Available online at www.sciencedirect.com

SCIENCE @ DIRECT®

Chaos, Solitons and Fractals 24 (2005) 759–765

CHAOS
SOLITONS & FRACTALS

www.elsevier.com/locate/chaos

An image encryption approach based on chaotic maps

Linhua Zhang [a,b,*], Xiaofeng Liao [a], Xuebing Wang [b]

[a] *Department of Computer Science and Engineering, Chongqing University, Chongqing 400044, China*
[b] *College of Science, Chongqing University, Chongqing 400044, China*

Accepted 14 September 2004

Abstract

It is well-known that images are different from texts in many aspects, such as highly redundancy and correlation, the local structure and the characteristics of amplitude–frequency. As a result, the methods of conventional encryption cannot be applicable to images. In this paper, we improve the properties of confusion and diffusion in terms of discrete exponential chaotic maps, and design a key scheme for the resistance to statistic attack, differential attack and grey code attack. Experimental and theoretical results also show that our scheme is efficient and very secure.

1. Introduction

With the fast development of computer network technology, it is so easy to obtain digital images through network and further use, process, reproduce and distribute them. Digital technology brings us much convenience, but it also gives attacker or illegal user an opportunity. Generally, there are two major approaches which are used to protect digital images. One is information hiding which includes watermarking, anonymity, steganography and cover channel. The other is encryption which includes conventional encryption and others such as chaotic encryption.

Chaotic systems have many important properties, such as the sensitive dependence on initial conditions and system parameters, the density of the set of all periodic points and topological transitivity, etc. Most properties are related to some requirements such as mixing and diffusion in the sense of cryptography. Therefore, chaotic cryptosystems have more useful and practical applications.

As early as in 1991, Toshiki Habutsu et al. proposed a scheme that a cipher-text was obtained by the iteration of an inverse chaotic map from an initial point which denoted a plain text [1]. However, chaos-based encryption is not always secure. In [2], an approach to chaotic block encryption, where the length of block could be changed, was designed. In [3], Baptista proposed a cryptosystem based on the property of ergodicity of chaotic system. But in [4], Álvarez and Montoya thought that they were not robust and secure. Recently there have been many papers on improvement of chaotic cryptosystems [5–9].

Since any chaotic output is based on floating-point analytical computation, the intruders can attack cryptosystems efficiently via certain basin structure. On the other hand, some conventional methods such as S-box transform can

[*] Corresponding author. Address: College of Science, Chongqing University, Chongqing 400044, China.
E-mail address: zhanglin@zszh.org (L. Zhang).

0960-0779/$ - see front matter © 2004 Elsevier Ltd. All rights reserved.
doi:10.1016/j.chaos.2004.09.035

greatly increase the difficulty of attacks. It is important to combine approaches of both chaotic and conventional cryptographic methods to enhance the security of cryptosystems in some ways [10,11].

For the purpose of diffusion and resistance to differential attack, first we analyze the performance of discrete exponential chaotic map, then a permutation of the pixels of image is designed and the "XOR plus mod" operation is applied in our scheme.

For resistance to statistic attack, grey code attack and entropy attack [4], we choose chaotic map elaborately and construct chaotic sequences which satisfy uniform distribution when design the key scheme.

2. Discrete exponential chaotic map (DECM) and permutation

When we design S-box, it is very important to find a proper permutation which has good properties in cryptology. We choose the following function g [13]. Let $g{:}M \to M$ be defined as

$$x \mapsto \begin{cases} a^x (\text{mod } 257) & \text{if } \bar{x} < 256 \\ 0 & \text{if } \bar{x} = 256 \end{cases} \tag{1}$$

where $\bar{x} = a^x(\text{mod } 257)$, $x \in M$, $M = \{0,1,2,\ldots,255\}$, it a is chosen so that it is a generator of the multiplicative group of nonzero elements of the Galois field of order 257. There are 128 different values of a. In this case, the map g performs one-to-one transformation.

Note that g is the discrete form of the following exponential chaotic map $e{:}x \to a^x$, where $x \in [0,1]$, $a > 1$, we have

(1) The multiplicative group of nonzero elements of the Galois field of order 257 is a cyclic group of order 256 and a is a generator. Without loss of generality, assume that $a = 45$. Because an arbitrary odd number is co-prime to 256, we obtain the set of all of generators which includes $45, 147, 69, \ldots, 40$. The distribution of generators is relatively uniform.

(2) The differential approximation probability of a given map f (DP_f for short) is a measure for differential uniformity and it is defined as

$$\text{DP}_f = \max_{\Delta x, \Delta y \neq 0} \left\{ \frac{\#\{x | g(x) \oplus g(x + \Delta x) = \Delta y\}}{256} \right\} \tag{2}$$

where x is the set of all possible input values and 2^8 is the number of its elements. If $f = g^2$, the experimental results show that the number of the maximal differential pairs can be 10, 12, 14 or 16, and concentrate on 10 or 12. The range of DP_f is $\{0.039063, 0.042969, 0.046875, 0.054688\}$. In a word, S-boxes constructed by the above discrete exponential map can resist to differential attack.

(3) Linear cryptanalysis which expressed in term of "linear expression", exploits a cipher's weakness. For a given S-box S, we define

$$NS(\alpha, \beta) = \#\left\{ x \middle| \bigoplus_{i=0}^{7} \alpha[i] \cdot x[i] = \bigoplus_{i=0}^{7} \beta[i] \cdot f(x)[i] \right\} \tag{3}$$

where α, β, $x \in M$, $\alpha \neq 0$, $\beta \neq 0$, $\oplus_{i=0}^{7} \alpha[i] \cdot x[i]$ denotes the parity of bit-wise product of α and x. So the probability p that linear expression holds equals $NS(\alpha,\beta)/256$. When $|p - 1/2|$ is small, the nonlinearity of the S-box is said to be high. For a basic linear attack [12], the number of known plain texts required to guess a correct key bit is given as

$$NL = |p - 1/2|^{-2} \tag{4}$$

By piling-up Lemma [18], we define

$$LP_g = \max_{\alpha,\beta \neq 0} \left(\frac{NS(\alpha,\beta) - 128}{128} \right)^2 \tag{5}$$

When our scheme has n active S-boxes, we have

$$LP \approx (LP_g)^n \tag{6}$$

Assume $f = g^2$ the range of LP_f is $\{0.0625, 0.070557, 0.079102, 0.088135, 0.10767\}$.

(4) For the one-to-one transformation g, we can regard it as an element of permutation group on M. For different generator a, the number of fixed points of g ranges from 0 to 4 only and concentrates on 0 and 1. Therefore, it is efficient

to permute the pixels of the image by g. In particular, 255 is not the fixed point of g or g^2 for an arbitrary generator a, which is crucial to design diffusion.

(5) The order of g is more than 254. Regarding g as an element of permutation group S_{256} on letters $0,1,\ldots,255$, we can write g as the product of disjoint cycles. Therefore, the order of g is the minimal common multiple of the lengths of those cycles. For example, let generator a be 45, g can be represented by the product of the following cycles: $(0,1,45,243,179,\ldots,251,252,254,255)$, $(147,109,224,\ldots,249,253)$, $(148,22,168,\ldots,236,247)$, $(127,217)$, (27), (87), (92). The lengths of the above cycles are 168, 42, 41, 2, 1, 1 and 1, respectively, hence the order of g is $[168,42,41,2,1]$, i.e., 6888. To sum up, after 50 rounds of iterations of g^2, an image of size 256×256 will not turn back to its original. This property of g is superior to that of 2D or 3D cat map [13].

The above permutations have good cryptographic properties, so we can use them to change the positions of pixels of plain-image and decorrelate it.

3. Key scheming

From the point of view of strict cryptography, chaotic sequences would better satisfy uniform distribution. Furthermore, we must choose the chaotic map in detail. Piece-wise linear map (PLM) is an ideal chaotic map which has uniform invariant density function and δ-like correlation, and it can be easily realized by both hardware and software [14]. But PLM depends on the computing precision excessively, and its phase portrait includes a clear linear structure. Hence, the cryptosystem based on PLM also depends on the computing precision excessively and has many weak keys [15].

Note that we can use two methods to enlarge the period of the chaotic sequence, one is high precision algorithm and the other is perturbation to chaotic sequence. So we improve cryptosystem by changing the linear structure of phase portrait for resistance to grey code attack and preserving uniform invariant density function of chaotic map for resistance to statistic attack.

In [16], a chaotic and stochastic sequence is given as

$$X_n = \sin^2(\theta\pi\eta^n) \tag{7}$$

where η is a irrational number and $\theta = \frac{1}{\pi}\arcsin\sqrt{X_0}$, θ can be chosen arbitrarily, $X_0 \in (0,1)$. Though $\{X_i\}_{i=0}^{i=\infty}$ is chaotic and unpredictable and has probability density function

$$P(X) = \frac{1}{\pi\sqrt{X(1-X)}} \tag{8}$$

Note that stochastic variable X does not distribute uniformly. It seems a good idea to use the transform

$$Y_n = \frac{2}{\pi}\arcsin\sqrt{X_n} \tag{9}$$

Eq. (9) converts $\{X_i\}_{i=0}^{i=\infty}$ to $\{Y_i\}_{i=0}^{i=\infty}$ which has an uniform probability density function [17].

In fact, $\{Y_i\}_{i=0}^{i=\infty}$ can be generated by p-adic map and it is chaotic but unpredictable!

In [18], some examples of conventional chaotic maps with ACI measures which satisfy the EDP are given, It is convenient to select proper maps to generate chaotic sequences. But we must pay attention to that the transform of stochastic variable may degrade the properties of sequences.

Recently, a method of constructing one class of chaotic running key generator has been proposed based on time-varied-parameter piece-wise linear map (TVPPLM).

Consider 1D piecewise linear map (PLM) on interval $[-1,1]$:

$$x(t+1) = \Phi_C(x(t)) = \begin{cases} -1 + \frac{2(x(t)-c_i)}{c_{i+1}-c_i}, & x(t) \in [c_i, c_{i+1}] \\ 1, & x(t) = 1 \\ \Phi_C(-x(t)), & x(t) \in [-1, 0] \end{cases} \tag{10}$$

where $c_0 = 0$, $c_{N+1} = 1$, $c_0 < c_1 < \cdots < c_i < \cdots < c_{N+1}$, $i = 0,1,\ldots,N$, $N \geqslant 1$, $C = [c_1, c_2, \ldots, c_N]$; $t = 1,2,\ldots$

When $N = 1$, we introduce time-varied-parameter $C(t)$ and suppose

$$y(t+1) = \Phi_{C_y}(y(t)), \tag{11}$$

$$C(t) = (1 + y(t))/2, \tag{12}$$

$$x(t+1) = \Phi_{c(t)}(x(t)). \tag{13}$$

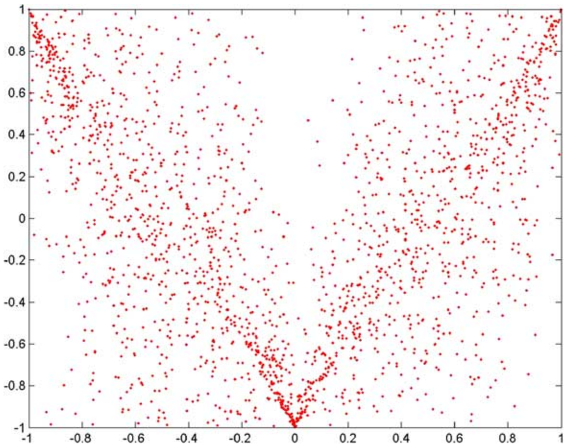

Fig. 1. The phase space of $\{x(t)\}_{t=0}^{t=\infty}$.

We get a 0–1 sequence $\{s_n(t)\}_{t=1}^{t=\infty}$ by Rademacher function

$$Q_n(x) = \begin{cases} 0, & x \in \cup_{d=0}^{2^{n-1}-1} I_{2d}^n \\ 1, & x \in \cup_{d=0}^{2^{n-1}-1} I_{2d+1}^n \end{cases} \tag{14}$$

i.e., $s_n(t) = Q_n(x(t))$, where $I_0^n, I_1^n, \ldots, I_{2^n-1}^n$ denote 2^n consecutive part intervals of $[-1, 1]$.

Theoretically, the phase space of chaotic sequence $\{x_n(t)\}_{t=0}^{t=\infty}$ satisfies uniform distribution property and does not include local linear structure in its phase portrait (see Fig. 1). Trials show that $\{s_n(t)\}_{t=1}^{t=\infty}$ have many characteristics of traditional cryptography, such as balanced 0–1 ratio, zero co-correlation and ideal nonlinearity. Therefore, image encryption based on TVPPLM can resist to grey code attack and statistic attack efficiently [19].

Furthermore, we can obtain many TVPPLM if only we make $C(t)$ satisfies uniform distribution on $(0, 1)$. The methods include

(1) Use p-adic map or zigzag map to generate $\{C(t)\}_{t=0}^{t=\infty}$.
(2) Use composite nonlinear discrete chaotic maps to generate $\{C(t)\}_{t=0}^{t=\infty}$.

We claim that the latter is a better method. Assume that

$$f_0(x) = \sqrt{|2x-1|}, \tag{15}$$

$$f_1(x) = 1 - \sqrt{|2x-1|}, \tag{16}$$

$$C(t+1) = f_i(C(t)), \quad i = 0, 1, \tag{17}$$

where i equals to 0 or 1 randomly. Because $f_0'(x) > 1$ and $f_1'(x) > 1$, (15) and (16) are nonlinear chaotic maps. By Perron–Frobinius operator, we can figure out $\rho(x) = 1$ where $\rho(x)$ is a probability density function of $\{C(t)\}_{t=0}^{t=\infty}$ on $(0, 1)$ [20]. In fact, the above method is applicable to (13) and corresponding properties follow.

4. Algorithm

In [21], some axioms and design steps for the chaotic cryptosystem are proposed. Referring to substitution and permutation structure in AES (in short, SP), we can use the following steps to carry out the image encryption scheme (see Fig. 2):

Step 1: With no loss generality, we assume that source image is a 256×256 image. For a smaller or larger image, we can divide it into blocks of size 256×256 or fill it up to a 256×256 image, respectively.
Step 2: Use TVPPLM to generate chaotic sequence S.

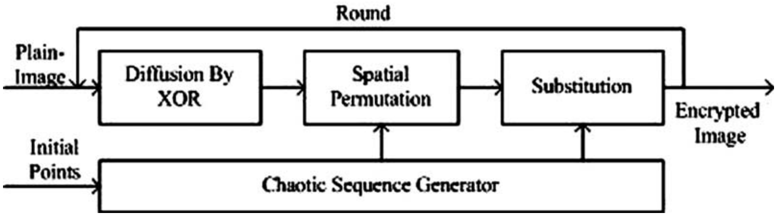

Fig. 2. Block diagram of the image encryption.

Step 3: Let I be the source image, J is a vector that is stung out from I. Note that $J(0)$ denotes the first element of J. We compute J according to the following formula:

$$J(k) = J(k-1) \oplus J(k), \quad k = 1, 2, \ldots, 256 \times 256 - 1.$$

Step 4: Define permutation $\varphi:(i,j) \mapsto (s,t)$, $(i,j) \in M \times M$ as

$$\begin{cases} s = f(i) \\ t = j \oplus (s + \text{round }(256 * k)(\text{mod}256)) \end{cases}$$

where k is extracted from chaotic sequence S.

Step 5: Construct 256×256 matrix by K in turn and compute I according to the following formula:

$$I = I + \text{round }(256 * K)(\text{mod}256).$$

Step 6: Go to Step 3 until the matrix satisfies the security requirement.

Step 7: End.

Note that the decipher procedure is similar to that of encryption process with reverse operational sequences to those described in Steps 3–5.

5. Experiments

In this section, simulation results have shown the effectiveness of the above algorithm. An indexed image "LENA" of size 256×256 is used as a plain-image, see Fig. 3(a). Let $y(0) = 0.1$, $x(0) = 0.09$, $C_y = 0.33$ in TVPPLM generate a sequence of length 1,000,000 and let the generator a be 45 in permutation f. We cut off the first 500,000 elements to be ready for S-box and chaotic encryption. A good distribution of pixels of ciphered image is shown in Fig. 3(c).

On the other hand, we use 0.09 as the initial point of $\{x(t)\}_{t=0}^{t=\infty}$ to decipher the ciphered image correctly, but, let the initial point be 0.091, we cannot obtain any useful information about plain-image (see Fig. 4).

6. Analysis

6.1. Correlation analysis of two adjacent pixels

Randomly select 1000 pairs of two adjacent (in vertical, horizontal, and diagonal direction) pixels from plain-image and ciphered image, and calculate the correlation coefficients, respectively (see Table 1). In fact, permutation f decorrelate pixels of plain-image efficiently.

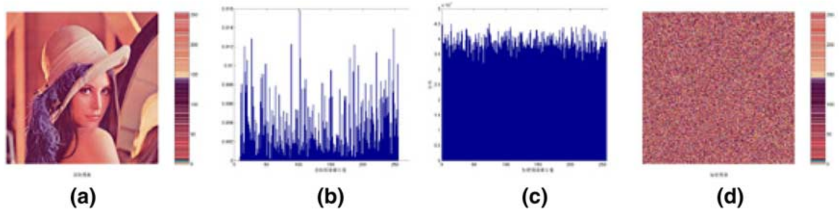

Fig. 3. (a) Plain-image, (b) histogram of plain-image, (c) histogram of encrypted image, (d) encrypted image.

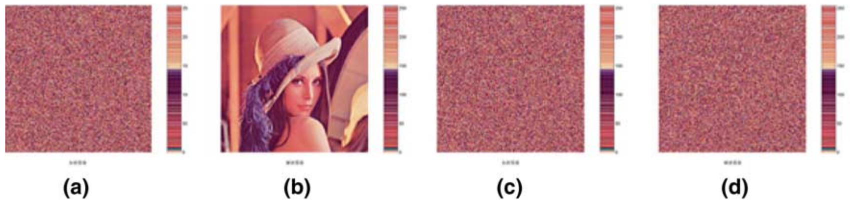

Fig. 4. Key sensitive test: (a) ciphered image, (b) deciphered image by using $\{x(t)\}_{t=0}^{t=\infty}$ where $x(0) = 0.09$; (c) ciphered image, (d) deciphered image by using $\{x(t)\}_{t=0}^{t=\infty}$ where $x(0) = 0.091$.

Table 1
Correlation coefficients of two adjacent pixels in plain-image and ciphered image

	Plain-image	Ciphered image
Vertical	0.65510	0.081586
Horizontal	0.55660	−0.040053
Diagonal	0.61361	−0.004715

6.2. NPCR analysis

NPCR means the change rate of the number of pixels of ciphered image while one pixel of plain-image is changed. We change the value of the last pixel of plain-image to be 22. When round more than 2, the measure NPCR is good enough.

6.3. UACI analysis

The unified average changing intensity (UACI) measures the average intensity of differences between the plain-image and ciphered image. Experimental results are shown in Table 2.

6.4. Randomness and uniform distribution analysis

We claim that pixels of encrypted image has rather good statistic properties of randomness and uniform distribution on M, where $M = \{0,1,\ldots,255\}$.

Suppose that two data sequences $\{a_i\}_{i=1}^{i=n}$ and $\{b_i\}_{i=1}^{i=n}$ be the completely random, and uniformly distribution in [0,1], and they are completely uncorrected from each other, then the average error between two data sequence is

$$e = \frac{1}{n}\sum_{i=1}^{n}|a_i - b_i| \approx \frac{1}{3} \tag{18}$$

The square root of variance of this error for the sequences of length n reads

$$\sigma = \left(\frac{1}{n}\sum_{i=1}^{n}(|a_i - b_i| - e)^2\right)^{1/2} \approx \frac{1}{3\sqrt{2}} \tag{19}$$

First, we select the first data sequence from pixels of 4-round encrypted image, and then change the last pixels of plain-image and encrypt it to obtain the second data sequence. Finally, note that the relation between the average error and UACI, we can verify (18) and (19) easily.

Table 2
NPCR and UACI

Measure	Round						
	1	2	3	4	5	6	7
NPCR (%)	0.00153	21.48	98.259	98.660	98.448	98.78	98.669
UACI (%)	0.00003	2.510	31.407	33.505	33.308	33.60	33.362

7. Conclusion

In this paper, first, for the resistance to differential attack and linear attack, we put forward the rather good statistic properties of discrete exponential chaotic maps, In virtue of them, we design a spatial S-box, and then, we design a key scheme for the resistance to statistic attack and grey code attack. In fact, our scheme can resist to the error function attack (EFA) which be regarded as a very effective attack recently. Finally, Experimental and analytic results show that our scheme is efficient and highly secure.

Acknowledgments

The work described in this paper was supported by grants from the National Natural Science Foundation of China (No. 60271019), by grants from the Doctorate Foundation of Ministry of Education PRC (No. 20020611007) and the Post-doctoral Scientific Foundation of China.

References

[1] Habutsu T et al. A secret cryptosystem by iterating a chaotic map. Eurocrypt 1991:127–40.
[2] Álvarez E, Fernandez A. New approach to chaotic encryption. Phys Lett A 1999;263:373–5.
[3] Baptista MS. Cryptography with chaos. Phys Lett A 1998;240:50–4.
[4] Álvarez G, Montoya F. Cryptanalytic methods in chaotic cryptosystems. Phys Lett A 2003;311:172–9.
[5] Jakimoski G, Kocarev L. Chaos and cryptography: block encryption ciphers based on chaotic maps. IEEE Trans Circ Syst—I 2001;48(20):163–9.
[6] Jakimoski G, Kocarev L. Analysis of some recently proposed chaos-based encryption algorithms. Phys Lett A 2001;291:381–4.
[7] Wang K-W. A combined cryptographic and hashing scheme. Phys Lett A 2003;307:292–8.
[8] Li S, Mou X. Performance analysis of Jakimoski–Kocarev attack on a class of chaotic cryptosystems. Phys Lett A 2003;307:22–8.
[9] Li S, Mou X. Improving security of a chaotic encryption approach. Phys Lett A 2001;290:127–33.
[10] Jakimoski G, Kocarev L. Differential and linear probabilities of a block-encryption cipher. IEEE Trans Circ Syst—I 2003;50(1):121–3.
[11] Tang G. Chaos-based cryptograph incorporated with S-box algebraic operation. Phys Lett A 2003;3189:388–98.
[12] Matsui M. Linear cryptanalysis method for Des cipher. In: Proceedings of Eurocrypt'93. Berlin: Springer-Verlag; 1991. p. 3–72.
[13] Chen G, Mao Y. A symmetric image encryption scheme based on 3D chaotic cat maps. J Chaos, Solitons & Fractals 2004;21:749–61.
[14] Zhou H, Ling X. Generating chaotic secure sequences with desired statistical properties and high security. Int J Bifurc Chaos 1997;7(1):205–13.
[15] Li S, Mou X. On the security of a chaotic encryption scheme: problems with computerized chaos in finite computing precision. Comput Phys Commun 2003;153:52–8.
[16] Gonzalez JA, Pino R. Chaotic and stochastic functions. Physica 2000;76:425–40.
[17] Li C. An image encryption algorithm based on random key and quasi-standard map. Chin J Comput 2003;26(4):465–9 [in Chinese].
[18] Kohda T. Information sources using chaotic dynamics. Proc IEEE 2002;90(5):641–61.
[19] Qiu Y, He C. Construction and analysis of one class chaotic running key generator. J Shanghai Jiaotong Univ 2002;136(3):344–7 [in Chinese].
[20] Li H, Feng D. Composite discrete chaotic dynamical systems and keyed hash functions. Chin J Comput 2003;26(4):460–4 [in Chinese].
[21] Götz M, Kelber K. Discrete-time chaotic encryption system—part I: statistical design approach. IEEE Trans Circ Syst—I 1997;44(10):963–70.