2011 International Conference on Computer Communication and Management
Proc .of CSIT vol.5 (2011) © (2011) IACSIT Press, Singapore

A Novel Encryption Algorithm for Transmitting Secure Data based on Genetic Hyper Chaos Map

Seyyed Mohammad Reza Farshchi[*,1], Iman Dehghan Ebrahimi [2]

[1]Department of Artificial Intelligence, Islamic Azad University, Mashhad Branch. *Shiveex@Gmail.Com*
[2]Department of Imaging Science & Lab, Islamic Azad University, Mashhad Branch. *Ivi.uni@Gmail.Com*

Abstract. A new color image encryption algorithm based on chaos genetic algorithm and control parameter chaotic map is proposed in this paper. Four chaotic sequences are generated from a 4D hyper chaos. To increase the security of the cryptosystem, Tent map is used to produce the control parameter, and the cubic map is used to get the chaotic sequence to produce the number of iterations. Performance analysis show that the proposed scheme achieve large key space, good statistical character, and can against brute-force attack, differential attack and entropy attack efficiently. The scheme possesses good performance in encryption/encryption speed and is suitable for real-time image encryption and transmission.

Keywords: image encryption, genetic algorithm, chaos encryption, stream cipher.

1. Introduction

A bulk of digital visual data is being stored on different media and exchanged over various sorts of networks nowadays. Often, these visual data contain private or confidential information or are associated with financial interests. As a consequence, techniques are required to provide security functionalities like privacy, integrity, or authentication especially suited for these data types. Besides watermarking, steganography, and techniques for assessing data integrity and authenticity, providing confidentiality and privacy for visual data is among the most important topics in the area of multimedia security.

Genetic Algorithm (GA) is applied to search for the optimal subset of eigen vectors. But GA has some disadvantages such as inclination to becoming premature convergence and low efficiency. To overcome the shortcomings, reference [3] proposed the chaos genetic algorithm which uses logistic map to generate the initial population; however, it still can't maintain diversity of the population in some complicated cases. In other research, like as [4] the author proposed two image encryption based on chaotic maps, the shuffling procedure is combined with pixel diffusion, similar to the structure of DES. The security of the schemes against brute force attack, statistical attack, known-plain text attack and chosen plain text attack are analysed in [4]. And a block cipher based on a suitable use of the chaotic standard map is proposed in [5]. In 2007, a chaotic stream cipher and is proposed and used in video protection in [7]. In 2008, K. W. Wong proposed a cryptosystems with the structure of multiple rounds of substitution and diffusion. And a certain diffusion effect is introduced in the substitution stage by simple sequential add-and-shift operations. Although this leads to a longer processing time in a single round, the overall encryption time is reduced as fewer rounds are required.

Based on these above existing encryption algorithm, a new image encryption algorithm based on the chaos optimization algorithm (COA), genetic algorithm (GA), and control parameter chaotic map was proposed, That combines with the strong global searching capability of the GA and the powerful local controllable searching capability of the COA. The cryptosystem with three chaotic maps, Logistic map is used to produce the chaotic sequence to replace the control parameter, and the Cubic map is used to produce the number of iterations to get the stream cipher. In this paper we introduce a chaotic mutation operator in the mutation of the excellent individuals in order to avoid the search being trapped in local optimum. The two kinds of chaotic mappings increase the diversity of population and expand the scope of the search.

Theoretical analysis and numerical simulations confirmed the feasibility and the superiority of the scheme in practical application.

The rest of the paper is organized as follows. In section II we describe the encryption algorithm in detail. Then, in section III we realize the simulations of the algorithm in computer. Finally, main conclusions are given in section IV.

2. The Proposed Chaos Genetic Algorithm

Chaos is a kind of certainty, irregular process in nonlinear system. It is definite in the short term, but it is unpredictable in the long term because of its sensitivity to the initial value. The process is neither cycle nor convergence and it is very sensitive to the initial value. This paper uses a combination of Logistic and Henon maps to generate chaos sequences to enhance the safety of the encryption algorithm. The Logistic System [2]:

$$x_{n+1} = \mu x_n (1 - x_n) \tag{1}$$

Where μ is a system parameter, When μ ∈ (3.569945, 4], the sequence x_n generated by discrete chaos system with the initial value $x \in (0,1)$ are non-cycle, non-convergence, not related, and it is very sensitive to the initial value.

By using these characteristics, a chaos optimization algorithm (COA) was proposed [6] that can solve complex function optimization and have a high efficiency of calculation.

Tent map [17] is the simplest kind of one-dimensional chaotic mapping, which is defined as:

$$x_{n+1} = \begin{cases} x_k / a, x \in [0, a] \\ (1 - x_k)/(1 - a), \ x \in (a, 1] \end{cases} \tag{2}$$

When $0 < a < 1, 0 \le x_0 \le 1$ the system is in a chaotic state and the mean of chaotic sequence is 0.5. In this paper, we take a =0.4. When the logistic map and tent map are respectively iterated for 10 000 times, the initial value of x_0 is 0.345.

2.1. Control the Parameters of Chaotic Map

A class of control parameter chaotic map with invariant measure can be shown as follows [7]:

$$\phi_n(x, a) = \frac{a^2 (1 + F(N, x))}{(a^2 + 1) + (a^2 - 1) F(N, x)} \tag{3}$$

Where $F(n, x)$ = cos (2N arccos $\sqrt{x}$), α is the control parameter. Obviously, $F(n, x) \in [0,1]$ and $\phi_2(x, \alpha) \in [0,1]$.

When N is 2 or 3, the bifurcation diagram of $\phi_2(x, \alpha)$ and $\phi_3(x, \alpha)$ is shown in Figs. 1 and 2 respectively.

It can be seen that for $0 < \alpha < 1$, $\phi_2(x, a)$ is ergodic and for $2 < \alpha < \infty$, it has a stable fixed point at x=1. For $1/3 < \alpha < 3$, $\phi_3(x, \alpha)$ is ergodic and for $0 < \alpha < 1/3$, it has a stable fixed point at x=0, while for $3 < \alpha < \infty$, it has a stable fixed point at x=1. It is shown that the control parameter chaotic map does not undergo period-doubling bifurcation to chaos. We use $\phi_2(x, a)$ for an example to study the encryption algorithm based on control parameter chaotic map in the subsequent parts of this article.

The sensitivity of $\phi_2(x, a)$ to control parameter and initial value is investigated. When the initial value is the same, α is 0.400000000001 or 0.4 respectively. It proved [4] that when n=35~40, the two chaotic sequence can be considered different completely.

2.2. Improved Chaos Genetic Algorithm

GA has some disadvantages in solving complex problems, such as inclination to becoming premature convergence and low efficiency. To overcome the shortcomings, we propose chaos genetic algorithm based on two kinds of chaotic mappings. This algorithm is improved from the following aspects:

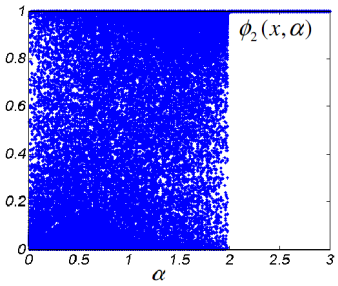

Fig. 1. Bifurcation diagram of $\phi_2(x, a)$

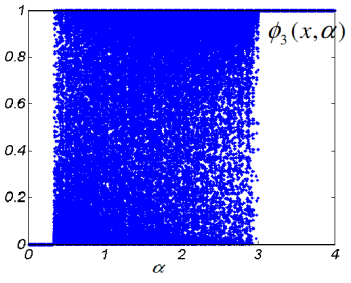

Fig. 2. Bifurcation diagram of $\phi_3(x,\alpha)$

1) *Using the tent map to generate the initial population:* Standard genetic algorithm commonly adopted random approach to generate initial population. However, these individuals may be unevenly distributed and away from optimal solution. This limits the algorithmic efficiency. Therefore we use tent map to generate well-distributed chaotic variables, and then translate the chaotic variables into the binary encoding to obtain initial population. This will improve the quality of initial population and calculated efficiency. The main process as follows:

The D initial values of small difference $x_{01}, x_{02,}, ..., x_{0D}$ are endowed in (3). It will generate D hyper chaotic variables $x_{ki} = \{x_{ki}, i = 1,2,..., D\}$ of different contrail. And then D chaotic variables are translated into binary encoding by the following equation:

$$f(x) = \begin{cases} 1, & x \geq 0.5 \\ 0, & x < 0.5 \end{cases} \tag{4}$$

We can obtain k binary strings of length D. For fixed k, $S_k = \{f(x_{k1}), f(x_{k2}), ..., f(x_{kD})\}$ represents a feasible solution, which corresponds to an individual.

2) *The chaotic mutation of excellent individuals:* In the evolution process, logistic map is introduced into some individuals with higher fitness value and then process chaotic mutation in the population. Chaotic mutation is an effective operator to increase and maintain the diversity of population, and is meanwhile an efficient method to avoid falling into local optimum solution and to overcome the premature convergence. The chaotic mutation designed in this paper uses the relatively large probability of logistic map in interval [0.9, 1], and the main process as follows:

a) *Degenerate the individuals and obtain chaotic variables*: Suppose the individual $X_i = x_{i1}, x_{i2}, ..., x_{iD}, x_{ij}$ equal to 0 or 1, as the excellent individual of a generation in evolution, we degrade the individual according to (5) and then obtain chaotic variables $T_i = t_{i1}, t_{i2}, ..., t_{iD}$.

$$t(x_{ij}) = \begin{cases} rand \times 0.085 + 0.9, & x_{ij} = 1 \\ rand \times 0.085 + 0.4, & x_{ij} = 0 \end{cases} \tag{5}$$

b) *Chaotic disturbance*: Using the logistic map to generate D chaotic variables $x_{k1}, x_{k2}, ..., x_{kD}$ and each of these is imposed on each component of T_i according to (6):

$$t^*_{k,j} = t_{ij} + \alpha\mu_{kj} \qquad 1 \leq j \leq D \tag{6}$$

Where k is the iterations; α is the adjusting coefficient, normally chosen as a small positive constant, here, α=0.025.

2.3. Stream Cipher Encryption Algorithm

Suppose the original image is $M_{m\times n}$, initially the plain text is transformed into $M_{(m\times n)\times 1}$, and let $h = m \times n$. The encryption algorithm can be described as follows. Firstly, starting from genetic chaos map as described in previous section. Let the control parameter $\alpha_i = 2y_i (i = 1,2,..., h)$, obviously, it is a chaotic sequence. Secondly, from the cubic map we have:

$$z_{n+1} = \lambda z_n (1 - z_n^2), \ \lambda = 2.59, \ z_i \in [0,1] \tag{7}$$

We get the number of iterations by the following equation:

$$m_i = 3 + round(h \times z_i) \bmod 30, \ i = 1,2,..., h. \tag{8}$$

Thirdly, from an initial value $x_0 \in [0, 1]$, using the parameter α_i iterate the control parameter chaotic map m_i times, we get the chaotic key stream $k_i, i = 1,2,...,h.$ The rest parameters are obvious in cryptosystem. The encryption function is defined as:

$$C_i = (\lfloor k_i \times 10^{14} \rfloor + P_i) \bmod 256 \tag{9}$$

The decryption process is similar to the encryption one. After get the same key stream as the encryption algorithm, the decryption function is defined as:

$$P_i = (C_i - \lfloor k_i \times 10^{14} \rfloor) \bmod 256 \tag{10}$$

Our cryptosystem employed three chaotic maps. Through make the control parameter and the number of iterations varying with the chaotic map each, the chaotic key stream produced by the control parameter chaotic map seems enhance security highly. Some other measures such as one-time pad and embedded the length of plain text in the encryption algorithm increase the difficult to attack also.

3. Experimental Analysis

Some experimental results are given to demonstrate the efficiency of our scheme which is based on control parameter chaotic map. A grey-scale image of 'lena.tif' sized 269×279 (see Fig. 3(a)) is used as a plain image and the encryption of this image is shown in Fig. 3(b), and Fig. 3(c) is the correct decryption image. We have used a personal computer with a CPU is Pentium-IV 2.4GHz, 512MB memory and 80GB hard-disk capacity, realized in MATLAB 7.0. The average encryption /decryption speed is 6.63M bits per second. To increase the speed of encryption/decryption more, one can generate the key stream off-line, thus the algorithm can be used to the real-time encrypt and transmit of information.

The cipher text has the same size as the plain text due to the cryptosystem maps bring about a one-to-one correspondence between them. The grey-scale histogram is shown in Fig. 4. The histogram of the encrypted image is nearly uniformly distributed, which makes statistical attacks difficult.

1) *Key spaces:* A good encryption scheme should be sensitive to the secret keys, and the key space should be large enough to make brute-force attacks infeasible. The secret keys of the proposed encryption algorithm consist of the parameters of (1-7) and related to the Intermediate ciphered text.

Fig. 5. shows the deciphered result of original image with the proposed algorithm with $\alpha_1 = 0.4000000000000001$, Although there is deviation of only 10-15, the original image cannot be restored. If the attacker adopts cipher text-only attack, in order to obtain the original image, he must search for a large volume of secret keys. Table.1. shows the estimation results of the secret key space, which indicates that the key space is large enough to resist brute-force attacks. The experimental results also demonstrate that our scheme is very sensitive to the secret key mismatch.

2) *Information Entropy:* Information Entropy can measure the distribution of the pixel values. The more even distribution of the pixel values of the image, the greater the image information entropy is. Only if all the pixel values of the image have the same probability, the greatest the Information Entropy is. The expression of Information Entropy is described as following:

$$H(x) = \sum p(x_i) \log_2^{p(x_i)} \tag{11}$$

In (11), x is a random variable, $p(x_i)$ is the probability of occurrence of x_i, it means the pixel value. We can calculate the Information Entropy of the image according (11), Table.2. Shows the Information Entropy contrast of 10 group's original and ciphered images. We can see that the mean Information Entropy after encrypted is 7.99902, which is so close to the theoretical maximum 8 (2^8=256).

4. Conclusion

A color image encryption algorithm based on hyper genetic chaos map is proposed in this paper. Four chaotic sequences are generated from a 4D hyper chaos. The R,G, B channels of plain image are firstly encrypted respectively according to the former three sequences with inter cross cipher-block chaining mode; then the encrypted image is permuted by choosing different channels. After several rounds of encryption, the cipher image is obtained. Experimental results indicated that: (1) the character of the Chaos systems makes the algorithm easy to be implemented, sensitive to the initial value with an excellent encryption outcome; (2)

The possible secret keys of the algorithm are of large number so that it is impossible to decrypt by exhaustion method. To conclude, the algorithm is shown to be a good candidate for the security of transferring the secure message on common medium such as Internet.

Fig. 3. The first row from left to right, a) original image and b) encrypted image. The bottom row from left to right: a) correct decrypted image and b) incorrect decrypted image

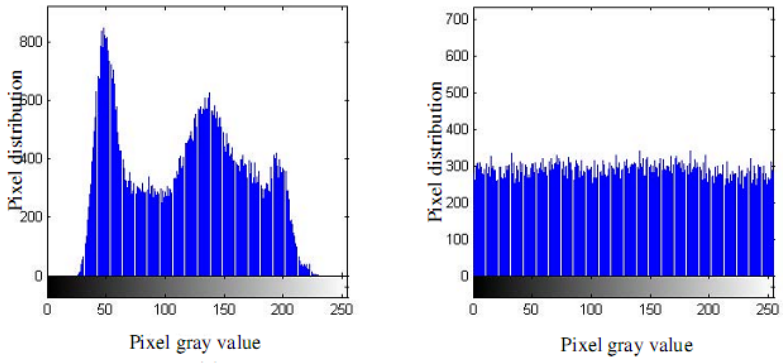

Fig. 4. from left to right, a) Histogram of plain image and b) Histogram of ciphered image

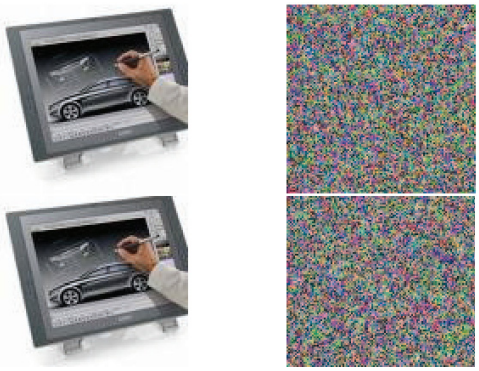

Fig. 5. The first row from left to right, a) original image and b) encrypted image. The bottom row from left to right: a) correct decrypted image and b) incorrect decrypted image

TABLE I. The estimation of secret key space

secret key	*range*	*size*
μ_1, μ_2	(3.57, 4]	0.86×10^{15}
α	(0, 1)	1×10^{14}
t	[1, 128]	0.86×10^{14}

TABLE II. The information entropy of 10 groups original and ciphered images

Group	$H_{ciphered}$	$H_{original}$	Group	$H_{ciphered}$	$H_{original}$
1st	7.9987	6.9773	6th	7.9992	7.6784
2nd	7.9991	7.5142	7th	7.9997	7.1502
3rd	7.9991	7.3486	8th	7.9899	7.3436
4th	7.9989	7.6293	9th	7.9989	7.7277
5th	7.999	7.5488	10th	7.9998	6.9519

5. References

[1] E. R. Davies. *Machine Vision. Theory, Algorithms, Practicalities*. San Francisco: Morgan Kaufmann , 2005.

[2] A.N. Pisarchik and M. Zanin. Image encryption with chaotically coupled chaotic maps. *Physica D*, 2008, **237**(1): 2638-2648.

[3] M.S.Baptista. Cryptography with Chaos. *Phys. Lett. A*. 1998, **240** (1): 50-54.

[4] S. G. Lian, J. S. Sun, Z. Q. Wang. A block cipher based on a suitable use of the chaotic standard map. *Chaos, solitons and Fractals*. 2005, **26** (1): 117-129.

[5] K. W. Wong, B. S. H. Kwok, W. S. Law. A fast image encryption scheme based on chaotic standard map. *Physics Letters A*, 2008, **372** (1): 2645–2652.

[6] H.S. Kwok and W.K.S. Tang. a fast image encryption system based on chaotic maps with finite precision represention. *Chaos Solitons Fractals*. 2007, **32** (1): 1518-1529.

[7] N.F. Johnson, Z. Duric, and S. Jajodia. *Information Hiding: Steganography and Watermarking — Attacks and Counter-Measures*. Kluwer Academic Publishers, 2000. Available at http://www.jjtc.com/Steganography/.

[8] S. S. Agaian, B. M. Rodriguez and J. P. Perez. Palette-based steganography used for secure digital image archiving. *IS&T Archiving Conference*, 2005.