Hindawi Publishing Corporation
International Journal of Optics
Volume 2016, Article ID 2053724, 14 pages
http://dx.doi.org/10.1155/2016/2053724

Research Article

Digital Image Encryption Algorithm Design Based on Genetic Hyperchaos

Jian Wang[1,2,3]

[1] *Graduate School, Yanshan University, Qinhuangdao 066004, China*
[2] *School of Information Science and Engineering, Yanshan University, Qinhuangdao 066004, China*
[3] *The First Hospital of Qinhuangdao, Qinhuangdao 066000, China*

Correspondence should be addressed to Jian Wang; dupeng198510@163.com

Received 10 December 2015; Revised 26 February 2016; Accepted 10 May 2016

Academic Editor: Chenggen Quan

In view of the present chaotic image encryption algorithm based on scrambling (diffusion is vulnerable to choosing plaintext (ciphertext) attack in the process of pixel position scrambling), we put forward a image encryption algorithm based on genetic super chaotic system. The algorithm, by introducing clear feedback to the process of scrambling, makes the scrambling effect related to the initial chaos sequence and the clear text itself; it has realized the image features and the organic fusion of encryption algorithm. By introduction in the process of diffusion to encrypt plaintext feedback mechanism, it improves sensitivity of plaintext, algorithm selection plaintext, and ciphertext attack resistance. At the same time, it also makes full use of the characteristics of image information. Finally, experimental simulation and theoretical analysis show that our proposed algorithm can not only effectively resist plaintext (ciphertext) attack, statistical attack, and information entropy attack but also effectively improve the efficiency of image encryption, which is a relatively secure and effective way of image communication.

1. Introduction

With the rapid development of Internet technology and information technology, digital communication is more and broader: people can release on the Internet all kinds of information anytime and anywhere. Digital image is the most intuitive, visual, and abundant information carrier, due to its convenience, speed, lack of geographical restrictions, low cost, high efficiency, and so forth; it has been more widely used and has become one of the main information network era expressions. However, people enjoy all sorts of convenience brought about by the digital image but also face some difficult security problems, such as personal privacy protection, business and military information protection, and electronic products illegal copying and dissemination. So how to protect digital image in the transmission process has become the focus of the industry.

In order to protect security of images which contain data and information, we use the original image that is encrypted to resolve the security hidden danger, so the image encryption research has become a hot research topic in the field of image analysis and processing. In general, the conventional image encryption mainly has image encryption in the spatial domain, transform domain of image encryption, image encryption based on neural network and based on chaotic image encryption. Spatial domain image encryption basically has the following two ways: one is scrambling by changing the position relationship of each image's pixels [1]. The other is to use certain encryption rules that change the pixel values of the original image and make the information entropy close to the maximum, namely, information entropy encryption [2]. Image scrambling encryption scheme is mainly used in digital image security process of pretreatment and posttreatment stage, so as to further guarantee the security of information contained in image; it can be used as a special digital image encryption method, but it is vulnerable to be attacked just by image scrambling encryption by statistical analysis; it cannot solve the information contained in the original image security problems. Image replacement and diffusion both change the relevance of the original image, making the information entropy change. And image diffusion is based on image correlation transformation among adjacent pixels according to certain rules, but it may cause some image information loss. Transform domain image encryption is mainly through some sort of orthogonal transformation on the image; then, it is encrypted when it is coding processing. Like image encryption based on tree structure [3] and image encryption based on SCAN language [4], these image encryption schemes involve the problem of how to generate pseudorandom sequences; now the problem has no good solution. By using neural network with the parallel distributed processing, highly nonlinear association memory [5], and other characteristics, to encrypt the image information, we call it artificial neural network image encryption. But the neural network needs a lot of neurons data to encrypt, because it cannot be adaptive to generate neural networks, then increases complexity of encryption, and reduces efficiency of encryption. In order to solve this problem, the related research scholars put forward using chaos theory to encrypt digital image, because the chaos theory [6] is sensitive to initial conditions and system parameters extremely, randomness of trajectory, pseudorandomness and ergodicity, and other special complex dynamics properties, making it very suitable for digital image encryption, forming a kind of chaotic image encryption algorithm. For example, Fridrich in 1998 for the first time introduced chaos theory as digital image encryption and put forward the two-dimensional Baker map image encryption [7] for image scrambling operation and then extended it to 3d. Due to 3d, Baker map image encryption efficiency is low, so Chen et al. put forward 3d Baker map [8] fast image encryption algorithm, which makes the security of encryption and efficiency improve to a certain extent. In [9], a standard map image encryption algorithm is proposed; then Wong et al. proposed on the basis of Baptista algorithm an improved fast image encryption algorithm [10]. At the same time, the document [11–17] was also, respectively, proposed by using Logistic mapping, Tent, Lorenz system, and one-way coupled map lattice, such as a variety of chaotic mapping algorithm for digital image encryption. Though these chaotic image encryption algorithms to a certain extent improve the security performance, but due to the varying complex degrees of the image, causing them to fail to solve the problem of encryption efficiency, it well often fail to solve the problem of security threats to a certain extent.

But genetic algorithm (GA) [18, 19] may solve this problem which provides a feasible technical way. Genetic algorithm is proposed by Holland of Michigan university in the United States [18] in the 1960s, and then in the late 80s Goldberg [19] summarized the basis of predecessors' research, finally forming the basic theoretical framework of genetic algorithm. Genetic algorithm is a new global optimization search algorithm, because it has the characteristics of group search technology; it can represent a set of solutions using the population and then through the operation of the selection, crossover and mutation of species, and so on finally gets a new generation of population, so that gradually makes the population evolution to the optimal solution or near optimal solution evolving, getting the best state of population. Because optimization constraints are less and objective function and constraint condition requirements are low, its actual operation is simple and practical, suitable for optimization. At the same time, its search is in the whole solution space and also is most likely to look for an optimal solution or approximate optimal solution; because it has such advantages, it is widely applied to aviation system [20], machine learning [21], pattern recognition [22], and so forth.

To this end, in this paper, we propose a new image encryption algorithm, which uses genetic algorithm optimization features and pseudorandomness and ergodicity of chaotic theory to solve the image features such as encryption of security threats and inefficiencies. First it goes through the chaos theory of image encryption, in the encryption process, using the genetic algorithm to carry out adaptive optimization on encryption process design parameters and then get the best encryption parameters, so that it will solve the problem of encryption security threats and inefficiencies, to achieve efficient, reliable, and secure encrypted image. Experimental analysis shows that this method not only can solve the problem of security threats, which improves the security performance, and can solve the problem of encryption efficiency but also greatly improves the efficiency of encryption, namely, to realize image encryption effect and receive a significant boost in performance.

2. The Basic Principle of Genetic Algorithm

2.1. The Basic Concept of Genetic Algorithm and Steps. Genetic algorithm is different from traditional search algorithm; it first randomly generates a set of initial solutions, namely, "population," where each individual in population, namely, a solution vector, which is called "chromosomes," begins the search process. These chromosomes evolve in the subsequent iterations and generate the next generation of chromosomes, called "offspring". The stand or fall of chromosomes in each generation through chromosome "fitness" is evaluated: a chromosome of higher fitness is more likely to be selected; instead, the possibility of fitness small chromosome which is selected is smaller, the selected chromosome by cross-generating (crossover and mutation) new chromosomes, "offspring." It passes through several generations, the algorithm converges to the best chromosome, and the chromosomes are likely to be the optimal solution of the problem or approximate optimal solution. The operation of the genetic algorithm steps is shown as follows:

(1) Randomly generate initial population pop(k).

(2) Go through fitness function to evaluate the chromosomes.

(3) Select chromosomes according to the fitness level and form a new population.

(4) Go through crossover and mutation operation which produces new chromosomes that *offspring*.

(5) Repeat steps (2)–(4), until getting the scheduled evolution algebra.

This method is shown in Figure 1; it is shown that the genetic algorithm is mainly composed of genetic operators

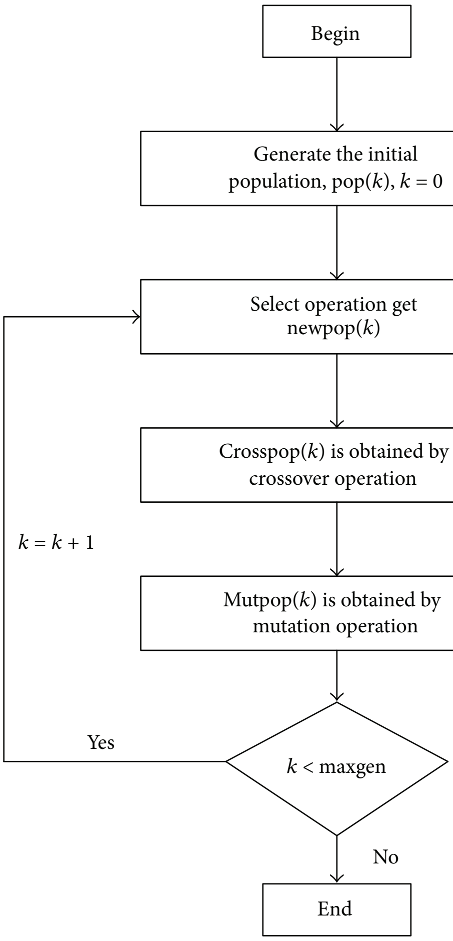

Begin
Generate the initial population, pop(k), $k = 0$
Select operation get newpop(k)
Crosspop(k) is obtained by crossover operation
Mutpop(k) is obtained by mutation operation
$k < \text{maxgen}$
Yes
No
$k = k + 1$
End

Figure 1: The flow chart of genetic algorithm iteration.

(crossover and mutation) and evolutionary computing (select). Genetic algorithm simulates the natural evolution of species turnover mechanism; it generates a new species to reach the purpose of searching the global optimal solution. Its evolutionary computation is through the competition mechanism constantly updating population process.

Crossover operation is the main genetic algorithm; the performance of genetic algorithm depends largely on the performance of its adopted crossover operation. Crossover operation operates the two chromosomes at the same time, combining the two features to produce new offspring. Variation is a basic operation; it spontaneously generates random variation on chromosome. Variation can offer gene which is not contained in the initial population or find missing gene in the selection process, providing new content for population.

2.2. The Application Design of Genetic Algorithm Design

2.2.1. Encoding Problem. Genetic algorithm through genetic operators (crossover and mutation) restructures individual in the population; by selecting operation, it constantly optimizes the individual structure and searches the optimal structure of the individual and, finally, achieves the goal of becoming closer to problem of the optimal solution. It can be seen that the genetic algorithm is the process of alternating work in the coding space and solution space and its genetic operation on chromosome in the coding, and it evaluates and chooses the solution in the solution space. The bridge between them is the encoding and decoding. Code is converting the solution of the problem space to variable chromosome of genetic space. On the contrary, the decoding is the operation where the chromosome coding is mapped in the problem space. The relationship between them is shown in Figure 2.

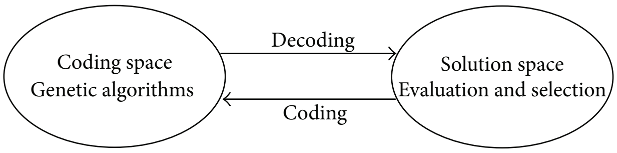


Figure 2: Coding space and solution space.

The original genetic algorithm uses the Holland coding scheme, namely, binary code. But for the application of many genetic algorithms, such as multidimensional, high accuracy algorithms, especially in the optimization of complex system, the simple encoding method shows many drawbacks: it cannot directly reflect the structure of the requirement problem To the problem of large range and high precision, the chromosome length and the length of the search space will be very big; such genetic search is very difficult. Adjacent binary code may have larger Hamming distance, so as to make the search efficiency of genetic operators reduced.

Selecting an appropriate coding method is the basis of genetic algorithm to solve practical problems. For the problem of any application, coding must consider the following aspects:

(1) *Completeness*. All the points (candidates) in the problem space can be used as genetic points (chromosome) in genetic space for performance.

(2) *Integrity*. The genetic space chromosome corresponds to all the problems of candidate solution space.

(3) *Nonredundancy*. Chromosomes and the candidate solution are in a one-to-one relationship.

One of the problems we know of is that it is difficult to design the coding scheme that could satisfy the requirement of the above three aspects at the same time, but these designs must meet the requirements of completeness.

2.2.2. Fitness Function. In the evolution process genetic algorithm, the stand or fall of chromosome is evaluated by a fitness function; the fitness function value is the basis for the selection operation. For theoretical analysis of convenience, it is best to guarantee the fitness function value is nonnegative; proper transformation must be adapted to the value of the negative. The relationship between the objective function and fitness function is different according to the optimization problem categories. Optimization problem was divided into two categories, a class of global maximum values for the objective function and another for the objective function of the global minimum. For these two kinds of optimization problem, a certain point of the objective function in the solution space converts to the fitness function of corresponding individual in search space, shown as follows.

For the problem of the maximum, one has the following:

$$F(X) = \begin{cases} f(X) + C_{\min}, & \text{if } f(X) + C_{\min} > 0 \\ 0, & \text{if } f(X) + C_{\min} \leq 0, \end{cases} \quad (1)$$

where $C_{\min}$ is an appropriate number of relatively small value.

The problem of the minimum is shown as follows:

$$F(X) = \begin{cases} C_{\max} - f(X), & \text{if } f(X) < C_{\max} \\ 0, & \text{if } f(X) \geq C_{\min}, \end{cases} \quad (2)$$

where $C_{\max}$ is an appropriate number of relatively big value.

The mapping relationship formula between the objective function and fitness function has other forms. Objective function converting into fitness function normally needs to follow two principles: (1) the objective function in the optimization process of the optimization direction (e.g., seeking the maximum or minimum value of the objective function) and in the process of population evolution fitness function value is increasing is in the same direction; (2) fitness function value must be greater than or equal to zero. In practical problems, we adopt the kind of conversion form according to the specific circumstances.

2.2.3. Selection Problem. Select operation is the direct driving force of evolution. Selection pressure is an implicit rule, where pressure is too large; the search will be prematurely terminated; Pressure is too small as the search will be very slow. Options include three basic aspects: sample space, the sampling mechanism, and selection probability.

(1) Sample Space. The size and the constitution of the sample space constitute the sample space. The sample space is divided into two: the regulatory sample space and the expanding sample space.

Put *popsize* as the size of the population and *popsize* 1 as the offspring size after crossover and mutation; the regulatory sample space which is to keep the population size remains the same. The choice diagram based on regulatory sample space is shown in Figure 3.

The expanding sample space is *popsize* + *popsize* 1; namely, sampling space includes all parents and offspring. Figure 4 depicts the choice diagram based on expanding sampling space. The most distinguishing feature of the expanding sample space is effective limiting the random fluctuation caused by high crossover rate and mutation rate.

(2) Sampling Mechanism. Sampling mechanism is a theory on how to choose the chromosomes from sampling space theory. The selection of individual species in principle can be divided into three types: random sampling, determined sampling, and mixed sampling.

(3) Select Probability. Holland's original roulette algorithm adopted by the genetic algorithm is a kind of proportional selection method; selection probability is proportional to the chromosome's fitness.

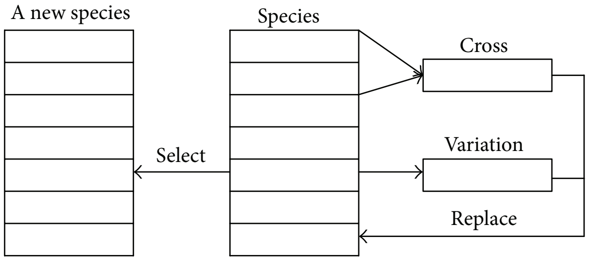


Figure 3: The choice diagram based on regulatory sample space.

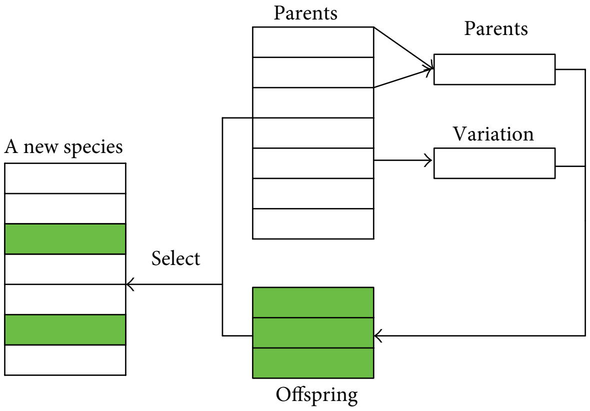


Figure 4: The choice diagram based on the expanding sampling space.

2.2.4. Crossover Operation. Crossover operation is the most important genetic operation; the population by cross generates new chromosomes and constantly expands the search space, finally achieving the goal of global search.

2.2.5. Mutation Operation. Mutation operation is changing some genes points of chromosome string.

2.2.6. The Selection of Main Parameters. Parameters in the genetic algorithm design mainly include population size, crossover rate, mutation rate, and evolution algebra. In addition, when choosing a specific operator, sometimes it involves the selecting of the parameters related with operator. The selection of genetic algorithm parameters is reasonable or does not directly relate to the convergence speed and accuracy of the algorithm. However, because there are many factors which can affect the parameter selection, some relate to the problem itself of connotation of objective laws and some relate to the selection operator, so it is difficult to find common rules.

(1) Population Size. Population size is the first parameter of genetic algorithm that needs to be determined; it is the main influencing factor in a local solution of the algorithm.

(2) Cross Rate. Cross rate is the main genetic algorithm; the performance of genetic algorithm depends largely on adopted crossover operator performance and the size of the cross rate.

Table 1: Genetic algorithm (GA) trial scope commonly used parameters.

Trial parameters	Population size	Crossover probability	Mutation probability	The biggest evolution algebra
Trial parameters	20–100	0.4–0.9	0.00001–0.1	50–1000

(3) Mutation Rate. Mutation rate refers to the number of the gene variations in a population accounting for the percentage of the total number of genes.

(4) Evolution Termination Conditions. Termination conditions can be controlled from two aspects: preset evolution algebra or control according to the evolution of the population. The evolution of population refers to the relationship between the current generation of maximum adaptation and the population average fitness. The evolution of termination conditions is decided according to specific circumstances.

The common value range of main operation parameters of genetic algorithm is shown in Table 1.

2.2.7. Handling of Illegal Individual Strategy. We usually obtain infeasible offspring when using genetic algorithm on chromosomes, so the core of the solution of nonlinear programming problem using the genetic algorithm is how to meet the problem of constraint. It can be used to reject and fix penalty policy for processing.

3. Hyperchaos Algorithm Basic Principle

3.1. The Definition of Chaos. We assume there exist continuous mappings in the interval I; if it meets the following conditions, then the mapping is called chaotic.

(1) f is the cycle without upper bound.

(2) On the closed interval I, there is uncountable subset S, and it can meet the following conditions:

(i) $\forall x, y \in S, x \neq y, \lim_{n\to\infty} \sup |f^n(x) - f^n(y)| > 0$.

(ii) $\forall x, y \in S, \lim_{n\to\infty} \inf |f^n(x) - f^n(y)| = 0$.

(iii) $\forall x \in S$ and f in any cycle point y, it get $\lim_{n\to\infty} \sup |f^n(x) - f^n(y)| > 0$.

3.2. Hyperchaotic System. Hyperchaos system is described using the following equation:

$$\begin{aligned} x_1 &= a(x_2 - x_1) + x_4 \\ x_2 &= dx_1 - x_1x_3 + cx_2 \\ x_3 &= x_1x_2 - bx_3 \\ x_4 &= x_2x_3 + rx_4, \end{aligned} \tag{3}$$

where a, b, c, d, and r are the control parameters, often taking $a = 35$, $b = 3$, $c = 12$, $d = 7$, under the condition of r in the following range: $[0, 0.085]$, $(0.085, 0.798]$, $(0.798, 0.90]$, the system of chaotic motion, chaotic motion, and periodic motion [23].

4. A Digital Image Encryption Algorithm Based on Genetic Hyperchaos System

4.1. Hyperchaos Randomly Generated Initial Population. The Logistic map gives m different initial values in the model; chaotic variables x_i, $i = 1, 2, \ldots, m$, m a different trajectory, according to formula (4), will make m a chaotic variable, respectively, mapped to the optimization variables within the scope of making it into a chaotic variable $x^*_{n_i}$:

$$x^*_{n_i} = a_i + (b_i - a_i)\, x_{n_i}. \tag{4}$$

Fixed $n, x^*_k = [x^*_{k,1}, x^*_{k,2}, \ldots, x^*_{k,m}]$ represents a feasible solution. Each feasible solution to calculate the fitness chooses fitness of high N individual initial population. In the process of chaos generation of initial population, chaotic sequence should take enough number of iterations (average value is 400), that is, to ensure that chaotic variables can adequately be traversal.

4.2. Pixel Position Scrambling. Advantages of the characteristics of digital image with digital array are as follows: it is used to analyze the image matrix step finite elementary matrix transformation and disturb the arrangement of image pixel position into a chaotic image and it is impossible to identify the purpose of the original image, which has the effect of image encryption.

Assume that the size of $M \times N$ of the original image $P_{M\times N}$ pixels matrix is expressed as

$$P_{M\times N} = \begin{pmatrix} p_1 & p_2 & \cdots & p_N \\ \cdots & \cdots & \cdots & \cdots \\ p_{N(M-1)+1} & \cdots & \cdots & p_{MN} \end{pmatrix}. \tag{5}$$

Specific steps are as follows.

(1) The Line Displacement. Transform matrix $P_{M\times N}$ according to the line for the row vector form is

$$P_{M\times N} = \left(\overbrace{p_1 p_2 \cdots p_{MN/k}}^{P_1} \underbrace{p_{MN/k+1} \cdots p_{2MN/k}}_{P_2} \overbrace{p_{2MN/k+1} \cdots p_{3MN/k}}^{P_3} \cdots \underbrace{p_{(k-1)MN/k+1} \cdots p_{MN}}_{P_k} \right). \tag{6}$$

Among them, the k in the parallel system is defined as the number of processors; number of k is defined as a group in a serial system, so each child vector, respectively, is

$$\begin{aligned} P_1 &= \left(p_1 p_2 \cdots p_{MN/k}\right), \\ P_2 &= \left(p_{MN/k+1} \cdots p_{2MN/k}\right), \\ P_3 &= \left(p_{2MN/k+1} \cdots p_{3MN/k}\right), \\ P_k &= \left(p_{(k-1)MN/k+1} \cdots p_{MN}\right). \end{aligned} \tag{7}$$

Using Runge-Kutta algorithm will cause hyperchaos of the system iterations N times, which is used to prevent the transition effect. For a given system, the number of iterations N may be associated with initial conditions and system parameters, $N = 200$ iterations before we throw away the data; then, we calculate

$$r_k = \operatorname{mod}\left(\left(\operatorname{abs}\left(x_k\right) - \operatorname{floor}\left(\operatorname{abs}\left(x_k\right)\right)\right) \times 10^{14}, \frac{MN}{k}\right) + 1. \tag{8}$$

Obviously, $r_k \in [1, MN/k]$. Iteration continues until this chaotic system produces MN/k completely different fairly r_k values. It is denoted by $\{r_k(i),\ i = 1, \ldots, MN/k\}$. Based on fairly r_k scrambling for vector P_k, we have

$$P_k^r(i) = P_k\left(r_k(i)\right), \tag{9}$$

after row scrambling matrix is expressed as P^r.

(2) Replacement. It converts line displacement matrix P^r according to the column to row vector form as

$$P^r_{M\times N} = \left(\overbrace{p_1^r p_2^r \cdots p^r_{MN/k}}^{P_1^r}\ \underbrace{p^r_{MN/k+1} \cdots p^r_{2MN/k}}_{P_2^r}\ \overbrace{p^r_{2MN/k+1} \cdots p^r_{3MN/k}}^{P_3^r} \cdots \underbrace{p^r_{(k-1)MN/k+1} \cdots p^r_{MN}}_{P_k^r}\right). \tag{10}$$

Among them, each child vector, respectively, is

$$\begin{aligned} P_1^r &= p_1^r p_2^r \cdots p^r_{MN/k}, \\ P_2^r &= p^r_{MN/k+1} \cdots p^r_{2MN/k}, \\ P_3^r &= p^r_{2MN/k+1} \cdots p^r_{3MN/k}, \\ P_k^r &= p^r_{(k-1)MN/k+1} \cdots p^r_{MN}. \end{aligned} \tag{11}$$

By the same token, we calculate

$$c_k = \operatorname{mod}\left(\left(\operatorname{abs}\left(x_k\right) - \operatorname{floor}\left(\operatorname{abs}\left(x_k\right)\right)\right) \times 10^{14}, \frac{MN}{k}\right) + 1. \tag{12}$$

Clearly, $c_k \in [1, MN/k]$. Iteration continues until this chaotic system produces MN/k completely different c_k values, as follows: $\{c_k(i),\ i = 1, \ldots, MN/k\}$. According to c_k, scrambling for vector P_k^r is shown as follows:

$$P_k^{\mathrm{rc}}(i) = P_k^r\left(c_k(i)\right). \tag{13}$$

P^{rc} is the original matrix P after hyperchaos scrambling matrix; Section 4.3 will introduce how to encrypt the P^{rc}.

4.3. The Diffusion Process of Pixels. First of all, for P' of scrambling image preprocessing, scrambling image P' is divided into P_a' and P_b'. Then, by adaptive image processing of the two parts, the P_a' data matrix and matrix P_b' are different or are replaced matrix operation points; likewise, P_{aa}' and P_b' are exclusive or replace the corresponding matrix operation points and will get the new image matrix P_{aa}' to go up and down. Finally, a random sequence of matrix and matrix PP' processing complete diffusion process. Specific process is shown as follows:

$$E_{i,j} = \begin{cases} qq_{ij} \oplus \operatorname{mod}\left(x_{m,n} \times 10^{10}, Q\right) & \text{if } i = 1 \text{ or } j = 1, \\ qq_{ij} \oplus \operatorname{mod}\left(x_{m,n} \times 10^{10}, Q\right) \oplus E_{i-1,j} \oplus E_{i,j-1} & \text{else}. \end{cases} \tag{14}$$

In formula (14), the radius is binary x or operations, $i = m = 1, 2, \ldots, M$ and $j = m = 1, 2, \ldots, N$ are image pixels and the space coordinates of chaotic state value, $E_{i,j}$ is the final image encryption, $qq_{i,j}$ is the adaptive processing of the image pixels, $x_{m,n}$ is the status value of chaos, and Q is digital image grayscale. Formula (14) corresponding to the inverse operation is as follows:

$$\begin{aligned} E_{i,j} &= qq_{ij} \oplus \operatorname{mod}\left(x_{m,n} \times 10^{10}, Q\right) \quad \text{if } i = 1 \text{ or } j = 1, \\ qq_{ij} &= E_{i,j} \oplus \operatorname{mod}\left(x_{m,n} \times 10^{10}, Q\right) \oplus E_{i-1,j} \oplus E_{i,j-1} \quad \text{otherwise}. \end{aligned} \tag{15}$$

Decryption is the inverse of the encryption process, namely, counter proliferation first and then the scrambling processing.

4.4. Pixel Values to Replace. Produced by Logistic mapping and hyperchaos system of random sequence, it is only related to the initial value and system parameters and does not rely on what seems to lead to clear bytes that can only affect the bytes of an encrypted cryptograph, bringing it to choose plaintext attack and chosen-ciphertext attack. In order to overcome this defect and improve the efficiency of encryption, we put forward new encryption schemes; the specific steps are shown as follows.

(1) Random sequences generated from chaotic system are calculated:

$$x_j = \bmod\left(\left(\text{abs}\left(x_k\right) - \text{floor}\left(\text{abs}\left(x_k\right)\right)\right) \times 10^{14}, 256\right) \qquad (J = 1, 2, 3, 4), \tag{16}$$

where $x_j \in [0, 255]$.

(2) P^{rc} ranks of displacement of matrix according to the line are converted to vector, respectively, for each child:

$$\begin{aligned} P_1^r &= p_1^r p_2^r \cdots p_{MN/k}^r, \\ P_2^r &= p_{MN/k+1}^r \cdots p_{2MN/k}^r, \\ P_3^r &= p_{2MN/k+1}^r \cdots p_{3MN/k}^r, \\ P_k^r &= p_{(k-1)MN/k+1}^r \cdots p_{MN}^r. \end{aligned} \tag{17}$$

And then we calculate the type:

$$\begin{aligned} E_1^r(i) &= x_1(i) \oplus P_1^{\text{rc}}(i)\, E_1^r(i-1) \\ E_2^r(i) &= x_2(i) \oplus P_2^{\text{rc}}(i)\, E_2^r(i-1) \\ &\vdots \\ E_k^r(i) &= x_k(i) \oplus P_k^{\text{rc}}(i)\, E_k^r(i-1), \\ & \qquad i \in \left[1, \frac{MN}{k}\right]. \end{aligned} \tag{18}$$

By the same token, the transform matrix E^r in columns as the row vector, and each child vector is obtained encryption cipher to:

$$\begin{aligned} E_1 &= E_1^{\text{rc}}(j) = x_1(j) \oplus E_1^R(j)\, E_1^{\text{rc}}(j-1) \\ E_2 &= E_2^{\text{rc}}(j) = x_2(j) \oplus E_2^r(j)\, E_2^{\text{rc}}(j-1) \\ &\vdots \\ E_k &= E_k^{\text{rc}}(j) = x_k(j) \oplus E_k^r(j)\, E_k^{\text{rc}}(j-1), \\ & \qquad j \in \left[1, \frac{MN}{k}\right]. \end{aligned} \tag{19}$$

(3) If all plaintext is encrypted, the encryption process is ended. Otherwise, go back to step (1). Decryption process is similar to the encryption process.

4.5. To Improve Species Diversity Index. In the process of genetic algorithm in the late fitness, some of the biggest individuals within the population repeat or converge. At this point, they have bigger probability to participate in the choice of the next generation of copy; offspring of crossover between them will not have the too big change with the father generation; it may lead to genetic algorithm to search the optimization process which is very slow, and it may also reduce the search efficiency. Therefore, we should correctly judge whether a species occurs at premature convergence and mainly should look at the population of the current fitness value which is larger in the individual, whether to repeat or mutually converge. Local optimization genetic algorithm is introduced in this paper; we first determine the degree of species diversity in Section 4.1. It is defined as follows.

Set the first t generation population by individual $X(t)_1, X(t)_2, \ldots, X(t)_N$, fitness value of $f(t)_1, f(t)_2, \ldots, f(t)_N$, which is the best individual fitness value of $f_{\max}$, individual $\overline{f} = (1/N)\sum_{t=1}^{N} f(t)$ total average fitness; fitness value is greater than individual fitness value of $\overline{f}$ which will do an average of $\overline{f}^*$, and using the defined $\overline{f}^*$ and the difference in value between $\overline{f}^*$ as $\Delta^* = f_{\max} - \overline{f}^*$, the $\Delta^* = f_{\max} - \overline{f}^*$ indicators are used to characterize the population of premature convergence.

4.6. Chaos Genetic Algorithm Basic Steps. Using chaos genetic algorithm in Sections 4.1–4.4 of the image encryption process for optimization operation, in order to obtain the best encryption to decrypt steps and performance plan, the optimization process is shown in Figure 5. Concrete steps are as follows.

(1) Coding and the parameters setting are still using real number coding; the method of natural intuitive can save the time and space overhead, the advantage of high computation efficiency. To the population size, chaos optimization iterations, such as fitness function parameters, are set.

(2) Chaos is used to generate the initial population.

(3) The expected value method and the choice of the optimal preservation strategy are used to implement the replication.

(4) The improved genetic algorithm is used in the adaptive adjusting the crossover probability of pc, pm mutation probability, crossover, and mutation operator.

(5) Calculate degree of species diversity, its outstanding individual to decide whether to use contemporary chaos optimization; if the degree of species diversity is less than a random number, use chaos optimization, and if they can get better individuals, it will be used as the optimal solution in the algebra.

(6) Repeat steps (3) to (5), until meeting the termination conditions of evolution. Termination conditions may be evolution algebra or best individual fitness function.

4.7. Theoretical Analysis and Experimental Simulation

4.7.1. Statistical Analysis. Simulating the process, in order to assess the performance of the proposed algorithm, this

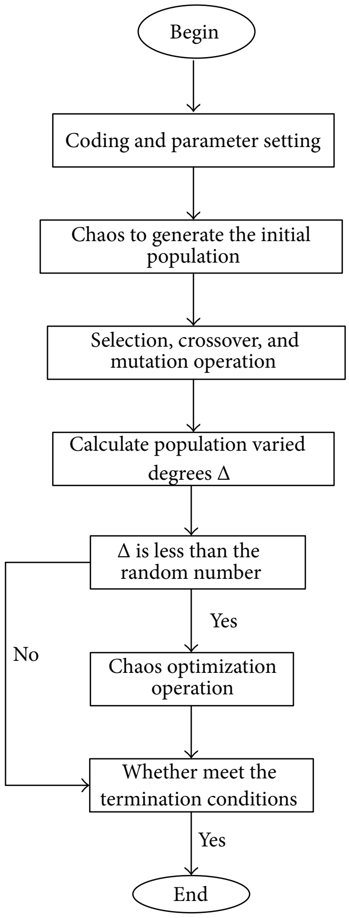

Begin
Coding and parameter setting
Chaos to generate the initial population
Selection, crossover, and mutation operation
Calculate population varied degrees Δ
Δ is less than the random number
Yes
No
Chaos optimization operation
Whether meet the termination conditions
Yes
End

Figure 5: Chaos genetic algorithm flow chart.

chapter chose 256 KB image file for simulation, according to the theory of Shannon; statistical analysis is often used to analyze and decipher the algorithm. Therefore, a password system should have good performance in terms of statistical attack resistance. The simulation results are shown in Figure 6: Figure 6(a) is 256 KB of original image; Figure 6(b) for image scrambling after visible, scrambling image pixel shading distribution, while great changes have taken place in picture similar to white noise, showed good scrambling effect. In the image scrambling, the fewer the numbers of the fixed points, the higher the secrecy, and then scrambling effect is better. The fixed point of statistical formula is as follows:

$$\delta = \left(\sum_{n=1}^{M\times N} \frac{\nabla_n}{M \times N} \right) \times 100\%,$$
$$\nabla_n = \begin{cases} 0 & \left(\text{find}\,(p_n)\,|p_n \in P \neq \text{find}\,(p_n)\big|_{p_n \in P^{\text{rc}}} \right) \\ 1 & \left(\text{find}\,(p_n)\,|p_n \in P = \text{find}\,(p_n)\big|_{p_n \in P^{\text{rc}}} \right). \end{cases} \tag{20}$$

Among them, *find* () used for the position of the Matlab command and p_n corresponding pixel values, M and N, are used to clear the size of the matrix. According to formula (20). The statistical Figure 6(b) is the scrambling of the fixed point. It is got from Figure 6(b) that the scrambling of the fixed point ratio is 3.21‰; it can obtain good scrambling effect. But after scrambling, image can only be destroyed by the original correlation between adjacent pixels, without changing the pixel value at every point, so the image of gray distribution histogram will not change and must be of scrambling image pixel values for further encryption. Eventually, the encrypted results are shown in Figure 6(c); it has completely hidden the original image, and it cannot see the outline of the original image. Figures 6(d) and 6(e) show these problems; we can compare with the uneven distribution of the original histogram; the encrypted flat histogram and gray value are evenly distributed. This shows that the ciphertext pixel values in [0, 255] are within the scope of the equal probability values, namely, uniform for the whole ciphertext space distribution characteristics. Thus, this algorithm can effectively prevent the statistical attack.

Table 2: Two kinds of algorithm ciphertext image information entropy.

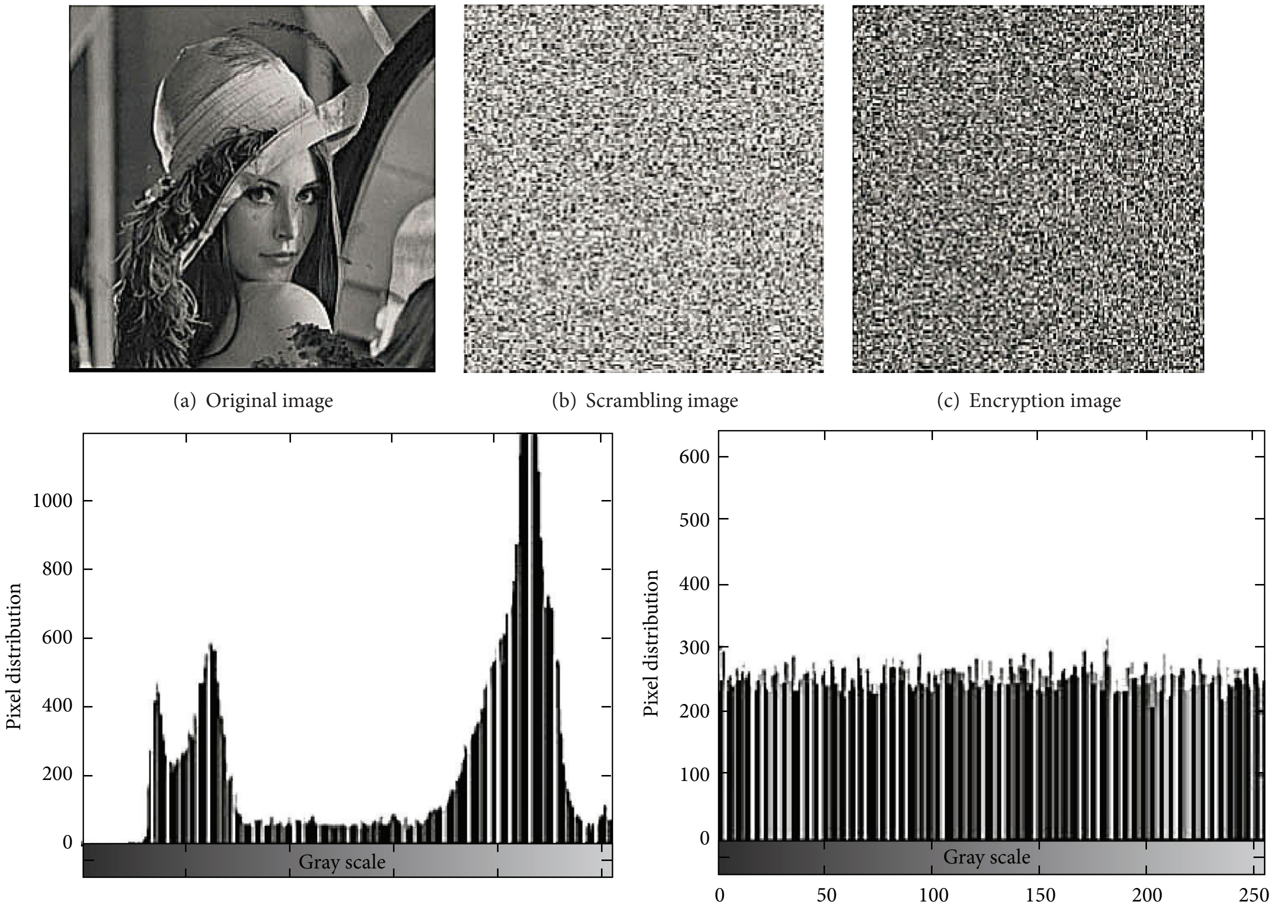
$H(x)$	7.1.10	7.2.01	Boat	Elaine	Gray21	Numbers
Gao	7.8673	7.6298	7.8967	7.5678	7.7645	7.7694
Ours	7.9378	7.9679	7.9786	7.9897	7.9903	7.9936

4.7.2. The Key Space and the Key Sensitivity Analysis. The key of the encryption algorithm for $K = \{\mu, \omega, \lambda, x_{0,0}, x_{m+1,0} = \lambda x_{m,0}(1 - x_{m,0}), x_{0,n+1} = \lambda x_{0,n}(1 - x_{0,n}, T)\}$; if the computer precision is effective for 10^{15}, key space size is about $10^{15\times 5\times M\times N}$; the algorithm has a large enough key space and it can effectively resist brute force attack. $x_{0,0} = 0.6167$ Barbara encryption image, respectively, in $x_{0,0} = 0.6167 + 0.1 \times 10^{-9}$ and $x_{0,0} = 0.6167 + 0.1 \times 10^{-14}$ under the condition of the same (other decryption key and encryption key) decrypted image is shown in Figure 7. We can see from Figure 7 that it is extremely sensitive to key encryption algorithm.

4.7.3. Information Entropy Analysis. A digital image information entropy can show the distribution of the gray value. If the gray value distribution is uniform, the amount of information of the image is greater. The definition of information entropy is the average amount of information; it is as follows:

$$H(x) = -\sum_{i}^{n} p(x_i) \log_2 p(x_i),$$
$$0 \le p(x_i) \le 1, \ (i = 1, 2, \ldots, n) \ \sum_{i}^{n} p(x_i) = 1. \tag{21}$$

In formula (21), $p(x_i)$ is concentrated symbol probability x_i in the message. In order to have a good contrast, Table 2 shows the 6 different images using this algorithm and Gao and Chen [24] encryption algorithm using the entropy value comparison. As shown, Gao algorithm of ciphertext image information entropy is smaller than the information entropy of the proposed algorithm, so its gray value distribution is not uniform. The algorithm of ciphertext image information entropy is close to a maximum of 8, of image gray value



(a) Original image

(b) Scrambling image

(c) Encryption image

(d) Original image histogram

(e) Encryption image histogram

Figure 6: The original image and the encryption image histogram.

distribution, and uniform. Therefore, from the perspective of information entropy attack, the algorithm is secure.

4.7.4. Correlation Analysis. Digital image of each pixel is not independent; its correlation is very large. This suggests the large area of gray value. In one of the digital TV images, for example, the same line of two adjacent pixels or adjacent two rows of pixels, the correlation coefficient is 0.9, and the correlation between the adjacent two television images is larger than frame correlation, so the image information redundancy is very big. For image encryption, one of the goals is to reduce the correlation between adjacent pixels, mainly including horizontal pixel, vertical pixels, and the correlation between diagonal pixels. Obviously correlation is smaller, and the better the image encryption, the higher the security.

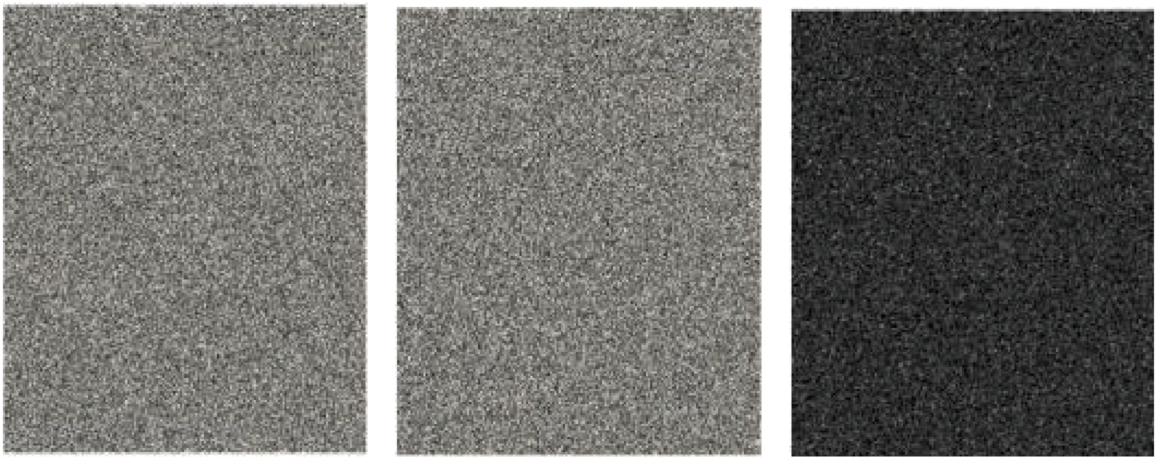
Figure 8 is expressed as the vertical direction and horizontal direction, the original image, and the algorithm of encryption image correlation of adjacent pixels. The correlation between the original image pixel rendering obvious linear relationship and encryption image pixels of correlation among random corresponding relation are visible.

Table 3 is for the original image and the proposed algorithm of ciphertext image between adjacent pixels according to the horizontal, vertical, and diagonal direction calculated using the correlation coefficient. For pixel correlation coefficient ρ_{xy} calculation method is shown as follows:

Table 3: The correlation coefficient of the original image and the cipher image pixel.

Correlation index	Original image	Encryption image
Level	0.8766893	0.0003875
Opposite angles	0.9047526	0.0098546
Vertical	0.9537689	0.0209381

$$\begin{aligned} E(x) &= \frac{1}{N}\sum_{i=1}^{N} x_i, \\ D(x) &= \frac{1}{N}\sum_{i=1}^{N} \left(x_i - E(x)\right)^2, \\ \operatorname{cov}(x,y) &= \frac{1}{N}\sum_{i=1}^{N} \left(x_i - E(x)\right)\left(y_i - E(y)\right), \\ \rho_{xy} &= \frac{\operatorname{cov}(x,y)}{\sqrt{D(x)D(y)}}. \end{aligned} \tag{22}$$

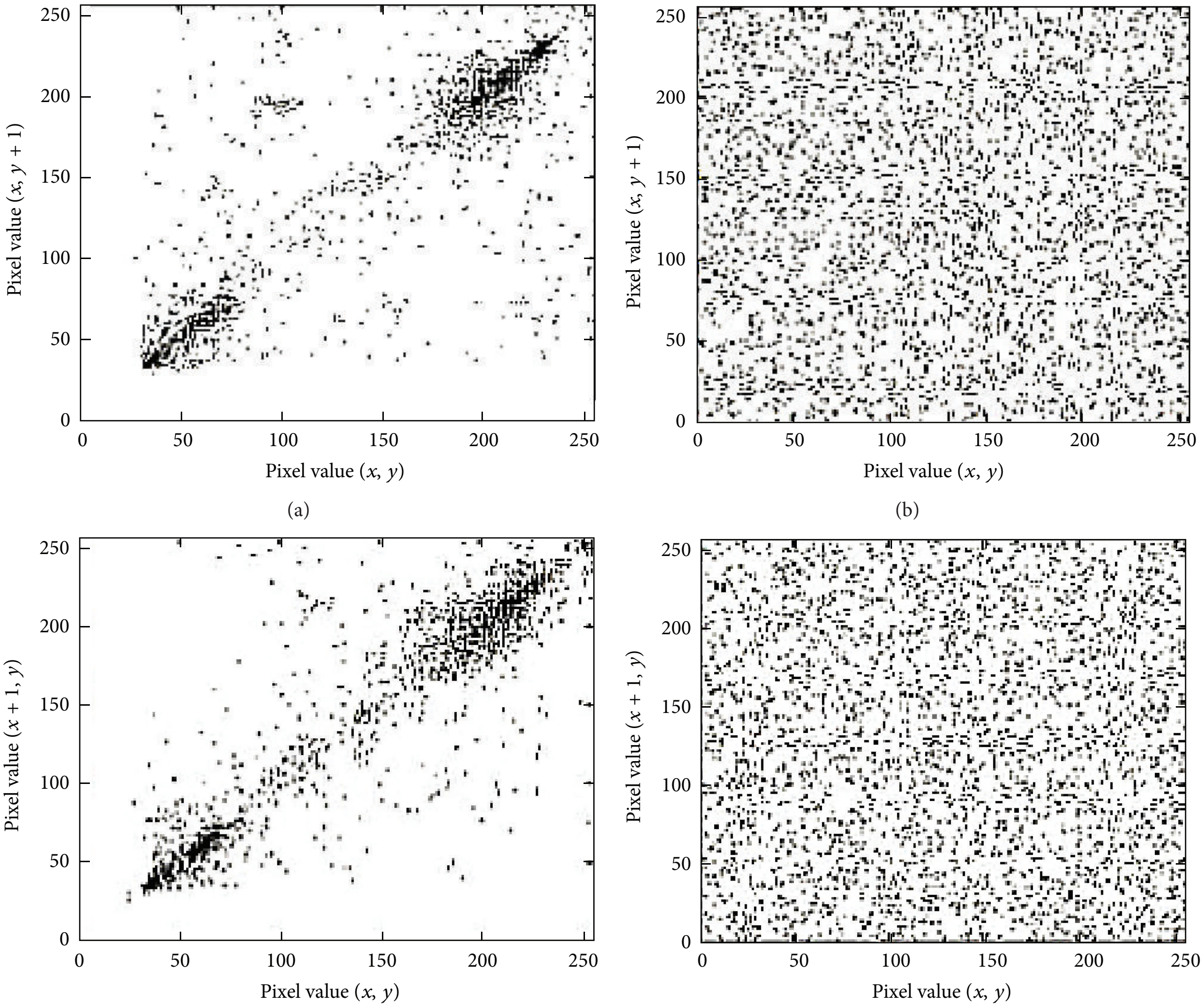


(a) $x_{0,0} = 0.6167 + 0.1 \times 10^{-9}$

(b) $x_{0,0} = 0.6167 + 0.1 \times 10^{-14}$

(c) (a) and (b) error

Figure 7: Wrong decryption keys under the image and the difference between them.



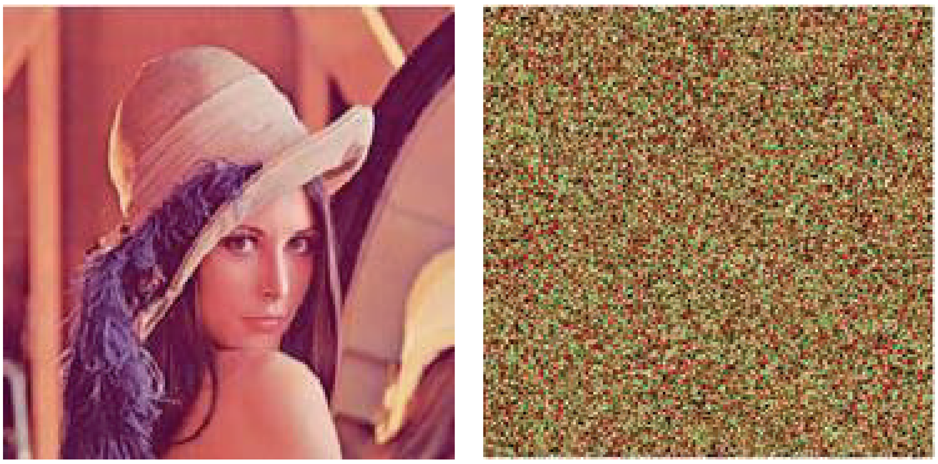
(a)

(b)

(c)

(d)

Figure 8: Adjacent pixels correlation.



(a) Original image

(b) Encrypted image

Figure 9: Original image and encrypted image.

In formula (22), x and y, respectively, are the image pixel values of two adjacent pixels and ρ_{xy} is the correlation coefficient of two adjacent pixels. As shown in Table 3, the adjacent pixels of the original image are highly correlated; their correlation coefficient is close to 1. And we concluded that encrypted ciphertext correlation coefficient of adjacent pixels of the image is very small; they are close to zero; the adjacent pixels have been largely irrelevant, which shows that the statistical characteristic of the original image has been spread to random ciphertext image.

4.7.5. Color Image. In order to demonstrate the effectiveness of the proposed encryption algorithm, the following will use the algorithm to analyze color image.

(1) Image Encryption and Statistical Analysis. Select 256 × 256 color Lena standard drawing as experimental object; make use of MATLAB 7.6 programming to do the experiment simulation; the experimental simulation results are shown in Figure 1. Figures 9(a) and 9(b) are the original image and the encryption image, respectively. We can see intuitively that the encrypted image cannot see any effective information of the original image. First of all, on the vision the encryption algorithm achieves good encryption effect.

Here, we calculate, respectively, scrambling degree of the three primary colors R, G, and B of encrypted image; after several test calculations we get the average:

R component image scrambling degree: $SM_{\mathrm{R}} = 0.942$.

G component image scrambling degree: $SM_{\mathrm{G}} = 0.975$.

B component image scrambling degree: $SM_{\mathrm{B}} = 0.914$.

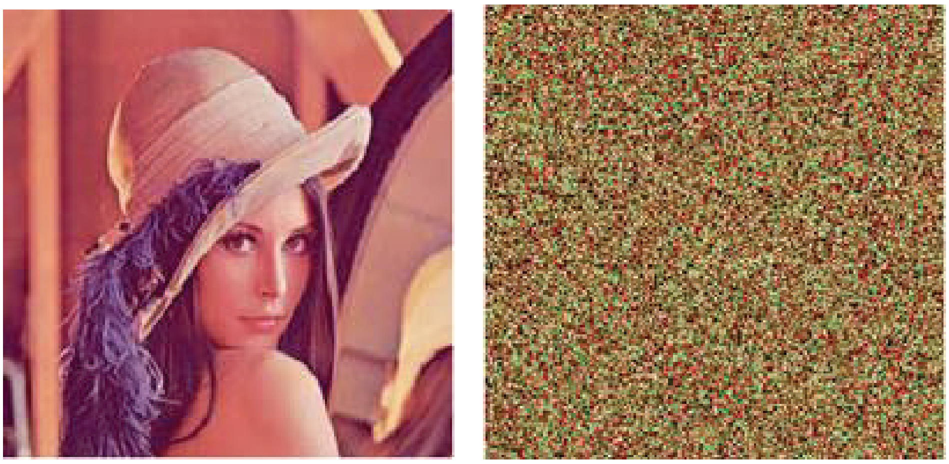
The result shows that scrambling degree of the algorithm is similar with magic square transformation and has good scrambling effect.

(2) The Key Space and the Key Sensitivity Analysis. Key of the encryption algorithm $K = \{\mu, \omega, \lambda, x_{0,0}, x_{m+1,0} = \lambda x_{m,0}(1 - x_{m,0}), x_{0,n+1} = \lambda x_{0,n}(1 - x_{0,n}, T)\}$; if the computer precision effectively is 10^{15}, key space size is about $10^{15*5*M*N}$, and due to the extreme sensitivity to the initial value of the chaos system, the key sequence generated by a key generator is complex and unpredictable, so the key sequence space is large enough; this indicates that the algorithm can resist brute force attack.

Through the tiny change of authenticated key influencing encryption result to measure sensitivity of the algorithm, as shown in Figure 10(b), the encrypted image uses right key and wrong key to decrypt the algorithm, respectively; the simulation results are shown in Figure 10, of which Figure 10(a) is the decrypted image which uses the correct key to decrypt, and Figure 10(b) is the error decrypted image obtained by keeping the other key parameters unchanged, taking x_0 values differently.

By observing the decrypted image, one can know that, with the key orders of magnitude difference error of only 10^{-10} keys to decrypt, the image is similar to the noise of the image, on the vision which fully does not see any effective information of the original image; it shows that the algorithm has a good sensitivity to key; that is, the initial key of tiny change will lead to the result of the encryption algorithm being completely different; this makes the attacker to not only attack from the ciphertext fragments obtained to judge the information of the original image.

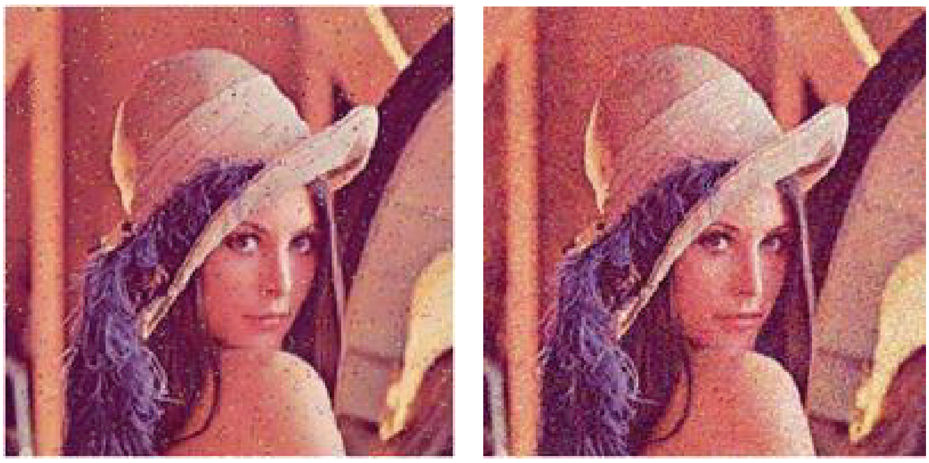
(3) Ability to Resist Noise Analysis. Shown in Figure 9(b) are the images after adding noise using the correct secret key to decrypt them; the decrypted image is shown in Figure 11, and Figures 11(a) and 11(b), respectively, show the decryption result after the encryption image is joined with the interference intensity of 20% salt and pepper noise and interference intensity of 15% gaussian noise, respectively, as shown in Figures 11(a) and 11(b). As you can see, to decrypt right the encryption image after adding noise, it can still be



(a) Correct decryption image

(b) Error decrypting image

Figure 10: Key sensitivity testing.



(a) Adding salt and pepper noise

(b) Adding Gaussian noise

Figure 11: Figure 9(b), the decrypted image, after different noise.

good to restore the original image information and to retain the original image information effectively, using decryption without distortion, and this shows that the algorithm has good anti-interference ability.

(4) The Correlation Analysis. The nature of the scrambling effect of encryption algorithm lies in breaking the correlation between pixel values of adjacent pixels, to resist the attack by any clear way. Therefore, the comparison of neighboring pixels correlation can be a good measure of a scrambling effect of the encryption algorithm; here, we compare the correlation of adjacent pixels of the three color components R, G, and B of the original image and encrypted image, respectively; pixel point, respectively, on the horizontal, vertical, and diagonal direction are analyzed, and the pixel correlation coefficient calculation method is shown as in formulae (22).

Do statistical tests on the correlation of adjacent pixels in the original image and the encrypted image, and randomly draw multiple pixels and calculate separately the correlation of adjacent pixels of the R, G, and B components on horizontal, vertical, and diagonal directions; the averaged results after multiple computations are shown in Tables 4, 5, and 6 [25].

Table 4: The correlation among adjacent pixels of R component.

Related systems	Original image	Encryption image
Horizontal	0.9372451	−0.0058392
Diagonal	0.8965389	0.0031983
Vertical	0.9209471	−0.0089638

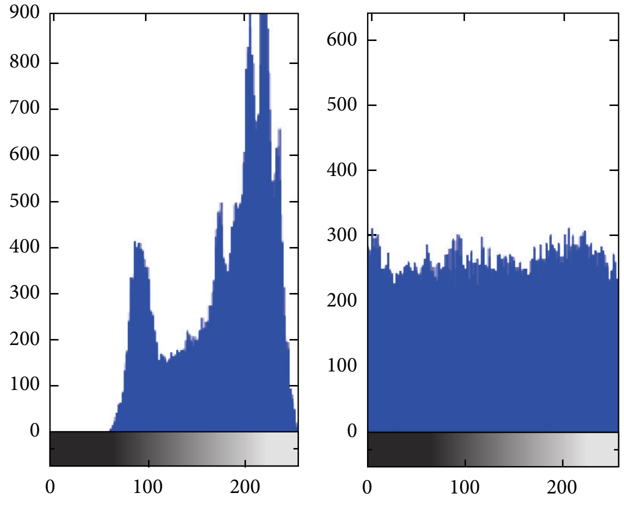
Observe that the correlation coefficient of the adjacent pixels no matter in horizontal, vertical, or diagonal line direction of the encrypted image is far less than the correlation coefficient of adjacent pixels of original image; this shows that the encryption algorithm has good scrambling effect, destroys the correlation between image pixels, and effectively conceals the statistical characteristics of the image.

Table 5: The correlation among adjacent pixels of G component.

Related systems	Original image	Encryption image
Horizontal	0.9689230	−0.00329842
Diagonal	0.8276401	0.00214621
Vertical	0.9737210	−0.00231832

Table 6: The correlation among adjacent pixels of B component.

Related systems	Original image	Encryption image
Horizontal	0.9012730	0.0005832
Diagonal	0.9103892	−0.0065932
Vertical	0.9101020	0.0090382



(a) The original image histogram (b) The encrypted image histogram

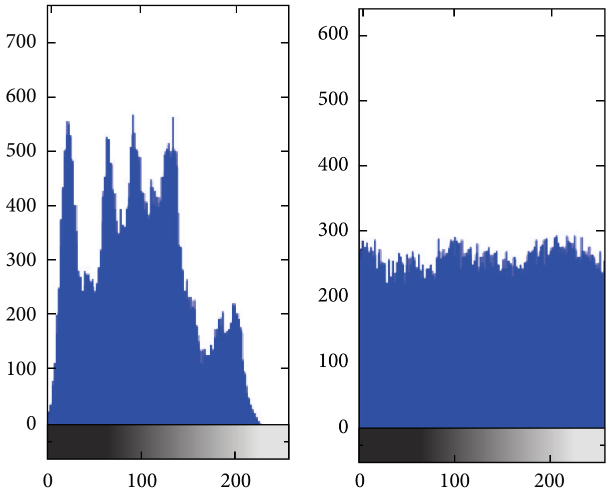
Figure 12: The histogram comparison of R component.

(5) Histogram Analysis. Histogram of the image is one of the important statistical characteristics of image; it directly reflects the relationship between the digital image of each grayscale and the occurrence of the grayscale. Extract the three colors of R, G, and B components from the original image of Figure 9(a) and the encrypted image of Figure 9(b); histograms are calculated, respectively, as shown in Figures 12, 13, and 14.

Looking at these figures, it can be seen that the encrypted image histogram is uniform; there is a world of difference with the original image; it shows that the encrypted image will not give the attacker any clear information; the algorithm has a strong ability to resist statistical attack.

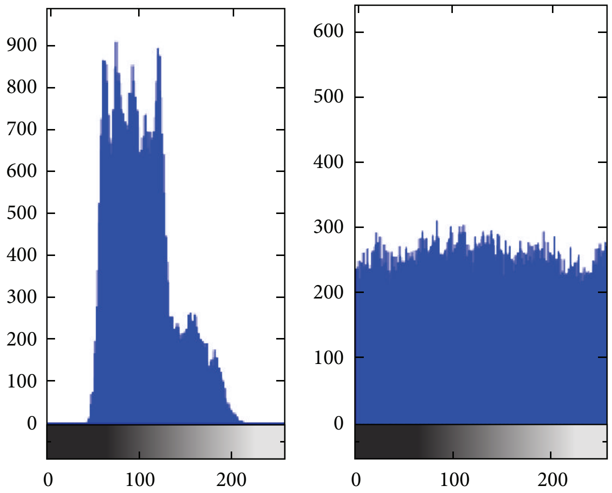
5. Conclusion

This paper analyzes the existing "scrambling to replace" type of some shortages which are chaotic image encryption algorithms; namely a plaintext byte can affect a cipher byte; it can be made use of to select plaintext attack and chosen-ciphertext attack is easy to decipher. That is to say, it will not be able to resist choosing plaintext attack and chosen-ciphertext attack. Aiming at the existence of some high dimensional chaotic encryption algorithm in the weak resistance to choose plaintext attack and chosen-ciphertext attack problems, we put forward a new kind of digital image encryption algorithm based on genetic chaos. The new algorithm is to make the following improvements: (1) in the process of scrambling encryption algorithm, the hyperchaos system is also introduced; it makes the image scrambling result not only depend on the chaotic sequence generated by the initial key but also depend on the characteristics of the image itself, making it have adaptive features to a certain extent; (2) for the introduction of the genetic algorithm for image encryption-decryption process parameters of dynamic optimization, it gets the best encryption-decryption process and steps; (3) for the diffusion in the encryption process, clear feedback mechanism is introduced in the algorithm and



(a) The original image histogram (b) The encrypted image histogram

Figure 13: The histogram comparison of G component.



(a) The original image histogram (b) The encrypted image histogram

Figure 14: The histogram comparison of B component.

improves the sensitivity to the plaintext, objectively improving the algorithm of plaintext and ciphertext attack resistance. Through the relevant experiment and safety analysis, we show that our proposed digital image encryption algorithm based on genetic hyperchaos not only can effectively resolve the current problems of weak resistance to aggressive encryption algorithm but also strengthened the sensitivity to the plaintext, enhanced ability to resist differential attacks, and improved the efficiency of encryption.

Competing Interests

The author declares that they have no competing interests.

Acknowledgments

This work is supported in part by the National Natural Science Foundation of China under Grants 61272466 and 61303233 and the Natural Science Foundation of Hebei Province under Grant F2014203062.

References

[1] Y. Liu, X. Tong, and S. Hu, "A family of new complex number chaotic maps based image encryption algorithm," *Signal Processing: Image Communication*, vol. 28, no. 10, pp. 1548–1559, 2013.

[2] Z.-H. Guan, F. Huang, and W. Guan, "Chaos-based image encryption algorithm," *Physics Letters, Section A: General, Atomic and Solid State Physics*, vol. 346, no. 1–3, pp. 153–157, 2005.

[3] W.-T. Wong, F. Y. Shih, and T.-F. Su, "Thinning algorithms based on quadtree and octree representations," *Information Sciences*, vol. 176, no. 10, pp. 1379–1394, 2006.

[4] R.-J. Chen and S.-J. Horng, "Novel SCAN-CA-based image security system using SCAN and 2-D von Neumann cellular automata," *Signal Processing: Image Communication*, vol. 25, no. 6, pp. 413–426, 2010.

[5] X. Xu, Z. Tang, and J. Wang, "A method to improve the transiently chaotic neural network," *Neurocomputing*, vol. 67, no. 1–4, pp. 456–463, 2005.

[6] S.-D. Liu, Shi-Shi, and Z.-W. Yan, *The Essence of Chaos*, Meteorological Press, Beijing, China, 1997.

[7] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," *International Journal of Bifurcation and Chaos in Applied Sciences and Engineering*, vol. 8, no. 6, pp. 1259–1284, 1998.

[8] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," *Chaos, Solitons and Fractals*, vol. 21, no. 3, pp. 749–761, 2004.

[9] S. Lian, J. Sun, and Z. Wang, "A block cipher based on a suitable use of the chaotic standard map," *Chaos, Solitons & Fractals*, vol. 26, no. 1, pp. 117–129, 2005.

[10] K.-W. Wong, B. S.-H. Kwok, and W.-S. Law, "A fast image encryption scheme based on chaotic standard map," *Physics Letters, Section A: General, Atomic and Solid State Physics*, vol. 372, no. 15, pp. 2645–2652, 2008.

[11] H. Zhu, C. Zhao, and X. Zhang, "A novel image encryption-compression scheme using hyper-chaos and Chinese remainder theorem," *Signal Processing: Image Communication*, vol. 28, no. 6, pp. 670–680, 2013.

[12] G. Alvarez and S. Li, "Cryptanalyzing a nonlinear chaotic algorithm (NCA) for image encryption," *Communications in Nonlinear Science and Numerical Simulation*, vol. 14, no. 11, pp. 3743–3749, 2009.

[13] M. Ghebleh, A. Kanso, and H. Noura, "An image encryption scheme based on irregularly decimated chaotic maps," *Signal Processing: Image Communication*, vol. 29, no. 5, pp. 618–627, 2014.

[14] S. Banerjee, L. Rondoni, S. Mukhopadhyay, and A. P. Misra, "Synchronization of spatiotemporal semiconductor lasers and its application in color image encryption," *Optics Communications*, vol. 284, no. 9, pp. 2278–2291, 2011.

[15] N. K. Pareek, V. Patidar, and K. K. Sud, "Image encryption using chaotic logistic map," *Image and Vision Computing*, vol. 24, no. 9, pp. 926–934, 2006.

[16] C. K. Volos, I. M. Kyprianidis, and I. N. Stouboulos, "Image encryption process based on chaotic synchronization phenomena," *Signal Processing*, vol. 93, no. 5, pp. 1328–1340, 2013.

[17] T. Xiang, X. F. Liao, G. Tang, Y. Chen, and K.-W. Wong, "A novel block cryptosystem based on iterating a chaotic map," *Physics Letters A*, vol. 349, no. 1–4, pp. 109–115, 2006.

[18] J. H. Holland, *Adaptation in Nature and Artificial Systems*, MIT Press, 1992.

[19] D. E. Goldberg, *Genetic Algorithms in Search, Optimization and Machine Learning*, Addison-Wesley, 1989.

[20] K. Krishnakumar, "Micro-genetic algorithms for stationary and non-stationary function optimization," in *Intelligent Control and Adaptive Systems*, vol. 1196 of *Proceedings of SPIE*, pp. 289–296, Philadelphia, Pa, USA, November 1989.

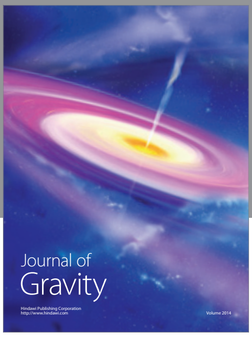
[21] D. Maclay and R. Dorey, "Applying genetic search techniques to drivetrain modeling," *IEEE Control Systems Magazine*, vol. 13, no. 3, pp. 50–55, 1993.

[22] Y. Davidor, *Genetic Algorithms and Robotics*, World Scientific, Singapore, 1991.

[23] J. H. Park, "Adaptive synchronization of hyperchaotic Chen system with uncertain parameters," *Chaos, Solitons and Fractals*, vol. 26, no. 3, pp. 959–964, 2005.

[24] T. G. Gao and Z. Q. Chen, "A new image encryption algorithm based on hyper-chaos," *Physics Letters A*, vol. 372, no. 4, pp. 394–400, 2008.

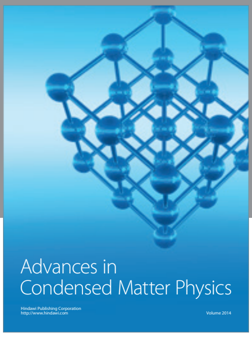
[25] Y.-Q. Zhang and X.-Y. Wang, "A new image encryption algorithm based on non-adjacent coupled map lattices," *Applied Soft Computing*, vol. 26, pp. 10–20, 2015.

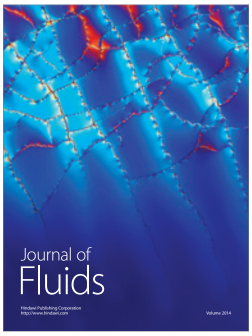

Journal of
Gravity

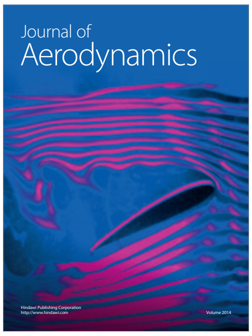
Journal of
Photonics

The Scientific
World Journal

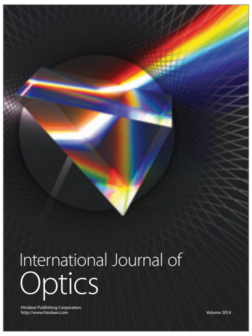
Journal of
Soft Matter

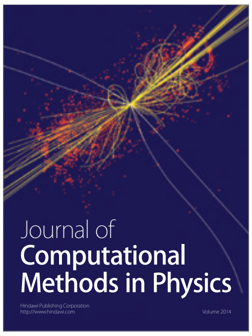

Advances in
Condensed Matter Physics

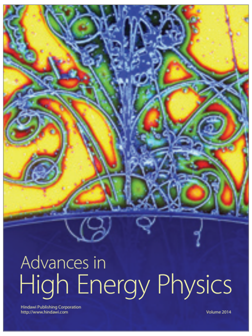

Journal of
Fluids


Journal of
Aerodynamics

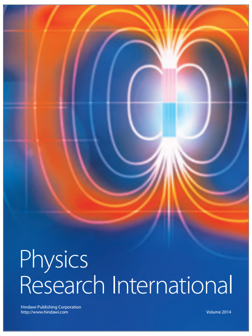
International Journal of
Statistical Mechanics

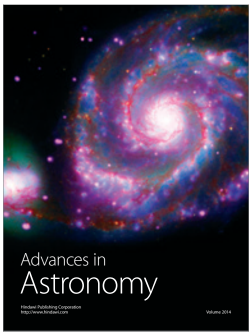

International Journal of
Optics


Journal of
Computational
Methods in Physics


Advances in
High Energy Physics

Journal of
Thermodynamics


Physics
Research International

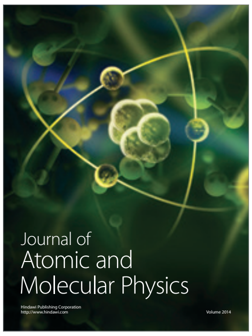

Advances in
Astronomy

Journal of
Solid State Physics

Journal of
Astrophysics

International Journal of
Superconductivity

Journal of
Biophysics


Journal of
Atomic and
Molecular Physics