A Systematic Approach for Image Encryption Using Chaotic 2D Logistic Map Using MATLAB

Harshitha S
Electronics and communication
Rajarajeswari college of Engineering
Bangalore , India

Ranjan D
Electronics and communication
Rajarajeswari college of Engineering
Bangalore, India

Madhushree B J
Electronics and communication
Rajarajeswari college of Engineering
Bangalore, India

Ashwini L
Electronics and communication
Rajarajeswari college of Engineering
Bangalore, India

Mrs. Chaithanya S
Assistant Professor, Department of ECE
Rajarajeswari college of Engineering
Bangalore, India

***Abstract*— Chaos maps and chaotic systems have been proved to be useful and effective for cryptography. In this paper, the two-dimensional logistic map with complicated basin structures and attractors are first used for image encryption. The proposed method adopts the classic framework of the permutation-substitution network in cryptography and thus ensures both confusion and diffusion properties for a secure cipher. The proposed method is able to encrypt an intelligible image into random-like from the statistical point of view and the human visual system point of view. Extensive simulation results using test images from the USC SIPI image database demonstrate the effectiveness and robustness of the proposed method. Security analysis results of using both the conventional and the most recent tests show that the encryption quality of the proposed method reaches or excels the current state of the arts. Similar encryption ideas can be applied to digital data in other formats, e.g. digital audio and video.**

Keywords*— *Image Encryption, Two Dimensional Logistic Map, Key Schedule, Sequence Generator, 2D Logistic Permutation, 2D Logistic Diffusion, 2D Logistic Transposition Introduction.

I. INTRODUCTION

Image security attracts extensive concerns from the public and the government in recent years. Unexpected exposure of private photos and divulged military and governmental classified images emphasizes the importance of the image security again and again. With the fast development of digital storages, computers and the world wide network, a digital image can be easily copied to mobile storage or transferred to the other side of the world within a second. However, such convenience could also be used by malicious/unauthorized users to rapidly spread the image information that it may cause uncountable losses for the owner(s) of images.

Among various image security technologies, the image encryption is a straight-forward one with concerns in encrypting an image to an unrecognized and unintelligent one, where the source image and the encrypted image are called plaintext image and ciphertext image, respectively. One common approach of image encryption is to treat the image data the same as the one-dimensional binary bit stream, which extracts a plaintext image bit by bit and then encrypts this binary bit stream. The advantage of this approach is able to encrypt a digital image using the existing block/stream ciphers designed originally for binary bit streams. These ciphers include the well known ciphers/standards: the Digital Encryption Standard (DES), the Advanced Encryption Standard (AES), the TwoFish cipher and the BlowFish cipher.

In the research of image encryption algorithms/ciphers, efforts are found in two groups: optical image encryption, and digital image encryption. The former group adopts optics or optical instruments to build physical systems for image encryption, which commonly relies on optics to randomize frequency components in an image. The later 2 group commonly takes advantages of a digital image and encrypts it either by an encryption algorithm in the form of software or a physical electronic device in the form of hardware.

Among various digital image encryption methods, the chaos-based image encryption method is a family of methods that are believed good for encryption purposes. Because a chaotic system has high sensitivities to its initial values, high sensitivities to its parameter(s), the mixing property and the ergodicity, it is considered as a good candidate for cryptography.

In this paper, we adopt the two-dimensional Logistic map for image encryption in the first time with careful considerations for the diffusion and confusion properties and possible attacks as well. This chaotic map is researched with respect to its

mathematical properties and physical dynamics previously and it has been showed that this coupled logistic map for two dimensions has more complicated chaotic behaviors like basin structures and attractors. We utilize this more complicated chaotic map to generate pseudo random sequences where we propose a key schedule algorithm to translate a binary encryption key to initial values and parameters used in the 2D logistic map. We develop an image encryption algorithm using these pseudo-random sequences under the framework of the permutation- substitution network, which is proven to be very effective to provide both confusion and diffusion properties in stream ciphers and block ciphers.

II. THE TWO-DIMENSIONAL LOGISTIC MAP

The two-dimensional logistic map is researched for its complicated behaviors of the evolution of basins and attractors. It has more complex chaotic behaviors than one-dimensional Logistic map.

Mathematically, this 2D logistic map can be discretely defined as Equation (1), where r is the system parameter and (x_i, y_i) is the pair-wise point at the i^{th} iteration.

$$\text{2D Logistic map:} \begin{cases} x_{i+1} = \mathrm{r}(3y_i + 1)x_i(1 - x_i) \\ y_{i+1} = \mathrm{r}(3x_i + 1)y_i(1 - y_i) \end{cases} \quad (1)$$

III. IMAGE ENCRYPTION USING THE 2D LOGISTIC MAP

Although the 2D logistic map has various behaviors according to different system parameters, in the paper we concentrate on the parameter interval r ∈ [1.1, 1.19], where the system is chaotic.

A. KEY SCHEDULE AND 2D LOGISTIC SEQUENCE GENERATOR

We define our encryption key K as a 256-bit string composed of five parts x_0, y_0, r, T, and $A_1 \ldots A_8$, where (x_0, y_0) and r are the initial value and the parameter in the 2D logistic map defined in Equation (1), and A and T are the parameters of the linear congruential generator. Specifically speaking, we calculate a fraction value v from a 52-bit string using the IEEE 754 double-precision binary floating-point format for the fraction part as shown in Eq. (2)

$$v = \sum_{i=1}^{52} b_{-i} 2^{-i} \quad (2)$$

Consequently, x_0, y_0, r and T, can be found. For coefficients $A_1 \ldots A_8$, each of which is composed of 6-bit string {b0, b1… b5}, we translate these 6-bit strings to integers and obtain the required coefficients.

x_0	y_0	r	T	$A_1 \cdots A_8$
52 Bits	52 Bits	52 Bits	52 Bits	48 Bits

IV. METHODOLOGY

Here, in this paper we mainly proceed with three methods: 2D Logistic Permutation, 2D Logistic Diffusion, 2D Logistic Transposition. In every method the image will get ciphered and it provides more security for the image.

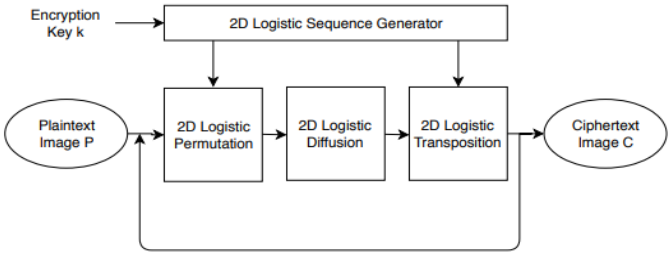

Fig. 1: The flowchart of image encryption using the 2D logistic map.

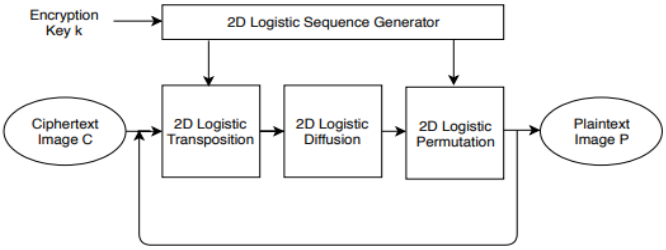

Fig. 2: The flowchart of image decryption using the 2D logistic map.

B. 2D LOGISTIC PERMUTATION

Without loss of generality, assume the size of the plaintext image P is $M \times N$. Therefore, the total number of pixels in P is MN. Consider the initial value used in a round is (x_0, y_0) .A sequence of pair-wise x and y of length MN (exclude the initial value) can be generated via the 2D logistic map using Equation (1). Let X_{seq} *and* Y_{seq} be the x coordinate sequence and the y coordinate sequence of the 2D logistic map, respectively, as in Equation (3).

$$\begin{cases} \mathrm{X_{seq}} = \{\mathrm{x_1}, \mathrm{x_2}, \ldots, \mathrm{x_{MN}}\} \\ \mathrm{Y_{seq}} = \{\mathrm{y_1}, \mathrm{y_2}, \ldots, \mathrm{y_{MN}}\} \end{cases} \quad (3)$$

Rearrange elements of X_{seq} *and* Y_{seq} whose number is M×N in the matrix form and obtain M×N matrices X and Y, respectively. In the 2D logistic permutation we perform shuffling in row wise and column wise. In this stage we obtain cipher image which will be further encrypted in the following method.

C. 2D LOGISTIC DIFFUSION

In order to achieve good diffusion properties, we apply the logistic diffusion for every S×S image block P_b within the plaintext image P over the finite field *Gf( )* as shown in Equation (4), where S is the block size variable determined by the plaintext image format, and Ld is the maximum distance separation matrix found from 4×4 random permutation matrices defined in Equation (5).

$$\begin{aligned} C_b &= (L_d . P_b . L_d) 2^8 \\ P_b &= (L_d^{-1} . C_b . L_d^{-1}) 2^8 \end{aligned} \quad (4)$$

$$L_d = \begin{bmatrix} 4 & 2 & 1 & 3 \\ 1 & 3 & 4 & 2 \\ 2 & 4 & 3 & 1 \\ 3 & 1 & 2 & 4 \end{bmatrix} \text{ and } \left(L_d{}^{-1}\right) 2^8 = \begin{bmatrix} 71 & 216 & 173 & 117 \\ 173 & 117 & 71 & 216 \\ 216 & 71 & 117 & 173 \\ 117 & 173 & 216 & 71 \end{bmatrix} \quad (5)$$

D. 2D LOGISTIC TRANSPOSITION

Unlike diffusion stages used in conventional diffusion-permutation network, the 2Dlogistic transposition process changes pixels values with respect to the reference image I, which is dependent on the logistic sequence generated from the previous stage.

First X and Y which the matrix version of $X_{seq} and\ Y_{seq}$ by arranging a sequence elements in a matrix, are added together to be Z via Equation (6).

$$Z = X+Y \quad (6)$$

Furthermore, each 4×4 block B in Z is then translated to a (pseudo) random integer matrix using the block function *f(B)* as shown in Equation (7), where B is a 4 × 4 block, and the sub function $g_N(.), g_R(.), g_S(.), g_D(.)$ are defined in Equation (8)-(11). The function *T (d)* truncates a decimal d from the 9th digit to 16th digit to form an integer, for example if b = 0.12345678901234567890, then T (d) = 90123456. The symbol F denotes the number of allowed intensity scales of the plaintext image format. In other words, F = 2 if the plaintext image P is a binary image and F = 256 if P is an 8-bit gray image.

$$I = f(B) = \begin{bmatrix} g_N(B_{1,1}) & g_R(B_{1,2}) & g_S(B_{1,3}) & g_D(B_{1,4}) \\ g_R(B_{2,1}) & g_S(B_{2,2}) & g_D(B_{2,3}) & g_N(B_{2,4}) \\ g_S(B_{3,1}) & g_D(B_{3,2}) & g_N(B_{3,3}) & g_R(B_{3,4}) \\ g_D(B_{4,1}) & g_N(B_{4,2}) & g_R(B_{4,3}) & g_S(B_{4,4}) \end{bmatrix} \quad (7)$$

$$g_N(d) = T(d)\ mod\ F \quad (8)$$

$$g_R(d) = \left[T\left(\sqrt{d}\right)\right] mod\ F \quad (9)$$

$$g_S(d) = T(d^2)\ mod\ F \quad (10)$$

$$g_D(d) = T(2d)\ mod\ F \quad (11)$$

When function *f(.)* is applied to all 4×4 block within the 2D logistic map associated random like matrix Z without overlapping, then a random integer matrix I is obtained, where each 4 × 4 block in I is actually mapped from a corresponding 4 × 4 block in Z with the function *f(.)* defined in Equation (7).

Finally, the 2D logistic transposition is achieved by shifting the each pixel in the plaintext image with the specified amount of the random integer image *I* over the integer space [0 , *F−1*] , i.e. the ciphertext image of 2D logistic map C is defined as Equation (12), where F is the number of allowed intensity scales of the plaintext image. For example, F = 256 for a 8-bit grayscale image.

$$C = (P+I) \bmod F \quad (12)$$

Similarly, we can use Equation (13) for decryption.

$$P = (C-I) \bmod F \quad (13)$$

V. RESULT

Thus the image will be more secured by undergoing encryption for so many times. The decryption process is obtained in the reverse process of the encryption.

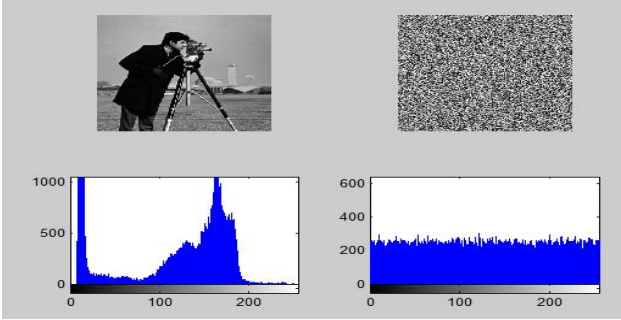

Fig 3: This figure shows the Plain image and encrypted image with their histogram respectively

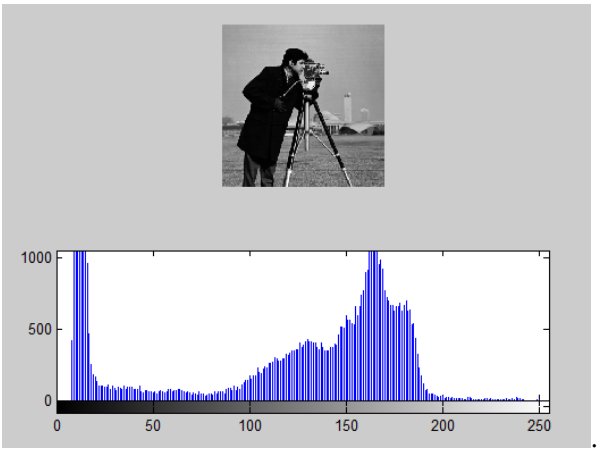

Fig 4: This figure shows the Decrypted image with its histogram.

VI. CONCLUSION

In this paper, the two-dimensional logistic map is used for image encryption for the first time. Unlike the conventional one-dimensional logistic map, the two-dimensional logistic map has chaotic behaviors in an additional dimension includes a time asymmetric feedback for two dimensions with both basins and attractors in evolution. Consequently, the pseudo number sequences generated from the two-dimensional logistic map for image encryption are more random-like and complicated.

The proposed image encryption method adopts a permutation-substitution network structure with good confusion and diffusion properties, where each cipher round includes the three encryption stages: 2D Logistic Permutation, 2D Logistic Diffusion and 2D Logistic Transposition, each of which is an image cipher. In such a way, the proposed image encryption method is able to resist many existing cryptography attack.

Extensive experimental results show that the proposed image encryption method is able to encrypt intelligible plaintext images to random-like ciphertext images. In other words, a ciphertext image obtained from the proposed image cipher is

unrecognizable and unintelligible and its statistical properties are very similar to those of a random image.

REFERENCES

1. M. Yang, N. Bourbakis, and S. Li,\Data-image-video encryption," in IEEE Potentials 23(3), 28{34 (2004).
2. D. R. Stinson, Cryptography: theory and practice, Chapman and Hall CRC (2006).
3. FIPS PUB 46, Data Encryption Standard (1977).
4. FIPS PUB 197, Avdanced Encryption Standard (2001).
5. B. Schneier, The two_sh encryption algorithm: a 128-bit block cipher, J. Wiley (1999).
6. R. Anderson and B. Schneier, \Description of a new variable-length key, 64-bit block cipher (Blowsh)," in Lecture Notes in Computer Science, 191{204, Springer Berlin Heidelberg (1994).
7. Y. Wu, J. P. Noonan, and S. Agaian, \Shannon entropy based randomness measurement and test for image encryption," in CoRR abs/1103.5520 (2011).
8. B. Hennelly, and J. T. Sheridan, \Optical image encryption by random shifting in fractional fourier domains," in Opt. Lett. 28, 269{271 (2003).
9. W. Chen, and X. Chen, \Space-based optical image encryption,"in Opt. Express 18, 27095{ 27104 (2010).
10. B. Zhu, S. Liu, and Q. Ran, \Optical image encryption based on multifractional fourier trans-forms," in Opt. lett. 25(16), 1159{1161 (2000).
11. W. Chen and X. Chen, \Optical image encryption using multilevel arnold transform and non-interferometric imaging," in Optical Engineering 50(11), 117001 (2011).
12. X. Shi and D. Zhao, \Color image hiding based on the phase retrieval technique and Arnold transform," in Appl. Opt. 50, 2134{2139 (2011).
13. G. Ye, \Image scrambling encryption algorithm of pixel bit based on chaos map," in Pattern Recognition Letter 31, 347{354 (2010)