一种基于混沌和矩阵变换的序列密码*)

顾国生　韩国强　李　闻
(华南理工大学计算机科学与工程学院　广州 510640)

摘　要　基于混沌的加密或扩频通信是当前的热门研究课题。但有限精度效应使得混沌序列密码存在密钥空间过小及周期退化的缺陷。本文通过引入一类特殊的(0，1)-矩阵类及三种矩阵变换，在二维混沌序列控制下不断地进行矩阵变换并以某种特殊方式扫描矩阵而产生 N 相伪随机序列。该序列满足作为密码序列的各项要求。实验结果同样显示该序列具有均匀分布、伪随机性好、复杂度高等优良统计特性，与理论分析的结论相符。

关键词　混沌，矩阵变换，(0,1)-矩阵类，序列密码

A Stream Cipher Based on Chaos and Matrix Transform

GU Guo-Sheng　HAN Guo-Qiang　LI Wen
(College of Computer Science and Engineering, South China University of Technology, Guanzhou 510640)

Abstract　Nowadays encryption and spread spectrum communication based on chaos is a hot research topic. Yet the limited precision of computer makes chaotic sequences degenerate to periodic ones and haven't enough key space. In the paper we have designed a stream cipher based on chaos and matrix transform. six two-dimensional chaotic sequences are used to control three kinds of matrix transform and the scanning of a sort of special(0,1)-matrices. The result sequence satisfies the requests for stream cipher. The simulation also implies it has good statistic characters.

Keywords　Chaos; Matrix transform, (0,1)-matrices, Stream cipher

1　引言

混沌序列具有类随机特性和不可预测性，将其应用于加密或扩频通信已成为一个热门的研究课题[1~5]。目前广泛应用于加密的混沌模型是一维离散系统(如 Logistic、Tent 映射)，其有着形式简单、产生混沌时序快等优点。二维混沌系统具有更复杂的动力学行为，不存在有效的无误差构造形式，进一步提高了加密系统的抗破译强度。但这些现有的混沌加密系统均存在以下缺陷：1)密钥空间小；2)有限精度效应，使混沌序列退化为周期序列且周期难以度量。本文引入了一类特殊的(0，1)-矩阵类及三种矩阵变换[6]，在二维混沌序列控制下不断地进行矩阵变换，并通过设定一条特殊的路径扫描矩阵而产生 $N=16$ 相密码序列，证明了所产生的密码序列具有良好的统计特性和密码特性。与二维混沌序列相比，较好地扩大了序列周期和密钥空间。

2　相关概念

2.1　二维混沌系统

二维混沌离散系统的一般形式为：

$$\begin{cases} x_{n+1}=a_1+a_2x_n+a_3x_n^2+a_4y_n+a_5y_n^2+a_6x_ny_n \\ y_{n+1}=a_7+a_8x_n+a_9x_n^2+a_{10}y_n+a_{11}y_n^2+a_{12}x_ny_n \end{cases}$$

式中 $a_1,a_2,\cdots,a_{12}$ 为待定常系数。

指定这十二个状态量的取值，然后计算系统的 Lyapunov 指数或利用相图分析的方法，就可以得到相应的二维混沌系统。为了缩短系统产生混沌序列的时间，尽可能选取形式简单的方程，例如具有一次耦合项形式的二维 Logistic 映射

$$\begin{cases} x_{n+1}=4\mu_1x_n(1-x_n)+\gamma y_n \\ y_{n+1}=4\mu_2y_n(1-y_n)+\gamma x_n \end{cases}$$

在 $\mu_1=\mu_2=0.89,\gamma=0.1$ 时系统是混沌的。亦可构造复杂度更高的二维超混沌系统[7]，例如 $\begin{cases} x_{n+1}=1.55y_n-1.3y_n^2 \\ y_{n+1}=0.1y_n-1.1x_n \end{cases}$ 有两个大于零的 Lyapunov 指数 0.238 和 0.166，是一个超混沌系统。

2.2　具有一定行和、列和向量的(0,1)-矩阵类[6]

设 m 和 n 是正整数，$R=(r_1,\cdots,r_m)$ 和 $S=(s_1,\cdots,s_n)$ 是非负整数向量，$U(R,S)$ 表示具有行和向量 R 和列和向量 S 的 $m\times n$ 阶(0，1)矩阵 $A=(a_{i,j})$ 的集合，即

$$\begin{cases} \sum_{j=1}^{n}a_{i,j}=r_i,i=1,\cdots,m \\ \sum_{i=1}^{m}a_{i,j}=s_j,j=1,\cdots,n \end{cases}$$

设 $A\in u(R,S)$，对任意 $0\leqslant i,j\leqslant 15$，$A$ 中包含元素 $a_{i,j}$ 的可能的二阶子方阵有四个(当 $a_{i,j}$ 处于矩阵边缘时只有两个或一个)，分别是：

$$\begin{pmatrix} a_{i-1,j-1} & a_{i-1,j} \\ a_{i,j-1} & a_{i,j} \end{pmatrix},\begin{pmatrix} a_{i-1,j} & a_{i-1,j+1} \\ a_{i,j} & a_{i,j+1} \end{pmatrix},$$

$$\begin{pmatrix} a_{i,j} & a_{i,j+1} \\ a_{i+1,j} & a_{i+1,j+1} \end{pmatrix},\begin{pmatrix} a_{i,j-1} & a_{i,j} \\ a_{i+1,j-1} & a_{i+1,j} \end{pmatrix},$$

考察 A 的形式为：

*)基金项目：国家自然科学基金(60573019)、广东省自然科学基金重点项目(05103541)、广东省自然科学基金博士科研启动基金(05300198)。
顾国生　博士研究生，主要研究方向为信息安全与多媒体应用技术。**韩国强**　教授，博士生导师，主要研究方向为信息安全与多媒体应用技术。
李　闻　博士研究生，主要研究方向为多媒体应用技术。

$$A_1=\begin{pmatrix}1&0\\0&1\end{pmatrix}\text{和}A_2=\begin{pmatrix}0&1\\1&0\end{pmatrix}$$

的二阶子方阵。把 A 的某个形如 A_1(或 A_2)的子方阵换成 A_2(或 A_1)同时不改动 A 的所有其他元素的变换称为 A 的对换变换。把 A 的第 i 行和第 j 行对调同时不改动 A 的所有其他元素的变换称为 A 的行变换,把 A 的第 i 列和第 j 列对调同时不改动 A 的所有其他元素的变换称为 A 的列变换。

下面的定理表明,在 $u(R,S)$ 中任意两个矩阵都可以通过对换从一个变成另一个。它是本文算法的理论核心。

定理 1(Ryser[10]) 设 $A,A'\in u(R,S)$,则可经过有限次对换把 A 变成 A'。

3 序列密码方案设计

取定 $m=n=16$ 和 $R=S=(9,9,9,9,9,9,9,9,9,9,9,9,9,9,9,9)$,即考察每行每列都恰好有 9 个 1 的 16 阶(0,1)-方阵类,记为 $u(R=S|16:9)$。例如

$$A=\begin{bmatrix}
0&1&1&1&0&1&0&1&0&0&0&1&0&1&1&1\\
0&1&1&0&0&1&1&0&1&0&0&1&1&1&0&1\\
1&1&1&1&1&0&1&1&0&0&0&0&0&0&1&1\\
0&0&1&0&1&1&0&1&1&1&0&1&1&1&0&0\\
1&1&0&0&0&1&0&1&0&1&1&1&1&1&0&0\\
1&0&0&1&1&1&0&0&0&1&1&1&1&0&1&0\\
0&1&1&0&0&0&1&1&1&1&1&0&1&0&1&0\\
0&1&0&1&1&0&1&1&1&0&0&0&0&1&1&1\\
1&0&0&0&1&0&1&1&1&0&1&1&0&1&0&1\\
1&0&0&1&1&0&0&0&1&1&1&1&0&0&1&1\\
0&1&1&0&0&0&0&1&0&1&1&0&1&1&1&1\\
1&0&0&1&1&1&1&0&0&0&1&1&0&1&1&0\\
1&1&0&0&1&1&1&1&1&1&1&0&0&0&0&0\\
1&0&1&1&1&1&0&0&1&1&0&0&1&1&0&0\\
1&0&1&1&0&0&1&0&1&1&0&1&1&0&0&1\\
0&1&1&1&0&1&1&0&0&0&1&0&1&0&1&1
\end{bmatrix}$$

就是 $u(R=S|16:9)$中的一个元。显然任意 A 属于 $u(R=S|16:9)$,A 经过 2.1 节的三种变换后仍属于 $u(R=S|16:9)$。我们最终要生成的是一个 16 相的整数密码序列,记为 $Z=\{z_l|z_l$ 是整数且 $0\leqslant z_l\leqslant 15\}_0^\infty$,称每个 $z_i(i\geqslant 0)$为 z_{i+1}的前缀,z_{i+1}为 z_i 的后续。密码序列 Z 产生过程需要选择三个二维(超)混沌映射,记为 f_1,f_2,f_3,以及六个初值 c_0,d_0,e_0,f_0,g_0,h_0,由 f_1,f_2,f_3 分别生成三对混沌序列$(\{c_l\}_0^\infty,\{d_l\}_0^\infty)$,$(\{e_l\}_0^\infty,\{f_l\}_0^\infty)$,$(\{g_l\}_0^\infty,\{h_l\}_0^\infty)$,用来控制矩阵 A 的三种变换。

首先说明对每个符号 $0\leqslant z\leqslant 15$,z 的后续是通过不断往返扫描矩阵 A 的第 z 行产生的,即以

$a_{z,0},\cdots,a_{z,15},a_{z,15},\cdots,a_{z,0}$,

$a_{z,0},\cdots,a_{z,15},a_{z,15},\cdots,a_{z,0}$,

$a_{z,0},\cdots,a_{z,15},a_{z,15},\cdots,a_{z,0}$,

…。

的路径扫描第 z 行,遇 0 元跳过,遇非 0 元(即 1)停止。设遇到的第一个非 0 元是 $a_{z,j}$,则以列下标 j 作为 z 的第一个后续,记下 $a_{z,j}$在路径中的位置,转去矩阵 A 的第 j 行以同样的路径扫描第 j 行确定符号 j 的第一个后续。每个符号都用同样的方法确定其第一个后续,当有符号重复出现,不失一般性仍设为 z,即当 z 重新出现时,接着上次在路径中记录的位置往后继续扫描寻找 z 的第二个后续,遇 0 元跳过,遇非 0 元停止,以遇到的第二个非 0 元 $a_{z,k}$的列下标 k 作为 z 的第二个后续,更新所记录的位置为当前 $a_{z,k}$ 所在的位置。往下用同样的方法确定 z 的其他后续。

以矩阵 A 和六个初值 c_0,d_0,e_0,f_0,g_0,h_0 作为初始密钥,密码序列 $Z=\{z_l\}_0^\infty$ 生成算法描述如下:

1)任意选取 $0\leqslant z\leqslant 15$;

2)设当前已产生 $z_0,\cdots,z_k$,按上述方法扫描矩阵 A 的第 z_k 行产生 z_k 的后续 z_{k+1};

3)f_1 输出一对值 c_l,d_l,量化为 0～15 的整数 $\bar{c}_l,\bar{d}_l$,对矩阵 A 的包含元素 $a_{\bar{c}_l,\bar{d}_l}$ 且具有 A_1(或 A)形式的所有可能的二阶子方阵进行对换变换;

4)f_2 输出一对值 e_l,f_l,量化为 0～15 的整数 $\bar{e}_l,\bar{f}_l$,对矩阵 A 的第 $\bar{e}_l$ 行和第 $\bar{f}_l$ 行进行行变换;

5)f_3 输出一对值 g_l,h_l,量化为 0～15 的整数 $\bar{g}_l,\bar{h}_l$,对矩阵 A 的第 $\bar{g}_l$ 列和第 $\bar{h}_l$ 列进行列变换;

6)转 2),直到生成的序列长度到达要求为止。

说明:步骤 4)、5)的目的是为了把 3)变换的结果在矩阵中扩散开来。

在计算机上实现时,由于精度有限的缘故,f_1,f_2,f_3 所生成三对混沌序列 $(\{c_l\}_0^\infty,\{d_l\}_0^\infty)$,$(\{e_l\}_0^\infty,\{f_l\}_0^\infty)$,$(\{g_l\}_0^\infty,\{h_l\}_0^\infty)$,并不是真正意义上的混沌序列,它们都会退化成周期序列从而使得最后产生的密码序列 Z 也是一个周期序列。但相对于$\{c_l\}_0^\infty,\{d_l\}_0^\infty,\{e_l\}_0^\infty,\{f_l\}_0^\infty,\{g_l\}_0^\infty,\{h_l\}_0^\infty$而言,$Z$ 的周期有所扩大,这是因为 $Z=\{z_l\}_0^\infty$ 要形成周期,控制矩阵变换的这六个混沌伪随机序列必须达到同步,因此 Z 的周期至少是这六个混沌伪随机序列周期的最小公倍数$[p_1,p_2,p_3,p_4,p_5,p_6]$。

实际上,我们对扫描路径稍作改动,可使得生成的序列 Z 成为非周期序列。把从左到右再折返一次从右到左的次序扫描矩阵 A 的第 z 行,即扫描

$a_{z,0},\cdots,a_{z,15},a_{z,15},a_{z,0}$

一趟,称作对第 z 行的一趟顺向往返扫描(简称为顺)。相应地把从右到左再折返一次从左到右的次序扫描第 z 行,即扫描

$a_{z,15},\cdots,a_{z,0},a_{z,0},a_{z,15}$

一趟,称作对第 z 行的一趟逆向往返扫描(简称为逆)。把算法中的扫描路径替换为如下路径:顺,逆,顺,顺,逆,逆,顺,顺,顺,逆,逆,逆,…。显然这是一条非周期路径,每个符号按该路径扫描产生的后续都不会出现周期重复,从而 Z 是非周期序列。

4 密码算法分析

为了方便后面的分析,我们首先计算密钥和密文空间。显然不同的密钥会产生不同的密文,因此只需要计算密钥空间的大小。定理 1 保证了矩阵 A 可取遍 $u(R=S|16:9)$的所有元,也就是要计算 $u(R=S|16:9)$中元素的个数。1957 年 Gale[8] 和 Ryser[9] 各自独立地得到了 $u(R,S)$的存在的充分必要条件,接着 Ryser 提出了 $u(R,S)$的计数问题。1982 年魏万迪[10]引入了全链的概念,导出了 $u(R,S)$的个数(记为$|u(R,S)|$)一个非平凡正下界。根据文[10],计算出矩阵 A 及其极左矩阵 $\bar{A}$ 的列和向量 S 和 $\bar{S}$,作出 S 到 $\bar{S}$ 的全链后计算可得:

$|u(R=S|16:9)|$

$$\geqslant \prod_{0\leqslant i\leqslant 14}\binom{S_\mu^i - S_\lambda^i}{\min(S_\mu^i - S_\mu^{i+1}, S_\lambda^{i+1} - S_\lambda^i)}$$

$$=\binom{16}{7}\cdot\binom{9}{2}\cdot\binom{14}{5}\cdot\binom{11}{4}\cdot\binom{12}{3}\cdot\binom{13}{6}\cdot\binom{10}{1}\cdot\binom{15}{7}\cdot\binom{8}{1}\cdot\binom{15}{6}\cdot\binom{10}{3}\cdot\binom{13}{4}\cdot\binom{12}{5}\cdot\binom{11}{2}\cdot\binom{14}{7}$$

$\approx 3.3948\times10^{39} > 2^{128}$。

接着考察 6 个初值 $c_0, d_0, e_0, f_0, g_0, h_0$ 的选择范围。在有限精度实现时，例如 16 位精度，也有约$(10^{16})^6$ 种选择，均达到了理想密钥空间的要求。

本文的序列密码体制不同于常规的混沌密码体制之处在于：不直接采用混沌序列或其量化序列作为密码序列，是通过混沌序列的控制对不断切换的 $u(R,S)$矩阵进行扫描而产生密码序列，这种结构具有如下优点。

(1)很好地掩蔽了混沌序列的迭代特性及回复特性

算法中采用的二维混沌映射及设定的扫描方式是完全非线性，可以防止线性预测或重构。如果破解者想要获得混沌映射的迭代规律，他必须把每个符号的每一轮循环从密码序列中正确分解出来。算法中的步骤 3)每执行一次，就会切换一个矩阵，相当于更换了一个扫描模型，由此来提高产生的密码序列的复杂性。即使有个别循环被分解出来，如上所述 $u(R=S|16:9)$中矩阵数量庞大，而且又在不断地切换，这种规律又被迅速扰乱，因此密码攻击者要想通过实验获得准确的迭代规律的机率是很小的。步骤 3)的矩阵切换的另一个优点是即使破解者获取了某一步的矩阵，或者部分的密文和相应的密文，他仍然难以预测后面的序列。这是因为每个符号的一轮扫描仅产生 9 个后续符号，很快就会进入下一轮扫描。一旦矩阵进行了切换，扫描次序就会发生改变。

(2)保证了产生的序列满足均匀分布、δlike 的自相关、0 互相关的性质

从混沌理论可知，二维混沌映射产生的混沌伪随机序列满足均匀分布、δ-like 的自相关、0 互相关的性质。由于 $u(R=S|16:9)$矩阵每行每列都具有相等个数的 1，在这些混沌序列控制下按上一节设定的路径扫描矩阵，定理 1 保证了 A 可取遍 $u(R=S|16:9)$中的所有矩阵，从而各个符号及其后续的输出概率是相等的，于是这些性质在 Z 中均得到保持。

(3)对初始密钥敏感

这是由混沌序列的对初值的敏感依赖性的得到的。即当初始密钥有轻微变化时，控制矩阵变换的混沌序列轨迹就会有很大的变化，相应地扫描产生的密码序列也就会有很大变化。

(4)改善了序列的周期性能

在有限精度的限制下，数值化的混沌序列会退化成为周期序列，有限的精度同时也限制了密钥空间的大小，这都大大降低了混沌序列的安全性能。尽管提高计算精度能够在一定程度上对这两方面有所改善，但是所要付出的硬件代价是很大的。本文引入了混沌序列控制矩阵扫描的机制，通过设定一种不会产生周期重复的扫描路径，得到了非周期的密码序列，同时也扩大了密钥空间，较好地解决了这两方面的缺陷。

5 仿真实验

实验产生一个长度为 2^{16} 的密码序列 Z。为了方便显示，我们截取前面的长度为 2^{12} 的子序列，将它的分布图示于图 1。

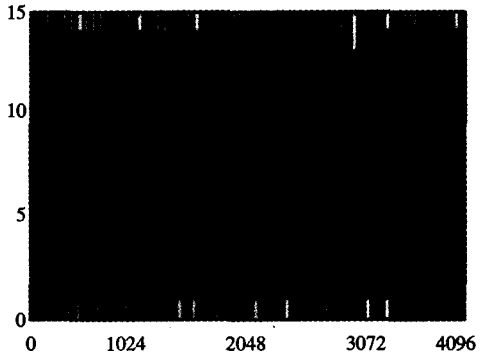


图 1 长度为 2^{12} 的密码序列分布图

序列 Z 包含各个符号的个数以及长度为 2 的符号段的个数分别列于表 1 和表 2。从图 1 和表 1、表 2 可以看到所产生的密码序列有较好的分布，接近于随机序列。我们再将密钥稍作改动(改变其中一个混沌初值，变化量少于 10^{-10})，产生另一长度同样为 2^{16} 的密码序列 Z'。图 2 显示了 Z 和 Z' 的自相关、互相关特性的实验结果其中序列 Z 的归一化自相关函数计算公式为：

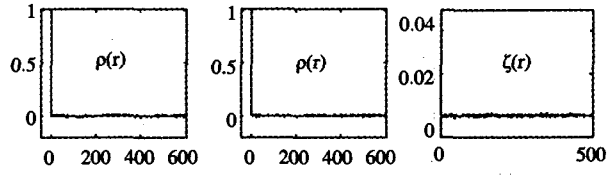
$$\rho(r)=\frac{\lim\limits_{J\to\infty}\frac{1}{J}\sum\limits_{l=1}^{J}(z_l-\bar{z})(z_{l+r}-\bar{z})}{\lim\limits_{J\to\infty}\frac{1}{J}\sum\limits_{l=1}^{J}(z_l-\bar{z})^2},\ (r\in Z^+),$$

其中均值 $\bar{z}=\lim\limits_{J\to\infty}\frac{1}{J}\sum\limits_{l=1}^{J}z_l$。

Z 和 Z' 的归一化互相关函数为：

$$\xi(r)=\frac{\lim\limits_{J\to\infty}\frac{1}{J}\sum\limits_{l=1}^{J}(z_l-\bar{z})(z'_{l+r}-\bar{z}')}{N^2}。$$

这些相关性实验结果都与前面的分析相吻合，并且与理想随机序列的相关值曲线几乎完全一致，说明该序列随机性很好。由于 Z 和 Z' 是在初始密钥作非常轻微的变化下生成的，它们几乎为 0 的互相关同时说明了本文的密码体制对初始密钥的变化是极其敏感的。



(a)序列 Z 的自相关曲线 (b)序列 Z′的自相关曲线 (c)序列 Z 和 Z′的互相关曲线

图 2

为了有效抵抗已知明文和密文对的攻击，输出的密码序列还需要有较好的复杂度特性，即理想的伪随机序列应具有尽可能大的序列复杂度。我们选用近似熵作为衡量伪随机序列复杂度的标准[14, 15]。序列的近似熵越大，说明它的复杂度就越高。根据文[14]，Logistic 混沌伪随机序列近似熵的最大值约为 0.693。对本密码系统所产生的密码序列进行近似熵分析，结果如表 3 所示。

最后通过一个图像加密实例来验证本序列密码的效果。对一幅 256×256 的灰度图像按位进行加密。由于灰度图像的每个像素包含 8 个二进制位，而本文的 16 相密码序列包含 4 个二进制位，所以把两个密码序列叠合起来刚好可以用来加密灰度图像，加密结果如图 3 所示。

表 1　序列 Z 包含符号 $0 \leqslant i \leqslant 15$ 的个数(理论值为 4096)

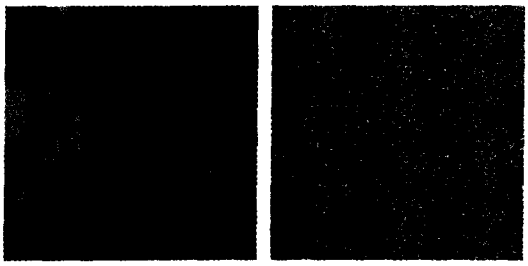
符号	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
个数	4076	4109	4113	4106	4073	4064	4115	4123	4137	4103	4121	4116	4069	4132	4004	4075

表 2　序列 Z 包含长度为 2 的符号段 i, j 的个数(理论值为 256)

符号 i \ 符号 j	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	246	262	250	246	261	258	268	269	259	251	266	272	239	267	242	268
1	250	240	246	249	257	256	257	252	268	268	260	258	249	273	268	272
2	256	259	247	269	281	250	284	252	247	270	241	266	249	268	243	251
3	263	257	255	239	246	247	246	247	263	266	262	259	254	272	258	250
4	271	248	255	277	276	248	262	253	256	258	276	259	272	241	252	273
5	253	261	265	261	259	237	246	249	250	259	252	249	258	248	253	256
6	260	271	260	248	257	259	239	257	241	250	250	261	248	265	268	260
7	244	253	264	249	252	242	240	245	264	267	242	260	250	278	259	247
8	267	268	241	255	251	248	262	246	240	251	262	258	259	257	255	248
9	271	241	261	258	261	264	258	253	260	244	266	268	243	266	248	262
10	264	256	257	255	257	263	260	257	245	244	219	255	270	256	259	256
11	261	259	257	254	262	266	266	269	262	248	270	237	254	259	264	249
12	249	249	270	254	255	267	246	250	247	247	257	258	228	250	250	247
13	257	283	270	248	268	253	246	266	265	266	259	265	251	242	252	254
14	245	268	258	271	267	243	249	248	245	265	258	250	252	257	238	255
15	268	248	278	245	266	257	263	245	256	268	235	263	249	244	262	247

表 3　近似熵分析

m	r	序列长度	近似熵
1	0.25	2^{10}	2.7106
		2^{11}	2.7440
		2^{12}	2.7585
		2^{13}	2.7658
		2^{14}	2.7690
		2^{15}	2.7719
		2^{16}	2.7719



(a) 原图　　(b) 密图

图 3

定义原图和密图之间的相关度为：

$$R(n)=\frac{|\#\{c_i=m_i,1\leqslant i\leqslant n\}-\#\{c_i\neq m_i,1\leqslant i\leqslant n\}|}{n}$$

其中 n 表示比特的总数，m_i $(1\leqslant i\leqslant n)$ 表示明文的各个比特，c_i 表示密文中相应于 m_i 的比特。

显然 $0\leqslant R(n)\leqslant 1$。$R(n)$ 越小，加密的效果越好。$R(n)=0$ 时是最理想的情形，此时明文经过序列密码的调制，它的每一比特都以相等的概率改变或保持不变，从而密文没有泄露明文的信息。同时密文序列中 0 和 1 的分布均匀，这使得算法可以有效地抵御统计分析。计算原图于密图的相关度，结果为 0.0084，接近于理想的情形。

结论　针对混沌密码序列的一些常见缺陷，本文提出了一种基于混沌和矩阵变换的序列密码算法。通过引入一类特殊的(0,1)-矩阵类及三种矩阵变换和特殊的扫描方式来增强密码序列的复杂度和安全性。由此产生的非周期密码序列具有理想的统计和密码学特性。实验结果和理论预测相吻合，说明了该方法是对现有混沌序列密码的一种有效改进。

参 考 文 献

1　Mitchell D E. Nonlinear key generators [J]. Cryptologia, 1990, 14: 350～354

2　Ffey D R. Chaotic digital encoding: An approach to secure communication [J]. IEEE Trans Circuit and Systems, 1993, 40(10): 660～666

3　Fridrich. Symmetric ciphers based on two-dimensional chaotic maps [J]. International Journal of Bifurcation and Chaos, 1998, 8: 1259～1284

4　Kocarel L, Jakimovski G. Chaos and cryptography: from chaotic maps to encryption algorithms [J]. IEEE Trans Circ System, 2001, 48(2): 163～169

5　Chen G R, Mao Y B, Chui C K. A symmetric image encryption scheme based on 3D chaotic cat maps [J]. Chaos, Solutions and Fractals, 2004, 21: 749～761

6　柳柏濂. 组合矩阵论[M]. 北京：科学出版社，1996. 145～158

7　程丽，等. 构造具有超混沌特性的二维离散系统. 东北师大学报(自然科学版)[J]，2002，34(3)：47～52

8　Gale D. A theorem on flows in networks [J]. Pacific J. Math., 1957, 7: 1073～1082

9　Ryser H J. Combinatorial properties of matrices of zeros and ones [J]. Canada J. Math., 1957, 9: 371～377

10　Wei W D. The class U(R, S) of (0, 1)- matrices [J]. Discrete Math., 1982, 39: 301～305