Design of a chaos-based digitlal image encryption algorithm in time domain

JiaYan Wang
GuangZhou Power Supply CO.,LTD, Guangzhou, China
wangjy_power@163.com

Geng Chen
Faculty of Automation, GuangDong University of technology
alex.chen@techyc.com

***Abstract*—In this paper a chaos-based digital image encryption scheme by a permutation-substitution structure is proposed. Its design and implement have been detailed discussed and tested. The results of simulation and analysis show that the proposed image encryption scheme provides a secure way for image encryption.**

Keywords-encryption; decryption;permutation; substitution;

I. INTRODUCTION

With the rapid development of the network communication, digital image encryption has becoming a field that has drawn much attention in the latest years. Digital image data have some particular characteristics such as bulk capacity, high redundancy and high correlation among image pixels. Traditional encryption technologies, such as DES, AES, IDEA, regard digital image data as common data without considering their special characteristics, thus they are unsuitable in protecting digital image data any more.

One of the most effective approaches for image encryption recently is to use chaos maps owning to their non-periodic, non-convergent, sensitivity to initial conditions and ergodicity properties. Chaotic system has interesting and close relationship with cryptography. They are considered the favorable tradeoff of the digital image encryption between the security and the speed. We can find a brief description of relationship between chaos and cryptography in [1, 2]. Fridrich [1] proposes an image encryption scheme based on two-dimensional discrete chaotic baker maps. To fulfill the request of Shannon's theory, the architecture of the scheme is composed of the confusion and diffusion criteria, which is regarded as the basic structure for chaos-based image encryption algorithms. Afterwards, various algorithms based on chaotic maps [3-15] have been proposed for securing image applications.

In this paper a chaotic cipher for gray images by a permutation-substitution structure is proposed. Chaotic maps with random initial conditions and parameters are used to generate random sequences with high sensitivity. Two of the sequences are produced from 2D chaotic map then used to design a two dimensional permutation. The initial values are derived from 1D Logistic map. Then elements of other two sequences are used to confuse pixel values by combined bit exclusive-OR and cyclic bit-shift operations.

Other sections of this paper are organized as follows. In the next section, a brief discussion of chaotic map is introduced. The proposed algorithm is put forward and discussed in section III. Simulation results and security analysis are described in section IV. Section V is a conclusion.

II. CHAOTIC SYSTEM

1D Logistic map is a simple chaotic map and has been widely used in many image encryption algorithms. It is defined by:

$$f(x) = \mu x(1-x), \qquad x \in (0,1). \tag{1}$$

Research shows that the system is in chaotic state under the condition that $3.99465 < \mu \le 4$. However, it may lead to insecure encryption algorithm due to its small key space and simple structure. Therefore high-dimensional chaotic systems which possess large key space will provide better security. For example, 2D discrete Super-chaotic map[3] is given by following equation.

$$\begin{cases} x_{n+1} = ay_n + by_n^2 \\ y_{n+1} = cy_n + dx_n \end{cases} \tag{2}$$

If we let $a = 1.55, b = -1.3, c = 0.1, d = -1.1$, the map will exhibit a chaotic state.

The Lyapunov exponents are usually be employed to measure the exponential rates of divergence and convergence of nearby trajectories in state space. For the above Super-chaotic map, it has two positive Lyapunov exponents, 0.238 and 0.166.

III. THE DESIGN OF IMAGE ENCRYPTION ALGORITHM

Let I denotes a gray scale image with size $M \times N$. Denotes $I(i, j)$ the gray scale value of the pixel at position $0 \le i \le M-1$ and $0 \le j \le N-1$. The proposed algorithm is a symmetrical image encryption method based on chaotic maps. The algorithm is composed of two processes, permutation and substitution, to fulfill the Shannon's criteria, confusion and diffusion.

978-1-4799-6023-1/15 $31.00 © 2015 IEEE
DOI 10.1109/CICT.2015.23

3.1 Permutation

The permutation process is to select a chaotic map to produce a matrix to permute the whole image. It is described as follows:

1. Randomly select a parameter μ_1 and an initial value x_1' for Eq.(1), all of them are served as secret encryption keys. Iterate Eq.(1) r_1 times to avoid the harmful affect of the initial values, where r_1 is a preset integer and served as secret encryption key, too.

2. Use Eq. (1) to generate two random values, x_0 and y_0, with the above parameters. Use Eq. (2) to generate two groups of random sequences, $\{x_i\}_{i=0}^{M\times N-1}$ and $\{y_i\}_{i=0}^{M\times N-1}$, with the different initial values of x_0 and y_0 respectively.

2. Rearrange the sequences $\{x_i\}_{i=0}^{M\times N-1}$ and $\{y_i\}_{i=0}^{M\times N-1}$ in ascending order and get two ordered sequences $\{x_i'\}_{i=0}^{M\times N-1}$ and $\{y_i'\}_{i=0}^{M\times N-1}$.

3. From sequence $\{x_i'\}_{i=0}^{M\times N-1}$ to find the index values of $\{x_i\}_{i=0}^{M\times N-1}$ and get the index transform sequence $\{X_i\}_{i=0}^{M\times N-1}$. Get another index transform sequence $\{Y_i\}_{i=0}^{M\times N-1}$ from $\{y_i\}_{i=0}^{M\times N-1}$ and $\{y_i'\}_{i=0}^{M\times N-1}$ in the same manner.

4. Rearrange $\{X_i\}_{i=0}^{M\times N-1}$ to a 2D permutation matrix $\{P_X\}_{M\times N}$ with size $M\times N$. Get another permutation matrix $\{P_Y\}_{M\times N}$ from $\{Y_i\}_{i=0}^{M\times N-1}$ in the same manner.

5. Permute the plain image $I_{M\times N}$ by permutation matrix $\{P_X\}_{M\times N}$ and $\{P_Y\}_{M\times N}$ one after another.

3.2 substitution

In this process, the image pixels are substituted by the random chaotic key stream values, which resulting in a uniformly distribution of the energy of the image. The substitution procedure is described as follows:

1. Randomly select a parameter μ_2 and an initial value x_2' for Eq.(1), all of them are served as secret encryption keys. Iterate Eq.(1) r_2 times to avoid the harmful affect of the initial values, where r_2 is a preset integer and served as secret encryption key, too.

2. Use Eq. (1) to generate two random values, g_0 and h_0, with Step. 1. Then use Eq. (2) to generate two groups of random sequences, $\{g_i\}_{i=0}^{M\times N-1}$ and $\{h_i\}_{i=0}^{M\times N-1}$, with the different initial values of g_0 and h_0 respectively.

3. Rearrange $\{g_i\}_{i=0}^{M\times N-1}$ to a 2D matrix $\{S_g\}_{M\times N}$ with size $M\times N$. Get another 2D matrix $\{S_h\}_{M\times N}$ from $\{h_i\}_{i=0}^{M\times N-1}$ in the same manner.

4. The substitution is designed to be composed of two operations: bit exclusive-OR and left cyclic shift. For a pixel $I(i,j)$, it is substituted by $S_g(i,j)$ and $S_h(i,j)$. First, two binary numbers, $u(i,j)$ and $v(i,j)$, of 8-bit length and a binary number $w(i,j)$ of 3-bit length are calculated by:

$$u(i,j)=\lfloor S_g(i,j)\times 10^{32}\rfloor \bmod 256 \quad (3)$$

$$v(i,j)=\lfloor S_h(i,j)\times 10^{32}\rfloor \bmod 256 \quad (4)$$

$$w(i,j)=\lfloor (S_g(i,j)+S_h(i,j))\times 10^{32}\rfloor \bmod 8 \quad (5)$$

Then apply the bitwise exclusive-OR to the permuted image pixels $I(i,j)$ by the following equations:

If $S_g(i,j)<S_h(i,j)$, then

$$T(i,j)=I(i,j)\oplus \mathrm{mod}(u(i,j)+32*w(i,j),256) \quad (6)$$

else

$$T(i,j)=I(i,j)\oplus \mathrm{mod}(v(i,j)+32*w(i,j),256) \quad (7)$$

Afterwards, apply the left cyclic shift operation to $T(i,j)$ by the following equations:

$$E(i,j)=ROL(T(i,j),w(i,j)) \quad (8)$$

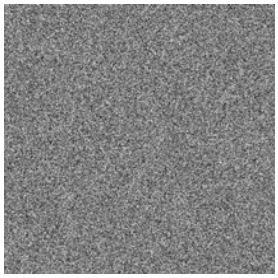
where $ROL(a,b)$ performs b-bit left cyclic shift on the binary value a.

Finally, in order to enhance the security, the permutation and substitution procedures will be repeated t ($t\geq 2$) times to get the latest encrypted image, where t is served as secret encryption key, too.

The decryption procedure is followed in a reversed order of the encryption procedure.

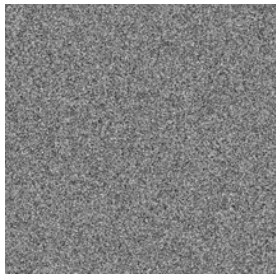
IV. SIMULATIONS AND PERFORMANCE ANALYSIS

(a) Original Barbara



(b) Encrypted Barbara

(c) Correctly decryption



(d) Incorrectly decryption

Figure 1. The original images and the encryption/decryption results

For simulations the standard gray scale image Barbara with size 512×512 is tested by the proposed encryption algorithm.

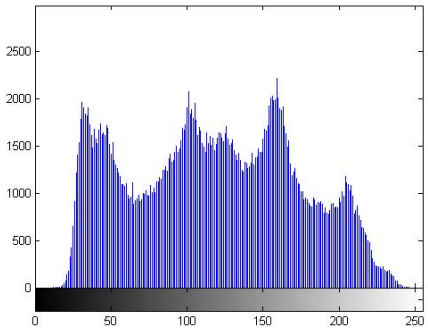
The encryption and decryption results of image Barbara are shown in Fig. 1. One can find that there is no any visual relationship between the original image and the encrypted one. This means the algorithm have a fine encryption effect. The correctly decrypted image with correct keys is shown in Fig. 1(c), which is identical to Fig. 1(a).

4.1 Key Space

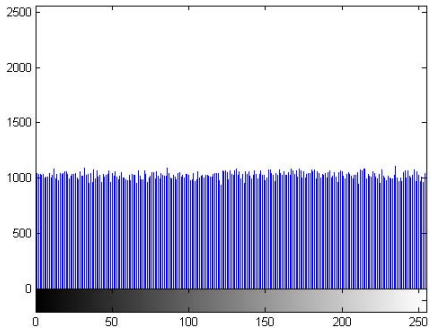
The key space of the proposed algorithm is consists of secret keys containing μ_1, μ_2, x_1', x_2', r_1, r_2, t. Suppose the precision of the computing system is 10^{16}, then the key space of the proposed algorithm is about $(10^{16})^7 \approx 2^{372}$. Thus the size of the key space is large enough to resist any brute force attack.

4.2 Histogram

Permutation shifts pixels' position from one position to another, Substitution alters pixel values. In the proposed algorithm, a combination of permutation and substitution occurs, increasing farther security. Fig. 2(a) and Fig. 2(b) depict the histograms of Fig. 1(a) and Fig. 1(b) respectively. The result indicates the proposed algorithm keeps better effect against the statistical analysis attack.



(a) Histogram of plain Barbara

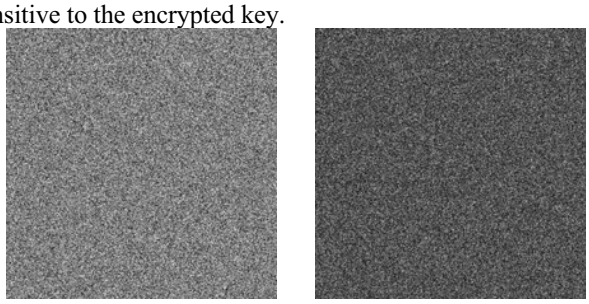


(b) Histogram of encrypted Barbara

Figure 2. The histogram distribution

4.3 Key Sensitivity

The original Barbara is encrypted with a slightly change key (Only the parameter x_1' is changed with a precision of 10^{-16} compared to the encrypted key used in Fig. 1(b)). The encrypted image with the changed key is showed in Fig. 3(a). Fig. 3(b) demonstrates the absolute differential image between Fig. 1(b) and Fig. 3(a). From the Figure we can see obviously the encryption of the proposed algorithm is quite sensitive to the encrypted key.



(a) (b)

Figure 3. Sensitivity Analysis

(a) Encrypted image with a slightly changed key;
(b) Differential image between Fig. 1(b) and Fig. 3(a).

The encrypted Barbara (See Fig. 1(b)) is decrypted with a slightly change key (Only the parameter x_2' is changed with a precision of 10^{-16} compared to the encrypted key used in Fig. 1(b)). The decrypted image with the changed key is showed in Fig. 1(d). From the Figure we can see obviously the decryption of the proposed algorithm is quite sensitive to the decrypted key, either.

4.4 Correlations between adjacent pixels

To analyze the correlations of adjacent pixels of the proposed algorithm, 1000 pairs of two adjacent pixels (in horizontal, vertical, and diagonal direction) are randomly selected from Fig. 1(a) and Fig. 1(b).

The correlation coefficients are calculated by the following formula:

$$r_{xy} = \frac{E(x - E(x)E(y - E(y))}{\sqrt{D(x)D(y)}} \quad (9)$$

where

$$E(x) = \frac{1}{L}\sum_{i=1}^{L} x_i \quad (10)$$

$$D(x) = \frac{1}{L}\sum_{i=1}^{L} (x_i - E(x))^2 \quad (11)$$

TABLE I. CORRELATION COEFFICIENTS OF FIG. 1(A) AND FIG. 1(B)

Correlations	Original image	Encrypted image
Horizontal	0.9792	0.0217
Vertical	0.9809	0.0086
Diagonal	0.9551	0.0118

The average results are given in Tab. 1. It is obviously that all kinds of the correlation coefficients are extremely near zero which denotes very low correlations.

V. CONCLUSION

This paper presents a simple but secure chaotic cipher for gray images by a permutation-substitution structure. Experimental tests demonstrate that the proposed algorithm possesses large key space, high security and good encryption effect. Thus it is suitable for digital image encryption in applications.

REFERENCES

[1] J. Fridrich, "Symmetric ciphers based on two-dimentional chaotic maps", *Int. J. Bifurcation and Chaos*, vol. 8, no. 6, 1998, pp. 1259-1284.

[2] L. Kocarev, G. Jakimoski, T. Stojanovski, U. Parlitz, "From chaotic maps to encryption schemes", *In Proc. IEEE Int. Symposium Circuits and Systems*, vol. 4, 1998, pp. 514-517.

[3] P J Burt, E H Adelson, "The Laplacian Pyramid as a Compact Image Code", IEEE Trans on Communications, 1983, 31 (4), pp. 532 – 5401.

[4] S. Li, X. Mou, Y. Cai, Z. Ji, J. Zhang, "On the Security of a Chaotic Encryption Scheme: Problems with Computerized Chaos in Finite Computing Precision", *Computer Physics Communications*, vol. 153, no. 1, 2003, pp. 52-58.

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

[6] A. N. Pisarchik, M. Zanin, "Image encryption with chaotically coupled chaotic maps", Physica D: Nonlinear Phenomena, 2008, 237(20), pp. 2638-2648.

[7] X. Tong, M. Cui, "Image encryption scheme based on 3D baker with dynamical compound chaotic sequence cipher generator", Signal Processing, 2009, 89(4) , pp. 480-491.

[8] Vinod Patidara, N.K. Pareekb, G. Purohita, K. K. Sud, "A robust and secure chaotic standard map based pseudorandom permutation-substitution scheme for image encryption", Optics Communications. 2011, 284(19) , pp. 4331-4339.

[9] W. Yong, W. W. Kwok, X. F. Liao, et al, "A new chaos-based fast image encryption algorithm", Applied Soft Computing. 2011, 11(1) , pp. 514-522.

[10] X. Y. Wang, X. Qin, "A new pseudo-random number generator based on CML and chaotic iteration", Nonlinear Dynamics. 2012, 70, pp. 1589-1592.

[11] S. M. Seyedzadeh, S. Mirzakuchaki, "A fast color image encryption algorithm based on coupled two-dimensional piecewise chaotic map", Signal Processing. 2012, 92(5) , pp. 1202-1215.

[12] A. Kanso, M. Ghebleh, "A novel image encryption algorithm based on a 3D chaotic map", Communications in Nonlinear Science and Numerical. 2012, 17(7) , pp. 2943-2959.

[13] C. Y. Song, Y. L Qiao, X. Z. Zhang, "An image encryption scheme based on new spatiotemporal chaos", Optik - Int. J. Light Electron Opt. 2012, http://dx.doi.org/10.1016/j.ijleo.2012.11.002

[14] Q. Zhang, L. Guo, X. P. Wei, "A novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system", Optik - Int. J. Light Electron Opt. 2013, http://dx.doi.org/10.1016/j.ijleo.2012.11.018

[15] N. Bigdeli, Y. Farid, K. Afshar, "A novel image encryption/decryption scheme based on chaotic neural networks", Engineering Applications of Artificial Intelligence, 2012, 25(4) , pp. 753-765.