一种新的数字化混沌扰动方案*)

刘 镔 张永强 刘粉林
(解放军信息工程大学信息工程学院 郑州450002)

摘 要 在混沌系统中施加主动扰动是混沌从理论研究向实际应用转化的有效手段。本文提出了一种对数字化混沌系统进行扰动的可行方案,该方案选择性地扩散数字化混沌系统的部分变量,以达到对整个系统的扰动。扰动后系统可生成具有均匀的不变分布和良好密码学特性的伪随机序列。实验的数据表明该扰动方案有效地补偿了数字化混沌系统动力学特性的退化。

关键词 数字化混沌,伪随机数,扰动系统变量,分段线性混沌函数

A New Scheme on Perturbing Digital Chaotic Systems

LIU Bin ZHANG Yong-Qiang LIU Fen-Lin
(Information Engineering Institute, The PLA Information Engineering University, Zhengzhou 450002)

Abstract A scheme on perturbing the values of variables in digital chaotic system is investigated. Perturbation-based algorithm can make those theories on chaos applicable for digital devices with finite precision. After being perturbed, chaotic system can generate chaotic binary sequences with uniform distribution and statistical properties invulnerable to cryptographic analysis. The simulation result shows that the perturbing scheme in this paper is effective.

Keywords Digital chaotic systems, Pseudo-random sequence, Perturbing value of variable, Piecewise linear chaotic map (PWLCM)

1 引言

序列密码算法多为对明文和密钥流进行异或运算得到密文,因而密钥流的产生是加密的关键,系统的安全性也由伪随机密钥流的统计性质所决定。

混沌序列具有良好随机性、相关性和复杂性,对初始条件极端敏感,难以被分析和预测,因而在密码学领域具有良好的应用前景。混沌系统在密码学特别是序列密码方面的运用成为近年来备受关注的热点。

在经典混沌理论中,动力学系统均为定义在连续域上,但在计算机和其他数字系统实际实现时,由于有限精度效应,需要对混沌系统数字化,不可避免地导致混沌系统的动力学特性退化(产生短周期效应,严重不平衡的分布函数和较低的线性复杂度等)。因此,能否在有限精度下实现是决定混沌系统可否应用于实际的关键,其核心问题是数字化混沌系统动力学特性退化的补偿。

目前补偿数字化混沌系统动力特性退化的方式主要有三种,分别为:1)提高精度,2)使用级联的多个混沌系统,3)对混沌系统施以主动的扰动。周红等[1]指出前两类方式中,提高精度的方式是一种消极的策略,难以保证混沌信号的周期绝对达到指定的要求,且精度的提高并不能使得混沌信号的平均周期相应地增加;而级联多个混沌系统的方式也不能完全避免短周期的出现。实际应用过程表明,对混沌系统进行扰动是目前所知的最简单有效的一种方式[2]。

现有对混沌系统的扰动方法主要有两类:扰动混沌系统参数和扰动混沌系统变量。在扰动混沌系统变量方面,有周红等[3]提出的使用线性反馈移位寄存器(LFSR)产生 m 序列的扰动策略,以及桑涛等[4]对周红提出的策略的改进,使用了简单满足均匀分布的伪随机数发生器(PRNG)对混沌变量进行扰动。但应当看到,应用这类策略扰动的数字化混沌系统,其产生出的伪随机序列周期上限会受到扰动信号周期的制约。本文提出的对混沌系统变量进行选择性扩散的策略在某种程度上克服了此类缺陷,可以有效地补偿数字化混沌系统动力学特性的退化。

2 扰动混沌系统变量算法的描述

在区间[0,1]上定义如下分段线性函数 g,将区间[0,1]分为 2^n 个等长片断 $I_1=[0,\frac{1}{2^n})$, $I_2=[\frac{1}{2^n},\frac{2}{2^n})$, $\cdots$, $I_{2^n}=[\frac{2^n-1}{2^n},1]$,在每个片断 I_i 上定义 g 为:$g(x)|I_i=g_i(x)=a_ix+b_i$,在片断 I_i 上的每个元素将由 g_i 映射到[0,1],即对$\forall i$, $i=1,\cdots,2^n$, $g_i:I_i\to[0,1]$为双射。

在分段线性函数 g 的基础上,构造如下函数 f:选取区间[0,1]的一个片断 I_k,并设定扩散系数 $e\in[0,1]$,将区间 I_k 按照 $e:1-e$ 的比例分为两个部分,记为 I_{k1} 和 I_{k2}。在每一次迭代中,如果系统变量未取到所选取的片断中即 $x\notin I_k$,则选取 $f=g$;如果 $x\in I_{k1}$,则 $x':=\frac{k-1}{e}(x-\frac{k-1}{2^n})$,并继续迭代过程得到 $f(x)=g(x')=g(\frac{k-1}{e}(x-\frac{k-1}{2^n}))$;如果 $x\in I_{k2}$,则得到 $x':=\frac{2^n-k}{1-e}(x-\frac{k-1}{2^n}-\frac{e}{2^n})+\frac{k}{2^n}$ 和 $f(x)=g(\frac{2^n-k}{1-e}(x-\frac{k-1}{2^n}-\frac{e}{2^n})+\frac{k}{2^n})$。

通过上述的算法,将所选择的片断 I_k 内的系统变量扩散

*)基金项目:国家自然科学基金(60374004);河南省杰出青年基金(0412000200)。刘 镔 硕士研究生,研究方向为混沌加密,信息隐藏;张永强 硕士研究生,研究方向为混沌控制,混沌保密通信;刘粉林 博士后,教授,主要研究方向为复杂系统控制,信息安全。

到了其他的片断中，达到了扰动系统变量的目的。

3 扰动算法分析

加入了上述的主动扰动后的迭代函数可以表示为：

$$f(x)=\begin{cases} g(x) & x\notin I_k \\ g(\frac{k-1}{e}(x-\frac{k-1}{2^n})) & x\in I_{k1} \\ g(\frac{2^n-k}{1-e}(x-\frac{k-1}{2^n}-\frac{e}{2^n})+\frac{k}{2^n}) & x\in I_{k2} \end{cases}$$

定理1 上述定义的函数 f 有如下的性质：1）f^{-1} 是 Lebesgue 意义下的保测变换；2）$x_{n+1}=f(x_n)$ 是个混沌迭代函数；3）函数 f 对应的不变分布为 $\rho(x)=1$。

证明：1）设 $I=(x_0,x_0+\Delta x)\subset[0,1]$，只要证明测度 $\mu(f^{-1}(I))=\Delta x$ 即可。

设 $f^{-1}(I)$ 对应于 $[0,\frac{k-1}{2^n}]$ 中的长度为 Δx_1，对应于 $[\frac{k}{2^n},1]$ 中的长度为 Δx_2，对应于 $[\frac{k-1}{2^n},\frac{k}{2^n}]$ 中的长度为 Δx_3，则有：

$$\frac{\Delta x_1}{(k-1)/2^n}=\Delta x,\frac{\Delta x_2}{(2^n-k)/2^n}=\Delta x$$

并且设 Δx_{31} 为将区间 I_{k1} 变换到 $[0,\frac{k-1}{2^n})$ 后所对应的区间长度，则 $\frac{(k-1)/2^n}{e/2^n}\Delta x_{31}=\Delta x$，$\Delta x_{32}$ 为将区间 I_{k2} 变换到 $[\frac{k}{2^n},1]$ 后所对应的区间长度，则 $\frac{(2^n-k)/2^n}{(1-e)/2^n}\Delta x_{32}=\Delta x$。此时，

$$\mu(f^{-1}(I))\Delta x_1+\Delta x_2+\Delta x_3=\Delta x_1+\Delta x_2+\Delta x_{31}+\Delta x_{32}$$
$$=\frac{k-1}{2^n}\Delta x+\frac{2^n-k}{2^n}\Delta x+\frac{e}{2^n}\Delta x+\frac{1-e}{2^n}\Delta x=\Delta x$$

所以，f 是 Lebesgue 意义下的保测变换。

2）上述函数 f 的 Lyapunov 指数为：

$$\lambda=\lim_{m\to\infty}\frac{1}{m}\sum_{i=1}^{m}\ln|f'(x_i)|=\lim_{m\to\infty}\frac{1}{m}\sum_{i=1}^{m}\lim_{x\to\infty}\ln 2^n=n\ln 2>0$$

因此，函数 f 为一个混沌函数。

3）要证明函数 f 对应的不变分布为 $\rho(x)=1$，只要证明概率 $P\{x|f(x)<y\}=y$ 即可。

$$P\{x|f(x)<y\}$$
$$=P\{x|f(x)<y,x\in\cup_{i=1}^{k-1}\}I_i \text{ 或 } x\in\cup_{i=k+1}^{2^n}I_i\}+P\{x|f(x)<y,x\in I_k\}$$
$$=\sum_{i=1}^{k-1}P\{x|f(x)<y,x\in I_i\}+\sum_{i=k+1}^{2^n}P\{x|f(x)<y,x\in I_i\}+P\{x|f(x)<y,x\in I_k\}$$
$$=\sum_{i=1}^{k-1}\frac{1}{2^n}y+\sum_{i=k+1}^{2^n}\frac{1}{2^n}y+P\{x|f(x)<y,x\in I_{k1}\}+P\{x|f(x)<y,x\in I_{k2}\}$$
$$=\frac{2^n-1}{2^n}y+\frac{e}{2^n}y+\frac{1-e}{2^n}y=y$$

故 $\rho(x)=1$ □

通过简单的转换操作，我们就可以得到各比特位独立同分布的0-1序列：

定理2 设 $\{x_i\}$ 是混沌函数 f 的迭代轨迹，对 $\forall\ j\in N$ 取 $T_j(x)=\lfloor 2^j x\rfloor \bmod 2$ 为 $[0,1]\to\{0,1\}$ 的算子，可将上述轨迹转化成二进制比特流 $\{s_i\}$。$S_i=T_j(x_i)=\lfloor 2^j x_i\rfloor \bmod 2$。则 $\{S_i\}$ 的各比特位独立同分布，即

$\forall\ (a_1,a_2,\cdots,a_n)\in F_2^n(F_2^n=\underbrace{F_2\times\cdots\times F_2}_{n})$，

$p(S_1=a_1,\cdots,S_n=a_n)=2^{-n}$。

证明：不失一般性，只对 $j=1$ 给出证明。

$$P(x_0:T_j(x_i)=0)=P(x_0:x_i\in[0,\frac{1}{2}))$$
$$=P(x_0:f(x_0)\in[0,\frac{1}{2}))$$

由 f 的保测性可知 $P(x_0:f(x_0)\in[0,\frac{1}{2}))=\frac{1}{2}$，所以

$$P(x_0:T_j(x_i)=1)=P(x_0:T_j(x_i)=0)=\frac{1}{2}$$

用数学归纳法证明，当 $n=1$ 时，$P(s_i=a_i)=\frac{1}{2}$ 成立；

当 $n=2$ 时，不妨设欲扩散区间为 $I_k\subset[\frac{1}{2},1]$。对于 $P(s_1=a_1,s_2=a_2)$，仅证明 $a_1=1,a_2=0$ 的情况。

$$P(s_1=0,s_2=1)=P\{x_1:x_2\in[0,\frac{1}{2}),x_1\in[\frac{1}{2},1]\}=P\{x_1:x_2\in[0,\frac{1}{2}),x_1\in I_k\}+P\{x_1:x_2\in[0,\frac{1}{2}),x_1\in[\frac{1}{2},1]\backslash I_k\}$$
$$=\frac{1}{2}P\{x_1:x_1\in[\frac{1}{2},1]\backslash I_k\}$$
$$=\frac{1}{2}\times(\frac{1}{2}-\frac{1}{2^n})$$

$$P\{x_1:x_2\in[0,\frac{1}{2}),x_1\in I_k\}$$
$$=P\{x_1:x_2\in[0,\frac{1}{2}),x_1\in[\frac{k-1}{2^n},\frac{k-1}{2^n}+\frac{e}{2^n}]\}+P\{x_1:x_2\in[0,\frac{1}{2}),x_1\in[\frac{k-1}{2^n}+\frac{e}{2^n},\frac{k}{2^n})\}$$
$$=\frac{e}{2^n}\times\frac{\frac{1}{2}\times P\{x_1:x_1\in[0,\frac{k-1}{2^n})\}}{P\{x_1:x_1\in[0,\frac{k-1}{2^n})\}}+\frac{1-e}{2^n}\times\frac{\frac{1}{2}\times P\{x_1:x_1\in[\frac{k}{2^n},1)\}}{P\{x_1:x_1\in[\frac{k}{2^n},1)\}}$$
$$=\frac{e}{2^n}\times\frac{1}{2}+\frac{1-e}{2^n}\times\frac{1}{2}=\frac{1}{2^{n+1}}$$

所以 $P(s_1=0,s_2=1)=P\{x_1:x_2\in[0,\frac{1}{2}),x_1\in I_k\}+P\{x_1:x_2\in[0,\frac{1}{2}),x_1\in[\frac{1}{2},1]\backslash I_k\}=\frac{1}{2}\times(\frac{1}{2}-\frac{1}{2^n})+\frac{1}{2^{n+1}}=\frac{1}{4}$

同理可证 $a_1=0,a_2=0$；$a_1=1,a_2=0$；$a_1=1,a_2=1$ 时的情况，即 $P(s_1=a_1,s_2=a_2)=\frac{1}{4}$。又同理，对 $\forall\ i$ 有 $P(s_i=a_i,s_{i+1}=a_{i+1})=\frac{1}{4}$。

假设 $n=k$ 时 $P(s_1=a_1,\cdots,s_k=a_k)=2^{-k}$ 成立，则当 $n=k+1$ 时，

$$P(s_1=a_1,\cdots,s_k=a_k,s_{k+1}=a_{k+1})$$
$$=P(s_{k+1}=a_{k+1}|s_1=a_1,\cdots,s_k=a_k)p(s_1=a_1,\cdots,s_k=a_k)$$
$$=2^{-k}P(s_{k+1}=a_{k+1}|s_1=a_1,\cdots,s_k=a_k)$$

由于 $s_1=a_1,\cdots,s_k=a_k$ 独立，因此

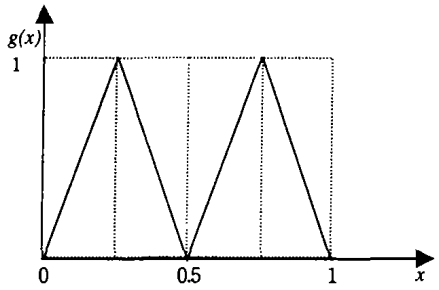
$$P(s_1=a_1,\cdots,s_k=a_k,s_{k+1}=a_{k+1})=2^{-k}p(s_{k+1}=a_{k+1}|s_k=a_k)$$
$$=2^{-k}\cdot\frac{1/4}{1/2}=2^{-k-1}$$

所以由数学归纳法可知，$s_1=a_1,\cdots,s_k=a_k$ 独立同分布。 □

4 算法实例及数据

程序运行平台为安装了 Microsoft Windows 操作系统的32位字长的普通 PC 机。首先构造如下一个分段线性函数：

$$g(x)=\begin{cases} 4x & 0\leqslant x\leqslant\frac{1}{4} \\ 2-4x & \frac{1}{4}\leqslant x\leqslant\frac{1}{2} \\ g(1-x) & \frac{1}{2}\leqslant x\leqslant 1 \end{cases}$$



函数定义区间的四个片断分别为 $c_1=[0,\frac{1}{4})$，$c_2=[\frac{1}{4},\frac{1}{2})$，$c_3=[\frac{1}{2},\frac{3}{4})$，$c_4=[\frac{3}{4},1]$。该函数为典型的分段线性混沌函数。由于有限精度的效应，实际得到的函数轨迹会出现短周期行为，图1为函数 $g(x)$ 迭代10,000次的轨迹（初值 $x_0=0.2776$），可以明显看到短周期的存在。

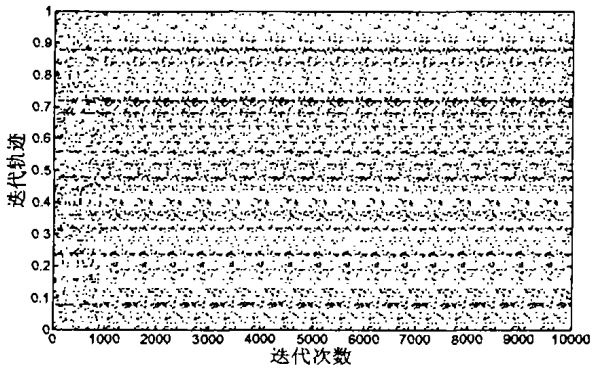


图1　混沌函数 $g(x)$ 的迭代轨迹 $g^n(x_0)$

不失一般性，可选择对 $g(x)$ 定义区间的第3子区间 $c_3=[\frac{1}{2},\frac{3}{4})$ 进行扩散，并设定扩散系数 $e=0.001$，将片断 c_3 按照 $e:1-e$ 的比例分成两段 $c_{31}=[\frac{1}{2},\frac{1}{2}+\frac{e}{4})$，$c_{32}=[\frac{1}{2}+\frac{e}{4},\frac{3}{4}]$，并按照选择性扩散的扰动算法形成新的函数：

$$f(x)=\begin{cases} g(x) & x\notin c_3 \\ g(\frac{2}{e}(x-\frac{1}{2})) & x\in c_{31} \\ g(\frac{(x-(\frac{1}{2}+\frac{e}{4}))}{1-e}+\frac{3}{4}) & x\in c_{32} \end{cases}$$

图2为扰动后函数 $f(x)$ 迭代10,000次的轨迹（初值 $x_0=0.2776$）

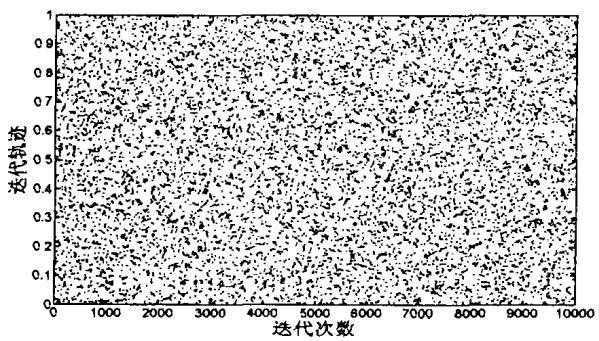


图2　混沌函数 $f(x)$ 的迭代轨迹 $f^n(x_0)$

实验中将函数迭代1,000,000次，并应用 $T_j(x)=\lfloor 2^j x \rfloor \bmod 2$ 对 $f(x)$ 的轨迹进行处理，得到长为1,000,000的0-1序列 S，序列 S 具有如图3所示的类 $\delta(\cdot)$ 的自相关函数，如图4的线性复杂度。

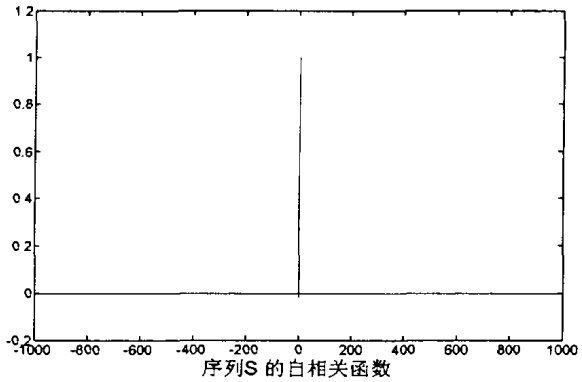


图3　序列 S 的自相关函数

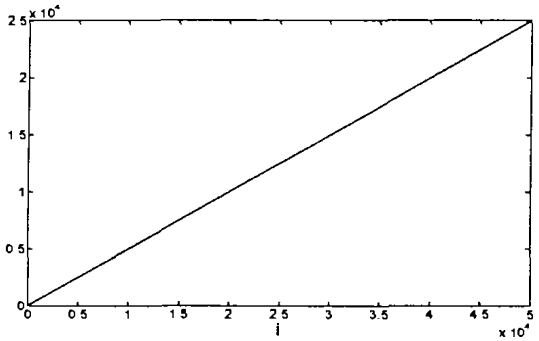


图4　线性复杂度

序列中0-1的比率为499147：500853，序列的0-1平衡性如图5所示。同时考虑不同初值得到序列的性能，从0开始以步长0.0001对[0,1]区间取样作为迭代初值，得到序列中0所占的比率如图6所示。

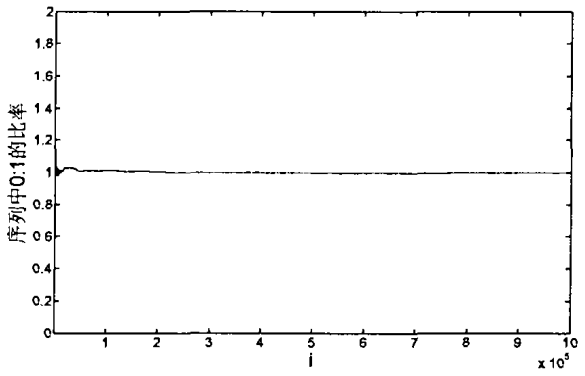


图5　序列中0:1比率

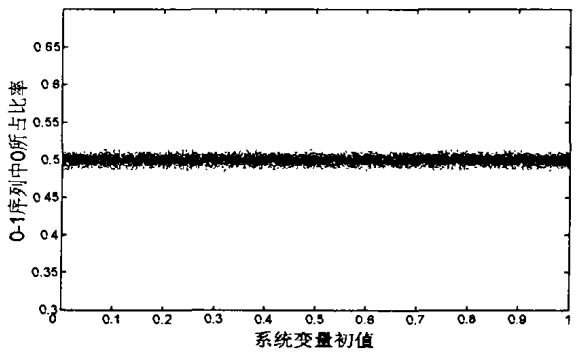


图6　不同初值得到序列中0所占的比率

结论　本文提出的选择性扩散混沌系统变量的扰动策略能够克服数字化混沌系统的短周期效应，对系统的动力学特性退化进行了有效的补偿。同时，该策略避免了因为使用外加

一个SPEA改进算法及其收敛性分析*)

吴作顺[1] 王 石[2]

(总参第六十一研究所 北京100039)[1] (国防科技大学电子工程学院 长沙410073)[2]

摘 要 SPEA是一种多目标优化算法。与其它多目标进化算法相比,SPEA算法具有设置参数少、解在空间分布均匀等优点。本文引入多点交叉和Cauchy变异对SPEA算法的收敛速度进行了改进,并对其收敛性进行了分析,文中给出的仿真算例证实了改进方法的有效性。

关键词 多目标优化,SPEA改进算法,收敛性分析

An Improved SPEA and its Convergence

WU Zuo-Shun[1] WANG Shi[2]

(PLA 61st Research Institute, Beijing100039)[1] (School of Electronic Engineering, Nat'l Univ. of Defense Tech., Changsha410073)[2]

Abstract SPEA (Strength Pareto-Optimal Evolutionary Algorithm) is a Multi-Objective Evolutionary Algorithm (MOEA). Compared with other MOEA's, it has the advantages of fewer parameters and well-distributed solutions in objective function spaces. In this paper, a new multiple-chromosome crossover operator and a Cauchy mutation operator are introduced into SPEA to speed up the algorithm. The convergence of the algorithm is also presented for the first time. The effectiveness of the improved SPEA is proved by our experiments.

Keywords Multi-objective optimization, Improved SPEA, Convergence analyses

1 引言

在实际工程应用中,经常遇到同时优化多个目标函数的问题,而且多目标一般是相互抵触的,这就是多目标优化问题。其一般数学模型可描述如下:

V-max $f(x)=[f_1(x),f_2(x),\cdots,f_n(x)]^T$

$x\in X$(X为一给定集合,称为状态空间)

其中V-max表示向量极大化,即$f(x)=[f_1(x),f_2(x),\cdots,f_n(x)]^T$中的各个子目标函数都尽可能地极大化。当然,也可等价地表示为V-min。

多目标优化问题一般没有唯一的完全解,而是具有一系列的非劣解(或非支配解)构成的解集合,通常称为Pareto最优解。非劣性的定义如下:

定义1 设X是多目标优化的状态空间,$f(x)$是向量目标函数,$x_1\in X$,$x_2\in X$,称x_2非劣于x_1,或x_2优于x_1,记作$x_1<x_2$,$\forall i\in\{1,2,\cdots,n\}$,$f_i(x_1)\leqslant f_i(x_2)\cdots\exists i\in\{1,\cdots,n\}$,$f_i(x_1)<f_i(x_2)$。

定义2 设X为多目标优化模型的状态空间,$f(x)$是向量目标函数。若$x\in X$,并且不存在比$\bar{x}$更优越的x,则称$\bar{x}$是多目标化模型的Pareto最优解。所有解$\bar{x}$构成的集合称为Pareto最优集。

多目标优化问题的本质在于多数情况下各个子目标是相互冲突的,要使多个子目标同时达到最优值是不可能的,而只能对它们进行协调和折衷处理,使各个子目标尽可能达到最优。

进化算法(EA:Evolution Algorithm)对整个群体进行的进化运算操作,它具有隐含的并行性,并着眼于个体集合的操作,而多目标优化问题的Pareto最优集一般也是一个集合,

*)受国家自然科学基金60303012资助。吴作顺 博士后,主要研究方向为网络安全与进化计算。王 石 博士后,主要研究方向为系统建模与仿真。

扰动信号而带来的对所产生序列周期长度的约束。在实际应用中,我们可以决定等分[0,1]区间的子区间的数目,并可以选择扩散若干个子区间的变量,而扩散系数e也可以自由选取。在混沌序列应用于序列密码时,这类参数都可以作为系统的密钥,从而极大地增大了密钥空间,增强了加密系统的安全性。

本方案的结果表明对混沌系统变量进行选择性扩散策略是混沌动力学从理论模型到实际应用的一个新的有效途径。

参 考 文 献

1 周红.一类混沌密码序列的设计方法及其有限精度实现问题分析:[复旦大学博士学位论文].1996

2 李树钧.数字化混沌密码的分析与设计:[西安交通大学博士学位论文].2003

3 周红,凌燮亭.有限精度混沌系统的m序列扰动实现.电子学报,1997,25(7):95~97

4 Sang Tao, Wang Ruili, Yan Yixun. Perturbance-based algorithm to expand cycle length of chaotic key stream. Electronics Letters, 1998,34(9):873~874

5 Li Shujun, Mou Xuanqin, Cai Yuanlong. Pseudo-random bit generator based on couple chaotic systems and its application in stream-ciphers cryptography. In: Progress in Cryptology - INDOCRYPT 2001, Lecture Notes in Computer Science vol. 2247, Sringer-Verlag, Berlin, 2001.316~329

6 赖溪松,等著,张玉清,肖国镇,改编.计算机密码学及其应用.国防工业出版社,2001