文章编号：1000-8608(2014)05-0581-08

基于两个离散混沌动力系统的序列密码算法

王丽燕[1]， 许佳佳[1]， 李海燕*[2]

（1.大连大学 信息工程学院，辽宁 大连 116622；
2.辽宁科技大学 理学院，辽宁 鞍山 114051）

摘要： 基于两个离散混沌动力系统提出了一种新的序列密码算法.该算法用分段非线性映射的上一次迭代的输出作为分段非线性映射的下一次迭代的输入，并将迭代序列通过离散化算子转化为0-1序列，由0-1序列来选择两个混沌动力系统中的分段非线性映射.对算法进行了仿真实验和安全性分析，并对该映射产生的序列的随机性、初始值敏感性及其他性质进行了研究.研究结果表明，算法呈现出密钥、明文与密文之间高度的敏感性，密文和明文之间的相关度极小等特点，从而起到有效防止密文对密钥和明文信息泄露的作用.

关键词： 混沌动力系统；分段非线性映射；序列密码

中图分类号： TN918 **文献标识码：** A **doi：** 10.7511/dllgxb201405015

0 引 言

序列密码可以看成是块长度为1的分组密码，是一种带密钥的密码体制.自从Habutsu等于1991年利用混沌动力系统对序列密码进行加密[1]以来，这方面的研究引起了学者们的极大关注，给出了很多加密算法.例如，周红等利用一种带有参数的分段线性映射，通过增加迭代次数提高混沌动力系统对初始值的敏感性，获得具有良好自相关特性的均匀分布的非线性前馈型流密码[2-3].桑涛等提出利用逐段二次方根混沌映射来克服文献[2-3]中使用的逐段线性混沌映射自身的缺陷，以提高加密算法的安全性[4].王相生等为了提高加密算法的保密性，通过随机改变混沌映射中的参数的方法提高混沌的复杂性，同时引入m序列，对输出的混沌序列进行随机干扰[5].李红达等提出了基于一对互补的非线性混沌动力系统的序列密码算法，以迭代的初始值和移位寄存器的初始值为密钥，利用一个二进制变换序列的结果选择用于加密的动力系统[6-7].尽管已经提出了许多混沌加密算法[8-10]，但有些加密算法存在对迭代的初始值即密钥的低bit位的变化不十分敏感的缺陷，使得某些算法的安全性受到质疑并得到了攻击方案[11-12].金晨辉等指出，周红和桑涛等在文献[2]和文献[4]中给出的密码算法都存在“对初始值的低bit位的变化不十分敏感”的缺陷，找到了信息泄露规律，并分别给出了分割攻击方案[13-14].其他一些用单一的混沌映射构造加密算法的弱点也逐渐被发现[15-17].为了解决由单一的混沌动力系统造成的输出结果对迭代初始值的低bit位的变化不十分敏感的问题，李广明等提出利用一一映射与混沌映射相结合，在数字滤波器的结构上产生混沌密码序列[18].张涛提出以线性反馈移位寄存器序列为初始序列，将Logistic映射和Chebyshev映射作为滤波函数，利用序列密码中的前馈模型设计一个混沌序列密码算法[19].文献[20]提出了一种基于复合混沌动力系统的序列密码算法，算法以迭代的初始值和离散化算子参数为密钥，将二维Logistic映射输出的纵坐标值进行变换后作为分段线性映射的分段参数P，并将二维Logistic映射输出的横坐标值作为分段线性混沌映射的输入，再用带有可变参数的分段线性混沌映射的输出构造加密算法.

本文首先给出两个分段非线性混沌映射，讨论它们的统计性质，进一步利用这两个混沌动力

收稿日期： 2013-12-25； **修回日期：** 2014-06-09.
基金项目： 国家自然科学基金资助项目(71072161).
作者简介： 王丽燕(1963-)，女，博士，教授，E-mail：wly1963@163.com；李海燕*(1964-)，女，教授，E-mail：lhyqmj@163.com.

系统提出一种新的同步序列密码加密方案,使得明文的任意一个 bit 位的改变都能对密文的每个 bit 位产生影响,克服明文的改变对低 bit 位的变化不十分敏感这一缺陷,以有效抵御切割分析攻击.

1 两个分段非线性混沌动力系统

定义两个分段非线性映射如下:

$$X(t+1)=f_0(X(t))=\begin{cases}\sqrt{X(t)/P}; & 0\leqslant X(t)<P\\ 1-\sqrt{(X(t)-P)/(0.5-P)}; & P\leqslant X(t)<0.5\\ \sqrt{(1-X(t)-P)/(0.5-P)}; & 0.5\leqslant X(t)<1-P\\ 1-\sqrt{(1-X(t))/P}; & 1-P\leqslant X(t)\leqslant 1\end{cases}\tag{1}$$

$$X(t+1)=f_1(X(t))=\begin{cases}1-\sqrt{X(t)/P}; & 0\leqslant X(t)<P\\ \sqrt{(X(t)-P)/(0.5-P)}; & P\leqslant X(t)<0.5\\ 1-\sqrt{(1-X(t)-P)/(0.5-P)}; & 0.5\leqslant X(t)<1-P\\ \sqrt{(1-X(t))/P}; & 1-P\leqslant X(t)\leqslant 1\end{cases}\tag{2}$$

其中 $X\in[0,1]$,$P\in(0,0.5)$. 当 $P=0.25$ 时,图 1 给出了映射 $f_0(X(t))$ 和 $f_1(X(t))$ 的图像.

定理 1 动力系统 $X(t+1)=f_r(X(t))(r=0,1)$ 是混沌迭代系统,且系统在$[0,1]$上是均匀分布的,即系统的不变分布密度函数 $\rho_r(x)=1$,自相关函数呈 δ 形态.

证明 由于在$(0,1)$上,$|f_r'(x)|>1$,则由动力系统的 Lyapunov 指数的定义可知 $X(t+1)=f_r(X(t))(r=0,1)$ 都是混沌动力系统.

由 Frobenius-Perron 算子[21]可知

$$\rho_r(x)=P_r\rho_r(x)=\frac{\mathrm{d}}{\mathrm{d}x}\int_{f_r^{-1}([0,x])}\rho_r(t)\mathrm{d}t$$

从而

$$\begin{aligned}\rho_0(x)=&\frac{\mathrm{d}}{\mathrm{d}x}\int_{f_0^{-1}([0,x])}\rho_0(t)\mathrm{d}t=\\ &\frac{\mathrm{d}}{\mathrm{d}x}\int_0^{Px^2}\rho_0(t)\mathrm{d}t+\frac{\mathrm{d}}{\mathrm{d}x}\int_{P+(0.5-P)(1-x)^2}^{0.5}\rho_0(t)\mathrm{d}t+\\ &\frac{\mathrm{d}}{\mathrm{d}x}\int_{1-P-(0.5-P)x^2}^{1-P}\rho_0(t)\mathrm{d}t+\\ &\frac{\mathrm{d}}{\mathrm{d}x}\int_{1-P}^{1-P(1-x)^2}\rho_0(t)\mathrm{d}t=\\ &2Px\rho_0(Px^2)+(1-2P-x+2Px)\rho_0\times\\ &[P+(0.5-P)(1-x)^2]+\\ &(x-2Px)\rho_0[1-P-(0.5-P)x^2]+\\ &2P(1-x)\rho_0[1-P(1-x)^2]\end{aligned}$$

容易得到 $\rho_0(x)=1$ 是满足条件的解. 同理可得 $\rho_1(x)=1$. 说明动力系统 $X(t+1)=f_r(X(t))(r=0,1)$ 在$[0,1]$上是均匀分布的.

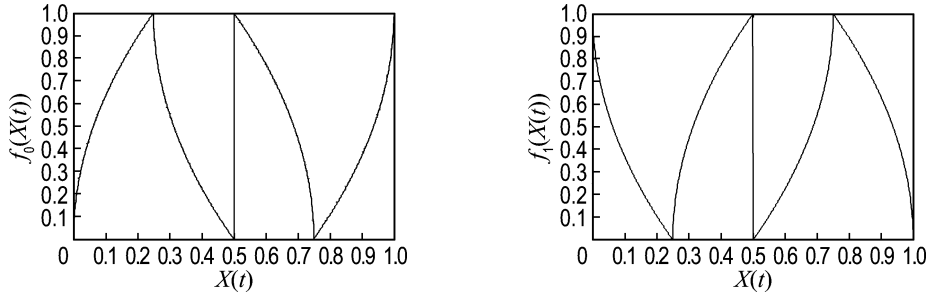
迭代序列$\{X(t+1)=f_r(X(t))\}$关于时间的自相关函数的定义为

$$C_r(m)=\frac{1}{\sigma^2}\lim_{N\to\infty}\sum_{i=0}^{N-1}(X_i-\overline{X})(X_{i+m}-\overline{X})$$

其中$\overline{X}$和σ^2分别是它的均值和方差. 由 Birkhoff 遍历性定理[22-23],上述等式又可以写成

$$C_r(m)=\frac{1}{\sigma^2}\int_{[0,1]}(x-\overline{x})(f_r^m(x)-\overline{x})\mathrm{d}x$$

其中 $f_r^m(x)$ 是迭代序列$\{X(t+1)=f_r(X(t))\}$的第 m 次迭代结果. 自相关函数反映对应二值序列的随机性,自相关函数值越小,说明对应二值序列的随机性越好.



(a) $f_0(X(t))$ (b) $f_1(X(t))$

图 1 分段非线性混沌映射 $f_0(X(t))$,$f_1(X(t))$

Fig. 1 Piecewise nonlinear chaotic map $f_0(X(t))$ and $f_1(X(t))$

由动力系统$\{X(t)\}$在$[0,1]$上服从均匀分布，可知$\bar{x}=0.5$，并由$f_0^m(x)=f_0^m(1-x)$，有

$$C_0(m)=\frac{1}{\sigma^2}\int_0^1(x-0.5)(f_0^m(x)-0.5)\mathrm{d}x=\frac{1}{\sigma^2}\Big[\int_0^P(x-0.5)(f_0^m(x)-0.5)\mathrm{d}x+\int_P^{0.5}(x-0.5)(f_0^m(x)-0.5)\mathrm{d}x+\int_{0.5}^{1-P}(x-0.5)(f_0^m(x)-0.5)\mathrm{d}x+\int_{1-P}^1(x-0.5)(f_0^m(x)-0.5)\mathrm{d}x\Big]$$

由于

$$\int_{1-P}^1(x-0.5)(f_0^m(x)-0.5)\mathrm{d}x=-\int_0^P(x-0.5)(f_0^m(x)-0.5)\mathrm{d}x$$

$$\int_{0.5}^{1-P}(x-0.5)(f_0^m(x)-0.5)\mathrm{d}x=-\int_P^{0.5}(x-0.5)(f_0^m(x)-0.5)\mathrm{d}x$$

所以$C_0(m)=0$.

同理，对于迭代序列$\{X(t+1)=f_1(X(t))\}$亦有相同的结论. 故其输出序列$\{X(t)\}$在$[0,1]$上是各态历经的，具有良好的自相关性且呈δ形态.

2　基于两个分段非线性混沌动力系统的序列密码

基于式(1)和式(2)这两个离散混沌动力系统，建立序列密码体系. 定义算子$T_j:[0,1]\to\{0,1\}$为$T_j(x)=[2^jx]\bmod 2$，用于将由离散混沌动力系统得到的迭代序列$\{x_i\}$转化为二进制序列$\{q_i\}$.

2.1　算法描述

算法的密钥由迭代初始值x_0、q_0和j构成. 其中$x_0\in(0,1)$，为迭代初始值；$q_0=0,1$，来控制迭代函数的选取；$j\in N$，为离散化算子T_j的参数. 迭代过程分两轮进行，同时也是获得迭代序列$\{x_i\}$和二进制序列$\{q_i\}$的过程. 第一轮对明文序列$M=m_1m_2\cdots m_L$进行顺序加密. 对明文的每一个 bit 位m_i，计算$q_i=T_j(f_0(x_{i-1}))\oplus q_{i-1}$，$c_i'=T_j(f_0(x_{i-1}))\oplus m_i\oplus q_i$. 若$c_i'\neq q_i\oplus q_{i-1}$，则$x_i=f_1(f_0(x_{i-1}))$，$i=1,2,\cdots,L$，获得中间序列$C'=c_1'c_2'\cdots c_L'$. 第二轮对中间序列$C'=c_1'c_2'\cdots c_L'$进行逆序加密. 对每一个 bit 位$c_{L+1-i}'$，计算$q_i=T_j(f_0(x_{i-1}))\oplus q_{i-1}$，$c_{L+1-i}=T_j(f_0(x_{i-1}))\oplus c_{L+1-i}'\oplus q_i$. 若$c_{L+1-i}\neq q_i\oplus q_{i-1}$，则$x_i=f_1(f_0(x_{i-1}))$，$i=1,2,\cdots,L$，从而获得密文$C=c_1c_2\cdots c_L$. 其中$L$表示二值序列的长度.

加密算法在完成第一轮后才能进行第二轮，具体流程如图 2 所示.

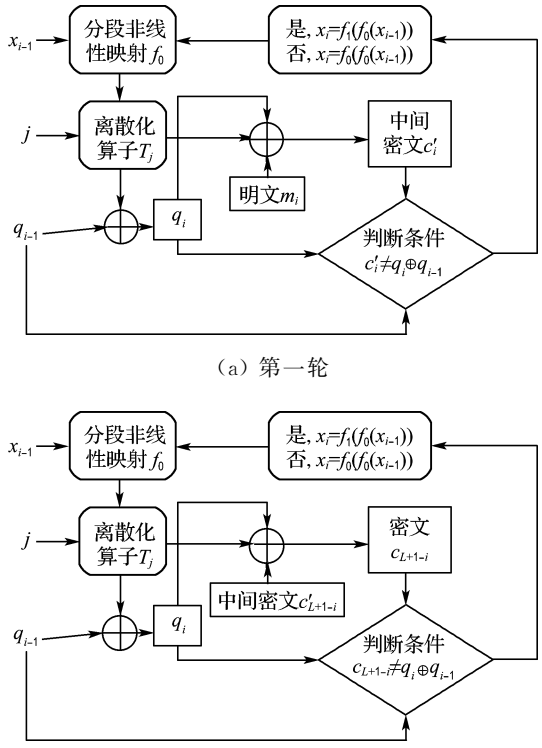


图 2　算法流程图

Fig. 2　Flow chart of the algorithm

具体的加密算法如下：

(1) 将明文字符串转化为 ASCII 码，再由 ASCII 码得到对应的用二进制表示的明文序列$M=m_1m_2\cdots m_L$. 其中$m_i(i=1,2,\cdots,L)$只取 0 或 1.

(2) 完成第一轮的加密. 选定迭代初始值x_0、q_0和j，计算$y_{i-1}=f_0(x_{i-1})$，$q_i=T_j(y_{i-1})\oplus q_{i-1}$；$x_i=f_0(y_{i-1})$，$c_i'=T_j(x_i)\oplus m_i\oplus q_i$. 若$c_i'\neq q_i\oplus q_{i-1}$，则$x_i=f_1(y_{i-1})$，$i=1,2,\cdots,L$，从而获得$C'=c_1'c_2'\cdots c_L'$.

(3) 完成第二轮的加密. 计算$y_{i-1}=f_0(x_{i-1})$，$q_i=T_j(y_{i-1})\oplus q_{i-1}$；$x_i=f_0(y_{i-1})$，$c_{L+1-i}=T_j(x_i)\oplus c_{L+1-i}'\oplus q_i$. 若$c_{L+1-i}\neq q_i\oplus q_{i-1}$，则$x_i=f_1(y_{i-1})$，$i=1,2,\cdots,L$，从而获得密文$C=c_1c_2\cdots c_L$.

(4) 由密文序列 $C = c_1c_2\cdots c_L$ 求出 ASCII 码序列,将 ASCII 码序列中小于 32 的 ASCII 码都加上 128,得到新的 ASCII 码序列,求出密文字符串.

相应的解密算法如下:

(1) 求出密文字符串的 ASCII 码序列,将 ASCII 码序列中大于 127 的 ASCII 码都减去 128,得到新的 ASCII 码序列.将新的 ASCII 码序列用二进制表示,得到二进制密文序列 $C = c_1c_2\cdots c_L$.

(2) 由迭代初始值 x_0、q_0 和 j,计算 $y_{i-1} = f_0(x_{i-1})$,$q_i = T_j(y_{i-1}) \oplus q_{i-1}$;$x_i = f_0(y_{i-1})$,$c'_{L+1-i} = T_j(x_i) \oplus c_{L+1-i} \oplus q_i$. 若 $c_{L+1-i} \neq q_i \oplus q_{i-1}$,则 $x_i = f_1(y_{i-1})$,$i = 1,2,\cdots,L$,获得第一轮的加密结果 $C' = c'_1c'_2\cdots c'_L$.

(3) 计算 $y_{i-1} = f_0(x_{i-1})$,$q_i = T_j(y_{i-1}) \oplus q_{i-1}$;$x_i = f_0(y_{i-1})$,$m_i = T_j(x_i) \oplus c'_i \oplus q_i$. 若 $c'_i \neq q_i \oplus q_{i-1}$,则 $x_i = f_1(y_{i-1})$,$i = 1,2,\cdots,L$,获得明文序列 $M = m_1m_2\cdots m_L$.

(4) 求出明文序列 $M = m_1m_2\cdots m_L$ 的 ASCII 码序列,最后求出明文字符串.

2.2 加密实例

例 1 明文:Chaotic cryptography and its application

将明文字符串转化为 ASCII 码,再由 ASCII 码得到对应的用二进制表示的如下明文序列:

```
10000111101000110000111011111101001101001
11000110100000110001111100101111001111000
01110100110111111001111110010110000111100000
11010001111001010000011000011101110110010000
01000001101001111010011100110100000110000101
11100001110000110110011010011100011110000101
11101001101001110111111101110
```

对于式(1)和式(2)混沌动力系统,取 $P = 0.25$.将得到的密文序列与明文比较,统计密文相对于明文改变的 bit 位数和改变率.

(1)取 $x_0 = 0.432\ 323$,$q_0 = 1$,$j = 3$,得到的密文为 z5âw+âè|ïXuDb $ Òo]æU"? 740:àï¥ë[&]%ù£J[YNC,改变的 bit 位数为 130,改变率为 0.464 3.

(2)取 $x_0 = 0.432\ 323 + 10^{-16}$,$q_0 = 1$,$j = 3$,得到的密文为 ;Q? Nb"}k%Ö,.ëäÉ<@P$_t$-âz/)ïbY%èäoBEöC_&(? o5,改变的 bit 位数为 137,改变率为 0.489 3.

(3)取 $x_0 = 0.432\ 323 + 2 \times 10^{-16}$,$q_0 = 1$,$j = 3$,得到的密文为)ÅÜÇwï¥Mïçqhî1pçlÖƒ Z)OTzü-¢êF£ ≠ ÿ),¢.>,改变的 bit 位数为 147,改变率为 0.510 7.

(4)取 $x_0 = 0.432\ 323$,$q_0 = 0$,$j = 3$,得到的密文为 +Éìï[QNtjˆïåëëÅUà′bT-~H5ÅÉE)G5_′iïQÆOV=,改变的 bit 位数为 138,改变率为 0.492 9.

(5)取 $x_0 = 0.432\ 323 + 10^{-16}$,$q_0 = 0$,$j = 3$,得到的密文为 ,Vö7ÖVàD > Em&8/$)åxDIcrd%| }ëa=qu¢Kv′}}m¢ë ,改变的 bit 位数为 139,改变率为 0.496 4.

(6)取 $x_0 = 0.432\ 323 + 2 \times 10^{-16}$,$q_0 = 0$,$j = 3$,得到的密文为 [!! = $ % Dêòc% Uæ2O[Zg5-qE¢Æåï′kƒö~jÅ¥:%öìDC,改变的 bit 位数为 131,改变率为 0.467 9.

用 0,1 序列的图形化表示如图 3 所示.其中,图 3(a)是明文的 0-1 序列,图 3(b)~(g)是在上述 6 种密钥的情况下得到的密文序列.从加密结果容易看出,迭代的初始值即密钥的任何微小改变都会引起密文的巨大变化.

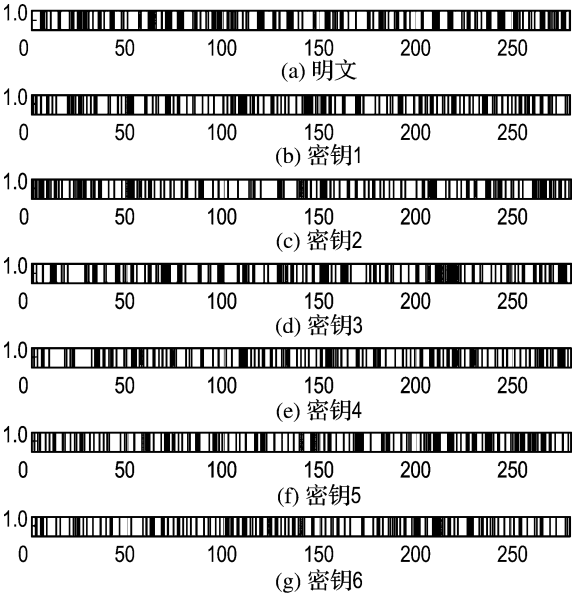


图 3 明文和不同初始值的密文序列图

Fig. 3 Sequence charts of plaintext and ciphers under different initial values

例 2 对于例 1 中给定的明文,使用密钥 $x_0 = 0.432\ 323$,$q_0 = 1$,$j = 3$ 进行加密得到的密文

如图 3(b) 所示，用正确的密钥可以精确地恢复得到明文. 但若将密钥变成 $x_0 = 0.432\ 323 + 10^{-16}$，$q_0 = 1$，$j = 3$，则解密得到 3i#[|4|. yJƒ5q™lŒb (f. Sk? >r"′_ü-jruZuv}"˜2R.

上述实例结果表明，只要密钥有极其微小的改变，就无法恢复得到正确的明文，这说明密文对密钥的变化高度敏感.

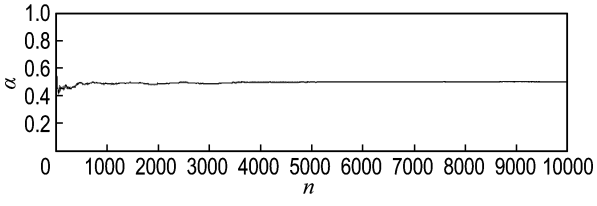
3　安全性分析

3.1　密文与明文的灵敏度检验

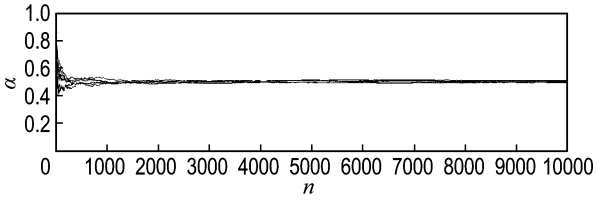
(1)对固定长度的 0 序列进行加密实验，得到改变的 bit 位数与序列长度 n 之比的函数关系图. 定义明文与密文之间改变的 bit 位数与消息长度之比为

$$\alpha(M, j, x_0, q_0, n) = \frac{1}{n}\#\{i : c_i \neq m_i, i \leqslant n\}$$

图 4(a) 是明文为 0 序列，长度 $N = 10\ 000$，选取密钥 $\{x_0, q_0, j\} = \{0.432\ 323, 1, 3\}$ 时改变的 bit 位数与序列长度之比的图像. 图 4(b) 为选取不同密钥 $x_0 = 0.432\ 323 + i \times 10^{-16}$ $(i = 0, 1, 2, 3, 4, 5)$ 时改变的 bit 位数与序列长度之比的图像.



(a) 密钥为 $\{x_0, q_0, j\} = \{0.432\ 323, 1, 3\}$



(b) 不同密钥 $x_0 = 0.432\ 323 + i \times 10^{-16}$ $(i = 0, 1, 2, 3, 4, 5)$

图 4　$\alpha(M, j, x_0, q_0, n)$ 的图像

Fig. 4　The $\alpha(M, j, x_0, q_0, n)$ image

(2)对于上述长度 $N = 10\ 000$ 的 0 序列，从该序列的第一个 bit 位开始，直至最后的 bit 位结束，每次改变 0 序列的一个 bit 位(即将 0 改为 1)后作为明文加密，将得到的密文序列与改变后的明文序列进行比较，统计总的改变 bit 位数与明文长度 $N = 10\ 000$ 之比. 图 5 是进行 10 000 次改变后实验的结果图像.

$$\beta(M_i, j, x_0, q_0) = \frac{1}{N}\#\{k : c_k \neq m_k, k \leqslant N\}$$

其中 $M_i = m_1 m_2 \cdots m_i \cdots m_N$，$m_1 = m_2 = \cdots = m_i = 1$，$m_{i+1} = m_{i+2} = \cdots = m_N = 0$.

容易看出，加密变换能够使明文序列的每个 bit 位有 50%的可能性发生改变或保持不变.

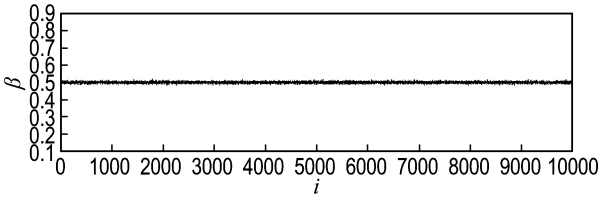


图 5　$\beta(M_i, j, x_0, q_0)$ 与 i 的关系

Fig. 5　Relationship between $\beta(M_i, j, x_0, q_0)$ and i

3.2　明文与密文的相关度检验

定义明文与密文之间的相关度为

$$R(x_0, q_0, j, n) = \frac{1}{n}(\#\{i : c_i = m_i, i \leqslant n\} - \#\{c_i : c_i \neq m_i, 1 \leqslant i \leqslant n\})$$

用密钥 $\{x_0, q_0, j\} = \{0.432\ 323, 1, 3\}$ 对长度 $N = 10\ 000$ 的 0 序列加密，得到的密文与明文的相关度如图 6 所示. 可以看出，本文算法的密文与明文的相关度很小.

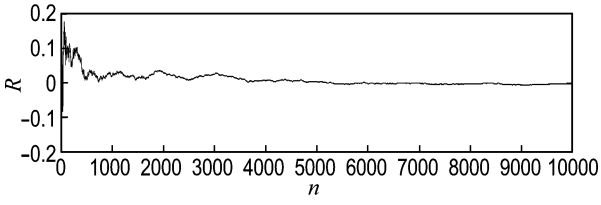


图 6　明文与密文的相关度

Fig. 6　Relevant degree of plaintext and ciphertext

3.3　密文中的频数检验

频数检验和平衡度检验[12] 能够保证 0-1 序列中 0 和 1 的个数大致相等，设密文序列 C 中 0 和 1 的个数分别为 n_0、n_1，计算 $\chi_1^2 = \dfrac{(n_1 - n_0)^2}{n^2}$. 与自由度为 1 的 χ^2 分布比较，检验水平 $\alpha = 0.05$，临界值 $\chi_{0.05}^2 = 3.84$，即只要得到的 χ_1^2 不大于 3.84，就认为 0-1 序列具有较好的随机性. 不同初始条件下的频数检验结果见表 1.

分析表明，算法能够通过频数检验，而且在不

同密钥下，序列的 χ_1^2 属于同数量级，说明算法生成的序列在不同密钥下的频数检验结果等效.

表 1 不同初始条件下的频数检验结果

Tab. 1 Frequency test results under different initial conditions

初始条件($j=3$)	n_0	n_1	χ_1^2
$x_0=0.432\ 323,\ q_0=1$	4 970	5 030	$3.600\ 0\times10^{-5}$
$x_0=0.432\ 323+10^{-16},\ q_0=1$	4 922	5 078	$2.433\ 6\times10^{-4}$
$x_0=0.432\ 323+2\times10^{-16},\ q_0=1$	4 975	5 025	$2.500\ 0\times10^{-5}$
$x_0=0.432\ 323,\ q_0=0$	5 077	4 923	$2.371\ 6\times10^{-4}$
$x_0=0.432\ 323+10^{-16},\ q_0=0$	4 916	5 084	$2.822\ 4\times10^{-4}$
$x_0=0.432\ 323+2\times10^{-16},\ q_0=0$	4 919	5 081	$2.624\ 4\times10^{-4}$

3.4 密文序列 0-1 的平衡度检验

定义平衡度为 $E(n)=|n_1-n_0|/n$，平衡度越小，说明序列中 0 和 1 的个数越接近，随机性越好. 图 7 的实验结果保证密文序列中 0 和 1 的分布大体均匀，可以保证算法能够有效地抵御统计分析.

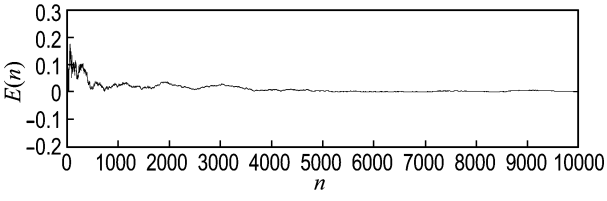


图 7 密文序列 0-1 平衡度

Fig. 7 The 0-1 balance of the ciphertext

3.5 密文序列的自相关性检验

定义二值序列的自相关系数为

$$r(n,m)=\frac{1}{n}\sum_{i=1}^{n-m}b_ib_{i+m};\ n\leqslant N$$

其中 m 为步长. 自相关系数的值与步长 m 有关，当步长一定而 n 变化时，自相关系数变化越小，说明对应二值序列的随机性越好. 图 8 给出了当 $m=1$ 时，密文序列的自相关系数与 n 的关系.

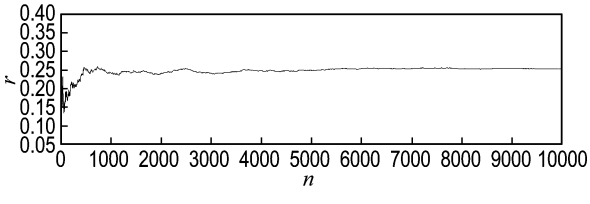


图 8 自相关系数与 n 的关系($m=1$)

Fig. 8 Relationship between r and $n(m=1)$

分析表明，当步长一定时，自相关系数的变化始终很小，说明对应二值序列的随机性很好.

3.6 密钥空间分析

本文给出的序列密码算法的密钥由迭代初始值 x_0、q_0 和离散化算子参数 j 构成，经过实验，仅在双精度下粗略地估算密钥空间不低于 2^{121}. 而且本文的两个分段非线性混沌动力系统的参数 P 也可以随机选择作为密钥，计算机的计算精度也远远超过双精度，所以本文算法的密钥空间完全可以抵抗蛮力攻击.

3.7 同其他算法的比较

利用混沌动力系统构造序列密码算法的研究很多，本文选取比较有代表性的算法进行比较，比如文献[3-4]所用的动力系统的不变分布密度函数只是接近于均匀分布，文献[24]证明了文献[25]所用的动力系统的不变分布密度函数不是均匀分布. 而由定理 1 知，本文所用的动力系统不仅不变分布是理想状态下的均匀分布，而且输出序列$\{X(t)\}$在$[0,1]$上是各态历经的，自相关函数呈 δ 形态. 这说明在统计性能上，本文算法比文献[3-4,25]中的算法更好.

文献[26]中采用的算法，频数检验的平均值是 0.778，本文所用的算法频数检验的平均值是 $2.185\ 3\times10^{-4}$，说明本文算法对应二值序列的随机性更好.

4 结 语

本文算法运用了一个混沌动力序列控制、选择混沌动力系统中的分段非线性映射，提高了整个加密过程的复杂程度. 加密过程分两轮进行，在完成第一轮后才能进行第二轮，使得输出序列具有大的周期长度和高度的非线性. 因此，明文的任何一个 bit 位的改变必将影响密文的每一个 bit 位，克服了明文的 bit 位改变只能影响密文的 bit 位后面的序列的改变这一缺陷，提高迭代过程对密钥和明文的敏感性. 算法密钥空间大，可以抵抗空间重构攻击. 本文给出的两个混沌动力系统自身的特点，决定了输出序列具有良好的统计特性，可以有效抵御统计分析攻击. 本文算法增强了抗已知明文/密文攻击的能力，有效提升了算法的安全性.

参考文献：

[1] Habutsu Toshiki, Nishio Yoshifumi, Sasase Iwao,

et al. A secret key cryptosystem by iterating a chaotic map [C] // Davies D W, ed. **Advance in Cryptology-EUROCRYPT′91. LNCS 547**. Berlin: Springer-Verlag, 127-140.

[2] 周　红,罗　杰,凌燮亭. 混沌非线性反馈密码序列的理论设计和有限精度实现[J]. 电子学报, 1997, **25**(10):57-60,56.
ZHOU Hong, LUO Jie, LING Xie-ting. Generating nonlinear feedback stream ciphers via chaotic systems [J]. **Acta Electronica Sinica**, 1997, **25**(10):57-60,56. (in Chinese)

[3] 周　红,俞　军,凌燮亭. 混沌前馈型流密码的设计[J]. 电子学报, 1998, **26**(1):98-101.
ZHOU Hong, YU Jun, LING Xie-ting. Design of chaotic feed forward stream cipher [J]. **Acta Electronica Sinica**, 1998, **26**(1): 98-101. (in Chinese)

[4] 桑　涛,王汝笠,严义埙. 一类新型混沌反馈密码序列的理论设计[J]. 电子学报, 1999, **27**(7):47-50.
SANG Tao, WANG Ru-li, YAN Yi-xun. The theoretical design for a class of new chaotic feedback stream ciphers [J]. **Acta Electronica Sinica**, 1999, **27**(7):47-50. (in Chinese)

[5] 王相生,甘骏人. 一种基于混沌的序列密码生成方法[J]. 计算机学报, 2002, **25**(4):351-356.
WANG Xiang-sheng, GAN Jun-ren. A chaotic sequence encryption method [J]. **Chinese Journal of Computers**, 2002, **25**(4):351-356. (in Chinese)

[6] 李红达,冯登国. 基于复合离散混沌动力系统的序列密码算法[J]. 软件学报, 2003, **14**(5):991-998.
LI Hong-da, FENG Deng-guo. Stream cipher algorithms based on composite nonlinear discrete chaotic dynamical systems [J]. **Journal of Software**, 2003, **14**(5):991-998. (in Chinese)

[7] 李红达,冯登国. 复合离散混沌动力系统与序列密码体系[J]. 电子学报, 2003, **31**(8):1209-1212.
LI Hong-da, FENG Deng-guo. Composite nonlinear discrete chaotic dynamical systems and stream cipher systems [J]. **Acta Electronica Sinica**, 2003, **31**(8):1209-1212. (in Chinese)

[8] Gotz M, Kelber K, Scharwarz W. Discrete-time chaotic encryption systems-part I: Statistical design approach [J]. **IEEE Transactions on Circuits Systems 1: Fundamental Theory and Applications**, 1997, **44**(10):963-970.

[9] Kocarev L. Chaos-based cryptography: a brief overview [J]. **IEEE Circuits and Systems Magazine**, 2001, **1**(3):6-21.

[10] XIANG Tao, Wong Kwok-wo, LIAO Xiao-feng. A novel symmetrical cryptosystem based on discretized two-dimensional chaotic map [J]. **Physics Letters A**, 2007, **364**(3-4):252-258.

[11] Alvarez G, Montoya F, Romera M, *et al*. Cryptanalysis of a chaotic encryption system [J]. **Physics Letters A**, 2000, **276**(1-4):191-196.

[12] Biham E. Cryptanalysis of the chaotic map cryptosystem suggested at EUROCRYPT′91 [C] // Davies D W, ed. **Advance in Cryptology-EUROCRYPT′91. LNCS 547**. Berlin: Springer-Verlag, 532-534.

[13] 金晨辉,高海英. 对两个基于混沌的序列密码算法的分析[J]. 电子学报, 2004, **32**(7):1066-1070.
JIN Chen-hui, GAO Hai-ying. Analysis of two stream ciphers based on chaos [J]. **Acta Electronica Sinica**, 2004, **32**(7):1066-1070. (in Chinese)

[14] 金晨辉,杨　阳,祁传达. 对混沌序列密码的相关密钥攻击[J]. 电子与信息学报, 2006, **28**(3):410-414.
JIN Chen-hui, YANG Yang, QI Chuan-da. A related-key attack on chaotic stream ciphers [J]. **Journal of Electronics & Information Technology**, 2006, **28**(3):410-414. (in Chinese)

[15] 张　斌,金晨辉. 对迭代型混沌密码的逆推压缩攻击[J]. 电子学报, 2010, **38**(1):129-134,140.
ZHANG Bin, JIN Chen-hui. Inversion and compression attacks to iterative chaotic ciphers [J]. **Acta Electronica Sinica**, 2010, **38**(1):129-134,140. (in Chinese)

[16] 汪海明,李　明,金晨辉. 对 XW 混沌密码算法的分割攻击[J]. 计算机应用研究, 2010, **27**(7):2625-2628
WANG Hai-ming, LI Ming, JIN Chen-hui. Divide-and-conquer attack on XW chaotic cipher [J]. **Application Research of Computers**, 2010, **27**(7): 2625-2628. (in Chinese)

[17] 尹汝明,袁　坚,山秀明,等. 混沌密码系统弱密钥随机性分析 [J]. 中国科学:信息科学, 2011, **41**(7):777-788.
YIN Ru-ming, YUAN Jian, SHAN Xiu-ming, *et al*. Weak key analysis for chaotic cipher based on randomness properties [J]. **Scientia Sinica: Informationis**, 2011, **41**(7):777-788. (in Chinese)

[18] 李广明,张 洪,肖慧娟. 一种混沌序列密码的产生[J]. 通信技术, 2009, **42**(5):227-229.
LI Guang-ming, ZHANG Hong, XIAO Hui-juan. Generation of chaotic cipher sequences [J]. **Communications Technology**, 2009, **42**(5):227-229. (in Chinese)

[19] 张 涛. 基于混沌的序列密码算法[J]. 计算机应用, 2010, **30**(5):1221-1223.
ZHANG Tao. Stream cipher algorithm based on chaos [J]. **Journal of Computer Applications**, 2010, **30**(5):1221-1223. (in Chinese)

[20] 王丽燕,李永华,贾思齐,等. 一种基于复合混沌动力系统的序列密码算法[J]. 大连理工大学学报, 2012, **52**(5):730-735.
WANG Li-yan, LI Yong-hua, JIA Si-qi, *et al*. A stream cipher algorithm based on composite chaotic dynamical systems [J]. **Journal of Dalian University of Technology**, 2012, **52**(5):730-735. (in Chinese)

[21] Lasota A, Mackey M. **Probabilistic Properties of Deterministic Systems** [M]. Cambridge: Cambridge University Press, 2008.

[22] Kosyakin A A, Sandler E A. Ergodic properties of a class of piecewise smooth transformations of an interval [J]. **Izvestiya Vysshikh Uchebnykh Zavedenii Matematika**, 1972, **118**(3):32-41.

[23] Cornfeld I P, Fomin S V, Sinai Y G. **Ergodic Theory** [M]. Berlin: Springer-Verlag, 1982.

[24] 谢邦勇,王德石. 对一类新型混沌密码序列的几点商榷[J]. 信息安全与通信保密, 2007(6):92-93.
XIE Bang-yong, WANG De-shi. Discussions on a class of new chaotic stream cipher [J]. **Information Security and Communications Privacy**, 2007(6):92-93. (in Chinese)

[25] 胡国杰,冯正进. 一类新型混沌密码序列的理论设计[J]. 通信技术, 2003(4):73-74.
HU Guo-jie, FENG Zheng-jin. Theoretical design for a class of new chaotic stream cipher [J]. **Communications Technology**, 2003(4):73-74. (in Chinese)

[26] 罗 轶. 一维时空混沌密码系统及安全性分析[J]. 湖南工业大学学报, 2010, **24**(5):50-53.
LUO Yi. One-dimension spatio-temporal chaotic cryptography and its security analysis [J]. **Journal of Hunan University of Technology**, 2010, **24**(5):50-53. (in Chinese)

A stream cipher algorithm based on two discrete chaotic dynamical systems

WANG Li-yan[1], XU Jia-jia[1], LI Hai-yan[*2]

(1. College of Information Engineering, Dalian University, Dalian 116622, China;
2. School of Science, University of Science and Technology Liaoning, Anshan 114051, China)

Abstract: A new stream cipher algorithm is designed based on two discrete chaotic dynamical systems. The algorithm uses the front output of the piecewise nonlinear map as the next input of the piecewise nonlinear map, and the iterative sequences are transformed into 0-1 sequence with discrete operator, and then, the 0-1 sequence is used to select the piecewise nonlinear maps of the two chaotic dynamical systems. The simulation test and security analysis are conducted to study the randomness, the initial value sensitivity and other properties of sequences generated by the map. The experimental results show that the algorithm has the characteristics of the high sensitivity of secret key, plaintext and ciphertext, and the small correlation between ciphertext and plaintext. These peculiarities can efficiently prevent ciphertext to leak the information of secret key and plaintext.

Key words: chaotic dynamical systems; piecewise nonlinear map; stream cipher