基于随机混沌序列的图像加密算法*)

杨华千[1,2] 张 伟[2] 韦鹏程[1,2] 黄 松[2]

(重庆大学计算机学院 重庆 400044)[1] (重庆教育学院计算机与现代教育技术系 重庆 400067)[2]

摘 要 混沌系统的参数敏感性、初值敏感性和以同一分布遍历各态的特性很好地对应了密码系统应具备的一些基本特性。本文提出了一种基于随机混沌序列的图像加密算法。在该算法的图像像素的空间置乱过程中,采用了离散的标准映射混沌系统。而在像素的扩散过程中,通过复合离散混沌系统隐藏了混沌序列产生时所经历的迭代次数。理论分析和仿真实验表明,本文提出的算法具有较高的安全性能,特别是在统计攻击、差分攻击和选择明文攻击能力方面具有很好的抗攻击性能。

关键词 混沌图像加密算法,标准映射,复合离散混沌系统,选择明文攻击

An Image Encryption Scheme Based on Random Chaotic Sequence

YANG Hua-Qian[1,2] ZHANG Wei[2] WEI Peng-Cheng[1,2] HUANG Song[2]

(Department of Computer Science and Engineering, Chongqing University, Chongqing 400044)[1]

(Department of Computer and Modern Education Technology, Chongqing Education College, Chongqing 400067)[2]

Abstract The chaotic properties of chaotic system such as ergodicity, mixing and sensitive dependence on initial conditions and system parameters, are corresponding with some important properties of cryptosystems. In the paper, an image encryption algorithm based on random chaotic sequence is presented. In the spatial permutation process, a discrete standard map is employed. When the chaos sequence, which is used to diffuse the pixels of the image, is generated, the iteration times are hidden to avoid cryptanalysis based on symbolic dynamic. Theoretical analyses and simulated experiment show that, the proposed algorithm has excellent performances against attacks, in particular statistical attack, differential attack and chosen plain image attack.

Keywords Chaos image encryption scheme, Standard map, Composite discrete chaotic system, Chosen plain-image attack

1 引言

当前,多媒体通信逐渐成为人们进行信息交流的重要手段,信息的安全与保密显得越来越重要。对于多媒体信息,尤其是图像和声音信息传统的加密技术将其作为普通数据流进行加密,不考虑多媒体数据的特点,因此有一定的局限性。混沌现象是在非线性动力系统中出现的确定性的、类似随机的过程,这种过程既非周期又不收敛,并且对初始值有极其敏感的依赖性。混沌系统的这些属性很好地对应了密码系统的特性。

然而混沌在本质上是确定的,有关文献已经证明这些算法的抗选择明文或已知明文攻击的能力较差[1~5]。这主要是因为,计算机的有限精度和混沌序列的离散化导致了混沌动力系统的性能退化。

本文提出了一种新的基于随机混沌序列的图像加密算法。在该算法的图像像素的空间置乱过程中,采用了离散的标准映射混沌系统。而在像素的扩散过程中,通过复合离散混沌系统隐藏了混沌序列产生时所经历的迭代次数,来避免常用的基于符号动力学的密码分析。因此,从计算安全性角度,提高了算法的抗明文攻击能力。

本文第2节描述了本文的基于随机混沌序列的图像加密算法。第3节对算法从理论和仿真实验两个方面进行了安全性分析。最后总结了本文。

2 基于随机混沌序列的图像加密方案

2.1 复合离散混沌系统的定义

定义 设两个离散混沌系统 $f(\cdot),g(\cdot):x_{n+1}=f(x_n,p_f)$,$y_{n+1}=g(y_n,p_g)$,则定义一个新的离散混沌系统 $\Phi(\cdot)$ 如下:

$$x_{n+1}=\Phi^{(M)}(x_n)=f^{(M)}(x_n,p_f) \tag{1}$$

其中,

$$M=\lceil Q(y_{n+1}-x_{\min})/(x_{\max}-x_{\min})\bmod Q\rceil+\Delta \tag{2}$$

Q 是大于0的自然数,$(x_{\min},x_{\max})$的典型取值区间是(0.2,0.8)。y_{n+1}是由 $g(\cdot)$产生的混沌序列,其值通常也要求在(0.2,0.8)之间;Δ 是 $f(\cdot)$的迭代次数修正量,其取值情况如下,如果 $f^{\lceil N(y_{n+1}-x_{\min})/(x_{\max}-x_{\min})\bmod N\rceil}(x_n)\in(x_{\min},x_{\max})$,则 $\Delta=0$。否则,继续迭代 $f^{\lceil N(y_{n+1}-x_{\min})/(x_{\max}-x_{\min})\bmod N\rceil}(x_n)$,直到其值介于区间$(x_{\min},x_{\max})$内,则 Δ 就等于继续迭代的次数。

2.2 图像的置乱过程

通常,图像的置乱并没有多大的密码作用,但它可以有效地打乱输入明文(或中间密文)的次序,进而能有效地掩盖明文(中间密文)的统计特性,从而有效地抵抗统计和差分攻击。通常情况下,对图像置乱有两种方式,一是直接对图像的各个像素点的坐标位置进行线性变换,二是先对图像进行分块,再置乱。但是分块后的置乱只在图像的局部进行,其置乱程度

*)重庆市教委资助项目(No. KJ061501,No. KJ051501),重庆市科委资助项目(No. CSTC,2005BB2286)。杨华千 博士生,研究方向为计算机信息安全。张 伟 教授,博士,研究方向为计算智能。韦鹏程 博士生,主要研究方向为信息安全和混沌密码学。

不高。线性变换中经常采用的有 Arnold 变换、幻方变换、3D 猫映射等。但是，这些置乱变换是线性确定的，与密钥无关，其安全程度也不高。例如，离散的 Arnold 变换定义如下：

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod N \tag{3}$$

其中，$x_n, y_n \in \{0,1,\cdots,N-1\}$，$a,b$ 是正整数。这种变换具有周期性。例如，当 $a=40, b=8$ 时，对一个 124×124 的图像进行 5 次 Arnold 变换后将还原为原始的图像。因此，在本文的算法中，将根据混沌密码学的思想，采用标准映射所产生的混沌序列对图像进行非线性置乱。二维标准映射是一种保守的离散系统，其一般形式为：

$$\begin{cases} x_{j+1} = x_j + k \sin y_j \\ y_{j+1} = y_j + x_{j+1} \end{cases} \tag{4}$$

离散化(4)式后，得到：

$$\begin{cases} x_{j+1} = (x_j + y_j) \bmod N \\ y_{j+1} = \left(y_j + k \sin \dfrac{x_{j+1} N}{2\pi} \right) \bmod N \end{cases} \tag{5}$$

设 $C(i,j)$ 和 $C_d(i,j)$ 分别表示(4)和(5)的连续和离散映射，则离散化过程满足下列渐进特性[6]：

$$\lim_{N\to\infty} \max_{0\leqslant i,j\leqslant N} |C(i/N, j/N) - C_d(i,j)| = 0 \tag{6}$$

2.3 图像的置混过程

根据 2.1 节的描述，本文选择 Logistic 映射作为 $\Phi(\cdot)$ 中的 $f(\cdot)$，Tent 映射作为 $\Phi(\cdot)$ 中的 $g(\cdot)$，构成改进的离散混沌系统 $\Phi(\cdot)$。Logistic 映射和 Tent 映射分别定义如下：

Logistic 映射：$x_{k+1} = 4x_k(1-x_k)$ (7)

Tent 映射：$y_{k+1} = \left(1 - 2\left|y_k - \frac{1}{2}\right|\right)$ (8)

则图像的置混过程如下：

(1)选定两个初始参数 i_l, i_t，分别作为 Logistic 映射和 Tent 映射的初始值。

(2)利用(8)式和 i_t 产生混沌序列 $y_1, y_2, \cdots, y_n$。

(3)利用(1)式得到 $\Phi(\cdot)$ 的混沌序列 $x_1, x_2, \cdots, x_k, \cdots, x_n$。

(4)利用(9)式将该序列离散化得到密钥流 $\phi(1), \phi(2), \cdots, \phi(k), \cdots, \phi(n)$。

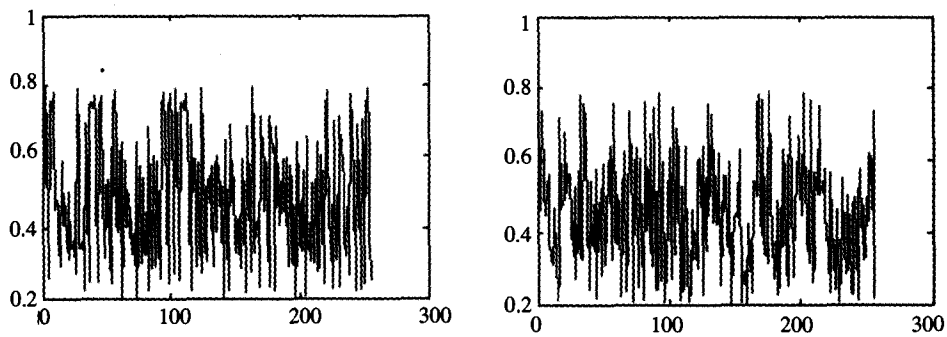
$$\phi(k) = \lfloor N(x_k - x_{\min})/(x_{\max} - x_{\min}) \bmod N \rfloor \tag{9}$$

N 是图像的颜色深度(对于 256 级的灰度图像，$N=256$)，$(x_{\min}, x_{\max})$ 的典型取值区间是(0.2,0.8)

(5)利用(10)式对 2.2 节的置乱后的图像像素流进行加密：

$$C(k) = \{\phi(k) \oplus \{[I(k) + \phi(k)] \bmod N\} \oplus C(k-1)\} \bmod 256 \tag{10}$$

得到图像的密文像素流：$C(1), C(2), \cdots, C(k), \cdots, C(n)$。注意，在计算过程中设定 $C(0)$ 为任意的 0 到 255 之间的一个正整数，$I(k)$ 是当前操作的像素值。Logistic 映射序列和复合映射序列如图 1 所示。



(a). Logistic map f (.)
(Initial value i_l: 0.926727294921857)

(b). Composite map $\Phi(.)$
(Initial value i_l: 0.926727294921857
i_t: 0.726727294921875)

图 1 Logistic 映射和复合映射

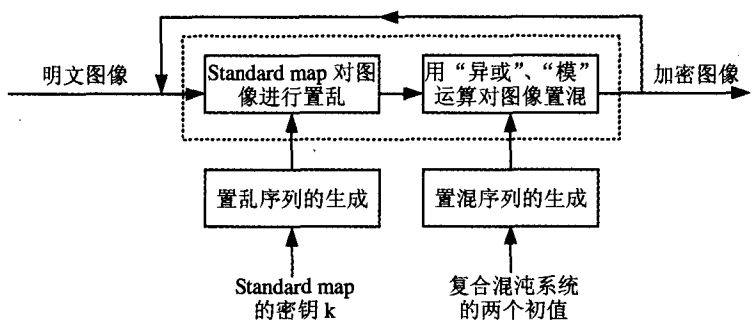


图 2 图像加密框图

2.4 图像的加密和解密过程

本文的加密算法框图如图 2 所示。

加密步骤如下：

(1)将明文图像按第 2.2 节的方法进行置乱。

(2)选定复合混沌系统的两个初始值 (i_l, i_t)，按 2.3 节方法对置乱后的图像进行置混。

出于安全性的需要，可重复(1)、(2)两步多次。

其解密过程与加密过程类似，还原置乱过程，采用式(5)

的逆变换，还原置混过程，采用式(10)的逆变换

$$I(k)=\{\{\phi(k)\oplus C(k)\oplus C(k-1)+N-\phi(k)\}\bmod N\}\bmod 256 \tag{11}$$

$C(k-1)$是前一位明文像素产生的密文像素，初始值 $I(0)=C(0)$，$C(0)$等于加密过程中的 $C(0)$，为任意的 0 到 255 之间的一个整数，$C(k)$是当前明文像素产生的密文像素。

3 算法的安全性分析

一个好的加密算法应该能够抵抗各种密码分析攻击，并且其安全性不应该依赖于加密体制或算法的保密，而只依赖于密钥。针对本文提出的加密方案进行的各种安全性分析如下。

3.1 密钥空间分析

根据第 2 节的描述，在整个加密系统中，使用了三个不同的混沌系统。在混沌序列的产生过程中，需要三个不同的初始条件。假设计算机的计算精度为 16 位，那么在混沌密钥流的产生过程中的密钥空间就为 10^{48}，这将是一个非常大的数，使得穷举攻击不可能。

3.2 密钥敏感性测试

对于一个好的图像加密方案，其加密和解密过程都应该对密钥非常敏感。这有两层含义：Ⅰ)加密密钥的细微改变，应该得到两个几乎完全不同的加密图像；Ⅱ)解密密钥的细微改变，其解密过程将失败。

为此，用密文像素变化率(Cipher-text Pixel Change Rate，CPCR)来衡量密钥的敏感性：

$$CPCR=\frac{\sum_{i=1}^{W}\sum_{j=1}^{H}Difp(I(i,j),I'(i,j))}{W\times H} \tag{10}$$

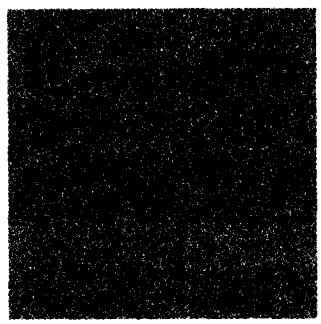
其中：

$$Difp(I(i,j),I'(i,j))=\begin{cases}1, & I(i,j)=I'(i,j)\\ 0, & I(i,j)\neq I'(i,j)\end{cases} \tag{11}$$

W,H 分别表示图像 I 和 I' 的宽和高。在本文的加密方案中，图像的置乱与置混是两个分离的过程。在下面的密钥敏感性测试实验中(512×512 的图像)，对于 $C(0)$直接取值 93。

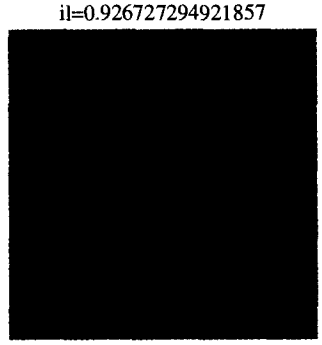
(1)加密密钥敏感性测试(表 1 和图 3)。

(a) Original Image



(b) Encrypted Image
it=0.726727294921875
il=0.926727294921857

(c) Encrypted Image
it=0.726727294921875
il=0.926727294921858



(d) Difference Image
(b) And (c)

图 3 加密密钥敏感性测试

(2)解密密钥敏感性测试。

实验结果表明，当密钥仅仅只有 2^{-16} 的微小变化时，加密后图像的像素灰度变化率都大于 99%，而解密几乎失败。因此，本文的算法具有很好的密钥敏感性。

3.3 抗选择明文图像攻击

对于文[1]提出的方案，在进行选择明文图像(整个图像的像素灰度值相同)密码分析的过程中，可以根据观察到的 $C(k)$，$C(k-1)$和 $I(k)$估算出 $\phi(k)$的取值区间，然后借助符号动力学和混沌迭代函数的逆映射，在计算机的有限精度下，可以得到混沌动力系统的初始值，即加密密钥，其详细过程见文[1]。这主要是因为常见的混沌加密系统中，在密钥流产生过程中泄漏了如下两个重要信息：每一位密钥产生的混沌动力系统以及每一位密钥产生所经历的迭代次数。而在本文的算法中，从式(1)和(2)可以看出，混沌序列依赖于两个混沌动力系统 $f(\cdot)$，$g(\cdot)$，并且在产生序列时，$f(\cdot)$所经历的迭代次数也是未知的，所以在进行文[1]中的选择明文图像密码分析时，将很难用符号动力学和混沌迭代函数的逆映射来分析加密密钥。在本文的算法中，如果取(2)式的 $Q=128$，则从 $\varphi(K)$计算混沌系统的初值 x_0 的上下边界时，执行的逆映射次数约为：

$$n_2=4\cdot 2^{6(k-1)} \tag{12}$$

在文[1]中，当 $K=42$ 时，得到了混沌系统的初值 x_0。如

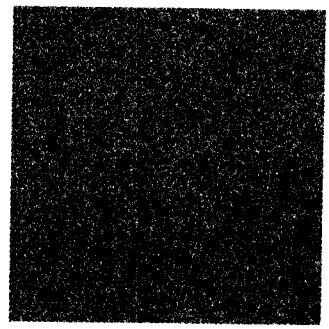
果按本文的算法加密，则得到混沌系统的初值 x_0 所经历的逆映射次数 $n_2=2^{248}$，并且这种逆映射次数将随着 K 的增大以指数形式增长，使得计算上不可能实现。

3.4 统计分析

一个好的图像加密算法应该具有好的抗统计分析攻击能力。下面的实验证明，本文的算法不仅具有良好的抗选择明文攻击能力，同时也具有良好的抗统计分析攻击能力。

(1)图像的灰度值统计直方图

(a) Original Image

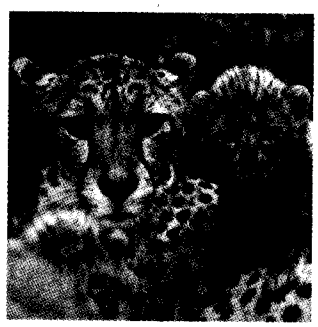


(b) Encrypted Image
it=0.726727294921875
il=0.926727294921857

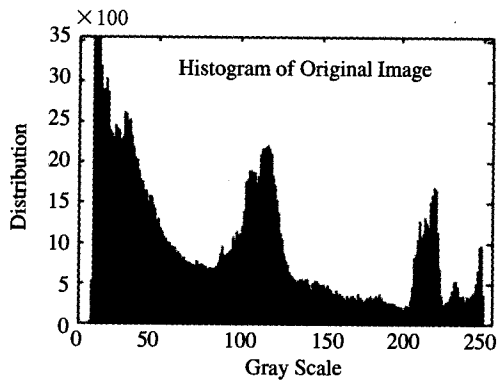
(c) Decrypted Image
it=0.726727294921875
il=0.926727294921857

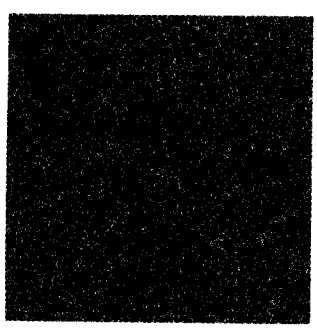
(d) Decrypted Image
it=0.726727294921875
il=0.926727294921858

图 4　解密密钥敏感性测试



(a) Original Image





(b) Encrypted Image

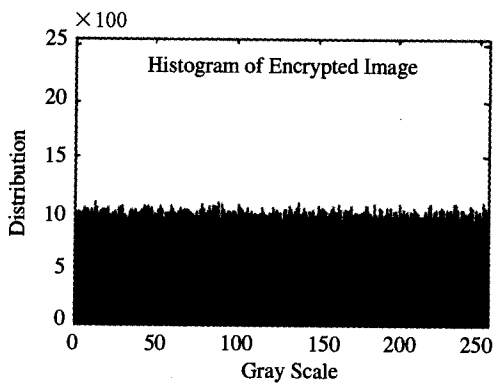


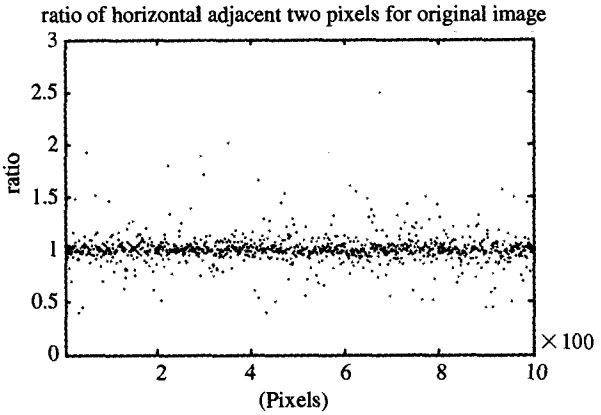
图 5　图像的灰度直方图

(2)两个相邻像素的相关性

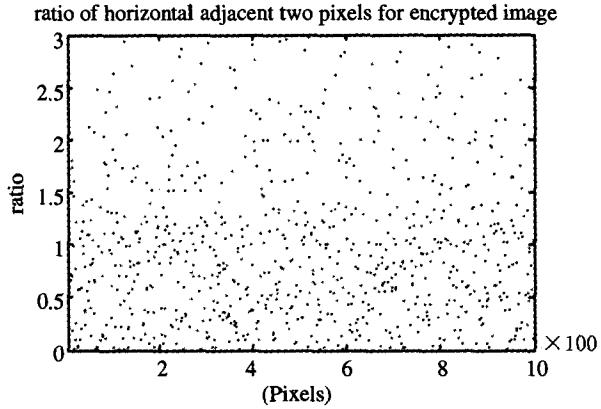
图像的本质特征决定了图像中相邻像素间存在较大的相关性，基于统计分析的攻击方法正是利用了图像的这一固有性质来进行密码分析。所以，一个好的图像加密算法应该破

坏像素间的这种相关性，从而增强算法的抗统计分析能力。可以借助概率论的相关系数来衡量相邻像素的相关性[7]，相关系数定义如下：

$$r_{xy}=\frac{\mathrm{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{13}$$



(a) 未加密图像的水平相邻像素的灰度值之比



(b) 加密图像的水平相邻像素的灰度值之比

图 6　图像的水平相邻像素的相关性

其中：x,y 是相邻像素的灰度值。在数值计算过程中，$E(\cdot)$，$D(\cdot)$和 $\mathrm{cov}(\cdot)$计算如下：

$$E(x)=\frac{1}{N}\sum_{i=1}^{N}x_i \tag{14}$$

$$D(x)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))^2 \tag{15}$$

$$\mathrm{cov}(x,y)=E[(x-E(x))(y-E(y))]=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))(y_i-E(y)) \tag{16}$$

仿真实验演示了从明文图像和加密图像中随机选取的1000个水平相邻像素对的灰度值之比(图6)。在图6(a)中，大多数水平相邻像素的灰度值之比接近于1，表明相邻像素的相关性比较高。而在图6(b)中，大多数水平相邻像素的灰度值之比比较分散，表明图像经加密后相邻像素的相关性较低。

结论　本文提出了一种新的基于随机混沌序列的图像加密算法，理论分析和仿真实验表明，本文的算法具有良好的密钥敏感性和很大的密钥空间，同时具有较好的抗统计攻击、差分攻击和选择明文攻击能力。不过，由于在加密的过程中，每个密钥的生成要经过多次迭代，因此本文的算法在加密的速度上有待进一步提高。

参 考 文 献

1 Wang K, Pei W J, Zou L H, et al. On the security of 3D Cat map based symmetric image encryption scheme. Physics Letters A, 2005, 343:432～439
2 Li S J, Mou X Q, Cai Y L, et al. On the security of a chaotic encryption scheme: problems with computerized chaos in finite computing precision. Computer Physics Communications, 2003, 153: 52～58
3 Alvarez G, Montoya F, Romera M, Pastor G. Cryptanalyzing an improved security modulated chaotic encryption scheme using ciphertext absolute value. Chaos, Solitons and Fractals, 2005, 23: 1749～1756
4 Alvarez G, Montoya F, Romera M, Pastor G. Cryptanalysis of dynamic look-up table based chaotic cryptosystems. Physics Letters A, 2004, 326: 211～218
5 Alvarez G, Montoya F, Romera M, Pastor G. Cryptanalysis of an ergodic chaotic cipher. Physics Letters A, 2003, 311: 172～179
6 Fridrich J. Symmetric ciphers based on two-dimensional chaotic maps. Int J Bifurcat Chaos, 1998, 8(6): 1259～1284
7 Chen G R, Mao Y B, Chui C K. A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos, Solitons and Fractals, 2004, 21: 749～761

(上接第 168 页)

5 Kennedy J, Everhart R C. Adiscrete binary version of the partical swarm algorithm. In: Proceedings 1997 Conference on Systems, Man and Cybernetics. Piscataway, NJ: IEEE Service Center, 1997. 4104～4109
6 Zeng Jianchao, Jie Jing, Cui Zhihua. Partical Swarm Optimization Algorithm. Beijing: Science Press, 2004
7 Liu Xiyu, Tang Mingxi, Frazer J H. An eco-conscious housing design model based on co-evolution. Advances In: Engineering Software, 2005, 36: 115～125
8 Miller BL, Shaw M J. Genetic algorithms with dynamic niche sharing for multimodal function optimization. In: Proc of the IEEE International Conference on Evolutionary Computation. Piscataway, NJ: IEEE. 1966. 786～791
9 Clearwater S H, Hogg T, Huberman B A. Cooperative problem solving. In: Computation: The Micro and Macro View, Singapore: World Scientific, 1992. 33～70
10 Cioppa A D, De Stefano C, Marcelli A. On the role of population size and niche radius in fitness sharing. IEEE Trans. Evolutionary Computation, 2004, 8(6): 580～592
11 van den Bergh F, Engelbrecht A P. A cooperative approach to particle swarm optimization. IEEE Trans Evolutionary Computation, 2004, 8(3): 225～239
12 Parsopoulos K E, Vrahatis M N. On the computation of all global minimizers through particle swarm optimization. IEEE Trans Evolutionary Computation, 2004, 8(3): 211～224
13 García-Pedrajas N, Hervás-Martínez C, Ortiz-Boyer D. Cooperative coevolution of artificial neural network ensembles for pattern classification. IEEE Trans Evolutionary Computation, 2004, 9(3): 271～302
14 Cioppa A D, De Stefano C, Angelo Marcelli. On the role of population size and niche radius in fitness sharing. IEEE Trans. Evolutionary Computation, 2004, 8(6): 580～592
15 Liu Xiyu, Tang Mingxi, Frazer J H. An eco-conscious housing design model based on co-evolution, Advances in Engineering Software, 2005, 36: 115～125
16 Eberhart R C, Simpson P, Dobbins R. Computational Intelligence PC Tools. Academic, 1996, 6: 212～226
17 Angeline P J. Using selection to improve particle swarm optimization. In: Proc IEEE World Congress on computational intelligence, ICEC-98, Anchorange, Alaska, 1998. 84～89
18 Angeline P J. Evolutionary optimization versus particle swarm optimization: philosophy and performance differences. In: Porto V W, Saravanan N, Waagen D E, et al. Eds. Evolutionary Programming VII, 7th International Conference, EP98. San Diego, CA, USA, 1998. 601～610
19 Suganthan P. Particle swarm optimiser with neighbourhood operator. In: Angeline, P J, Michalewicz Z, Schoenauer M, Proceedings of the Congress of Evolutionary Computation. Vol 3. IEEE Press, 1999. 1958～1962
20 Kennedy J. Small worlds and mega-minds: effects of neighborhood topology on particle swarm performance. In: Proc Congress on Evolutionary Computation. Piscataway, NJ: IEEE Service Center, 1999. 1931～1938
21 Clerc M, Kennedy J. The particle swarm-explosion, stability, and convergence in a multidimensional complex space. IEEE Trans. Evolutionary Computation, 2002, 6: 58～73