基于离散动力学反控制的混沌序列密码算法

赵耿，李文健，马英杰

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.210300116

基于离散动力学反控制的混沌序列密码算法

赵　耿[1,2]　李文健[1,2]　马英杰[2]
1 西安电子科技大学通信工程学院　西安 710071
2 北京电子科技学院密码系　北京 100070
(zg@besti.edu.cn)

摘　要　针对离散混沌动力学系统在数字域上存在退化简并的问题,提出了一种可以配置系统的Lyapunov指数全部为正的算法,该算法基于混沌反控制原理,首先引入一个反馈矩阵,将该矩阵中的所有参数做了细致的规定设置,从理论角度证明了该算法能将Lyapunov指数配置为全正。随后对系统轨道的有界性和Lyapunov指数的有限性进行了证明,再通过几个算例对配置的数值进行仿真分析和性能比较,验证了所提算法能产生无简并的离散混沌系统,而且在数值准确性和算法运行时间方面存在一定的优势。再利用配置好的混沌系统生成序列然后量化,量化方案为取出序列有效数字组合,对该序列进行一些动态变换处理加强输出序列的随机性和序列的复杂性。将经过变换的输出序列转换为二进制序列,进行多项随机性和统计性测试,与一般混沌序列进行性能比较,测试结果表明该序列有着更好的随机特性,能够应用于混沌序列密码体制中。

关键词:反控制;Lyapunov指数;混沌系统;序列密码
中图法分类号　TN918.91

Chaotic Sequence Cipher Algorithm Based on Discrete Anti-control

ZHAO Geng[1,2],LI Wen-jian[1,2] and MA Ying-jie[2]
1 School of Telecommunication Engineering,Xidian University,Xi'an 710071,China
2 Department of Cryptography,Beijing Electronic Science and Technology Institute,Beijing 100070,China

Abstract　Aiming at the degeneracy problem of discrete chaotic dynamics system in the digital domain,an algorithm that can configure the Lyapunov exponents of the system to be all positive is proposed. The algorithm is based on the principle of chaos anti-control. First,a feedback matrix is introduced. All the parameters in the set are specified carefully,and it is proved from a theoretical point of view that the algorithm can configure the Lyapunov exponent to be fully positive. Subsequently,the boundedness of the system orbit and the finiteness of the Lyapunov exponent are proved,and the numerical simulation analysis and performance comparison of the configuration are carried out through several examples,so as to verify that the algorithm can produce a discrete chaotic system without degenerate. There are certain advantages in numerical accuracy and algorithm running time. The configured chaotic system is then used to generate the sequence and then quantized. The quantization scheme is to take out the effective digital combination of the sequence. Some dynamic transformation processing on the sequence can enhance the randomness and complexity of the output sequence. We convert the transformed output sequence into a binary sequence,perform a number of randomness and statistical tests,and compare the performance with the general chaotic sequence. The test results show that the sequence has better random characteristics and can be used in a chaotic sequence cipher system.

Keywords　Anti-control,Lyapunov exponent,Chaotic system,Sequence cipher

1　引言

20世纪90年代,混沌和密码的诸多一致性被人们发现,将混沌理论应用在密码学之中的依据是混沌的基本特征,即对初始条件的敏感依赖性、拓扑传递性和长期不可预测性,与密码学中强调的“扩散”与“混淆”相对应,将该混沌信号应用于通信加密中,能够很好地保障密码体制的安全性。经过多年的探索,混沌密码学已成为保密通信和信息安全领域[1-3]的一个重要分支。

在对动力学混沌的研究与分析中,Lyapunov指数(LE)[4]是混沌系统特征的定量表达方式,它能很好地表现出混沌轨迹运动行为对初始参数的敏感性。当LE小于0时,

到稿日期:2021-03-11　返修日期:2021-07-22
基金项目:国家自然科学基金面上项目(61772047);2018－2021年北京市“高精尖”学科建设项目创新类项目(3201017)
This work was supported by the National Natural Science Foundation of China(61772047) and “High-Precision” Program Construction Project in Beijing Universities (3201017).
通信作者:李文健(594253850@qq.com)

对应周期运动，这种状态下对系统初始值不敏感；当 LE 等于 0 时，对起始的微小差异不起放缩作用，此时为稳定系统。当 LE 值为正时，状态空间中的相邻轨道按照指数的方式发散，相邻点会快速发生分离，这一现象会使得系统轨迹局部不稳定，在全局有限的情况下，轨迹的相互靠近和分散形成了难以预测的混沌态运动。

在针对离散动力学系统的反控制研究方面，Chen 等[5-6]取得了很多成果，他们首先提出了一种反馈控制算法，该算法通过加入反馈控制器，并给控制器的形式做一定限制，保证系统 LE 配置大于预先设置的一组正常数，与此同时还能产生 Devaney 和 Li-Yorke 意义的混沌。后来 Wang 等[7]设计了另一种新的 Wang-Chen 算法，首先加入适合的控制器，再针对系统进行部分扰动，其也能达到和前者相同的效果。这两种算法为解决离散系统反控制的问题奠定了基础，一定程度上缓冲了离散动力学系统产生退化等问题。

近年来，有许多学者利用混沌反控制法[8]来加强混沌效应。文献[9]提出给定一组非对角反馈矩阵，但是当系统快速扰动时，会使控制性能受到一定程度的影响。文献[10]提出了一个脉冲控制器，应用脉冲控制的方法来达到稳定线性系统混沌化，但其只能解决一类稳定线性系统混沌化问题。文献[11]提出了一类较为通用的的反馈器，首先添加某种形式的反馈系统，再对受控系统进行取余运算，根据原矩阵中各个特征值与特征向量的关系来确定控制矩阵，从而对整个系统的 Lyapunov 指数进行配置。文献[12]引入了一个线性控制反馈器，构成了一套渐近稳定线性系统，从而可以配置多个正 Lyapunov 指数，随后给出了 4 维和 5 维系统的配置步骤。

本文第 2 节介绍了混沌系统退化简并的原因以及抗退化的技术方案；第 3 节提出了一个基于混沌反控制技术配置 LE 全部为正的算法，来实现系统的无简并；第 4 节将配置的混沌系统生成的实数值序列量化，得到二进制序列，然后在 matlab 中进行仿真测试，对序列进行多项随机性测试，并分析结果；最后进行全文总结。

2　混沌退化分析及抗退化方法

因为实际计算平台中只能保留有效位数来进行运算，而单个混沌系统在经过有限次迭代之后，小数点后的位数可能已经超出了软硬件所能表示的精度[13]的上限，此时就出现了保留多少位有效位的问题。以 Logistic 混沌系统为例，如果当前软件的计算精度为 N 位，则可以计算出该映射在[0,1]区间上最多有 10^N+1 个不同的数据点。因此，在有限精度效应下混沌迭代的序列，最终要么收敛于不动点，要么进入到一个循环，下面对 Logistic 映射 $x_{n+1}=\mu x_n(1-x_n)(\mu=4)$ 进行计算和分析。

(1)精度取 1 位有效数字

如果当前计算平台只能保存有限位数字，比如这里取小数点后 1 位，则在[0,1]区间上一共能保存 $10^1+1=11$ 个不同的数据点(0,0.1,0.2,0.3,0.4,0.5,0.6,0.7,0.8,0.9,1.0)，遇到多位小数，一般采取四舍五入的方法离散，则有图 1 所示的状态。

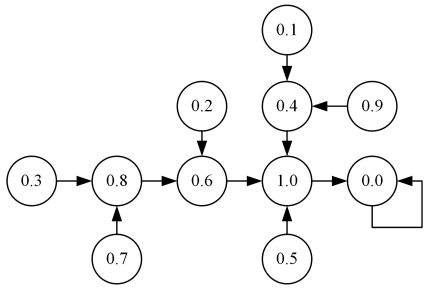

图 1　Logistic 映射状态转移图

Fig. 1　Logistic mapping state transition diagram

可以看出，各状态值最终都会收敛于不动点 0.0。

(2)精度取 2 位有效数字

当有限位取小数点后 2 位时，则在[0,1]上一共有 $10^2+1=101$ 个不同的数据点，通过对 Logistic 方程进行多次迭代计算，发现存在两个不动点 0.00 和 0.75，而且数据点还会进入一个循环 0.12→0.42→0.97→0.12。

在计算平台只能保留有限位数来进行运算的情况下，最后发现序列不是到达于某个不动点，就是进入到一个循环。为了解决有限精度效应带来的混沌系统退化简并问题，学者们进行了多年的分析研究，下面介绍一些研究成果来描述如何克服有限精度效应。

(1)提高计算精度[14]。显然，精度的提高会使相空间内的离散点数量增加，系统轨道会更加分离，周期性也得到改善，然而这种方法会大大增加计算的代价，所以在实际中并不常见。

(2)级联多个混沌系统[15]。级联是将多个系统串联并使状态值在之间传递，该方案能有效增加输出序列的周期，在某些情况下可以使部分已经退化的混沌系统重新回归到混沌状态。然而多个混沌系统的叠加可能导致系统轨道的相互重合，从而产生比之前更严重的退化状态。

(3)混沌反控制法[8]。在有限精度效应下，混沌系统相邻近的轨道会发生重合现象，正的 LE 在系统发生行为改变时会发生简并的情况，产生的结果是正的 LE 随着运动轨迹的汇聚转化为负的 LE。对于离散系统而言，假如系统轨迹全局有界，且至少有一个 LE 为正，那么系统就是混沌的；如果有两个以上 LE 为正，那么系统就是超混沌的。系统中正的 LE 个数越多，则混沌行为越强。因此，混沌系统的抗退化只需要 LE 为正的个数大于 1，而无退化、无简并的离散混沌系统则需要全部的 LE 都为正。

因此在设计时，通过混沌的反控制方法，考虑引入一个受控制的反馈系统，让整个系统正的 LE 个数达到最大，来实现系统的无简并，从而最大程度地改善系统的周期性和随机性。对于 n 维离散系统来说，正的 LE 个数的最大值为 n[16-18]。

3　离散混沌系统无简并：配置 Lyapunov 指数全部为正的算法

3.1　受控系统矩阵的配置原理和步骤

针对一个 n 维的离散时间系统：

$$x_{k+1}=\boldsymbol{A}x_k \tag{1}$$

其中，$x_k\in R^n$ 为某时刻的状态，且矩阵 $\boldsymbol{A}$ 如下：

$$\boldsymbol{A}=\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \tag{2}$$

若想通过反控制的方式来实现系统的无退化，需要设计一个反馈控制器 u_k，来使整个系统具有不错的混沌性能，即受控系统为全局有界并且具有正的 LE，而且符合 Devaney 混沌定义或者 Li-Yorke 混沌定义。

现有如下状态反馈系统，如式(3)所示：

$$u_k=\boldsymbol{B}x_k \tag{3}$$

其中，$\boldsymbol{B}\in R^{n\times n}$ 为待定矩阵。则整个系统如式(4)所示：

$$x_{k+1}=\boldsymbol{A}x_k+\boldsymbol{B}x_k \tag{4}$$

受控系统(4)的 Jacobi 矩阵如式(5)所示：

$$\boldsymbol{J}_k(z)=\boldsymbol{A}+\boldsymbol{B}=\boldsymbol{J} \tag{5}$$

记 $\boldsymbol{T}_k$ 为：

$$\begin{aligned}\boldsymbol{T}_k&=\boldsymbol{T}_k(x_0,\cdots,x_k)\\&=\boldsymbol{J}_k(x_k)\boldsymbol{J}_{k-1}(x_{k-1})\cdots\boldsymbol{J}_1(x_1)\boldsymbol{J}_0(x_0)\\&=\boldsymbol{J}_k\end{aligned} \tag{6}$$

并记 λ_i^k 为：

$$\lambda_i^k=\lambda_i[\boldsymbol{T}_k^{\mathrm{T}}\boldsymbol{T}_k] \tag{7}$$

λ_i^k 为第 k 个乘积矩阵 $\boldsymbol{T}_k^{\mathrm{T}}\boldsymbol{T}_k$ 的第 i 个特征值，也即矩阵 $\boldsymbol{T}_k$ 的第 i 个奇异值的平方。

通过 LE 的相关定义，整个系统(4)的第 i 个 LE 为：

$$LE_i=\lim_{k\to\infty}\frac{1}{2k}\ln|\lambda_i[\boldsymbol{T}_k^{\mathrm{T}}\boldsymbol{T}_k]|,i=1,2,\cdots,n \tag{8}$$

即$\{\boldsymbol{T}_k\}$奇异值序列的极限。

为了保证系统(4)的全部 LE 个数都可以计算出结果，并且满足所有 LE 数值大于 0 的条件，需要计算出反馈增益矩阵 $\boldsymbol{B}$，使得式(9)成立。

$$\begin{cases}LE_i<\infty, & \forall i\in\{1,\cdots,n\}\\ LE_i>c, & \forall i\in\{1,\cdots,n\}\end{cases} \tag{9}$$

因此，接下来要通过指定反馈矩阵 $\boldsymbol{B}\in R^{n\times n}$ 的形式，来达到所有 LE 数值大于 0 的目的，最后得到的整个系统的 LE 将会满足式(9)。

下面先介绍线性代数中一些相关的定理和性质，方便之后的证明。

性质 1 对于 n 阶矩阵，若每个主对角元素模都大于与同行的其他元素模的和，则该矩阵“严格对角占优”，即 $|a_{ii}|>\sum_{j=1,j\neq i}^{n}|a_{ij}|,i=1,2,\cdots,n$。

严格对角占优矩阵有两个相关的性质：

(1)如果矩阵严格对角占优，那么它一定可逆；

(2)如果实对称矩阵(满足严格对角占优)的主对角元素 $a_{ii}>0$，那么它一定为正定矩阵。

定理 1 对于对称矩阵 $\boldsymbol{X}$ 和 $\boldsymbol{Y}$，满足以下关系式 $\boldsymbol{X}>0$，$\boldsymbol{Y}>0$，$\boldsymbol{X}-\boldsymbol{Y}>0$，那么特征方程 $|\boldsymbol{X}-\lambda\boldsymbol{Y}|=0$ 的根均大于 1。

本文算法将设计矩阵 $\boldsymbol{B}\in R^{n\times n}$ 的形式如下：

$$\boldsymbol{B}=\begin{pmatrix} -a_{11}+e^c+N & -a_{12}+b_{12} & \cdots & -a_{1n}+b_{1n} \\ -a_{21}+b_{21} & -a_{22}+e^c+N & \cdots & -a_{2n}+b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{n1}+b_{n1} & -a_{n2}+b_{n2} & \cdots & -a_{nn}+e^c+N \end{pmatrix} \tag{10}$$

其中，c 为预先给定的正常数，$N>0$，且对于每一行的 b_{ij}，$i\neq j,i=1,2,\cdots,n,j=1,2,\cdots,n$，需满足 $N>n\times\sum_{j=1,j\neq i}^{n}|b_{ij}|,i=1,2,\cdots,n$，于是得到总的状态方程 $\boldsymbol{A}+\boldsymbol{B}$ 如下：

$$\boldsymbol{A}+\boldsymbol{B}=\begin{pmatrix} e^c+N & b_{12} & \cdots & b_{1n} \\ b_{21} & e^c+N & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \cdots & e^c+N \end{pmatrix} \tag{11}$$

由 b_{ij} 的限定条件和性质 1 可知，$\boldsymbol{A}+\boldsymbol{B}$ 一定是严格对角占优的，为了方便描述证明，我们把 $\boldsymbol{A}+\boldsymbol{B}$ 分解成如下两个矩阵：

$$\begin{aligned}\boldsymbol{A}+\boldsymbol{B}&=\begin{pmatrix} e^c+N & b_{12} & \cdots & b_{1n} \\ b_{21} & e^c+N & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \cdots & e^c+N \end{pmatrix}\\&=\begin{pmatrix} e^c+N & 0 & \cdots & 0 \\ 0 & e^c+N & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}+\begin{pmatrix} 0 & b_{12} & \cdots & b_{1n} \\ b_{21} & 0 & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \cdots & 0 \end{pmatrix}\\&=(e^c+N)\boldsymbol{E}+\boldsymbol{D}\end{aligned} \tag{12}$$

其中，$\boldsymbol{E}$ 为单位矩阵，$\boldsymbol{D}$ 为我们设定的一般矩阵。于是得到了这样一个结果：按照式(4)和式(10)的形式加入控制反馈矩阵，使得整个 n 维离散系统，所有的 LE 满足下式：

$$LE_i=\lim_{k\to\infty}\frac{1}{2k}\ln|\lambda_i[\boldsymbol{T}_k^{\mathrm{T}}\boldsymbol{T}_k]|>c,i=1,2,\cdots,n \tag{13}$$

由定理 1 可知，$\boldsymbol{X}=\boldsymbol{J}_k^{\mathrm{T}}\boldsymbol{J}_k$，$\boldsymbol{Y}=[\boldsymbol{T}_{k-1}\boldsymbol{T}_{k-1}^{\mathrm{T}}]^{-1}e^{2kc}$，根据性质 1，$\boldsymbol{X}>0$，证明如下：

根据 $\boldsymbol{J}_k(z)=\boldsymbol{A}+\boldsymbol{B}=\boldsymbol{J}$，得：

$$\begin{aligned}\boldsymbol{X}&=\boldsymbol{J}_k^{\mathrm{T}}\boldsymbol{J}_k=(\boldsymbol{A}+\boldsymbol{B})^{\mathrm{T}}(\boldsymbol{A}+\boldsymbol{B})\\&=((e^c+N)\boldsymbol{E}+\boldsymbol{D})^{\mathrm{T}}((e^c+N)\boldsymbol{E}+\boldsymbol{D})\\&=(e^c+N)^2\boldsymbol{E}+(e^c+N)(\boldsymbol{D}^{\mathrm{T}}+\boldsymbol{D})+\boldsymbol{D}^{\mathrm{T}}\boldsymbol{D}\end{aligned} \tag{14}$$

由于矩阵 $(e^c+N)(\boldsymbol{D}^{\mathrm{T}}+\boldsymbol{D})+\boldsymbol{D}^{\mathrm{T}}\boldsymbol{D}$ 是实对称，$\boldsymbol{D}$ 的范围又是有限的，因此存在正数 $N>0$，使得 $\boldsymbol{X}=\boldsymbol{J}_k^{\mathrm{T}}\boldsymbol{J}_k$ 主对角线严格占优且元素全大于 0，即 $\boldsymbol{X}$ 为正定矩阵，所以 $\boldsymbol{X}>0$。

对于 $\boldsymbol{T}_k=J_k$，同理可证 $[\boldsymbol{T}_{k-1}\boldsymbol{T}_{k-1}^{\mathrm{T}}]$ 为正定矩阵，正定矩阵的逆也是正定的，即 $[\boldsymbol{T}_{k-1}\boldsymbol{T}_{k-1}^{\mathrm{T}}]^{-1}>0\,e^{2kc}>0$。于是有 $\boldsymbol{Y}=[\boldsymbol{T}_{k-1}\boldsymbol{T}_{k-1}^{\mathrm{T}}]^{-1}e^{2kc}>0$。

还需证明 $\boldsymbol{X}-\boldsymbol{Y}=\boldsymbol{J}_k^{\mathrm{T}}\boldsymbol{J}_k-[\boldsymbol{T}_{k-1}\boldsymbol{T}_{k-1}^{\mathrm{T}}]^{-1}e^{2kc}>0$ 也成立，具体如下：

当 $k=1$ 时，$\boldsymbol{J}_1^{\mathrm{T}}\boldsymbol{J}_1-[\boldsymbol{T}_0\boldsymbol{T}_0^{\mathrm{T}}]^{-1}e^{2c}>0$ 的证明和式(14)类似，也是成立的。

于是假设在 $k=m$ 的情况下，有 $\boldsymbol{J}_m^{\mathrm{T}}\boldsymbol{J}_m-[\boldsymbol{T}_{m-1}\boldsymbol{T}_{m-1}^{\mathrm{T}}]^{-1}e^{2mc}>0$ 成立。

那么在 $k=m+1$ 时，有：

$$\begin{aligned}&\boldsymbol{J}_m^{\mathrm{T}}\boldsymbol{J}_m-[\boldsymbol{T}_{m-1}\boldsymbol{T}_{m-1}^{\mathrm{T}}]^{-1}e^{2mc}>0\\&\quad\rightarrow[\boldsymbol{J}_m^{\mathrm{T}}]^{-1}\boldsymbol{J}_m^{\mathrm{T}}\boldsymbol{J}_m[\boldsymbol{J}_m]^{-1}-[\boldsymbol{J}_m^{\mathrm{T}}]^{-1}[\boldsymbol{T}_{m-1}^{\mathrm{T}}]^{-1}[\boldsymbol{T}_{m-1}]^{-1}\\&\qquad[\boldsymbol{J}_m]^{-1}e^{2mc}>0\\&\quad\rightarrow\boldsymbol{E}-[\boldsymbol{T}_{m-1}^{\mathrm{T}}\boldsymbol{J}_m^{\mathrm{T}}]^{-1}[\boldsymbol{J}_m\boldsymbol{T}_{m-1}]^{-1}e^{2mc}>0\\&\quad\rightarrow\boldsymbol{E}-[\boldsymbol{T}_m^{\mathrm{T}}]^{-1}[\boldsymbol{T}_m]^{-1}e^{2mc}>0\\&\quad\rightarrow\boldsymbol{E}-[\boldsymbol{T}_m\boldsymbol{T}_m^{\mathrm{T}}]^{-1}e^{2mc}>0\\&\quad\rightarrow\boldsymbol{J}_{m+1}^{\mathrm{T}}\boldsymbol{J}_{m+1}>\boldsymbol{J}_{m+1}^{\mathrm{T}}\boldsymbol{J}_{m+1}[\boldsymbol{T}_m\boldsymbol{T}_m^{\mathrm{T}}]^{-1}e^{2mc}>e^{2c}[\boldsymbol{T}_m\boldsymbol{T}_m^{\mathrm{T}}]^{-1}\end{aligned}$$

$$e^{2mc}$$

$$\rightarrow \boldsymbol{J}_{m+1}^{\mathrm{T}}\boldsymbol{J}_{m+1} > [\boldsymbol{T}_m\boldsymbol{T}_m^{\mathrm{T}}]^{-1}e^{2mc}\cdot e^{2c}$$

$$\rightarrow \boldsymbol{J}_{m+1}^{\mathrm{T}}\boldsymbol{J}_{m+1} > [\boldsymbol{T}_m\boldsymbol{T}_m^{\mathrm{T}}]^{-1}e^{2(m+1)c} \tag{15}$$

即在 $k=m+1$ 的情况下，$\boldsymbol{J}_{m+1}^{\mathrm{T}}\boldsymbol{J}_{m+1}-[\boldsymbol{T}_m\boldsymbol{T}_m^{\mathrm{T}}]^{-1}e^{2(m+1)c}>0$ 也成立，综上 $\boldsymbol{X}-\boldsymbol{Y}>0$。

则特征方程变形如下式：

$$|\boldsymbol{X}-\lambda\boldsymbol{Y}|=0$$

$$\rightarrow |\boldsymbol{J}_k^{\mathrm{T}}\boldsymbol{J}_k-\lambda e^{2kc}[\boldsymbol{T}_{k-1}\boldsymbol{T}_{k-1}^{\mathrm{T}}]^{-1}|=0$$

$$\rightarrow |e^{-2kc}\boldsymbol{J}_k^{\mathrm{T}}\boldsymbol{J}_k-\lambda[\boldsymbol{T}_{k-1}]^{-1}[\boldsymbol{T}_{k-1}^{\mathrm{T}}]^{-1}|=0$$

$$\rightarrow |[\boldsymbol{T}_{k-1}^{\mathrm{T}}]|\cdot|e^{-2kc}\boldsymbol{J}_k^{\mathrm{T}}\boldsymbol{J}_k-\lambda[\boldsymbol{T}_{k-1}]^{-1}[\boldsymbol{T}_{k-1}^{\mathrm{T}}]^{-1}|\cdot|[\boldsymbol{T}_{k-1}^{\mathrm{T}}]|=0$$

$$\rightarrow |e^{-2kc}\boldsymbol{T}_{k-1}^{\mathrm{T}}\boldsymbol{J}_k^{T}\boldsymbol{J}_k\boldsymbol{T}_{k-1}-\lambda\boldsymbol{T}_{k-1}^{\mathrm{T}}[\boldsymbol{T}_{k-1}^{\mathrm{T}}]^{-1}[\boldsymbol{T}_{k-1}]^{-1}\boldsymbol{T}_{k-1}|=0$$

$$\rightarrow |e^{-2kc}\boldsymbol{T}_k^{\mathrm{T}}\boldsymbol{T}_k-\lambda\boldsymbol{E}|=0 \tag{16}$$

由定理 1，特征方程的根均大于 1，则矩阵 $e^{-2kc}\boldsymbol{T}_k^{T}T_k$ 的特征值均大于 1，即 $\lambda_i[e^{-2kc}\boldsymbol{T}_k^{\mathrm{T}}\boldsymbol{T}_k]>1$，也即 $\lambda_i[\boldsymbol{T}_k^{\mathrm{T}}\boldsymbol{T}_k]>e^{2kc}$。所以整个系统的 LE 计算结果如下：

$$LE_i=\lim_{k\to\infty}\frac{1}{2k}\mathrm{In}|\lambda_i[\boldsymbol{T}_k^{\mathrm{T}}\boldsymbol{T}_k]|$$

$$=\lim_{k\to\infty}\frac{1}{2k}\mathrm{In}|e^{2kc}|>c,i=1,2,\cdots,n \tag{17}$$

考虑到系统还需要满足混沌特性，系统轨道必须运动在有限范围内，即满足增益矩阵 $\boldsymbol{X}$：

$$\sup_{0\leqslant k<\infty}\|\boldsymbol{X}\|_2\leqslant M<\infty \tag{18}$$

其中，M 表示一个常数，$\|\cdot\|_2$ 为 2-范数，$\boldsymbol{B}$ 的范围有限。所以 $\sup_{0\leqslant k<\infty}\|\boldsymbol{B}\|_2<\infty$，此时只要保证受控矩阵 $\boldsymbol{A}$ 满足一致有界的条件，即有正常数 N，满足 $\sup_{0<k<\infty}\|\boldsymbol{A}\|_2\leqslant N<\infty$，最后因为矩阵 $\boldsymbol{X}=\boldsymbol{A}+\boldsymbol{B}$ 和矩阵 $\boldsymbol{A}$ 和 $\boldsymbol{B}$ 都有界，所以式(18)也是成立的。

上述证明已经为配置 LE 为全正提供了理论保障，下面将针对离散时间系统 $x_{k+1}=\boldsymbol{A}x_k$，具体说明本文算法配置的步骤。

步骤 1　根据矩阵 $\boldsymbol{A}$ 的形式给出 $\boldsymbol{B}$，即设定于每一行的 b_{ij} 使其满足 $N>n\times\sum_{j=1,j\neq i}^{n}|b_{ij}|,i=1,2,\cdots,n$，在主对角线上则添加 e^c+N(c 为给定正常数，$N>0$)。

步骤 2　计算 Jacobi 矩阵 $\boldsymbol{J}=\boldsymbol{A}+\boldsymbol{B}$ 并记 $\boldsymbol{T}_k=\boldsymbol{J}_k(x_k)\boldsymbol{J}_{k-1}(x_{k-1})\cdots\boldsymbol{J}_1(x_1)\boldsymbol{J}_0(x_0)=\boldsymbol{J}^k$，选取 N 和 $\boldsymbol{B}$ 中的 b_{ij} 使 $[\boldsymbol{T}_k\boldsymbol{T}_k^{\mathrm{T}}]$ 主对角线严格占优。

步骤 3　采用如下模运算[5,11,16]：

$$x_{k+1}=\boldsymbol{A}x_k+\boldsymbol{B}x_k(\mathrm{mod}\ 1) \tag{19}$$

前两个步骤使整个系统的 LE 全部为正，即轨迹在全部运动方向上都是呈指数级发散，起到拉伸作用，步骤 3 的取模处理则使系统轨迹在全局范围上有界，起到折叠作用，这样 3 个步骤的共同作用就能使整个系统产生无简并的混沌行为。

由上述推导可知，该算法通过引入反馈器，设计出其矩阵具体的参数，来达到系统的 LE 全部为正的目的，并不限制原本系统的形式和参数，相对于 Wang-Chen 算法只适合受控系统渐进稳定、输入与输出有界来说，该算法的适用范围更广。在低维系统中，反馈器形式简洁，容易理解，在基于混沌设计出的密码体制中，不存在混沌产生退化、简并等不安全因素。

3.2　混沌轨道的全局有界性和 Lyapunov 指数的有限性

当前主要采用两种方法来保证系统轨道的有限性：

(1)Chen-Lai 算法。其针对整个受控系统取模，使其在整个相空间上有界，对系统的种类性质较不敏感，适用范围较广，得到的应用更多。

(2)Wang-Chen 算法。其仅对控制器取模，而不是针对整个系统做相应处理，适用范围有限。

本文算法参考 Chen-Lai 算法的思想，对系统采取如下处理：

$$x_{k+1}=\boldsymbol{A}x_k+\boldsymbol{B}x_k(\mathrm{mod}\ 1) \tag{20}$$

文献[5]已证明式(20)将使系统轨迹在有界区域产生混沌，能够保证整个系统轨迹的全局有界。

下面将证明该方法能保证 LE 的有界性，如式(21)所示：

$$LE_i<\infty\ (i=1,2,\cdots,n) \tag{21}$$

根据 2-范数的定义，可得：

$$LE_i=\lim_{k\to\infty}\frac{1}{2k}\mathrm{In}|\lambda_i[\boldsymbol{T}_k^{\mathrm{T}}\boldsymbol{T}_k]|$$

$$\leqslant\lim_{k\to\infty}\frac{1}{2k}\mathrm{In}|\max_i\{\lambda_i[\boldsymbol{T}_k^{\mathrm{T}}\boldsymbol{T}_k]\}|$$

$$=\lim_{k\to\infty}\frac{1}{2k}\mathrm{In}\,|\max_i\{\sqrt{\lambda_i[\boldsymbol{T}_k^{\mathrm{T}}\boldsymbol{T}_k]}\}|^2$$

$$=\lim_{k\to\infty}\frac{1}{k}\mathrm{In}|\,\|\boldsymbol{T}_k\|_2| \tag{22}$$

根据 2-范数的相关性质，可得：

$$\|\boldsymbol{T}_k\|_2=\max_i\{\sqrt{\lambda_i(\boldsymbol{T}_k^{\mathrm{T}}\boldsymbol{T}_k)}\}=\|\boldsymbol{J}_k\boldsymbol{J}_{k-1}\cdots\boldsymbol{J}_0\|_2$$

$$=\|[(e^c+N)\boldsymbol{E}+\boldsymbol{D}]\cdot\cdots\cdot[(e^c+N)\boldsymbol{E}+\boldsymbol{D}]\|_2$$

$$\leqslant\|(e^c+N)\boldsymbol{E}+\boldsymbol{D}\|_2\cdot\cdots\cdot\|(e^c+N)\boldsymbol{E}+\boldsymbol{D}\|_2$$

$$\leqslant(\|(e^c+N)\boldsymbol{E}\|_2+\|\boldsymbol{D}\|_2)\cdot\cdots\cdot(\|(e^c+N)\boldsymbol{E}\|_2+\|\boldsymbol{D}\|_2)$$

$$=(e^c+N+\boldsymbol{H})\cdot\cdots\cdot(e^c+N+\boldsymbol{H})$$

$$=(e^c+N+\boldsymbol{H})^k \tag{23}$$

其中，$\boldsymbol{H}$ 为矩阵 $\boldsymbol{D}$ 的 2-范数，因为矩阵 $\boldsymbol{D}$ 中的每个元素都需要满足 $N>n\times\sum_{j=1,j\neq i}^{n}|b_{ij}|$，所以 $\boldsymbol{H}$ 也有限。

结合式(22)和式(23)，可得到式(24)：

$$LE_i=\lim_{k\to\infty}\frac{1}{2k}\mathrm{In}|\lambda_i[\boldsymbol{T}_k^{\mathrm{T}}\boldsymbol{T}_k]|$$

$$\leqslant\lim_{k\to\infty}\frac{1}{2k}\mathrm{In}|\max_i\{\lambda_i[\boldsymbol{T}_k^{\mathrm{T}}\boldsymbol{T}_k]\}|$$

$$=\lim_{k\to\infty}\frac{1}{k}\mathrm{In}|\,\|\boldsymbol{T}_k\|_2|$$

$$\leqslant\lim_{k\to\infty}\frac{1}{k}\mathrm{In}(e^c+N+\boldsymbol{H})^k$$

$$=\mathrm{In}(e^c+N+\boldsymbol{H}) \tag{24}$$

即必然存在常数 N 和 $\boldsymbol{H}$，使得式(24)中的 $LE_i\leqslant\mathrm{In}(e^c+N+\boldsymbol{H})<\infty$ 成立，由此证明了 LE 的有限性。

3.3　算子示例

3.3.1　线性反馈 Cat 映射算例

考虑 Cat 映射二维混沌映射系统如式(25)所示：

$$\begin{bmatrix} x_{1,n+1} \\ x_{2,n+1} \end{bmatrix} = \boldsymbol{A} \begin{bmatrix} x_{1,n} \\ x_{2,n} \end{bmatrix} (\mathrm{mod}\ 1) \tag{25}$$

经典 Cat 映射的矩阵 $\boldsymbol{A}$ 的形式一般取：

$$\boldsymbol{A} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \tag{26}$$

因此设计反馈矩阵 $\boldsymbol{B}$ 的形式如下：

$$\boldsymbol{B} = \begin{bmatrix} -a_{11} + e^c + \boldsymbol{N} & -a_{12} + b_{12} \\ -a_{21} + b_{21} & -a_{22} + e^c + \boldsymbol{N} \end{bmatrix} \tag{27}$$

若想让系统的 LE 全部大于 3，我们令预先给定的常数 $c=3$，$\boldsymbol{N}$ 为矩阵 $\boldsymbol{A}$ 的 2-范数，然后选取 $b_{12}=0.4$，$b_{21}=0.8$。

根据 LE 的定义，最后求得该算例的两个 LE 分别为 3.0958 和 3.1486。由上述结果可知，该方法能够使得 n 维混沌系统正的 LE 个数达到最大的可能性，即 $L=n=2$。

3.3.2 微扰反馈 Lü 映射算例

针对如下三维 Lü 混沌系统，如式(28)所示：

$$\begin{cases} \dot{x} = a(y-x) \\ \dot{y} = -xz + cy \\ \dot{z} = xy - bz \end{cases} \tag{28}$$

令 $a=36$，$b=3$，c 作为状态变量，此时系统呈现出混沌行为。

一般我们使用线性方式来使得 Lü 系统达到稳定状态，在定点 $O(0,0,0)$ 处，令状态变量 $c=20$，使系统出现混沌行为，线性方程的系数矩阵如下：

$$\boldsymbol{A} = \begin{bmatrix} -36 & 36 & 0 \\ 0 & 20 & 0 \\ 0 & 0 & -3 \end{bmatrix} \tag{29}$$

因此设计反馈矩阵 $\boldsymbol{B}$ 的形式如下：

$$\boldsymbol{B} = \begin{bmatrix} -a_{11} + e^c + \boldsymbol{N} & -a_{12} + b_{12} & -a_{13} + b_{13} \\ -a_{21} + b_{21} & -a_{22} + e^c + \boldsymbol{N} & -a_{23} + b_{23} \\ -a_{31} + b_{31} & -a_{32} + b_{32} & -a_{33} + e^c + \boldsymbol{N} \end{bmatrix} \tag{30}$$

若想让系统的 LE 全部大于 5，我们令预先给定的常数为 5，$\boldsymbol{N}$ 为矩阵 $\boldsymbol{A}$ 的 2-范数，然后选取 $b_{12}+b_{13}=3$，$b_{21}+b_{23}=5$ 和 $b_{31}+b_{32}=7$。

最终本文算法得到的 LE 分别为：$LE_1=5.2870$，$LE_2=5.2986$，$LE_3=5.3303$，也可以使得 3 维混沌系统正的 LE 个数达到最大数值，即 $L=n=3$。

3.4 性能分析

下面将从 4 个方面对本文配置的混沌系统的 LE 性能进行研究与分析：1)离散混沌系统 LE 的准确性；2)计算复杂度；3)算法的运行时间；4)混沌轨迹图和吸引子相图。

3.4.1 Lyapunov 指数准确性分析

按照本文算法的思想，为使 Lyapunov 指数结果与期望值更接近，可以将 N 设置为 0.1。然后将本文配置的 Lyapunov 指数结果与 Chen-Lai 算法、文献[11]的算法做比较。可以看出，本文算法配置出的数值更接近期望值，而且在期望值越小时配置结果越精确，体现了本文算法的优势。3 种算法配置 LE 的比较结果如表 1 所列(映射采用 3.3.1 节中的 Cat 映射)。

表 1 Lyapunov 指数准确性的结果对比

Table 1 Comparison of Lyapunov index accuracy results

LE of expected configuration	Our Method	Chen-Lai Algorithm	Literature[12]
1	1.0182	1.7437	1.0903
	1.0537	2.0737	1.1498
3	3.0958	3.1392	3.0201
	3.1486	3.2317	3.0131
5	5.0034	5.0200	5.0089
	5.0101	5.0347	5.0102

3.4.2 计算复杂度分析

在配置系统的 Lyapunov 指数时，从计算复杂度上考虑，本文算法与 Chen-Lai 算法的区别不大，主要部分有：计算矩阵加法和矩阵乘法、计算 Jacobi 矩阵、计算 2-范数。

Chen-Lai 算法的计算复杂度如下：

(1)计算 $\boldsymbol{A}+\boldsymbol{B}$：$o_{加}(n^2)$；

(2)计算 Jacobi 矩阵：$o_{\mathrm{jacobi}}(n^2)$；

(3)计算 2-范数(矩阵乘)：$k * o_{乘}(n^3)$。

因此，Chen-Lai 算法的计算复杂度为：

$$O_{\text{Chen-Lai}} = o_{加}(n^2) + o_{\mathrm{jacobi}}(n^2) + k * o_{乘}(n^3) \tag{31}$$

本文算法的计算复杂度如下：

(1)计算 $\boldsymbol{A}+\boldsymbol{B}$：$o_{加}(1)$；

(2)计算 Jacobi 矩阵：$o_{jacobi}(n^2)$；

(3)计算 2-范数(矩阵乘)：$k * o_{乘}(n^3)$。

因此，本文算法的计算复杂度为：

$$O_{本文} = o_{加}(1) + o_{\mathrm{jacobi}}(n^2) + k * o_{乘}(n^3) \tag{32}$$

其中，n 表示混沌系统的维数，k 表示矩阵 $\boldsymbol{A}$ 的秩。根据上述分析可以看出，本文算法计算 Jacobi 矩阵和 2-范数的复杂度与 Chen-Lai 算法相同，但本文在处理矩阵 $\boldsymbol{X}=\boldsymbol{A}+\boldsymbol{B}$ 时，可以直接将 $\boldsymbol{X}$ 表示为式(12)的形式，省去了一步加法计算，因此本文算法运算矩阵 $\boldsymbol{A}+\boldsymbol{B}$ 时的计算复杂度为常数项 $o_{加}(1)$，综合比较，本文算法总的计算复杂度比 Chen-Lai 算法小 $o_{加}(n^2)-o_{加}(1)$，所以本文算法将在计算效率上有一定程度的提升，具有实际应用价值。

3.4.3 算法运行时间比较

本文在混沌系统分别处于 3 维、4 维和 5 维的情况下，统计了本文算法的运行时间，并将其与 Chen-Lai 算法、文献[11]的算法进行比较(3 种算法均在 Windows 10，Matlab 9.0 下运行)，结果如表 2 所列。

表 2 3 种算法运行时间的结果对比

Table 2 Comparison of running time results ofthree algorithms

Dimension of chaotic system	Our Method /s	Chen-Lai Algorithm/s	Literature[11]
3	0.0709	0.0746	0.0672
4	0.0887	0.0955	0.0923
5	0.1123	0.1531	0.1266

从表 2 可以看出，本文算法在计算速度上有所提升，而且随着维度的提高，提升效果更加显著。因此，将基于本文算法设计出的混沌系统用于序列密码方案之中，相对应地提高了序列密码体制的加解密速度，具有实际的应用意义。

3.4.4 混沌轨迹图和吸引子相图分析

下面将利用本文算法对 3.2 节的 Cat 系统和 Lü 系统

进行配置并仿真验证，生成的 2 维混沌系统的吸引子相图和混沌轨迹图如图 2、图 3 所示（初始值取(1/3,2/3)），生成的 3 维混沌系统的吸引子相图如图 4 所示（初始值取(1/4,1/2,3/4)）。

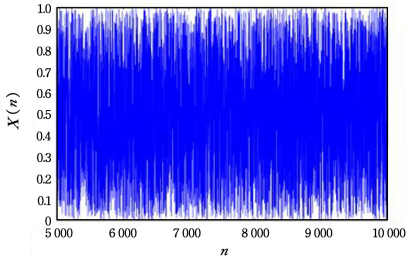

图 2　二维 Cat 映射轨迹图

Fig. 2　Two-dimensional Cat mapping trajectory graph

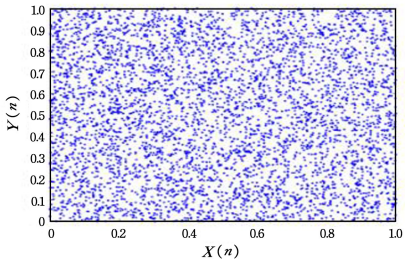

图 3　二维 Cat 映射吸引子相图

Fig. 3　Two-dimensional Cat map attractor phase diagram

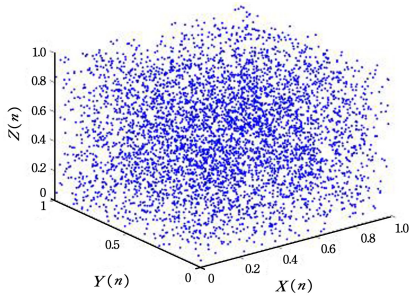

图 4　三维 Lü 映射吸引子相图

Fig. 4　Three-dimensional Lü map attractor phase diagram

从吸引子状态图和轨迹状态图可以看出本文设计的算法配置的混沌系统轨道运动情况，其轨迹遍布了整个相空间，表明该系统具有很强的混沌特性，混沌反控制法取得了良好的效果。使用该系统能够同时产生多个相关性不高的伪随机序列，如果取这些序列某些位连接后构成新的序列将具有更好的随机性，并且很难进入周期循环。使用基于本文算法设计的离散混沌映射来生成混沌序列，可以更有效地抵抗非线性密码攻击以及其他的密码攻击方法，有效地保障了基于该混沌系统设计出的序列密码体制的安全性。

4　基于无简并混沌系统的序列量化方案

4.1　量化方案设计

本文采取的混沌序列量化方式是取出第 3 节配置的混沌系统迭代生成序列中的有效数字组合，然后组成一个 16 位或者 32 位大整数并对 256 取模，得到一个 0～255 内的数，这样就可以表示成 8 位的二值序列，最后对该序列进行变换处理，可以加强输出序列的随机性和序列的复杂性。该方案可以用来对抗涉及到混沌加密的一些特有攻击。针对一些基本的混沌加密方案，文献[19]总结了混沌理论在图像加密应用的一些研究成果，明确指出大量基于混沌的密码体制还有不少安全隐患。而文献[20]做了一些针对混沌多媒体的安全的分析，其提出靠指数分析得到的结果是不可靠的。而本文将采用动态变换对序列进行处理，对原有序列采取置换和对换，从而改善上述问题。

本文设计的量化方案如下。

步骤 1　利用第 3 节提到的 Lü 系统结合反控制方法处理之后，产生 3 组离散混沌序列，分别记为 X_n, Y_n, Z_n。经验表明，按顺序选取 X_n, Y_n, Z_n 的有效位然后拼接，所得的序列随机性会比单独选取某组序列更好，这是因为每组混沌序列值相邻之间的数值会有相似性。因此将 3 个序列按取模方式选取，选取方式如下：

$$x_n=\begin{cases}X_n, & \text{if } n(\bmod 3)=0\\ Y_n, & \text{if } n(\bmod 3)=1\\ Z_n, & \text{if } n(\bmod 3)=2\end{cases} \tag{33}$$

舍弃前 1 000 次迭代产生的序列，最后生成一个混沌数值序列$\{x_i \mid i=1,2,\cdots,N\}$，这样处理能尽量减少子序列之间的重复性，从而增强最终输出序列的随机性。

步骤 2　从序列 x_N 中取出小数点后的有效数字，然后形成整数对 256 取模得到一组整数序列 t_N，范围为 0～255，公式如下：

$$t_k=x_k\times 10^{16}(\bmod 256), k=0,1,2,\cdots,N \tag{34}$$

步骤 3　新建一个变换表数组 a，其大小为 256 位，初始化 a_n。

$$a_i=i, 0\leqslant i\leqslant 255 \tag{35}$$

式(35)的输入为一段连续的正整数：0～255。接着从 $n=0$ 开始，按照式(36)从数字化序列 t_N 中，每次按顺序抽取一个整数 j。

$$j=t_k, j\neq i, 0\leqslant i\leqslant 255 \tag{36}$$

将 a_i 与 a_j 的值互换，最后 $n=255$，则完成一轮完全交换，因为 j 来源于混沌序列取整后值，其值一直在随机变化，即数组 a 内部元素的交换也是随机的，考虑到该过程对于输出序列的随机性很重要，可以将此变换重复数十轮，最终得到一个随机性良好的序列，用于之后的输出。

步骤 4　对换形式 1：从数字化序列 t_N 中每次抽取 2 个值 j_1 和 j_2。

$$\begin{aligned}&j_1=t_k, j_2=t_{k+1}\\ &j_1\neq j_2, 0\leqslant j_1, j_2\leqslant 255\end{aligned} \tag{37}$$

将 a_{j_1} 与 a_{j_2} 的值交换，从而实现一轮对换 1，j_1 与 j_2 也是来源于混沌序列取整后的值，将数组 a 内部元素再次进行随机交换，考虑到增强随机性的需要，可对此过程进行数十轮。

对换形式 2：从数字化序列 t_N 中每次抽取 3 个值 j_1, j_2 和 j_3。

$$\begin{aligned}&j_1=t_k, j_2=t_{k+1}, j_3=t_{k+2}\\ &j_1\neq j_2\neq j_3, 0\leqslant j_1, j_2, j_3\leqslant 255\end{aligned} \tag{38}$$

将 a_{j_1} 与 a_{j_2} 的值交换，a_{j_3} 与 a_{j_2} 的值交换，从而实现一轮

对换 2，继续将数组 a 内部的元素进行随机交换，考虑到增强随机性的需要，可对此过程重复数十轮。

步骤 5 在得到混沌实数值 x_N 序列取整的结果 t_k 后，在变换表中输入得到对应的输出值 $a[t_k]$，将其转化为二进制结果，即为所需的加密密钥。

本文量化方案可以通过算法 1 的伪代码描述。

算法 1

```
Input:(Xn,Yn,Zn)//输入混沌序列
Output:(result)//输出序列
1. Initialize:x←0,t←0//初始化序列 x 和 t2. for i←0 to n do//步骤 1,拼接三组序列
3.    if i(mod 3)is 0
4.       xi←Xi
5.    else if i(mod3)is 1
6.       xi←Yi
7.    else
8.       xi←Zi
9. end
10. for k←0 to n do//步骤 2:取整后再取模
11.       tk←xk×10^16(mod256)
12. end
13. Initialize:a[i]←i//步骤 3:初始化数组 a
14. for r←0 to 20 do//步骤 3:交换
15.       for i←0 to 256 do
16.          j←tr×256+i
17.          Swap (a[i],a[j])//交换 a[i]和 a[j]
18.       end
19. end
20. for r←20 to 40 do//步骤 4:对换形式 1
21.       for i←0 to 256 do
22.          j1←tr×256+i
23.          j2←tr×256+i+1
24.          Swap (a[j1],a[j2])//交换 a[j1]和 a[j2]
25.       end
26. end
27. for r←40 to 60 do//步骤 4:对换形式 2
28.       for i←0 to 256 do
29.          j1←tr×256+i
30.          j2←tr×256+i+1
31.          j3←tr×256+i+2
32.          Swap (a[j1],a[j2])//交换 a[j1]和 a[j2]
33.          Swap (a[j2],a[j3])//交换 a[j2]和 a[j3]
34.       end
35. end
36. for k←0 to n do
37.       resultk←a[tk]
38. end
```

得到一轮随机性序列之后，还可对变换表展开新一轮的完全交换或者对换，来准备输出下一轮的密钥。在此过程中可以采取不同的变换机制，例如：在每次提取密钥后采取一轮步骤 3 中的完全交换，在提取 100 个元素后采取一轮步骤 4 中的对换 1，提取 10000 个元素后采取一轮步骤 4 中的对换 2。采取何种机制可由使用者根据实际应用场景随时调整。变换处理不但能提高序列随机性，还可以增大系统的周期性和复杂度。最终结果表明，序列在量化后通过动态变换，得到的输出体现了良好的随机性。

如果需要将量化后的二值序列应用于混沌序列密码之中，则要保证序列满足一定的随机性。本文将对设计的无退化混沌系统输出的实数值序列取整后，经过一系列变换处理，分别生成 10000 比特，20000 比特和 40000 比特的序列，进行单位测试、频数检验、序列检验、扑克测试、游程测试、相关性检验以及初值敏感性检验等多项测试，并对测试得到的结果进行分析。将本文算法与文献[12]中的方案（选取序列长度为 20000 位的混沌序列 1）进行性能比较，证明了该混沌二进制序列能够通过所有测试，说明该序列具有良好的随机性，因此该序列能够作为序列密码算法中的密钥流加以应用。

4.2 量化序列随机性测试检验

4.2.1 单位测试

一个合格的密钥流生成器生成的二进制序列，首先要求该序列中“0”和“1”的个数应当是近似相等的。本文将对 4.1 节量化产生的长度为 10000 位、20000 位和 40000 位的序列进行单位测试，结果用序列中的“1”表示，具体如表 3 所列。

表 3 单位测试的结果对比

Table 3 Comparison of unit test results

Number of sequences/bit	Our Method/bit	Literature[13]/bit
10000	5010	
20000	10004	10014
40000	20018	

根据表 3 结果可以看出，本文量化方案所产生的 10000 位、20000 位和 40000 位长度的序列中的“1”十分接近序列总长度的一半，说明本文方案可以通过该项测试。

4.2.2 频数检验

此项假设性检验是通过计算 0-1 频数来确定该序列的平衡性，主要是判定式(39)是否近似满足自由度为 1 的卡方分布，如下式所示：

$$\chi^2=\frac{(n_1-n_0)^2}{n} \tag{39}$$

其中，n 为序列总数，n_1 为”1”的个数，n_0 为”0”的个数。

若选取显著水平为 5%时，式(39)计算的值小于 3.84，则说明得到的二进制序列具有良好的随机性，而且序列的平衡性与该结果成反比，该值越小，表明平衡性越好。表 4 为量化后长度分别为 10000 bit，20000 bit，40000 bit 序列在测试时所得的频数检验结果。

表 4 频数检验的结果对比

Table 4 Comparison of frequency test results

Number of sequences/bit	Our Method/bit	Literature[12]/bit
10000	0.0400	
20000	0.0032	0.0196
40000	0.0324	

根据表 4 结果可以看出，本文的量化方案所产生的

10000 位、20000 位和 40000 位长度的序列该项检验结果均小于3.84，说明本文设计的量化方案能够通过该项检验。

4.2.3　序列检验

此项假设性检验用来计算序列的转移概率，若 11，10，01，00 这 4 种组合出现的概率大概相同，表明该序列具有不错的置乱效果，通过计算式(40)来判断序列是否近似服从自由度为 2 的卡方分布。

$$\chi^2=\frac{4}{n-1}\sum_{i=0}^{1}\sum_{j=0}^{1}(n_{ij})^2-\frac{2}{n}\sum_{i=0}^{1}[(n_i)^2+1] \tag{40}$$

其中，$n_{ij}(i,j=0,1)$表示序列 ij 出现的次数，当显著水平为 5%时，式(40)的计算值小于或等于 5.991 时，则说明产生的混沌二进制序列能够通过序列检验。表 5 为由本文量化所得到的不同长度序列进行序列检验的测试结果。

表 5　序列检验的结果对比

Table 5　Comparison of serial test results

Number of sequences/bit	Our Method/bit	Literature[12]/bit
10000	−1.1033	
20000	−0.7958	0.0635
40000	0.2701	

根据表 5 结果可以看出，本文量化方案所产生的 10000 位、20000 位和 40000 位长度的序列在该项检验上的结果均小于 5.991，说明本文设计的量化方案能够通过该项检验。

4.2.4　扑克测试

此项假设性检验主要用于检测二进制序列中若干位不重叠的子序列的每一种模式的个数是否接近。对于总长为 M 的二进制序列，排列组合一共有 2^M 种不同的情况。将长度为 N 位的待测二进制序列以长度 m 进行划分，划分为 $\left[\frac{N}{M}\right]$个子序列，通过下式计算统计值 V：

$$V=\sum_{i=1}^{2^m}\frac{(N_i-k/2^m)^2}{k/2^m}=\frac{2^m}{k}\left(\sum_{i=1}^{2^m}N_i^2\right)-k \tag{41}$$

统计值 V 需要近似满足自由度为(2^M-1)的卡方分布，M 一般取 4 或者 8，本文中取 $M=4$，则一共存在 16 种子序列，计算统计值 V 是否近似服从自由度为 15 的卡方分布，若 $1.03<V<57.4$，则说明该序列可以通过扑克测试。表 6 为本文量化方案所得的扑克测试结果。

表 6　扑克测试的结果对比

Table 6　Comparison of poker test results

Number of sequences/bit	Our Method/bit	Literature[12]/bit
10000	9.6352	
20000	13.4031	13.9254
40000	21.6496	

根据表 6 结果可以看出，本文量化方案所产生的 10000 位、20000 位和 40000 位长度的序列在该项测试上的结果均小于 57.4 且大于 1.03，说明本文设计的量化方案能够通过该项检验。

4.2.5　游程检验

此项假设性检验主要用于判断序列的游程是否满足预期要求，本文将以量化后长度为 20000 bit 的序列进行游程测试，假如最终结果中的每个游程长度都在所要求的范围之内，则表明序列可以满足游程测试条件。表 7 为本文方案生成的二值序列游程的测试结果。

表 7　游程检验的结果对比

Table 7　Comparison of run test results

Run length	Range requirements	Our Method	Literature[12]
1	2315～2685	2486	2469
2	1114～1386	1247	1256
3	527～723	600	619
4	240～384	325	317
5	103～209	151	148
6+(6 or more)	103～209	167	157

根据表 7 结果可以看出，本文量化方案所产生的 20000 位长度的序列在该项测试上的结果均能满足该项测试的范围要求，说明本文方案可以通过该项测试。

4.2.6　初值敏感性测试

该项测试是指当初值只有细微改变后有多少比例的二值序列产生了改变，在最理想情况下，变化率应为 50%。本文将初始值改变10^{-10}然后进行计算和测试，最终得到如表 8 所列的结果。

表 8　初值敏感性测试结果对比

Table 8　Comparison of initial sensitivity test results

Methods	Rate of change/%
Our Method	50.03
Literature[13]	50.01

根据表 8 结果可以看出，改变初值后新产生的序列较原来序列有近 50%的序列数值产生了变化。因此可以得出结论：本文方案生成的序列具有非常强的初值敏感性。

4.2.7　NIST 随机性标准测试

下面将根据 NIST 标准来检测本文设计的量化方案产生的序列是否能够通过 NIST 标准测试，NIST 所提供的每个测试指标最后都会得出一个 *P-Value*，在此值大于 0.01 的情况下，则可认定此序列可以通过该测试项目，当序列悉数通过所有测试项目的情况下，就意味着此序列随机性良好，本文选取长度为 32 000 000 位的序列进行测试，结果如表 9 所列。

表 9　NIST 随机性测试结果

Table 9　NIST randomness test results

STATISTICAL TEST	*P-Value*	Pass/Fail
Frequency	0.323153	Pass
Block Frequency	0.749490	Pass
Cumulative Sums	0.603609	Pass
Runs	0.441870	Pass
Longest Run	0.603609	Pass
Rank	0.223109	Pass
FFT	0.728031	Pass
Non Overlapping Template	0.128715	Pass
Overlapping Template	0.764872	Pass
Universal	0.607257	Pass
Approximate Entropy	0.087605	Pass
Random Excursions	0.109804	Pass
Random Excursions Variant	0.390436	Pass
Serial	0.706302	Pass
Linear Complexity	0.671469	Pass

根据表 9 的测试结果可以看出，基于本文量化方案产生的序列均通过了全部 NIST 标准测试指标，表明该序列具有良好的随机性，可以用于序列密码算法以及应用之中。

本文量化方案对第 3 节设计的无简并混沌系统产生的实数值序列进行取整后再取模，在得到整数序列之后即可进行变换操作，变换的形式在输出部分序列之后也可以做切换，变换方式的多样性保证了使用者在具体应用场景中能有更多的选择，使得攻击者更难分析出变换规律，最后将二值序列进行多项随机性和统计性测试。测试结果表明，本文方案产生了很好的效果，能生成随机性能良好的序列，最终能够应用于混沌序列密码体制中。

结束语 针对离散混沌动力学系统在数字域上会存在退化、简并等问题，具体表现为在有限精度效应下，混沌实数值序列在计算机中迭代时，正的 LE 在系统发生行为改变时会转化汇聚成负的 LE，本文提出了一种基于混沌反控制的方法来将系统的所有 LE 全都配置为正数，通过引入一个反馈矩阵，将该矩阵中所有的参数做了细致的规定设置。仿真结果证明，本文算法可以将整个系统的 LE 配置为全正，而且在数值准确性和算法运行时间方面具有一定的优势，将基于本文算法设计出的混沌系统用于加密之中，相对应地提高了加解密速度，具有实际的应用意义。利用本文配置的混沌系统产生实数值序列，取出有效数字后进行变换操作，可以生成随机性能良好的序列，表明本文方案能够应用于混沌序列密码体制中。

参 考 文 献

[1] CUI J, WANG Y, ZHANG J. Full Session Key Agreement Scheme Based on Chaotic Map in Vehicular Ad hoc Networks [J]. IEEE Transactions on Vehicular Technology, 2020, 69(8): 8914-8924.

[2] SURESHKUMAR V, AMIN R, OBAIDAT M S, et al. An enhanced mutual authentication and key establishment protocol for TMIS using chaotic map[J]. Journal of Information Security and Applications, 2020, 53: 102539.

[3] CHEN S K, YU S M, LÜ J H, et al. Design and FPGA-based realization of a chaotic secure video communication system [J]. IEEE Transactions on Circuits and Systems for Video Technology, 2018, 28(9): 2359-2371.

[4] ZHOU S, WANG X Y. Simple estimation method for the largest Lyapunov exponent of continuous fractional-order differential equations[J]. Physica A: Statistical Mechanics and its Applications, 2021, 563: 125478.

[5] CHEN H K, LEE C I. Anti-control of chaos in rigid body motion [J]. Chaos Solitons & Fractals, 2004, 21(4): 957-965.

[6] CHEN G R, WANG X F. Chaos of Dynamical System—Theory, Method and Application [M]. Shanghai: Shanghai Jiaotong University Press, 2006.

[7] WANG C, FAN C, DING Q. Constructing Discrete Chaotic Systems with Positive Lyapunov Exponents[J]. International Journal of Bifurcation & Chaos, 2018, 28(7): 1850084.

[8] ZHANG L, TANG J S, OUYANG K J. Anti-control of period doubling bifurcation for a variable substitution model of Logistic map[J]. Optik-International Journal for Light and Electron Optics, 2017, 130: 1327-1332.

[9] YUAN C G, CHEN X. Generalized Chaos Control of Discrete Systems[J]. Mathematics in Practice and Knowledge, 2013, 43(23): 206-212.

[10] LIU N. Research on chaos anti-control of a class of linear systems[J]. China Science and Technology Information, 2012(12): 60-61.

[11] ZHAO G, LI H, MA Y J, et al. Discrete dynamic system without degradation-configuration of N positive Lyapunov exponents [J]. Journal of Electronics and Information, 2019, 41(9): 2280-2286.

[12] ZHAO L. Research on Anti-degradation Sequence Cipher[D]. Xi'an: Xidian University, 2020.

[13] XIANG H Y, LIU L F. A new perturbation-feedback hybrid control method for reducing the dynamic degradation of digital chaotic systems and its application in image encryption[J]. Multimedia Tools and Applications, 2021, 80(1): 1-25.

[14] WU T, JIN J G, WEI M J. A Hash function algorithm based on variable parameter cascade chaos[J]. Computer Research and Development, 2016, 53(3): 674-681.

[15] SHI J P, YANG L T. Design and circuit simulation of a switched chaotic system [J]. Modern Electronic Technology, 2019, 42(8): 59-62, 67.

[16] YU S M, LU J H, CHEN G R. Anti-control method of power system and its application[M]. Beijing: Science Press, 2013.

[17] WEN H P, YU S M, LU J H. Encryption algorithm based on Hadoop big data platform and non-degenerate high-dimensional discrete hyperchaotic system [J]. Acta Physica Sinica, 2017, 66(23): 76-89.

[18] GAN Q Y. Voice chaotic secure communication based on multicast and WAN transmission and ARM implementation [D]. Guangdong University of Technology, 2016.

[19] OZKAYNAK F. Brief review on application of nonlinear dynamics in image encryption[J]. Nonlinear Dynamics, 2018, 92(2): 305-313.

[20] PREISHUBER M, HUTTER T, KATZENBEISSER S, et al. Depreciating motivation and empirical security analysis of chaos-based image and encryption[J]. IEEE Transactions on Information Forensics And Security, 2018, 13(9): 2137-2150.

ZHAO Geng, born in 1964, Ph. D, professor, Ph.D supervisor, is a member of China Computer Federation. His main research interests include chaotic secure communication and information security.

LI Wen-jian, born in 1996, postgraduate. His main research interests include chaotic sequence and information secu-rity.

（责任编辑：喻藜）