A New Combined Chaotic System for Image Encryption

Tong Zhang
Department of computer and information science
Faculty of Science and Technology
University of Macau
Macau, China
ztony86@gmail.com

Yicong Zhou
Department of computer and information science
Faculty of Science and Technology
University of Macau
Macau, China
yicongzhou@umac.mo

C.L. Philip Chen, IEEE Fellow
Department of computer and information science
Faculty of Science and Technology
University of Macau
Macau, China
philipchen@umac.mo

***Abstract*—Due to the random-like property and high sensitivity for initial values and parameters, chaotic systems are usually proposed as a solution to image encryption. In this study, the authors introduce a new chaotic system called LS chaotic system using the Logistic map and Sine map. It shows excellent chaotic behaviors. Applying the new chaotic system, a novel image encryption algorithm is also introduced based on the substitution and permutation network structure. The experimental results show that the proposed algorithm's excellent performance in image encryption. It can also be applied to provide security for other multimedia.**

Keywords-chaotic system; LS chaotic system; image encryption; encryption key

I. INTRODUCTION

Owing to the development of communication technology, it is so easy to get images through internet. Meanwhile, it also gives an attacker or an illegal user an opportunity. Many applications demand providing security to digital images and videos, including medical image systems, cable TVs, and personal online photograph albums. Encryption techniques have been developed during the last decade [1-3].

Chaotic theory has been used in many research areas, such as: physics, economics, biology, and philosophy [4]. It has many useful and practical applications due to its important properties, including the sensitivity to the initial conditions and system parameters, the density of all periodic points and topology transitivity [5]. These are satisfied with the requirements of cryptography. Therefore, chaotic system based image encryption algorithms have proposed in the past few years [6, 7]. Unfortunately, it is possible to predict some behaviors of a chaotic system under some circumstances and may provide privileged services to an attacker by estimating the parameters and initial values in a chaotic system based image cipher [8-10].

In cryptography, after applying an algorithm to the image information, no one can read the image except those possessing special knowledge (security key). Such manipulation process of the program is the so called image encryption [11]. The result of the process is encrypted information. Mathematically, encryption algorithms are usually written in a form of transformations defined in equation (1):

$$C = E_K(P) \qquad (1)$$

where P is the original information called the Plaintext, C is the encrypted information called the Ciphertext, and K is the secret key, which is always be a finite sequence of letters or numbers set by the senders or receivers [12, 13].

In this paper, we introduced a new chaotic system called LS chaotic system, which is derived from the Logistic map and Sine map. Compared with the traditional one-dimensional chaotic systems, the output sequence of the LS chaotic system has excellent chaotic behaviors. Using this property, we also introduce a novel image encryption algorithm. Simulation results are given.

The remainder of this paper is organized as follows. In the next section, a brief review of the Logistic Map and the Sine Map will be given. Then, the new LS chaotic system will be introduced and discussed in section III. And Section IV will introduce the new image encryption algorithm using the proposed LS chaotic system based on the structure of the substitution and permutation network (SPN). The experimental results will be shown and analyzed in Section V. Section VI reaches a conclusion.

II. BACKGROUND

In this section, we briefly review two traditional chaotic maps, the Logistic map and the Sine map

1) Logistic Map

The Logistic map is a one-dimensional discrete chaotic map widely used in different arrears. It uses a rational number X_0 between 0 and 1 as an initial value and generates a random sequence using the following rule,

$$X_{t+1} = r \cdot X_t(1 - X_t) \qquad (2)$$

where r is the control parameter, which ranges from [0, 4], t is an iteration number, $t = 0, 1, 2, \cdots$. The bifurcation diagram of the Logistic map is shown in Figure 1 while$X_0 = 0.5$. The control parameter r and the possible long-term

978-1-4673-0089-6/12/$26.00 ©2012 IEEE

population values of the input X of the Logistic map are shown on the horizontal and vertical axes respectively. As can be seen, the Logistic map has chaotic behaviors when $r \in [3.57, 4]$. The parameter r and the possible long-term population values of the input X of the Logistic map are shown on the horizontal axes and vertical axes respectively.

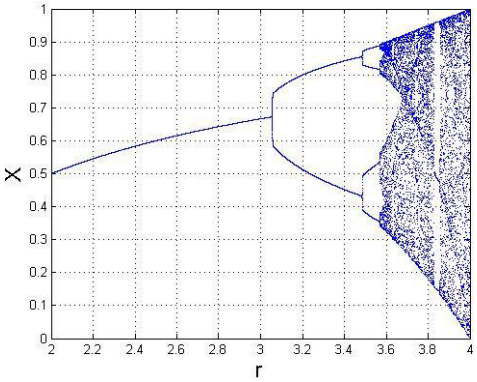


Figure 1. Bifurcation diagram of the Logistic map.

2) Sine Map

The Sine map is also a traditional one-dimensional chaotic map. It also uses X_0 between 0 and 1 as an initial value, and generates the chaotic sequence according to equation (3):

$$X_{t+1} = a \cdot \sin(\pi X_t) \qquad (3)$$

where $a \in \mathbb{R}$ is the control parameter, t is an iteration number, $t = 0, 1, 2, \cdots$.

When the initial value of X is set to 0.5, the bifurcation diagrams of the Sine map is shown in Figure 2. The control parameter a is shown on the horizontal axis, while the vertical axis shows the possible long-term population values of the input X of the Sine map. The Sine map has chaotic behaviors when $a \in [0.867,\ 1]$.

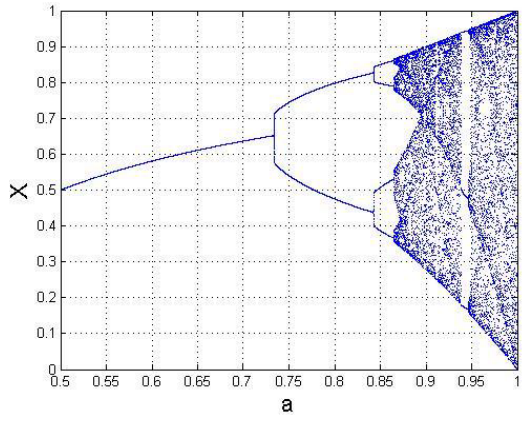


Figure 2. Bifurcation diagrams of the Sine map.

III. LS CHAOTIC SYSTEM

In this section, we introduce a new chaotic system called the LS chaotic system.

Derived from the Logistic and Sine maps, the LS chaotic system is defined in Equation (4).

$$X_{t+1} = a \cdot \sin[\pi \cdot 4a \cdot X_t(1 - X_t)) \qquad (4)$$

where a is the parameter with the range [0, 1], t is an iteration number, $t = 0, 1, 2, \cdots$. The bifurcation diagram of the new LS chaotic map is shown in Figure 3.

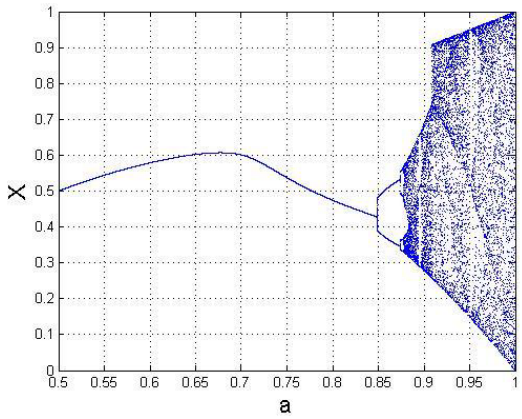


Figure 3. Bifurcation diagrams of the new LS chaotic system.

The bifurcation diagram shows that the new LS chaotic system has good chaotic behaviors when $a \in [0.867,\ 1]$.

IV. NEW IMAGE ENCRYPTION ALGORITHM

To investigate the application of the LS chaotic system in image processing, this section introduces a new image encryption algorithm integrating the LS system with the SPN structure.

To obtain both confusion and diffusion properties of the cryptogram C from a given $m \times n$ plaintext image P, the new encryption algorithm uses a N −round substitution and permutation network (SPN) [14], The algorithm is described below.

Step1. Set the iteration value of N, parameter a and set $i = 1$.

Step2. Give the initial value X_{i0} of the i-th iteration.

Step3. Use equation (4) to generate the chaotic sequence S_i where $t = 0, 1, 2, \cdots, m \times n - 1$.

Step4. According to the configuration of the encryption algorithm to perform the permutation or substitution to image pixels.

Step5. If $i < N$, $i = i + 1$ and go back to step 2.

Step6. End.

Finally, the cryptogram C can be obtained in the final step. The new encrypt algorithm is shown in Figure 4.

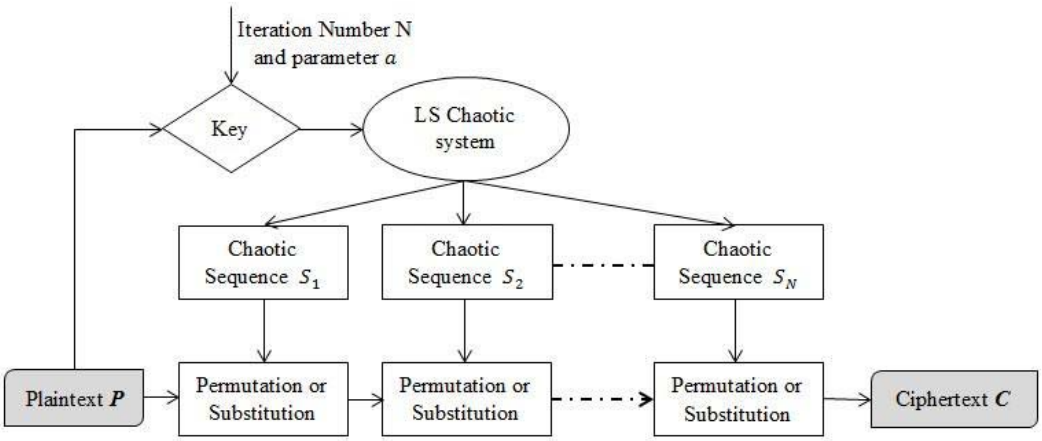


Figure 4. New Image encrption algorithm using the LS chaotic system.

The permutation and substitution in the proposed encryption algorithm are depend on the pre-configuration before encrypt process. In this paper, we choose the first and the last operations as the pixel permutation and all others as the pixel substitution. Namely, the chaotic sequences S_1 and S_N are used for the pixel permutation, $S_2, S_3, \cdots, S_{N-1}$ are used for the pixel substitution. The detail operations are illustrated as the following.

a) The encryption key

First, the parameter a, the iteration numbers N and the initial value X_0 and the format coefficient F should be defined. In order to apply different initial input values to obtain the different output sequences of the LS chaotic system. We define the initial values based on Equations (5)-(7).

$$Sum = \sum_{j=1}^{m}\sum_{i=1}^{n} p_{ij} \quad (5)$$

$$K_i = fshift([Sum]_{base\,5}, 5i) \quad (6)$$

$$X_{i0} = 0.001 \times str2num(K_{i1}K_{i2}K_{i3}) \quad (7)$$

where *Sum* is the sum of all pixel values in the input image, $fshift(q,t)$ is to circularly shift the sequence q with t elements. $[x]_{base\,5}$ denotes base 5 number of x. $str2num(y)$ is to transfer the char data type into numeral type. The equations (6) and (7) ensure that all initial input X_0 values vary within (0, 0.5) and different from each other.

Since the size of the given plaintext image P is $m \times n$, the length of output sequence generated by the LS chaotic map should be mn. In other words, the length of the generated chaotic sequence is equal to the length of the given plaintext image.

b) Pixel Permutation

For the pixel permutation process, we sort the chaotic sequence by a permutation mapping $\mathcal{P}$ defined as equation (8).

$$S_i' = \mathcal{P}(S_i) \quad (8)$$

In such a way, the pixel permutation is realized by using the same mapping to the corresponding sequence as defined in Equation (9).

$$P' = \mathcal{P}(P) \quad (9)$$

c) Pixel Substitution

A new random like sequence $\hat{S}$ is obtained via Equation (10) for pixel substitution.

$$\hat{S} = mod(\lfloor S \cdot 100{,}000 \rfloor, F) \quad (10)$$

where F is called the format coefficient determined by the format of given plaintext image, if the image is gray $F = 256$. Mod denotes the module operator, $\lfloor\ \rfloor$ denotes the rounding function towards to zero. Then, the pixel substitution was realized by using Equation (11).

$$C = mod(\hat{S} + P, F) \quad (11)$$

where P is the pixel values before substitution.

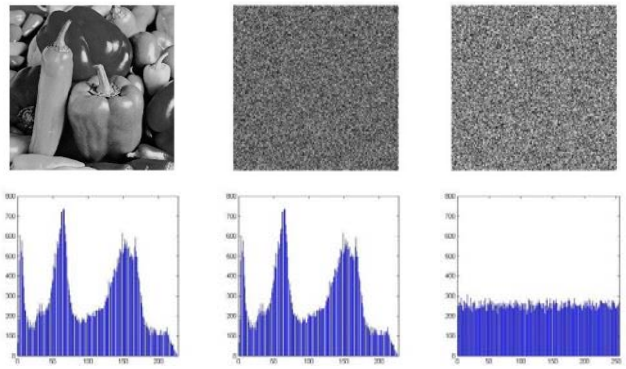
The final encrypted Ciphertext is obtained after all permutation and substitution processes are accomplished. The security key of the proposed image encryption algorithm consists of four components, namely the parameter a, iteration times N, initial input value of the LS chaotic system X_0 and the format coefficient F. Because the possible choices of these four components are sufficiently large, the security key space of the prosed encryption algorithm is large enough to resist brute-force attacks. The decryption process is simply the reverse of the encryption process using the same security key.

V. EXPERIMENTAL RESULTS

This section provides the simulation results. In those results, we set the security key as: $a = 1, N = 9, F = 256$.

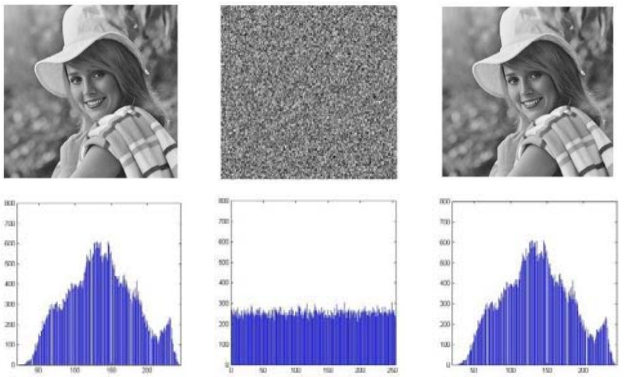
Histogram analysis is one of direct methods, which can evaluate the encryption quality [15, 16]. The experimental results of the histogram analysis for the image encryption

using proposed algorithm are presented in Figure 5 and Figure 6. Here we compare among the plaintext image, the image after the first permutation and the final encrypted image.



(a) (b) (c)

Figure 5. Experimental results by applying the new LS chaotic based encryption algorithm on Peppers image. (a) Original Peppers image and its histogram,; (b) Ciphertext image after the first pixel permutation and its histogram,; (c) Cipher image after permutation and substitution and its histogram.



(a) (b) (c)

Figure 6. Experimental result by applying proposed encryption algorithm on Elaine image. (a) Original Elaine image and its histogram; (b) Encrypted Elaine image and its histogram; (c) Decrypted Elaine image and its histogram.

It can be seen that there is no difference between the histograms of the original and encrypted images after the pixel permutation process even if they are visually completely different as shown in Figure 5 (a) and (b) respectively. This demonstrates that the pixel permutation process does not change image pixel values. Only the pixel positions have been changed according to the mapping operator $\mathcal{P}$. The histogram distributions of two cipher texts in Figures 5(c) and 6(b) look like flat. This shows that the substitution processes in the proposed encryption algorithm scramble the pixel values to a balanced point. Figure 6(c) illustrates the decryption process can completely reconstruct the original image. Thus, the new encryption algorithm has a good performance for image encryption.

VI. CONCLUSIONS

In this paper, a new chaotic system called LS chaotic system has been introduced using two traditional one dimensional chaotic maps: the Logistic map and Sine map. By analyzing the bifurcation diagram of the new LS system, the plot shows the system's random-like property and high sensitivity to initial values and parameters. All these properties benefit to image encryption.

To apply the LS chaotic system to image encryption, this paper has introduced a new image encryption algorithm based the SPN structure. The simulation results show that the LS chaotic system is suitable for image encryption.

The proposed encryption algorithm can be also applied to secure communication and data encryption for other multimedia.

ACKNOWLEDGMENT

This research is supported by the University Research Committee under Grant SRG007 -FST12-ZYC and the research grant of the National Grand Fundamental Research 973 Program of China under Grant 2011CB302801.

REFERENCE

[1] Y. Zhou, K. Panetta, S. Agaian, and C. L. P. Chen, "Image encryption using P-Fibonacci transform and decomposition," *Optics Communications,* vol. 285, pp. 594-608, 2012.

[2] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," *Chaos, Solitons & Fractals,* vol. 21, pp. 749-761, 2004.

[3] C. C. Chang, M. S. Hwang, and T. S. Chen, "A new encryption algorithm for image cryptosystems," *Journal of Systems and Software,* vol. 58, pp. 83-91, Sep 1 2001.

[4] *Chaotic theory*. Available: http://en.wikipedia.org/wiki/Chaos_theory

[5] L. Zhang, X. Liao, and X. Wang, "An image encryption approach based on chaotic maps," *Chaos, Solitons & Fractals,* vol. 24, pp. 759 - 765, 2005.

[6] G. M. Kumar and V. Chandrasekaran, "A novel image encryption scheme using Lorenz attractor," 2009, pp. 3662 -3666.

[7] A. Kumar and M. K. Ghose, "Extended substitution–diffusion based image cipher using chaotic standard map," *Communications in Nonlinear Science and Numerical Simulation,* vol. 16, pp. 372-382, 2011.

[8] G. Jakimoski and L. Kocarev, "Analysis of some recently proposed chaos-based encryption algorithms," *Physics Letters A,* vol. 291, pp. 381-384, 2001.

[9] D. Arroyo, G. Alvarez, S. Li, C. Li, and J. Nunez, "Cryptanalysis of a discrete-time synchronous chaotic encryption system," *Physics Letters A,* vol. 372, pp. 1034-1039, 2008.

[10] G. Alvarez, F. Montoya, M. Romera, and G. Pastor, "Cryptanalysis of a chaotic encryption system," *Physics Letters A,* vol. 276, pp. 191-196, 2000.

[11] *Encryption*. Available: http://en.wikipedia.org/wiki/Encryption

[12] B. Preneel, V. Rijmen, and A. Bosselaers, "Recent Developments in the Design of Conventional Cryptographic Algorithms State of the Art in Applied Cryptography." vol. 1528, ed: Springer Berlin / Heidelberg, 1998, pp. 105-130.

[13] H. E. Papadopoulos and G. W. Wornell, "Maximum-likelihood estimation of a class of chaotic signals," *Information Theory, IEEE Transactions on,* vol. 41, pp. 312-317, Jan. 1995.

[14] D. Stinson, *Cryptography: theory and practice*: CRC press, 2006.

[15] Q. G. Zhengjun Liu, Lie Xu, "Double image encryption by using iterative random binary encoding in gyrator domains," *Opt. Express,* vol. 18, pp. 12033--12043, May 2010.

[16] Y. Wu, J. P. Noonan, and S. Agaian, "A wheel-switch chaotic system for image encryption," in *System Science and Engineering (ICSSE), 2011 International Conference on*, Macau, 2011, pp. 23-27.