2012 IEEE International Conference on Systems, Man, and Cybernetics
October 14-17, 2012, COEX, Seoul, Korea

Image Encryption Algorithm Based on A New Combined Chaotic System

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

Tong Zhang
Department of Computer and information science,
University of Macau
Macau, China
ma96530@gmail.com

Yicong Zhou*, IEEE, Member
Department of computer and information science,
University of Macau
Macau, China
*yicongzhou@umac.mo

***Abstract*—Chaotic theory has been applied to image encryption as an effective and robust technique due to its unique properties. In this paper, we introduce a new combined chaotic system, which shows better chaotic behaviors than the traditional ones. Applying this chaotic system to image processing, a new image encryption algorithm is introduced based on the confusion and diffusion in encryption procedure. Experimental results show that the proposed algorithm has a higher security level and excellent performance in image encryption.**

Keywords-chaotic theory; image encryption; logistic map; comebined chaotic system;

I. INTRODUCTION

Nowadays, it is possible for anyone to transform digital information easily. Several security problems, which are associated with the development of digital signal transmission over an open network, are rising up. Many of application, such as medical image system, cable TV, personal online photograph album, have strong demand for providing security in digital signal transmission.

During the last decade, researcher have proposed various types of efficient and robust encryption algorithms based on different principles [1-6]. Chaos based encryption is one of these efficient techniques due to its unique properties, such as the sensitive dependence on initial conditions and system parameters i.e. a tiny change of the initial input values leads to a great different of the output, unpredictable and its random-like properties, which are satisfied the requirements of cryptography [7, 8]. Especially, chaotic systems based image ciphers are very popular with the researchers as a good solution to image encryption in the past few years [9-11]. However, since the chaotic maps become more familiar to the public and the key space is small, there exists some weakness in security. As long as a little priori information, it has a possible way to predict some behaviors of traditional chaotic systems under some circumstances. In other words, it may provide privileged services to an attacker by estimating the parameters and initial values in a chaotic system based image cipher [12].

To overcome these weaknesses, this paper develops a new combined chaotic system, which is a nonlinear combination of several traditional chaotic maps. The relations between the chaotic systems are controlled by the encryption keys. Compared with traditional chaotic systems, the output chaotic sequence generated from the new system is more complicated dynamics. It keeps all fundamental properties of traditional ones.

Using the proposed chaotic system, this paper introduces a new image encryption algorithm. The algorithm has a larger key space and a higher level security compared to the traditional ones. The new algorithm has been demonstrated to be an effective approach to protect other digital information.

The rest of this paper is organized as follows. Section II briefly reviews the Logistic Map and Sine Map. Then, the new chaotic map is proposed. Some comparative study is made by analyzing the bifurcation diagrams and trajectories of chaotic maps in this section. In Section III, a new image encryption algorithm based on the proposed chaotic map is introduced. The experimental results are shown and analyzed in Section IV. Finally, Section V is the conclusion of this paper.

II. NEW COMBINED CHAOTIC SYSTEM

The Logistic map and the Sine map are one-dimensional traditional chaotic maps, which are widely used in different areas [13].

Then, we introduce a new combined chaotic system, which will be used in image encryption algorithm. It comes from the Logistic map and Sine map. This system can be defined as Equation (1)

$$X_{t+1} = r_t \cdot X_t(1 - X_t) \tag{1}$$

For the control parameters r_t defined by Equation (2),

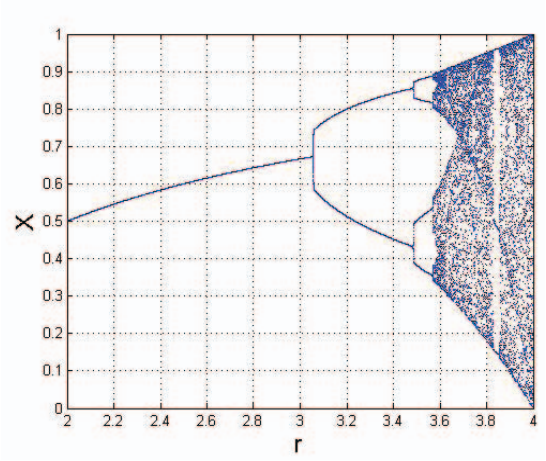
$$r_t = a \cdot \sin(\pi \cdot r_{t-1}) \tag{2}$$

where a is the parameter, $a \in R$; integer t is the iteration index number, $t = 1, 2, 3, \cdots$.

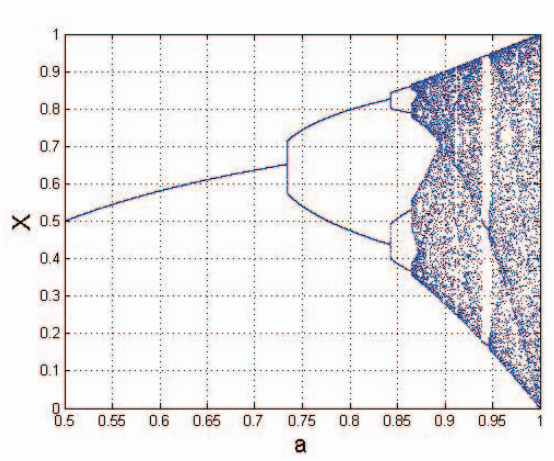
This research was partially sponsored by the National Grand Fundamental Research 973 Program of China under Grant 2011CB302801, Macau Science and Technology development fund under Grant No. 008/2010/A1 and conference grant at University of Macau.

978-1-4673-1714-6/12/$31.00 ©2012 IEEE

As we can see from Figure 1(a) and (b), we can see the Logistic map and the Sine map have good chaotic behaviors when $r \in [3.57,\ 4]$ and $a \in [0.867\ ,1]$, respectively.



(a)



(b)

Figure 1. Bifurcation diagram. (a) The Logistice map; (b) The Sine map

The bifurcation diagram of the new combined chaotic map is shown in Figure 2.

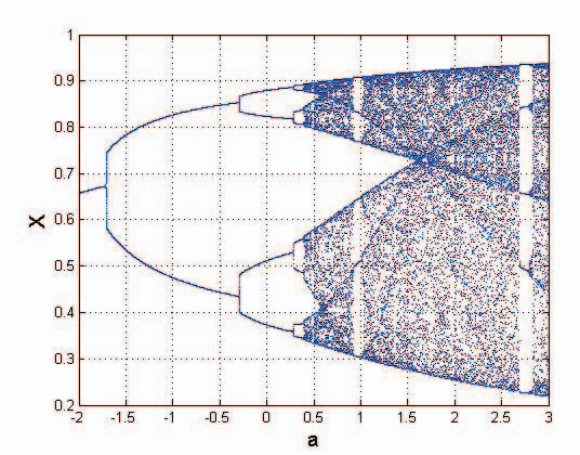


Figure 2. Bifurcation diagrams of the new combined chaotic map.

It's obvious that the new combined chaotic map has a better chaotic behavior than the Logistic map and Sine map because the control parameter of the new combined chaotic map has a larger chaotic interval.

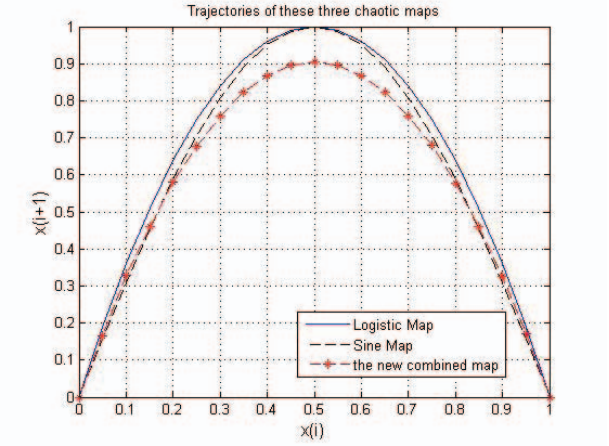


Figure 3. Trajectories of the Logistic map, the Sine map and the new combined chaotic map.

Fig. 3 shows the trajectory of the new combined chaotic map, the Logistic map and the Sine map respectively.

The trajectories of the three chaotic maps are similar as shown in Figure 3. However, three maps can generate completely different sequences even their initial values are the same. In other words, the new combined chaotic map is completely a new chaotic map, which is different from the other two maps.

III. NEW IMAGE ENCRYPTION ALGORITHM

In this section, we will apply the new combined chaotic system to a new image encryption algorithm. Both the confusion and diffusion processes can be achieved by using the chaotic sequences of the proposed chaotic system. The system was controlled by given control parameter a and initial input value x_0 .

Assume that a given plaintext (the original image to be encrypted) P is an $m \times n$ image, the length of the generated chaotic sequence will be mn . Then, the encryption process can be summarized as an N round permutation and substitution structure (SPN) [14]. And the procedure of substitution and permutation will be described in the following in order to obtain confusion and diffusion properties.

a) Initial Input Value of The Combined Chaotic System

In order to apply different initial input values to the new combined chaotic system to obtain different output sequences. The initial input vector $x_0 = (x_{10}, x_{20}, \cdots, x_{N0})$ can be determined by Equations (3) and (4).

$$Sum = \sum_{i=1}^{m} \sum_{j=1}^{n} p_{ij} + K_0 \tag{3}$$

$$X_{i0} = 0.001 \times i \times \mathrm{mod}(Sum, 99) \quad (4)$$

where p_{ij} is the pixel value of the i th row and j th column; Sum stands for the sum of pixel value. k_0 is the initial input parameter to control the input vector x_0; and $\mathrm{mod}(x, y)$ denotes the module operation of x respect to y.

Equations (3) and (4) ensure that all initial input values x_{i0} vary within [0, 1] and different with each other.

b) Confusion and Diffusion

To realize the confusion and diffusion properties, the pixel permutation and substitution processes are defined below. In the permutation process, we sort the generated chaotic sequences by a permutation mapping ψ, which is defined in Equation (5).

$$S_i' = \psi(S_i) \quad (5)$$

In such a way, the confusion property is achieved by applying the same mapping to the corresponding sequence as defined in Equation (6).

$$P = \psi(P) \quad (6)$$

For substitution process, a new random-like sequence $\tilde{S}$ is obtained via Equation (7).

$$\tilde{S} = \mathrm{mod}(S \cdot 10^{32}, F) \quad (7)$$

where the format coefficient F is determined by the format of given plaintext image. For gray images, $F = 256$.

Then, the diffusion property is achieved by Equation (8).

$$C = \mathrm{mod}(\tilde{S} + P, F) \quad (8)$$

where P are the pixel values before substitution. C is the encrypted pixel value.

Finally, the Ciphertext (the encrypted plaintext) is obtained after all permutation and substitution processes are accomplished.

c) The Security key

The security keys of the proposed image encryption algorithm consist of the iteration number N, initial input parameter k_0, control parameters a, r , and the format coefficient F. Because the possible choices of these five components are sufficiently large, the security key space of the proposed encryption algorithm is large enough to resist brute-force attacks.

In addition, the control parameter a has a much larger chaotic interval compared with the Logistic map and Sine map. The new combined chaotic map has a high level of security.

The decryption process is a simple reverse process using the same security key. We summarize the encryption process as below.

Step1. Set the values of the encryption key K, which has four components, the iteration number N, parameter k_0 and a and the format coefficient F. Then set $i = 1$.

Step2. Applying Equations (3) and (4) to generate the chaotic sequence $X_i = \{X_{i1}, X_{i2}, \cdots X_{ij}\}, j = m \times n - 1$.

Step3. Using Equations (5) and (6) to perform the permutation process or Equations (7) and (8) to perform the substitution process.

Step4. If $i < N$, $i = i + 1$ and go back to step 2. Or, go to step 5.

Step5. *End.*

IV. Experimental Results

Simulation results are shown in this section. Firstly, we set the security keys as Table I.

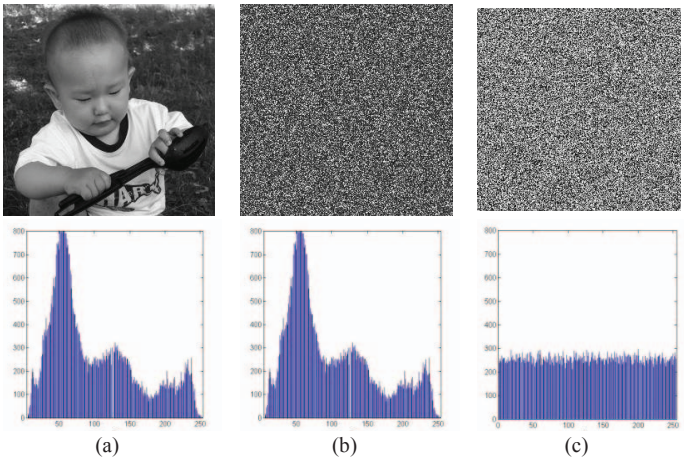
TABLE I. Security Keys

KEYS					
	N	k_0	a	F	r
K_1	10	1000000	1	256	0.21
K_2	10	2000000	0.7	256	0.57

We apply the proposed image encryption algorithm with K_1 and K_2 respectively to encrypt images. Two security analysis methods, histogram analysis and differential attacks, are then tested [15].

1) Histogram Analysis

Histogram analysis is one of direct methods to evaluate the encryption quality, which reveals the distribution of pixel values within an image. The experimental results of the histogram analysis for the image encryption using proposed algorithm are presented in Figures 4 and 5.



(a) (b) (c)

Figure 4. Experimental results by applying proposed encryption algorithm on a child image. (a) Original child image and its histogram, (b) Encrypted image after the permutation process and its histogram, (c) Encrypted image after the permutation and substitution processes and its histogram.

It can be seen that there is no difference between the histogram of the original and encrypted images after applying only the pixel permutation process as shown in Figures 4(a) and (b), respectively. Figure 4(c) almost reaches to a balanced point as we can see the pixel values distribute uniformly. This means the proposed algorithm is effective for image encryption.

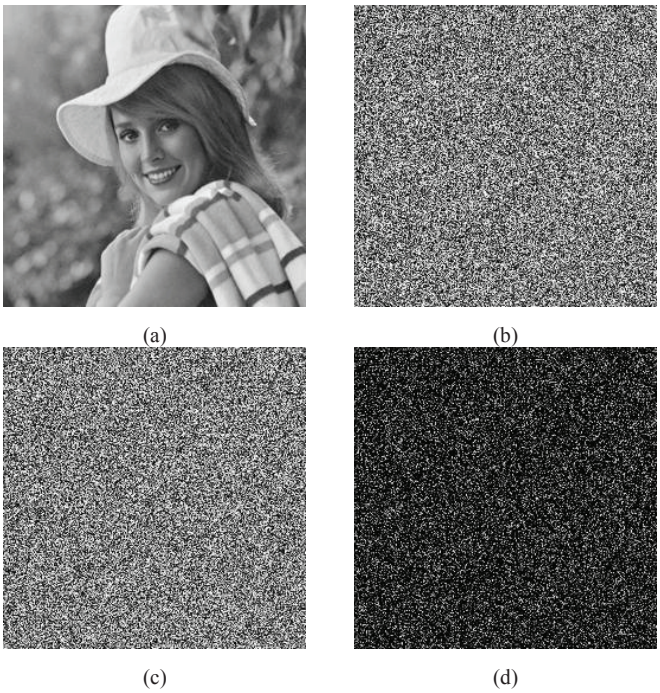


Figure 5. Encryption results using different security key sets. (a) Original Elaine image, (b) Encrypted image using the security key set K_1, (c) Encrypted image using the security key set K_2 (d) Difference between (b) and (c).

For further analysis, the sensitivity of the encryption key was tested. We apply the proposed image encryption algorithm to Elaine image with different sets of security keys in Table I, K_1 and K_2. The encryption results are shown in Figure 5. From the Fig. 5(d), we can see that the encrypted images obtained from the same original image using K_1 and K_2 are completely defferent.

2) Differential Attacks

In order to test the sensitivity of the proposed encryption algorithm to the pixel value changes in the plaintext. We change only one pixel value in the original image, and then measure the difference between the encrypted images using the same security key.

We change the Peppers image only by setting $P_{16,16}=0$., and then encrypt this image using the same security key, K_1. From Figure 6(f), we can see the the encrypted images is are almost difference different everywhere in the entire image.

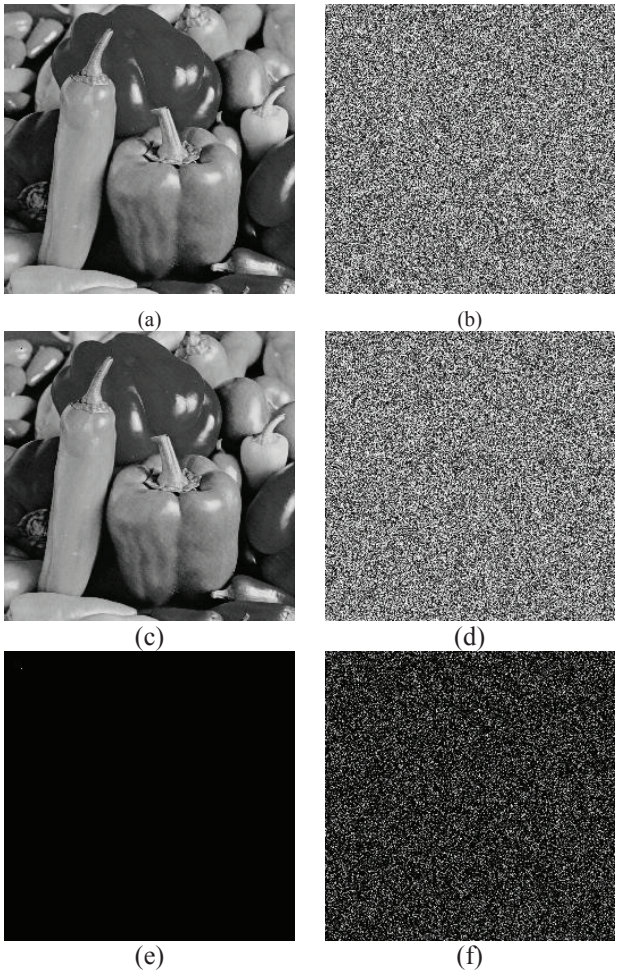


Figure 6. Encryption results using the same security key K_1 with one pixel change in the original image. (a).The original Pepper image; (b) Encrypted result C_1 of the image in (a); (c) Peppers image with $p_{16,16}=0$; (d) Encrypted result C_2 of the image in (c); (e) Difference between (a) and (c); (f) Difference between (b) and (d).

The number of pixels change rate (NPCR) and unified average changing intensity (UACI) [16] are two common tests defined by,

$$NPCR=\frac{1}{m\times n}\sum_{i=1}^{m}\sum_{j=1}^{n}D(i,j)\times 100\% \tag{9}$$

$$UACI=\frac{1}{m\times n\times 255}\sum_{i=1}^{m}\sum_{j=1}^{n}\left|C_1(i,j)-\right|C_2(i,j)\times 100\% \tag{10}$$

where $D(i,j)$ determined by equation (11).

$$D(i,j)=\begin{cases}0 & \mathrm{C}_1(i,j)=C_2(i,j)\\ 1 & \mathrm{C}_1(i,j)\neq C_2(i,j)\end{cases} \tag{11}$$

The tested image is Elaine image, and get the $NPCR=99.63\%$, $UACI=33.50\%$, respectively. Both tests are close to the theoretical values (put theoretical values here).

So, the proposed scheme is able to resist the differential attacks.

V. CONCLUSIONS

In this paper, we proposed a new combined chaotic system using two traditional chaotic maps: the Logistic map and Sine map. The bifurcation diagram and trajectory of the proposed chaotic map demonstrated its better random-like property and high sensitivity to its initial values and parameters. Moreover, the control parameter has a larger chaotic interval compare with traditional chaotic maps. This ensures the proposed chaotic system more suitable for cryptography applications.

Using the proposed chaotic system, a new image encryption algorithm based a SPN structure has been introduced. Simulation results have shown that the proposed algorithm has excellent performance in image encryption.

REFERENCES

[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. Zhang and Q. Liu, "A novel image encryption method based on total shuffling scheme," Optics Communications, vol. 284, pp. 2775-2780, 2011.

[3] H. Liu and X. Wang, "Color image encryption using spatial bit-level permutation and high-dimension chaotic system," Optics Communications, vol. 284, pp. 3895-3903, 2011.

[4] 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.

[5] W. T. Zhu, "A Cost-Efficient Secure Multimedia Proxy System," IEEE Transactions on Multimedia, vol. 10, pp. 1214-1220, 2008.

[6] Y. Zhou, K. Panetta, and S. Agaian, "Image Encryption Based on Edge Information," in IS&T / SPIE Electronic Imaging 2009: Multimedia on Mobile Devices 2009, San Jose, CA, 2009, pp. 725603-11.

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

[8] Y. Mao and G. Chen, "Chaos-Based Image Encryption," in Handbook of Geometric Computing: Applications in Pattern Recognition, Computer Vision, Neuralcomputing, and Robotics, ed, 2005, pp. 231-265.

[9] F. Chiaraluce, L. Ciccarelli, E. Gambi, P. Pierleoni, and M. Reginelli, "A new chaotic algorithm for video encryption," IEEE Transactions on Consumer Electronics, vol. 48, pp. 838-844, 2002.

[10] G. Heidari-Bateni and C. D. McGillem, "A chaotic direct-sequence spread-spectrum communication system," Communications, IEEE Transactions on, vol. 42, pp. 1524-1527, 1994.

[11] A. Akhshani, S. Behnia, A. Akhavan, H. A. Hassan, and Z. Hassan, "A novel scheme for image encryption based on 2D piecewise chaotic maps," Optics Communications, vol. 283, pp. 3259-3266, 2010.

[12] G. Álvarez, F. Montoya, M. Romera, and G. Pastor, "Cryptanalysis of an ergodic chaotic cipher," Physics Letters A, vol. 311, pp. 172-179, 2003.

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

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

[15] S. S. Agaian, E. E. Danahy, and K. A. Panetta, "Logical System Representation of Images and Removal of Impulse Noise," IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans, vol. 38, pp. 1349-1362, 2008.

[16] C. K. Huang and H. H. Nien, "Multi chaotic systems based pixel shuffle for image encryption," Optics Communications, vol. 282, pp. 2123-2127, 2009.