基于复合符号混沌的伪随机数生成器及加密技术*

王福来†

(浙江财经学院应用数学研究所,杭州 310018)

(2011 年 4 月 16 日收到;2011 年 6 月 21 日收到修改稿)

提出了复合符号混沌序列的概念;并以符号动力学的揉序列为基础,将已知的伪随机数与揉序列规则下的短序列复合后得到新的符号混沌序列,再转换成二进制序列,从而得到长度随迭代次数成几何级数增加的伪随机序列(PRN). 理论与实证分析都表明这是一个有效的伪随机生成器. 为应用到图像的加解密技术中,建立了一个新型元胞自动机. 该元胞自动机能有效地避免数据膨胀,加密效率高,并能产生显著的"雪崩效应",提高了加密技术的安全性.

关键词: 复合符号混沌序列, 符号动力学, 伪随机序列, 元胞自动机

PACS: 05.45.Vx

1. 引 言

伪随机数生成器(pseudo random number generators, PRNG)是图像加解密、通讯等许多科学与工程方面的关键技术[1—4]. 现代伪随机数生成方法往往是利用各种不同的函数生成混沌时间序列再转换成伪随机序列码,因此伪随机数生成方法有两个关键环节:1)用函数来生成混沌时间序列;2)使用不可逆转函数将混沌时间序列转换成伪随机数. 当前文献中,研究对象主要是放在第一个环节上. 为了得到具有良好随机性能的密钥,人们先考虑得到复杂的混沌时间序列,于是利用复合混沌、高维混沌、混杂混沌等函数[5—9]. 这样做带来的缺陷是:1)能避免产生弱密钥同时得到序列周期充分长的函数仍然是不多的,即函数空间仍然较小,从而密钥空间不大[10,11];2)复合混沌、混杂混沌等函数是否仍具有混沌行为是不易在理论上证明的,如 Almeida 等[12]提出了"混沌 + 混沌 = 有序",张荣等[13]又提出了"有序 + 有序 = 混沌"理论及实例. 这说明混杂混沌、复合混沌等可能具有复杂的或难以预料的动力学行为,但必须深入讨论它们的动力学行为,而不能简单地认为复合之后一定会产生更复杂的行为. 而对于高维混沌,目前也没有理论证实由它生成的"0, 1"伪随机序列质量一定较高些. 伪随机数生成方法的第二个环节比第一个环节更难以研究,因为它不是利用一些已知的函数进行复合或改变参数就可以达到的,因此它一直未得到深入研究. 文献[1]针对第二个环节,提出了一种转换方式,理论与实证结果均表明生成的伪随机数质量较以往方法要好. 但它一次产生的伪随机数长度相对于图像的加解密技术仍十分有限;而在加密技术中(如加密 lenna 图像),则通常要求能产生 10^5 以上的流密码[14—16]. 文献[17]建立的元胞自动机要将 7200 个数据进行至少 73 次迭代才能产生所需长度的数据,即至少需要传递 73 次才能将画面从发射端传到接收系统;并且由于误差扩散机理不明确(无理论保障),故导致局部"雪崩效应"不明显,误差传递慢,在密钥的某一位产生 1 bit 误差仍能解密出大致图像,缺乏安全性.

本文的重点仍是继续研究伪随机数生成方法关键环节的第二个环节. 它是以符号动力学的揉序列为基础,将已知的伪随机数与揉序列下的短序列复合后得到新的混沌符号序列,再转换成"0—1"序列,从而得到长度增加几倍的伪随机序列. 第 2 节定义了复合符号混沌的概念,并给出了伪随机数生成器的算法. 第 3 节给出理论分析,第 4 节给出了伪随机数生成器的实证分析. 第 5 节是应用到图像的加

* 国家自然科学基金(批准号: 10871168)资助的课题.

† E-mail: flyerwon@sina.com

解密技术中,建立了一个新的元胞自动机规则.

2. 定义及算法步骤

2.1. 定 义

定义 1(复合符号序列) 设 $X = \{x_i\}_1^{N_1}$ 为一长度为 N_1 的符号序列,状态集为 $A = \{a_1, a_2, \cdots, a_k\}$,若 X 在状态集 A 的符号分别由状态集为 $B = \{0,1\}$ 的有限序列 $B_1, B_2, \cdots, B_k$ 替换得到长度为 N_2 的符号序列 $Y = \{y_i\}_1^{N_2}$,则称 $\{y_i\}_1^{N_2}$ 为复合符号序列.

定义 2(复合符号混沌序列) 如果将复合符号序列 $Y = \{y_i\}_1^{N_2}$ 的长度为 d 的子序列视为二进制实数,则顺次得到的 $N_2 - d + 1$ 个实数构成一个时间序列(Z).若 Z 为混沌的,则称 Z 为复合符号混沌序列. 这里的混沌定义指具有对初值的敏感依赖性及确定的概率密度的时间序列.

例如,序列 $X = \{232435\}$ 的符号"2,3,4,5"分别由"1001,1100,1110,1010"替换后得到复合符号序列为 $Y = \{100111001001111011001010\}$,长度扩大为原来的 4 倍. 当 $d = 6$ 时进一步得到二进制实值序列 $Z = \{100111, 1110, 11100, \cdots, 1010\}$. 第 3 节将证明若 X 是混沌的,则 Z 也为混沌的,从而为复合符号混沌序列.

为表述方便,这里引用文献[1]的均匀映射的定义.

定义 3[1](均匀映射) 设 $X = \{x_i\}_1^{N_1}$ 为一个混沌时间序列,均匀映射 $g(\cdot)$:

$$y_n = g(x_n) = \frac{K(x_n)}{N}, \quad n = 1, 2, \cdots, N. \quad (1)$$

其中 $K(x_n)$ 为 x_n 在混沌序列 $\{x_n\}_1^N$ 中按升序排列的序号.

为生成混沌序列密码,引入不可逆转函数 $T(x_n)$. 转换函数定义如下:

$$T(x_n) = \begin{cases} 0, & x_n \in \bigcup_{d=1}^{m} B_{2d-1}^{2m}, \\ 1, & x_n \in \bigcup_{d=1}^{m} B_{2d}^{2m}, \end{cases} \quad (2)$$

其中 $2m$ 为正整数, $B_0^{2m}, B_1^{2m}, B_2^{2m}, \cdots, B_{2m}^{2m}$ 是 $[0,1]$ 区间的 $2m$ 个连续的等分区间. $T(x_n)$ 的作用即是将 $2m$ 个连续区间交替变成 0、1 符号序列. 一般随序列长度 N 的增大 $2m$ 也取得大些.

2.2. PRNG 算法步骤

步骤 1 取长度为 $N_1 + 1$ 的"0—1"伪随机序列 $M = \{m_i\}_1^{N_1+1}$(如由文献[1]的方法得到),当 (m_i, m_{i+1}) 分别为"0,0", "0,1", "1,0", "1,1"时,令 y_i 分别为"2,3,4,5",从而得到状态集为 $A = \{2,3,4,5\}$ 且长度为 N_1 的伪随机序列 $X = \{x_i\}_1^{N_1}$;将 X 作为密钥.

步骤 2 记 $D = \{10100, 110100, 110010, 11100\}$. 将 X 的 2,3,4,5 分别由 D 的四个元素 10100, 110100, 110010, 11100 替换;若 X 的任一个符号发生变化,则 D 中的任一个符号发生变化,如第 4 个变为"1".

步骤 3 由 X 得到子序列长度为 d 的复合符号序列 $Y = \{y_i\}_1^{N_2}$,并由定义 2 得到时间序列 $Z = \{z_i\}_1^{N_1}$,其中 $N_2 = N_1 - T + 1$,再由文[1]的方法得到"0—1"伪随机序列 $S = \{s_i\}_1^{N_1}$.

步骤 4 将 S 作为 X,返回步骤 1. 直到生成伪随机数列的长度达到要求.

显然,执行 n 次,即可生成"0—1"伪随机序列 $\{y_i\}_1^{N_2}$,其中 $N_2 > 5^n N_1$,即长度呈几何级数增加.

3. 理论分析

本节中的记号如不作另行说明,沿用第 2.2 节中的含义. 第 2 节的理论基础来自于符号动力学. 由符号动力学知[18],当揉序列已知,在揉序列规则下,由其中的某些子序列进行任意组合,都可组成符合允字条件的周期序列. 如果组合的方式是充分随机的,则这样的周期序列长度就可以充分长.

3.1. Lorenz 映射[18,19]与揉序列

Lorenz 映射有多种形式,为表述方便,下面列出其中一种简单的[18].

(1) Lorenz 映射

$$f: [0,1] \to [0,1] \quad (0 < a < 1),$$

$$f_a(x) = \begin{cases} x + a, & x \in [0, 1-a), \\ h(x + a - 1), & x \in (1-a, 1]. \end{cases} \quad (3)$$

对于任何参数下的 Lorenz 映射,其符号序列的排序规则很简单,任给两个符号序列,它们的大小排序规则为

$$\Sigma 0 \cdots < \Sigma D \cdots < \Sigma C \cdots < \Sigma 1 \cdots, \quad (4)$$

这里,Σ 为两个符号序列的公共字头,D 和 C 为临

界点.

由符号动力学知 $M = \{m_i\}_1^{N_1+1}$ 的任何长度为 d 的子序列 $[m_i] = \{m\}_i^{i+d-1}$ 必须满足允字条件:

$$A([m_i]) \leqslant f(D) = K_-,$$
$$B([m_i]) \geqslant f(C) = K_+, \qquad (5)$$

其中 A,B 分别表示序列 $[m_i]$ 中所有字母 0 和 1 的后继序列, (K_-,K_+) 为揉序列. 揉序列是移位最大序列,它本身也必须满足允字条件(4).

Lorenz 映射(1)中,当 $a = 0.3, h = 3.2$ 时我们得到揉序列

$$K_- = [11101000110101001001010010001101011010110010100\cdots\cdots],$$
$$K_+ = [00010110010011010101101000111001001011001011001\cdots\cdots],$$
$$W = \{10, 100, 1000, 110, 1100, 11000, 1110, 11100, 111000\}.$$

令 $D = \{10100,110100,110010,11100\}$. 文献[18]指出,当 $a = 0.3, h = 3.2$ 时,由 W 中的任意几个的组合(含自身)都可构成 Lorenz 映射的符号周期序列.

由于 $Y = \{y_i\}_1^{N_2}(y_i \in \{0,1\})$ 是 M 与 D 的复合,故 $5N_1 < N_2 < 6N_1$. Y 的每个子序列都满足允字条件,Z 是 Y 的二进制实值序列,满足顺序规则. 由文献[1]的方法得到 0—1 序列 $S = \{s_i\}_1^{N_1}$.

3.2. Z 的性质

性质 1 Z 为非周期序列.

因为 X 为随机序列,故 Y 为非周期序列,从而 Z 为非周期序列.

性质 2 Z 具有确定的概率密度.

由于 X 中 $P\{X=2\} = P\{X=3\} = P\{X=4\} = P\{X=5\} = 1/4$, D 为确定的数组,故 Y 具有确定的概率密度,从而 Z 也具有确定的概率密度.

性质 3 当 d 与 N_2 充分大,则 Z 具有对初值条件的敏感依赖性.

当 d 充分大, Y 中没有两个点是相同的,现设 Y 中两点间的最大距离为 $d_{\max}$. 由于 X 的随机性,必存在 k, 使得 Y 中任两个点 Y_i, Y_j 的距离 $|Y_i, Y_j|$ 在 k 步后达到 $|Y_{i+k}, Y_{j+k}| > \frac{1}{2}d_{\max}$, 即 Y 具有对初值条件的敏感依赖性,也即 Z 具有敏感依赖性.

从敏感依赖性与确定的概率密度上讲, Z 是混沌时间序列. 由定义 2 知, Z 是复合符号混沌序列. 又由文献[1]的证明可知它可由均匀映射及转换函数生成高质量的 0—1 伪随机序列 $S = \{s_i\}_1^{N_1}$.

性质 4 可将"0"与"1"的任意组合作为 D 的元素,所得 Y,Z 具有上述性质 1—性质 3.

由 Lorenz 映射可知及符号动力学, (K_-,K_+) 可取满足 $0^\infty < K_+ < K_- < 1^\infty$ 的任意组合,故性质 4 成立.

性质 5 设在转换映射 T 中, $2m$ 充分大. 若改变 D 的一个符号得到 D', 并由此得到相应的 Y', Z', S', 则 S' 与 S 是不相关的.

由符号动力学移位映射的特点知, $|z_k, z'_k| \neq |z_{k+1}, z'_{k+1}|$, 且有 $|z_k, z'_k| < |z_{k+1}, z'_{k+1}|$. 由文献[1]的定理 1 知 z_{k+1} 与 z'_{k+1} 取 0 或 1 的事件是相互独立的.

对性质 5 可举一简单例子. 令 $X = \{23223\}$, $D = \{100,11\}$, $D' = \{100,10\}$, $d = 12$. 则

$$Y = \{1001110010011\}, Y' = \{1001010010010\},$$
$$y_1 = (100111001001), y_2 = (001110010011),$$
$$z_1 = (100111001001), z_2 = 1110010011,$$
$$y'_1 = (100101001001), y'_2 = (001010010010),$$
$$z'_1 = 100101001001, z'_2 = 1010010010,$$

显然有 $|z_k, z'_k| < |z_{k+1}, z'_{k+1}|$.

4. 实证分析

4.1. 游程分析

本节取 $d = 15$, 转换函数 T 中取 $2m = 120$.

1)令 $D = \{10100,110100,110010,11100\}$. 用 $P^{(i)}(i = 1,2,3,4)$ 表示 i 游程出现的频率均值, $P_{ij}(i,j = 0,1)$ 表示"(i,j)"出现的频率,得表 1.

2)当其他条件不变,当 D 的第 4 个符号由 0 改为 1 变为 D', 即 $D' = \{10110,110100,110010,11100\}$, 得表 2.

为比较,我们引入文献[20]的结果如下(见表 3):

表 1 短游程频率

项目	(P_0,P_1), $P^{(1)}$	$(P_{00},P_{01},P_{10},P_{11})$, $P^{(2)}$
频率	(0.5000,0.5000)	(0.2481,0.2519,0.2518,0.2481),0.2500
理论值	(0.5000,0.5000)	(0.2500,0.2500,0.2500,0.2500)
项目	$(P_{000},P_{010},P_{100},P_{011})$, $(P_{101},P_{110},P_{000},P_{111})$, $P^{(3)}$	$P^{(4)}$, $\sum_{i=1}^{4}P^{(i)}$
频率	(0.1221,0.1261,0.1286,0.1261),(0.1232,0.1258,0.1232,0.1249), 0.1250	0.0625, 0.9375
理论值	0.1250·(1,1,1,1,1,1,1,1)	0.0625, 0.9375

表 2 短游程频率

项目	(P_0,P_1), $P^{(1)}$	$(P_{00},P_{01},P_{10},P_{11})$, $P^{(2)}$
频率	(0.5000,0.5000),0.5000	(0.2494,0.2506,0.2506,0.2494),0.2500
项目	$(P_{000},P_{010},P_{100},P_{011})$, $(P_{101},P_{110},P_{000},P_{111})$, $P^{(3)}$	$P^{(4)}$, $\sum_{i=1}^{4}P^{(i)}$
频率	(0.1236,0.1258,0.1253,0.1258),(0.1252,0.1248,0.1253,0.1241), 0.1250	0.0625, 0.9375

表 3 用 Monte-Carlo 方法从混沌时间序列获得的伪随机数列的短游程频率

序列或映射 \ 频率均值	$P^{(1)}$	$P^{(2)}$	$P^{(3)}$	$P^{(4)}$	$\sum_{i=1}^{4}P^{(i)}$
m 序列	0.4773	0.2345	0.1529	0.0640	0.9287
Logistic	0.5563	0.2441	0.0861	0.0473	0.9338
Chebyshev 序列	0.5787	0.1843	0.0737	0.0598	0.8965
SCQC(二相混沌扩频序列)	0.4854	0.2613	0.1275	0.0704	0.9447
TD-ERCS(基于切延迟的椭圆反射腔映射)	0.4857	0.2495	0.1243	0.0706	0.9301

比较表 1 与表 2 可知,改变复合元素的某个符号并不会导致伪随机数的质量降低;比较表 1、表 2 与表 3,同时比较文献[2—4,17],可知,采用本文算法生成的 0—1 伪随机序列的游程频率更接近理论值.

4.2. 自相关与互相关分析

(1) 取两序列位置距离步长(Lags)变化范围为 $[-500, 500]$,得自相关系数与互相关系数如图 1.

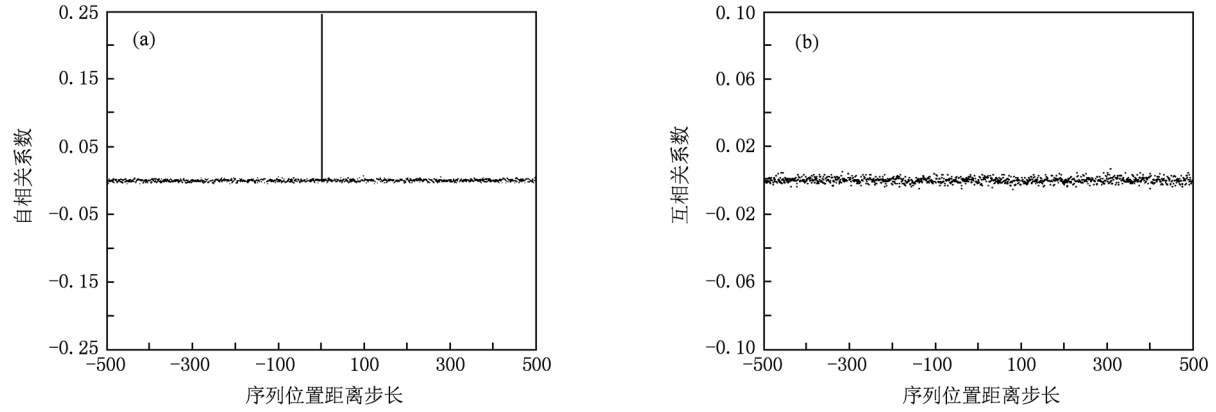

图 1 (a) 序列 A 的自相关系数;(b) D,D' 对应的两序列 S,S' 的互相关函数

自相关系数在不考虑与自身的相关系数时变动范围是 $[-0.0061,0.0046]$, 均值为 -0.0003; 互相关系数变动范围是 $[-0.0060,0.0054]$, 均值为 -0.6703×10^{-16}. 由此可见自相关系数与互相关系数是十分理想的. 任意改变 D 的一个符号,可得到一个完全不同的伪随机序列. 这大大地增加了密钥空间.

5. PNG 算法在图像加密技术中的应用

5.1. 元胞自动机

定义 4[17] (元胞自动机) 一维元胞自动机 CA 是一个三元组 $CA=(S,R,f)$,其中,S 为有限状态

集;R 为邻域半径;f 为映射函数,又简称为规则.

定义 5[17] (全局状态配置) 设 CA 是由 N 个元胞构成的有限元胞自动机,各元胞排列成一行,按顺序编号为 1, 2, …, N ,称 $G^{(t)} = (s^t(1), s^t(2),\cdots,s^t(N))$ 为元胞自动机在 t 时刻的一个全局状态配置.

理想的元胞自动机是,第 k 次与第 $k+1$ 次迭代生成的流密码应有 50% 的 bit 位发生改变,即发生"雪崩效应". 我们将两个序列 bit 数改变比值记作 $V(\cdot,\cdot)$.

如果采用当前文献的做法,由定义 4,为避免密钥数据膨胀, X 的长度不能过大;邻域半径 R 应该取得更小些,否则迭代后生成的流密码长度过短,因此 V 值总是不够理想的.

现采用第 2 节的 PNG 算法来设置元胞自动机. 元胞自动机迭代法则即是第 2.2 节的步骤. 可见每次迭代生成的流密码以几何级数增加,并由性质 5 可知所有的前后两次迭代的流密码是不相关的,应具有理想的"雪崩效应".

为显示本文元胞自动机产生的流密码的"雪崩效应",在第 2.2 节的参数下,取 $N_1 = 3600$. 记加密端第一次的 3600 bit 的流密码为 X_0, 第 $k(k = 1,2,\cdots)$ 次迭代生成的流密码为 X_k, X_k 的长度为 $L_k(k = 0,1,\cdots)$. 则有 $L_{k+1} > 5L_k$. 令 $E = \{X_0, X_1, X_2, X_3\}$, $\sum_{k=0}^{3} L_k > (1 + 5 + 25 + 125)N_1 = 561600$. 从 X_{k+1} 中提取 5 个互不相交的长度为 L_k 子集合 $X_{k+1}^i(i = 1,2,\cdots,5)$, 计算 $V(X_k, X_{k+1}^i)(i = 1,2,\cdots,5, k = 0,1,2)$ 如图 2.

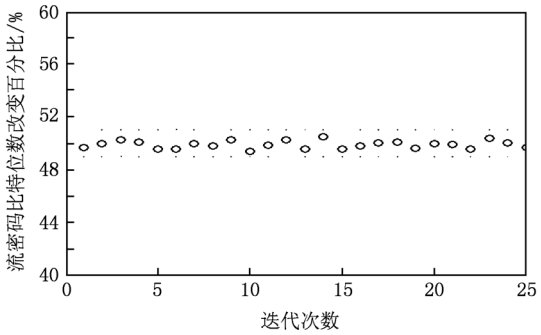

图 2 密钥改变 1 bit 时各次输出流密码的总改变率($V(\cdot,\cdot)$)

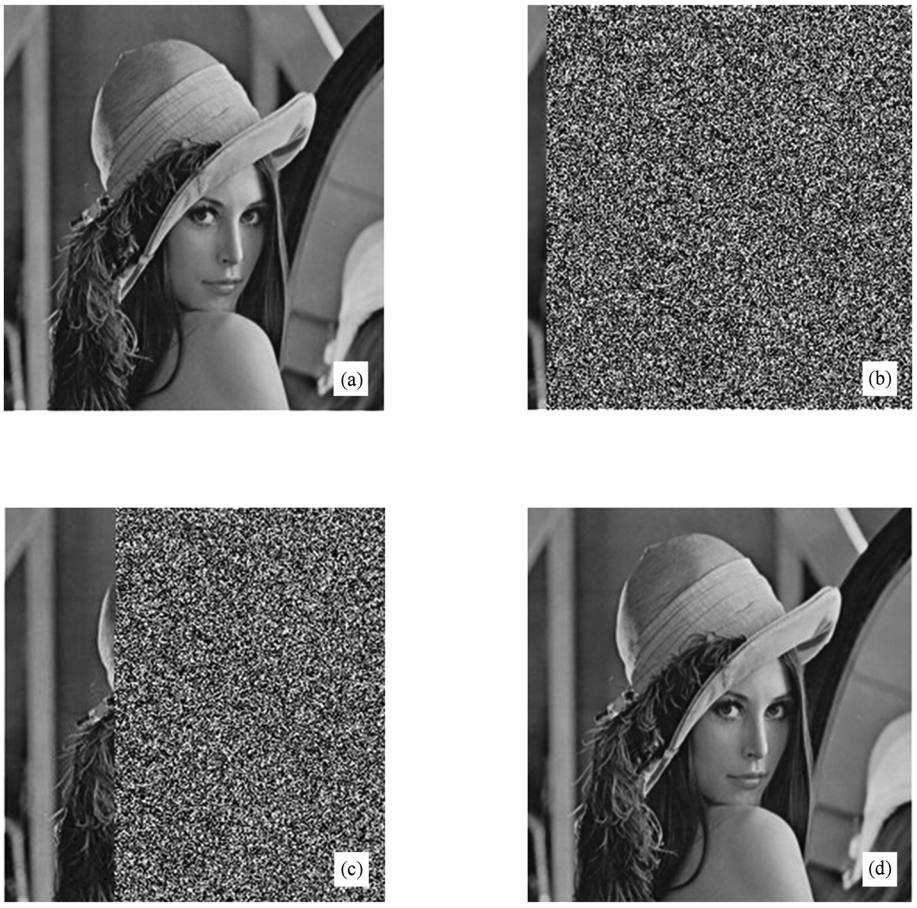

图 3 (a) 原始 Lenna 图像;(b) X_0 发生 1 bit 扰动后的解密图像;(c) X_2 发生 1 bit 扰动时的解密图像;(d) 正确解密图像

5.2. 元胞自动机加密技术

为给像素为 256 × 256 的采用 unit8 型数组的 lenna 图像加解密,从 $E = \{X_0, X_1, X_2, X_3\}$ 中取前 256 × 256 × 8 个数据进行加解密每次在加密端输入流密码 $X_i (i \geqslant 0)$,利用产生的 X_{i+1} 对像素置乱. 由于 $\sum_{k=1}^{3} L_k > 558000 > 256 \times 256 \times 8 = 524288$,故只要 3 次输入流密码就可以对图像进行加密并传送到解密端. 加密与解密效果如图 3 所示.

从上述的加解密效果看,比较文献[17],本文的算法需要的初始密码只有文献[17]的 1/2,并且传送 3 次(文献[17]需要 73 次)就可以将图像传送到接收端,并且在任何一次的任何一个位置出现 1 bit 的误差,则解密就出现很大的误差,可见误差扩散效果很理想.

6. 结 论

本文提出的 PNG 算法是一个全新的算法,理论与实证分析都表明生成的伪随机数质量十分理想. 应用中,元胞自动机的规则简炼,机理明确,避免了数据膨胀,需迭代次数少,加密效率高. 文中的算法如何推广到其他不同序列规则下的复合序列,值得进一步研究.

[1] Wang F L 2010 *Chin. Phys.* B **19** 0605151

[2] Sheng L Y, Xiao Y Y, Sheng Z 2008 *Acta Phys. Sin* **57** 4007 (in Chinese) [盛利元、肖燕予、盛 喆 2008 物理学报 **57** 4007]

[3] Ping P, Zhao X L, Zhang H, Liu F Y 2008 *Acta Phys. Sin.* **57** 6188 (in Chinese) [平 萍、赵学龙、张 宏、刘凤玉 2008 物理学报 **57** 6188]

[4] Zhang X, Ren W, Tang D N, Tang G N 2010 *Acta Phys. Sin.* **59** 5281 (in Chinese) [张 旭、任 卫、唐冬妮、唐国宁 2010 物理学报 **57** 5281]

[5] Liu Y Z, Lin C S, Li X C, Liu H P, Wang Z L 2011 *Acta Phys. Sin.* **60** 030502 (in Chinese) [刘扬正、林长圣、李心朝、刘海鹏、王忠林 2011 物理学报 **60** 030502]

[6] Guan Z H, David J H, Shen X M 2004 *International Conference on Control, Automation, Robotics and Vision*, Kunming China 320

[7] Sun F Y, Lu Z W 2011 *Acta Phys. Sin.* **60** 040503 (in Chinese) [孙福艳、吕宗旺 2011 物理学报 **60** 040503]

[8] Sun F Y, Liu S T 2008 *Chaos, Solitons & Fractals* **38** 631

[9] Sun F Y, Liu S T 2009 *Chaos, Solitons & Fractals* **41** 2216

[10] Sánchez S, Criado R, Vega C 2005 *Math. & Coput. Model.* **42** 809

[11] Wang L, Wang F P, Wang Z J 2006 *Acta Phys. Sin.* **55** 3964 (in Chinese) [王 蕾、汪芙平、王赞基 2006 物理学报 **55** 3964]

[12] Almeida J, Peralta S D, Romera M 2005 *Physica* D **200** 124

[13] Zhang R, Xu Z Y, Yang Y Q 2011 *Acta Phys. Sin.* **60** 010515 (in Chinese) [张 荣、徐振源、杨永清 2011 物理学报 **60** 010515]

[14] Gutowitz H 1994 *Method and Apparantus for Encryption, Decryption and Authentication Using Dynamical Systems USA*: 5, 395, 589

[15] Li K P, Gao Z Y 2005 *Chin. Phys.* **14** 930

[16] Qian Y S, Shi P J, Zeng Q, Ma C X, Lin F, Sun P, Wang H L 2010 *Chin. Phys.* B **19** 048201

[17] Zhang X, Ren W, Tang D N, Tang G N 2010 *Acta Phys. Sin.* **59** 5281 (in Cinese) [张 旭、任 卫、唐冬妮、唐国宁 2010 物理学报 **57** 5281]

[18] Wang F L 2010 *Advances in Difference Equations* Doi: 10.1155/2010/985982 Article ID 985982

[19] Zheng Y, Zhang X D 2010 *Chin. Phys.* B **19** 010505

[20] Sheng L Y, Cao L L, Sun K H, Jiang W 2005 *Acta Phys. Sin.* **54** 4031 (in Chinese) [盛利元、曹莉凌、孙克辉、闻 姜 2005 物理学报 **54** 4031]

A new pseudo-random number generator and application to digital secure communication scheme based on compound symbolic chaos*

Wang Fu-Lai†

(*Institute of Applied Mathematics, Zhejiang University of Finance and Economics, Hangzhou* 310018, *China*)

(Received 16 April 2011; revised manuscript received 21 June 2011)

Abstract

A new concept of compound symbolic chaotic series is proposed. According to the kneading pair series in symbolic dynamics, by compounding a pseudo-random series with sub-series on condition of kneading rules we obtain a new symbolic chaotic series which is then transformed into a pseudo-random binary number (PRN) series. The length of the new PRN series elongates at a speed of geometric procession with iteration number. Theoretical and experimental analyses both prove that the above algorithm provides an effective PRN generator. To apply the algorithm to digital secure communication, a new cellular automata is established. With the automata, the data expansion is avoided, the encryption is finished quickly, the obvious avalanche effect can be produced, and thus the security is improved.

Keywords: compound symbolic chaotic series, symbolic dynamics, pseudo-random series, cellular automata

PACS: 05.45.Vx

* Projected supported by the National Natural Science Foundation of China (Grant No. 10871168).

† E-mail: flyerwon@sina.com