initial conditions/system parameters, etc. can be considered analogous to some ideal cryptographic properties for image encryption [2,3]. a plain image is firstly shuffled by a two-dimensional area-preserving chaotic map with the purpose to erase the high correlation between adjacent pixels. Then pixel values are modified sequentially using pseudorandom key stream elements produced by a certain qualified chaotic map in the diffusion procedure. This architecture forms the basis of numerous chaos-based image crypto- systems proposed subsequently [5–24]. Meanwhile, recent cryptanalysis works have demonstrated that some chaos-based image cryptosystems are insecure against various attacks, and have been successfully broken [14–20]. The weaknesses in these insecure algorithms include insensitiveness to the changes of the plain image, weak secret keys, and the most serious one is that the key stream is completely depending on the secret key. That means identical key stream will be used to encrypt different plain images if the secret key remains unchanged. This property allows the attacker to launch known-plaintext attack [30–33,35] or chosen-plaintext attack [17,18,19,20,21] so as to retrieve the equivalent key stream elements. Therefore, to further enhance the security, the key stream elements extracted from the same secret key should better be distinct and related to the plain image [22] the present paper proposes a novel chaos-based image encryption scheme with a dynamic state variables selection mechanism (DSVSM). This cryptosystem can satisfy the security requirements suggested in [1,2] and well address the flaws existing in the cracked algorithms by employing innovations in four aspects. (1) Chaotic state variables used in our cryptosystem are generated from three-dimensional or hyper chaotic systems, and will be shared in permutation and diffusion procedures. Accordingly, a slight change in the secret key will not only affect the diffusion module but also influence the permutation procedure simultaneously. Besides, the chaotic state variables sharing mechanism can also significant advance the utilization efficiency of the chaotic map iteration. (2) The state variable allotted for each pixel's encryption is decided by DSVSM, which is plain pixel-related. When ciphering different plain images, distinct key streams will be produced both in the permutation and diffusion procedures, even though adopt the same secret key. The attacker cannot obtain useful information by encrypting some special images, as the resultant information is self-related to the chosen-images. This property ensures the resistance to known/chosen-plaintext attacks. (3) Pixel-swapping based image confusion approach is proposed as a replacement of the traditional permutation approaches. This confusion strategy can produce confusion and certain diffusion effects simultaneously in the permutation stage, so as to accelerate the overall diffusion effect of the cryptosystem. (4) Image diffusion in our scheme is implemented in snake-like mode. In coordination with the pixel-swapping based confusion strategy and DSVSM, the difference spreading effect produced in the confusion stage can be further scattered to the whole cipher image in the first round diffusion. The efficiency of the cryptosystem is therefore remarkably improved. Experiment results dem-onstrate that the proposed scheme has a high security level and satisfactory operation efficiency for practical secure image applications.

In this paper, a fast adaptive image encryption method based on chaos we'll discuss. MATLAB simulation has been performed, and the test generally uses in image processing on the proposed encryption algorithm studied. The proposed method consists of three main parts, for the 1st step we employ an image total shuffling matrix to shuffle the positions of image pixels and then uses logistic map chooses appropriate number of pixels which is equal to the number of pixels exists in one row. At last using hyper-chaotic Chen system to confuse the relationship between the plain-image and the cipher-image. In advance, we will discuss a little about The architecture of typical chaos-based image cryptosystem and the Arnold mapping. And, the chaotic Chen system introduces. Subsequently the proposed method and the simulation results demonstrate.

2. THE ARCHITECTURE OF TYPICAL CHAOS-BASED IMAGE CRYPTOSYSTEMS

The architecture of typical chaos-based image cryptosystems is shown in Fig. 1. There are two stages in the cryptosystems of this kind, namely, the permutation stage and diffusion stage.

In the permutation stage, image pixels are generally shuffled by a two-dimensional area-preserving chaotic map, without any modification to their values. Traditionally, three types of chaotic maps, Arnold cat map, standard map and baker map are employed, and their discretized versions are given by Eq. (1) , respectively.

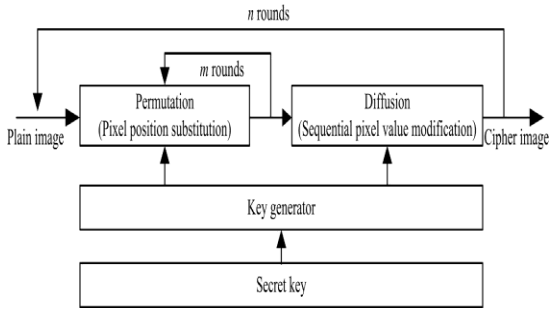

Fig1. The architecture of typical chaos-based image cryptosystem

In these equations, N is the width or height of the square image, (p, q) and K represent the control parameters of these maps, respectively. All pixels are scanned sequentially from upper-left corner to lower-right corner, and then the confused image is produced. Now we can infer from Eq. (1) that the confused image totally depends on the control parameters of the permutation maps, the difference between plain images will be moved to a new position rather than spread out in the permutation stage. In other words, there is no diffusion effect when using traditional permutation techniques. So the duty of image diffusion
entirely relies on the diffusion module, which is the highest cost of the cryptosystem. Therefore, it is of great significance to investigate a novel permutation approach that can simultaneously produce certain diffusion effect so as to accelerate
the diffusion performance of the cryptosystem. Besides, when using the same secret key, distinct key streams should better be produced for ciphering different plain images so as to effectively resist the known/chosen-plaintext attacks [20].

3. ARNOLD MAPPING

In 1960, Russian mathematician Vladimir Arnold used the most general two-dimensional chaotic map for an image [9]; the name was Arnold Cat Map. If a matrix N * N, pixel with coordinates (x, y), we wrote to Arnold in equation (1) will be:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = A \begin{bmatrix} x \\ y \end{bmatrix} (\text{modN}) = \begin{bmatrix} I & t \\ q & tq+I \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} (\text{modN}) \qquad (1)$$

Which q and t are the control parameters of the matrix A, and should be chosen so that the determinant of the matrix A is equal to one. These two parameters will be part of the encryption key. Fig.3 shows the falling cat image by mapping Arnold. Mod is the remainder divided by n, for each of the components. This is because the values obtained from the image matrix size are not exceeded. Pixels of an image map Arnold moved, so the image cannot be understood, if it is sufficient to repeat the original image will be generated again.

4. HYPER CHAOS CHEN DYNAMIC

In this section, DSVSM was given out to improve the security and efficiency of image cryptosystems. This mechanism is proposed for dynamically assigning chaotic state variables for encrypting each pixel, and can collaborate with any three-dimensional or hyper chaotic systems that are used for key stream generation. In this paper, the Chen's chaotic system is employed as an example for illustrating DSVSM clearly, as described by Eq. (2).

$$\begin{aligned} \dot{X}_1 &= a(x_2 - x_1) \\ \dot{X}_2 &= -dx_1 + cx_2 - x_1 - x_4 \\ \dot{X}_3 &= x_1 x_2 - bx_3 \\ \dot{X}_4 &= x_1 + k \end{aligned} \qquad (2)$$

Where $x_i (i = 1,2,3,4)$ the states and a, b, c, d are positive constant parameters of the system and -0.7<k<0.7 [10].

If the parameters of equation (2) as: $a = 36, b = 3, c = 28, d = -16$, behavior of the system (2) as shown in Fig.4 will be.

5. THE PROPOSED METHOD

With each of the Chen's chaotic map iteration, three state variables will be generated, denoted as X, Y and Z, respectively. In DSVSM, the chaotic state variables that will be used for key stream element generation are selected according to the previous processed pixel. The current processing image (plain image in the confusion phase or the confused image in the diffusion stage) with M x N pixels are viewed as a one-dimensional array, pixels are represented by P = {P(0), P(i), ...,P(M x N - i)} from the upper-left corner to the lower-right corner. In order to demonstrate the DSVSM properly, the following definitions have to be declared firstly

1) The state variable used for each pixel's encryption will be selected from state variables combination, which consists of a state value of x_1,x_2 and x_3. assume that Assume that $\{X1_i, X2_j, X3_k\}$ is the current state variable combination, where $X1_i$,$X2_j$, and $X3_k$ are the states of x_1,x_2 and x_3 in ith, Jth and kth iteration, respectively

2) Calculate index according to Eq.(3)

$$\begin{cases} index = \text{mod}((x_1 + x_2 + x_3 + x_4), 4) \\ index = index + 1 \end{cases} \qquad (3)$$

Now we can come to the following intrinsic features of DSVSM from the abovementioned procedures.

1. Iteration efficiency. In DSVSM, the chaotic map is iterated when necessary. The iteration count is not necessarily equal to the pixel number of the plain image, and it depends on the distribution of the pixel values. In oursimulation of ciphering Cat, little more than 1/3 * (M * N) times iteration are required in one overall encryption round. The simulation results and detailed analyzes will be reported in Section 6.
2. Choosing pixels is based on Logistic map theory, this algorithm chooses number of pixels equal to one row.

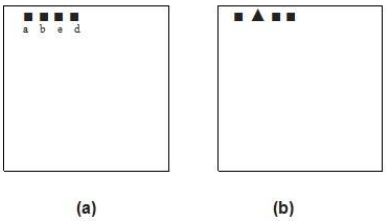

Fig.2 (a) Plain Image Pixels. (b) pixel chooses by logestic map theory

Dynamic property and diffusion effect. At this stage, the pixels in disarray, and their values change using hyper chaotic Chen encryption. First, one of the four variables produced by Chen is set aside. The system repeats the number of all pixels in the image. Index variable that will be excluded from the equation (3) becomes apparent.

3.

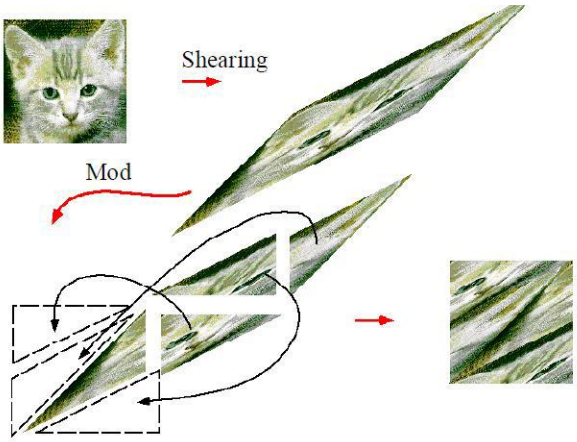

Fig.3 Arnold mapping process

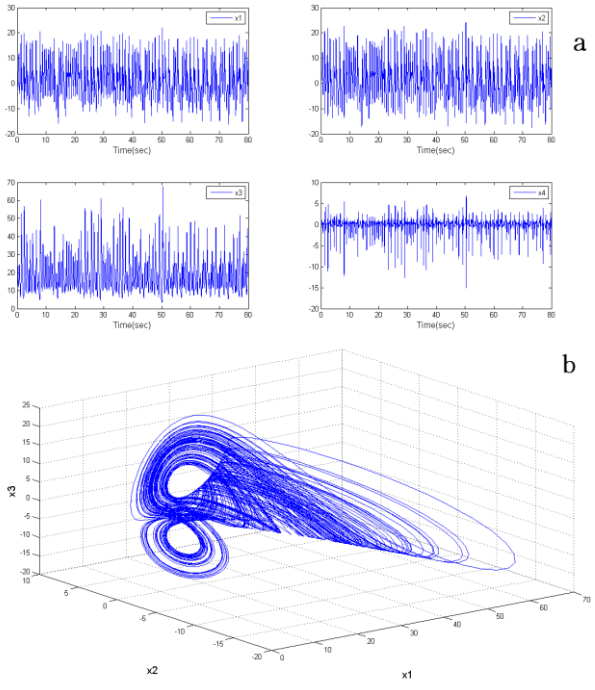

Fig.4 a: State variables and b: Phase plane trajectory of hyper Chen system

For all pixels, all $i = 1, 2, 3, 4$ are calculated, and the remainder divided by 4, the index variable is stored.

In the second phase, the remaining three variables from the previous stage, respectively, with the colors red, green and blue pixels are all cluttered image according to equation (4).

$$CR_i = R_i \oplus (x_1)_2$$
$$CG_i = G_i \oplus (x_2)_2 \qquad (4)$$
$$CB_i = B_i \oplus (x_3)_2$$

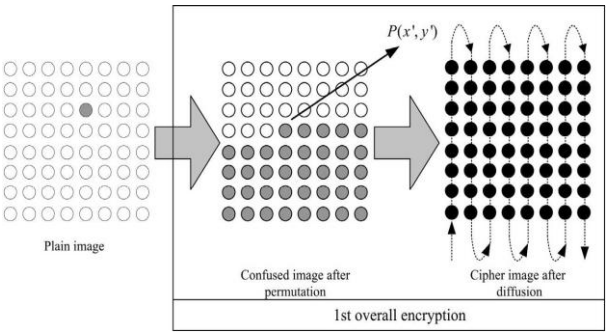

Fig5. 1st overall encryption

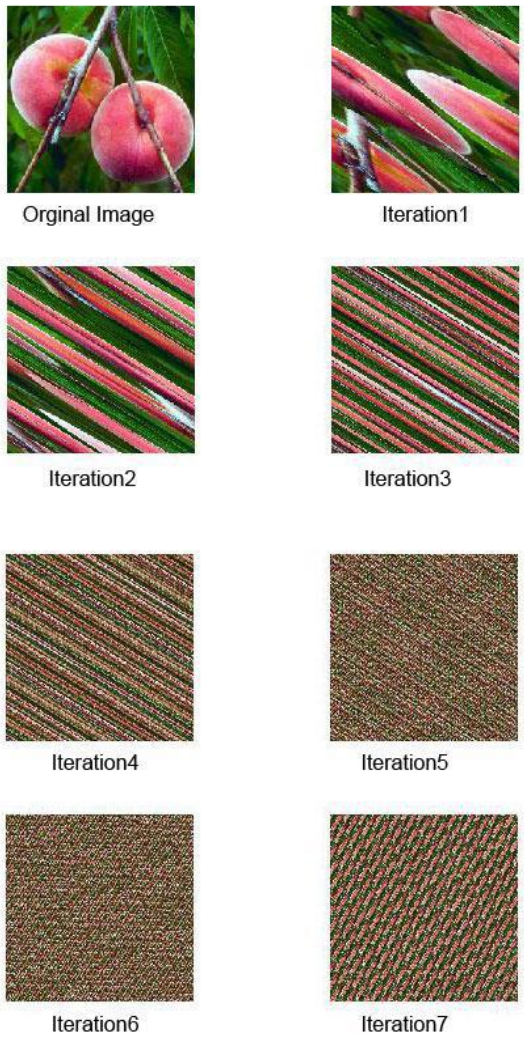

Fig.6 Arnold mapping the image on fruit

If the cipher image histogram monotony (if the difference of two levels is less than determined standard deviation) achieved, the encrypted image along with a digit (demonstrates how many intervals has been used) give back to the user. Otherwise the algorithm repeat again until the conditions are satisfied.

5.1 Decryption

The decryption of the proposed method discusses. The algorithm to decrypt the cipher image, Chen the basic values of the parameters t, q, and number of repetitions of the Arnold map is available.

Now we should all go back to decryption of process to be reversed. The initial value x_i and system parameters pulse the digit which demonstrates the number of intervals are the key, so x_i is in the stage production. Then, according to equation (3), we calculate the index is excluded. Finally, the color of each pixel of the image is encrypted with xi according to equation (4) is XOR.

Now, at this stage, the first step is reached. Now, at this stage, the first step is reached. The seven steps, we can apply the inverse Mapping Arnold on the image to the original image is reached (Note: The number of repetitions Arnold Mapping is part of the key). The inverse Arnold map to the original image in the form of equation (5) obtained.

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = A \begin{bmatrix} x \\ y \end{bmatrix} (\text{modN}) = \begin{bmatrix} tq+I & -t \\ -q & I \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} (\text{modN}) \quad (5)$$

6. EXPERIMENTAL RESULTS

In this section, experimental results obtained using MATLAB software will be described. Performance of the proposed method is evaluated by tests will be common in image processing.

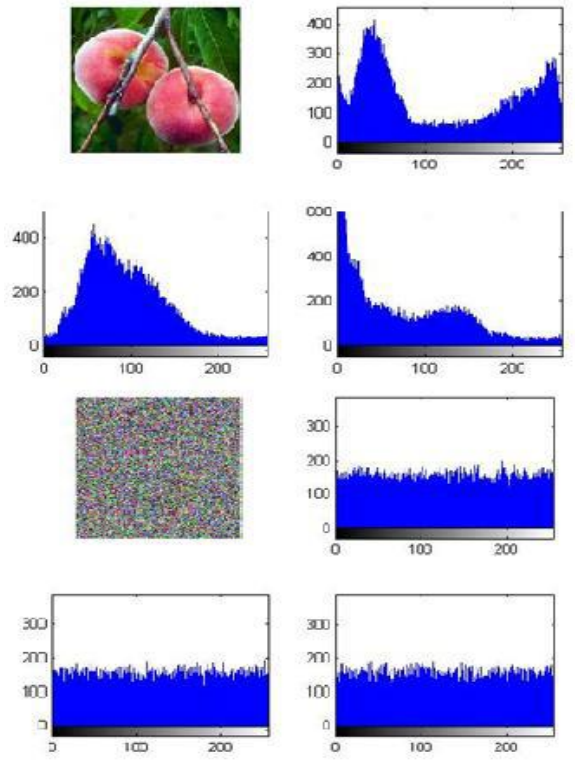

Fig.7 histogram of the original image and encrypted image

6.1 Histogram analysis

Histogram, show the number of pixels in each gray level for an image [11]. By comparing the encrypted image and the original image, it can be seen that the proposed method of image histogram encoded by appropriate uniformity. That is to say, the probability calculated from the histogram of the original image by the attackers will be very weak. To better understand, see Fig.4

6.2 Sensitivity to the wrong key

Sensitivity to key mistake in this article only for Chen system parameters is studied. If you enter the correct parameters are expected in other words, the image of Arnold Mapping get cluttered. Now, beginning with the correct key, and then with little change in the parameters, trying to get the image Mapping. In other words, this test shows that the chaotic system is sensitive to the initial conditions. Hyper Chen system with the initial conditions $x_0 = [12 \quad 8 \quad 25 \quad 4]^T$, and with a little different initial conditions $x_0 = [12 \quad 8.000001 \quad 25 \quad 4]^T$. Table 1 illustrates results.

6.3 Key space analysis

Decryption key of the proposed method are: $(t, q, it, x_{1,2,3,4}, \text{a}, \text{b}, \text{c}, \text{d}, \text{k})$, that the values as : (1,1,7,12,8,25,4,36,3,28,-16,0.4) respectively, Calculating the size of the key binary code (00101100), and the 8 bits allocated to each of them. This means that there are 2^{184} possibilities for the permutation. Desired key length to resist fierce attack by guessing is 70 bits [13]. Hence, the key will be achieved by the proposed method highly desirable.

6.4 The proposed method of resistance against attacks

In fact, a frenzied attack, guess the key through the various permutations. On the other hand, specific encryption mechanisms and the key are needed. Otherwise attack exposure cannot be applied [12, 15]. Due to the hyper chaotic Chen system and the stage of bollix, key length is long. So, it is almost impossible to guess the key is to have a great time. Attack Rhouma and Belghith, one of the most interesting episodes introduced to deal with the chaos-based encryption. However, when used in the encryption mechanism is available. Otherwise, image access to, image encrypted by not possible [16]. The solution to this type of attack is that for each image, different values of the parameters and initial conditions in hyper chaos, is available.

7. CONCLUSION

In this paper, a color image encryption method based on chaos was introduced. First, the picture becomes cluttered Arnold mapping, then the image obtained with the combination of by hyper Chen chaos. The results of the simulation are: 1. simple structure 2. Sensitivity of hyper chaos 3. To implement bollix image obtained 4-length key. It was demonstrated that the proposed method can resist the attack of the crazy.

8. REFERENCE

[1] Geol, Amnesh, and Nidhi Chandra, "A Technique for Image Encryption with Combination of Pixel Rearrangement Scheme Based On Sorting Group-Wise Of RGB Values and Explosive Inter-Pixel Displacement", pp.16-22, 2012

[2] J.C. Yen, J.I. Guo, "A New Chaotic Key-Based Design for Image Encryption and Decryption", Proceeding IEEE

International Conference on Circuits and Systems,vol.4, pp. 49-52, 2000

[3] R.Valerij, "Symmetry of the modified Mandelbrot set", Pi in the Sky(9):20–1.2005

[4] Narendra Singh, Aloka, "Optical image encryption using fractional Fourier transform and chaos", Optics and Lasers in Engineering.Vol 46, Issue 2, Pages 117–123.February 2008

[5] Kadir, Abdurahman, Wang, "A chaotic image encryption algorithm based on perceptron model", Nonlinear Dynamics, Vol. 62, pp. 615-623, 2011.

[6] Liao X, Chen G, Wang Y, "A new chaos-based fast image encryption algorithm", Applied Soft Computing Journal, Vol.11, PP. 514-522,

[7] Alireza Jolfaei, Abdolrasoul Mirghadri, "Image Encryption Using Chaos and Block Cipher", Computer and Information, Vol 4, No 1, pp 172-179, 2011.

[8] Tiegang Gao, Zengqiang Chen, ""A new image encryption algorithm based on hyper-chaos", Physics Letters A ,Vol.372, Issue 4, PP 394–400, 21 January 2008

[9] R Jun, P., J. Shangzhu, and L. Yongguo," Design and Analysis of an Image Encryption Scheme Based on Chaotic Maps", International Conference ICICTA, pp. 1115-1118, 2010

[10] Li, Ling, Weinan Wang, and Jinjie Li, "A Novel Image Encryption Algorithm Based on High-dimensional Compound Chaotic Systems", International Conference on Multimedia Technology (ICMT), pp.5715-5718, July 2011.

[11] Jolfaei, Alireza, and Abdolrasoul mirghadri, "An Image Encryption Approach Using Chaos and Stream Cipher", Journal of Theoretical and Applied Information Technology, pp120-122, 2010

[12] S, Rakesh, Ajitkumar A Kaller, Shadakshari B C, and Annappa B, "Image Encryption using Block Based Uniform Scrambling and Chaotic Logistic Mapping", International Journal on Cryptography and Information Security, (IJCIS),Vol.2, No.1, pp 49-57, 2012.

[13] Gao, Tiegang, Qiaolun Gu, Zengqiang Chen, and Renhong Cheng, "An Improved Image Encryption Algorithm Based on Hyper-chaos", Fourth International Conference on Innovative Computing Information and Control (ICICIC), pp.1281-1284, 2009

[14] Prasad, Manjunath, and K.L.Sudha, "Chaos Image Encryption using Pixel shuffling.",pp.170-177, 2011

[15] Bruce Schneier, "Applied Cryptography, Second Edition: Protocols, Algorthms, and Source Code in C", John Wiley & Sons, Inc, Publication Date 1996

[16] R, Rhouma, and Belghith S "Cryptanalysis of a new image Encryption Based on hyper chaos", Physics letters pp.5973-5978, 2008

[17] Rhouma R, Solak E, Belghith S. Cryptanalysis of a new substitutiondiffusion based image cipher. Commun Nonlinear Sci Numer Simul Co—2010;15(7):1887-92

[18] Rhouma R, Solak E, Belghith S. Cryptanalysis of a new substitutiondiffusion based image cipher. Commun Nonlinear Sci Numer Simul Co—2010;15(7):1887-92

[19] Li C, Li S, Lo K. Breaking a modified substitution diffusion image cipher based on chaotic standard and logistic maps. Commun Nonlinear Sci Numer Tjff] Simul 2011;16(2):837-43

[20] Li C, Li MAS, Nunez J, Alvarez GCG. On the security defects of an image encryption scheme. Image Vis Comput 2009;27(9):1371-82.

[21] Cokal C, Solak E. Cryptanalysis of a chaos-based image encryption algorithm. Phys Lett A 2009;373(15):1357-60.