空间混沌序列的加密特性研究*

孙福艳† 吕宗旺

(河南工业大学信息科学与工程学院,郑州 450001)

(2010 年 1 月 13 日收到;2010 年 7 月 12 日收到修改稿)

提出一个基于空间混沌系统的伪随机序列发生器,对空间混沌产生的伪随机位序列进行了 FIPS140-1 统计性检验和相关性分析,并应用空间混沌产生的各态历经矩阵实现图像的加密解密,实验的结果表明这种基于空间混沌系统的伪随机序列产生器具有优良的随机性,巨大的密钥空间和敏感性.

关键词: 伪随机序列, 空间混沌系统, 图像加密

PACS: 05.45.-a, 05.45.Gg

1. 引 言

在很多实际应用中都会用到伪随机序列,包括计算机仿真、数字分析中的 Monte-Carlo 技术、统计采样、随机最优方法、图像水印和密码学等. 在传统的伪随机序列产生法中,线性同余法和移位反馈寄存器法是比较常用的. 在应用密码学里, ANSIX9.17 和 FIPS 186 比较常用. 目前,已经有一些科学工作者提出用混沌动态系统可以产生伪随机序列,这是由混沌系统的类随机性、不可预测性、确定性系统和实现简单等特点所决定的,这些都使得它作为伪随机序列产生器具有潜在的优点.

目前,对于 1D 混沌系统理论、伪随机序列器以及在加密系统中的应用研究已经有十分丰富的结果见文献[1—10],这些结果逐步形成了一维混沌系统的基本理论体系,而随着科学技术、工程技术、数字滤波、多变量网络的实现、多维数学图像综合处理等领域,往往涉及到许多 2D 离散空间模型的非线性动力学性质等许多问题,并且很多模型可以利用数学分析中的魏尔斯脱拉斯(Weierstrass)一致逼近定理和相应的数学变换,可以清楚地看到这些模型有着典型的空间非线性特征,它们可以归结到下面的空间非线性离散动力系统:

$$x_{m+1,n} + \omega x_{m,n+1} = f(\mu, (1+\omega)x_{m,n}),$$

在一定的条件和参数情况下,上面系统会展现空间的混沌现象. 而对空间混沌系统的研究,它的混沌、同步、控制以及应用等等都已有一些内容[11—18],对于空间混沌系统与一维混沌系统的对照和比较来看,也应当有空间混沌行为的相应结果.

本文提出一种基于空间混沌系统的伪随机序列发生器,对空间混沌产生的伪随机位序列进行了统计性分析和相关性分析,并应用空间混沌产生的各态历经矩阵实现图像的加密/解密,实验的结果表明这种基于空间混沌系统的伪随机序列即保存了一维混沌系统的优点,又拥有巨大的密钥空间和敏感性.

2. 空间混沌系统

空间推广的 2D 系统差分形式如下[11—18]:

$$x_{m+1,n} + \omega x_{m,n+1} = f(\mu, (1+\omega)x_{m,n}), \quad (1)$$

这里 $f(\mu,(1+\omega)x_{m,n})$ 是非线性函数,m,n,x_{mn} 是三维空间的几何坐标,μ 是实数,ω 是常数. 实际上,方程(1)可以被认为是下面偏差分方程的离散形式:

$$\frac{\partial v}{\partial x} + \omega \frac{\partial v}{\partial y} = f(\mu, (1+\omega)v). \quad (2)$$

方程(2)是一个在物理学中十分典型的带驱动项的对流方程,因此,对于方程(1)的定性研究能为方程(2)的研究提供一些有用的信息.

注意到当 $n = n_0$, $\omega = 0$,系统可以化为下面一

* 国家自然科学基金(批准号:61001099,10971120),全国百篇优秀博士学位论文专项研究基金(批准号:200444)资助的课题.

† E-mail: fuyan.sun@gmail.com

维形式:

$$x_{m+1,n_0} = f(\mu, x_{m,n_0}), \tag{3}$$

因为 n_0 是常数,上面的方程可以写为

$$x_{m+1} = f(\mu, x_m). \tag{4}$$

这是我们熟悉的一维形式. 当 $f(\mu, x_m) = \mu x_m(1 - x_m)$,方程可以写为

$$x_{m+1} = \mu x_m(1 - x_m). \tag{5}$$

这是众所周知的典型的一维 Logistic 映射. 当 $3.7 < \mu < 4$,系统是混沌的. 显而易见,当 $f(\mu, (1+\omega)x_{m,n}) = 1 - (\mu(1+\omega)x_{m,n})^2$,2D 离散动态系统可以写为

$$x_{m+1,n} + \omega x_{m,n+1} = 1 - \mu((1+\omega)x_{m,n})^2. \tag{6}$$

研究表明当 $2 > \mu \geqslant 1.55$, $\omega \in (-1, 1)$,系统呈现混沌状态. 由于有两个迭代变量,我们称系统(6)为空间的推广的 2D 标准 Logistic 系统.

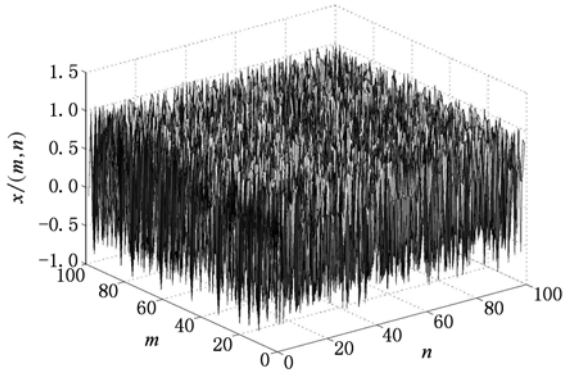

图 1 当 $\mu = 1.68$, $\omega = -0.05$ 时,空间混沌系统的混沌行为

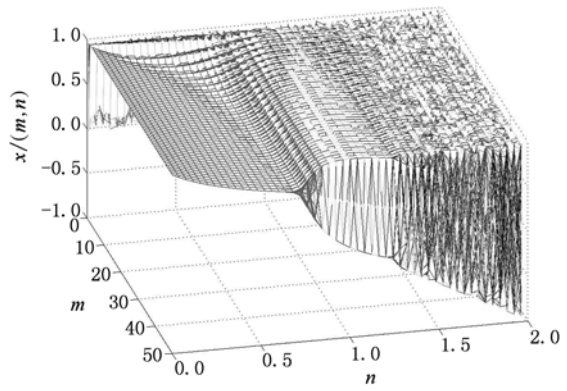

图 2 系统(6)的空间分叉行为

空间混沌系统是一维混沌映射的推广形式,和一维 Logistic 混沌映射相比,在空间混沌系统中,不仅有两个控制参数 μ, ω,而且研究表明推广的空间混沌系统的轨道对参数变化是极其敏感的,并且系统(6)产生混沌行为有更宽的参数范围,所以参数 μ, ω 和初始条件都能用来作为密钥. 当 $\mu = 1.68$, $\omega = -0.05$,系统(6)的混沌和分叉行为如图 1—3 所示.

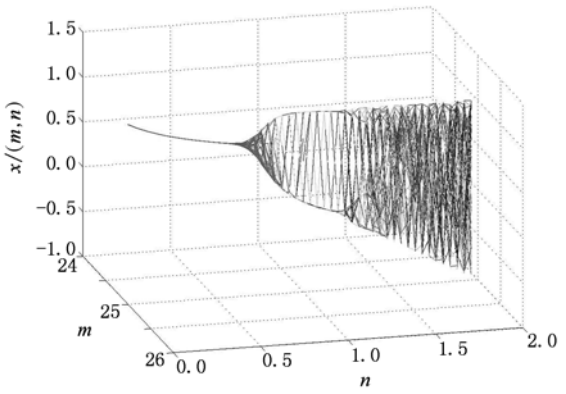

图 3 系统(6)的空间分叉现象的截面图

3. 性能分析

3.1. 产生伪随机位序列方案

下面我们采用传统的量化方法从混沌实值信号产生二值位序列,即

$$b_x = \begin{cases} 1, & x_{mn} > c \\ 0, & x_{mn} < c, \end{cases} \tag{7}$$

其中,c 是为状态变量 x_{mn} 选择的近似阈值. 选择 c 的值,应该遵循使 $x_{mn} > c$ 的概率与 $x_{mn} \leqslant c$ 的概率近似相等的原则,这里 $c = 0.5$.

3.2. 相关性分析

根据 Golomb 的关于伪随机序列的三个假设[19],即理想的伪随机序列应该具有下面的统计特性:均值为零;自相关性为 δ 函数;互相关性为零特性. 当系统参数 $\mu = 1.65$, $\omega = -0.05$,初始条件 $x_{00} = 0.789$ 和 0.789×10^{-14}, $x_{0,n+1} = x_{m+1,0} = 4x(1-x)$ 时,这种二进制序列的相关性如图 4 所示. 由图可见,这种相关性是理想的.

3.3. 统计性分析

FIPS-140-1 具体实现了 4 种随机性统计测试方法,当系统参数 $\mu = 1.65$, $\omega = -0.05$ 和初始条件 $x_{00} = 0.789$, $x_{0,n+1} = x_{m+1,0} = 4x(1-x)$ 时,由该系统输

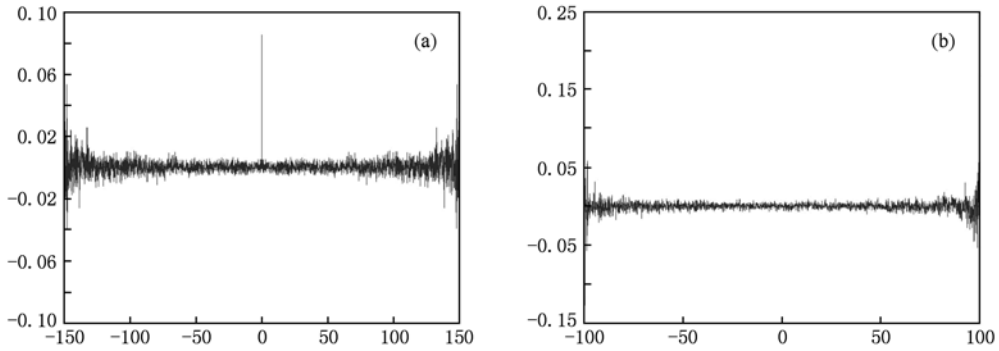

图4 自相关和互相关特性

出的长为20000位(bit)的位流(bitstream),接受下面的4个测试,若其中任何一个测试失败,则该生成器便不能通过FIPS-140-1统计测试. 其中,游程检验中,连续的"0"称为"沟",连续的"1"称为"块". 游程长度表示连续"1"或"0"的个数. 检验结果如表1所示.

3.3.1. 频数检验

1) 从20000位的位流中,数出1的个数,记作 X.

2) 如果 $9654 < X < 10,346$,则通过检验.

3.3.2. 扑克检验

1) 按临近的4位一组,把20000位的位流分成5000组,计算出4位的16种可能值出现的数目,$f(i)$记作每4位值为i的数量,其中 $0 \leqslant i \leqslant 15$.

2) 求出 $X = \frac{16}{5000}\left(\sum_{i=0}^{15}[f(i)]^2\right) - 5000$ 的值.

3) 如果 $1.03 < X < 57.4$,则通过检验.

3.3.3. 游程检验

1) 一个游程是指在20000位的位流中,最大的连续的所有1的序列或者所有0的序列位数. 在采样的20000位的位流中,记下所有游程长度($\geqslant 1$)的连续的0或者连续的1出现的次数.

2) 如果每一个游程(长度从1到6)出现的数量都落到相应的指定的间隔内,则通过检验. 这里对0和1都要检验,也就是说12次检验要都在相应的指定的间隔内. 大于6的游程作为6处理.

3.3.4. 长游程检验

1) 一个长游程是指长度为34或者大于34(1或者0)的游程.

2) 在采样的20000位的位流中,如果没有长游程则通过检验.

表1 FIPS140-1统计检验结果

FIPS140-1统计检验		要求满足的区间	检验结果	
频数检验		9654—10346	10112	
扑克检验		1.03—57.4	48.205	
	游程长度		沟	块
	1	2,267—2,273	2282	2375
	2	1,079—1,421	1154	1125
游程检验	3	502—748	637	608
	4	223—402	338	314
	5	90—223	172	125
	6+	90—223	198	181
长游程检验	≥34	0	0	0

从表1中可以看出,空间混沌系统有很好的统计特性.

另外,在其他条件不变情况下,当参数 $\mu = 1.65 \times 10^{-10}$ 发生微小变化时,位变化率均可达100%,初始条件 $x_{00} = 0.789 \times 10^{-10}$ 发生微小变化时,位变化率也可达到100%,并且都能够通过上述的统计性检验.

4. 空间混沌系统的应用

为了检验基于空间混沌伪随机序列的加密性,对于一个数字灰度图像 I,其大小为 $M \times N$,通过下面描述的算法即可对图像 I 进行加密和解密.

步骤1 给定具体初始条件和参数,对空间混沌系统进行迭代,产生一个 $M \times N$ 的各态历经的矩阵 $X_{M \times N}$;

步骤2 对图像 I 的每一个像素执行下面简单

运算

$$C_i = I_i \mathrm{XOR}(X_i \times 10^{14} \bmod 256), \quad i = 1,2,3,\cdots,M \times N, \tag{8}$$

其中 $C_{M\times N}$ 就是加密后的图像.

解密过程是加密过程的逆过程,这里不再赘述.

5. 实验结果和安全分析

取 256×256 Camera 灰度图像进行实验,这里密钥取为 $\mu = 1.65$, $\omega = -0.05$, $x_{00} = 0.764$, $x_{0,n+1} = 4x_n(1-x_n)$, $x_{m+1,0} = 3.9x_m(1-x_m)$. 注意到这里 $x_{0,n+1}$, $x_{m+1,0}$ 取一维 Logistic 混沌映射作为空间混沌系统初始的迭代序列. 图 5 是原始图像和加密后的图像,图 6 是原始图像的直方图和加密图像的直方图,可见,加密过程将原始图像像素值的不均匀分布变成了像素值的均匀分布,使密文像素值在[0,255]整个空间范围内取值概率均等,明文的统计特性完全被打破,使明密文的相关性大大降低. 图 7(a)是用正确密钥解密后的图像,图 7(b)是初值 x_{00} 相差 10^{-15} 时得到的解密结果. 可见,仅当一个初始密钥微小的改变,将导致解密结果截然不同于正确结果. 改变其他几个密钥,也得出同样的结果. 实验表明,密文对密钥具有高度的敏感性.

5.1. 密钥空间

一个好的加密方案应该是对密钥敏感的,应该具有足够大的密钥空间抗强有力的攻击. 若以混沌系统初值和参数为密钥,采用精确到小数点后 15 位的双精度实数表示,则密钥空间为 $10^{5\times 15\times m\times n}$,其中 $m \geqslant M$, $n \geqslant N$, M, N 为图像的尺寸. 可见密钥空间是与空间混沌系统的迭代次数有关的,也就是说图像越大,密钥空间越大,完全可以抵抗强力攻击,更适合数据量大的图像加密.

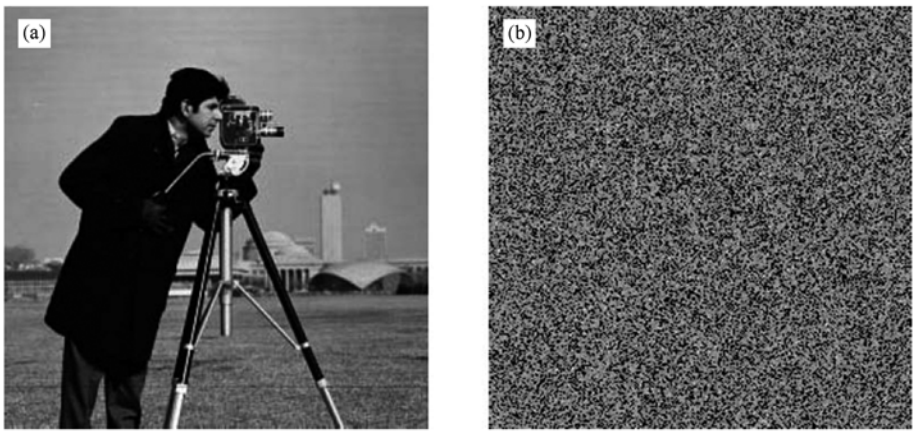

图 5 原始图像和加密后的实验结果 (a) 原始图像;(b) 加密后的图像

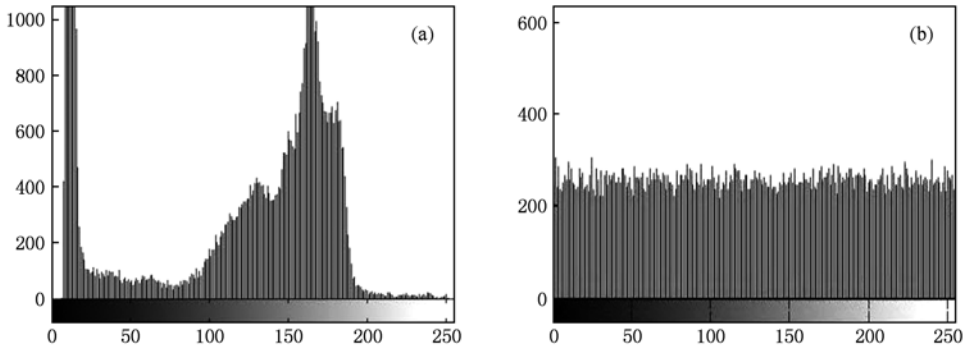

图 6 原始图像和加密后图像的直方图 (a) 原始图像的直方图;(b) 加密后图像的直方图

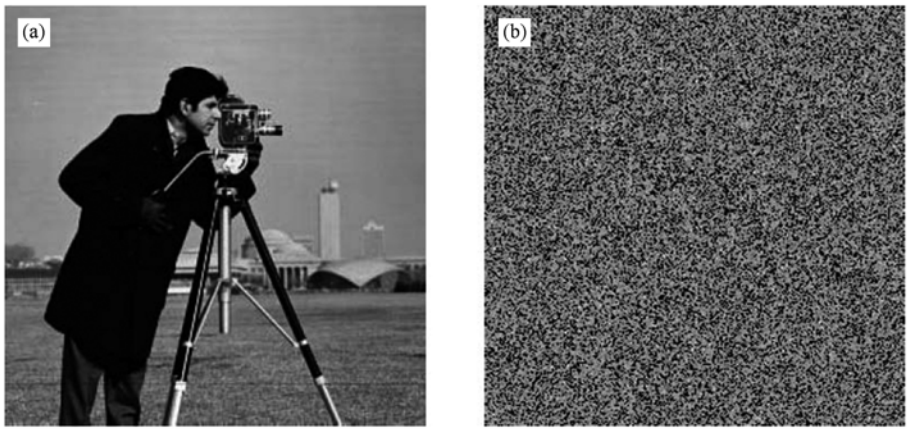

图 7 解密后的图像 (a) 经过正确密钥后的解密图像;(b) 经过错误密钥后的解密图像 $\mu = 1.65, \omega = -0.05, x_{00} = 0.764 + 10^{-15}, x_{0,n+1} = 4x_n(1 - x_n), x_{m+1,0} = 3.9x_m(1 - x_m)$

5.2. 相邻像素的相关性分析

为了测试加密后图像中相邻像素之间的相关性,我们从原始图像和加密后图像中分别随机地选取 1000 对两个相邻的像素(垂直的、水平的和对角方向的),相关指数通过下面公式计算:

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i, \tag{9}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))^2, \tag{10}$$

$$\mathrm{cov}(x,y) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))(y_i - E(y)). \tag{11}$$

这里 x 和 y 是图像中两个相邻像素的灰度值. 图 8 (a) 和(b)各自展示了原始图像和加密后图像的两个水平的相邻像素的相关分布,表 2 出示了相关指数. 这些相关性分析证明了这种混沌加密算法满足零相关性.

表 2 原始图像和加密后图像中两个相邻像素的相关指数

	原始图像	加密后的图像
水平方向	0.995	−0.0024
垂直方向	0.961	0.0131
对角方向	0.96	−0.0096

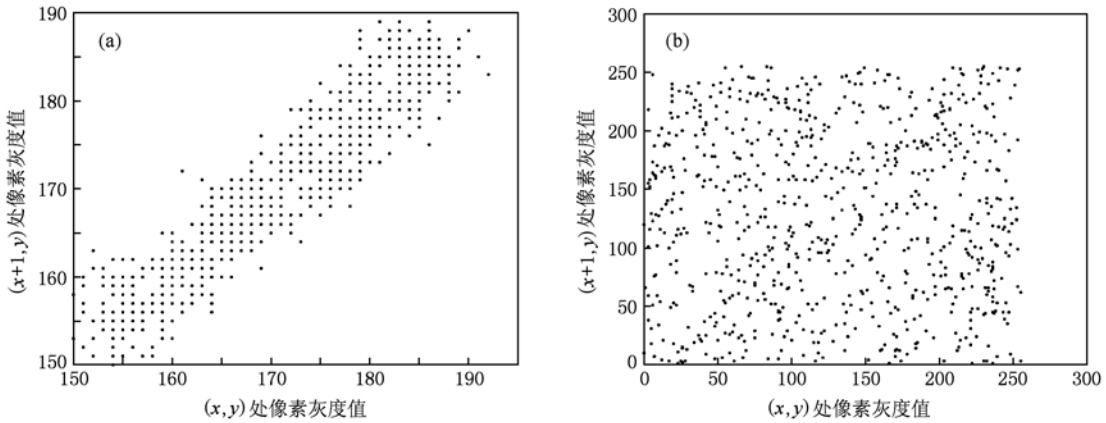

图 8 在原始图像和加密图像中两个相邻的水平像素之间的相关性

6. 结 论

本文提出了用空间混沌作为伪随机序列发生器的思想. 我们对这种伪随机二进制序列进行了在密码学领域中常用的 FIPS-140-1 统计检验. 结果这种伪随机二进制序列成功的通过了所有检验. 通过相关性分析也证明这种由空间混沌系统生成的伪

随机二进制序列十分类似于随机序列. 另外,应用空间混沌系统对图像进行加密,实验结果和安全分析表明,基于空间混沌系统的伪随机序列具有高度敏感性,以系统初值和参数为密钥,密钥空间与所加密图像大小成正比,大大地拓宽了密钥空间,使加密系统具有抵御穷举攻击的能力,可见,空间混沌系统是优良的伪随机序列产生器.

[1] Xiang F, Qiu S S 2008 *Acta Phys. Sin.* **57** 6132 (in Chinese) [向 菲、丘水生 2008 物理学报 **57** 6132]

[2] Wang X Y, Wang M Y 2008 *Acta Phys. Sin.* **57** 731 (in Chinese) [王兴元、王明军 2008 物理学报 **57** 731]

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

[4] Sun Q C, Wang G Q 2005 *Acta Phys. Sin.* **54** 1267 (in Chinese) [谢 鲲、雷 敏、冯正进 2005 物理学报 54 1267]

[5] Sun F Y, Liu S T, Lü Z W 2007 *Chin. Phys.* **16** 3616

[6] Yang X L, Xu W 2008 *Chin. Phys.* B **17** 2004

[7] Wong W K, Lee L P, Wong K W 2001 *Computer Physics Communications* **138** 234

[8] Papadimitriou S, Bountis T, Mavaroudi S 2001 *Int. J. Bifurcation and Chaos* **11** 3107

[9] Jakimoski G, Kocarev L 2001 *IEEE Trans. Circuits and Systems* Ⅰ **48** 163

[10] Palacios A, Juarez H 2002 *Physics Letters* A **303** 345

[11] Yang W M 1991 *Chaos, Solition & Fractal* **1** 389

[12] Chen G, Liu ST 2003 *Int. J. Bifurcation Chaos Appl. Sci. Eng.* **15** 867

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

[14] Sun F Y, Liu S T 2009 *Sci. China Ser* G **52** 177

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

[16] Liu S T, Chen G 2003 *Int. J. Bifurcation Chaos Appl. Sci. Eng.* **15** 1163

[17] Liu S T, Sun F Y, Chen S L 2007 *Chinese Physics Letters* **24** 3530

[18] Chen G, Liu ST 2003 *Chaos, Solitons & Fractals* **15** 311

[19] Xiao J, Hu G, Qu Z 1996 *Phys. Rev. Lett.* **77** 4162

Cryptographic spatial chaos sequence*

Sun Fu-Yan† Lü Zong-Wang

(*College of Information Science and Engineering Henan University of Technology, Zhengzhou* 450001, *China*)

(Received 13 January 2010; revised manuscript received 12 July 2010)

Abstract

In this paper, a novel pseudo-random sequence generator (PRSG) based on spatial chaos system is proposed. The statistical tests and correlation analysis on the proposed PRSG are performed by the well-known Federal Information Processing Standards FIPS140-1, and the experimental results show that the image encryption based on spatial chaos ergodic matrix has good random statistical characteristics, large key space and great sensitivity of the sequence.

Keywords: pseudo-random sequence, spatial chaotic system, image encryption

PACS: 05.45.-a, 05.45.Gg

* Project supported by the National Natural Science Foundation of China (Grant Nos. 61001099, 10971120) and the Foundation for the autor of National Excellent Doctaral Dissertation of China (Grant No. 200444).

† E-mail: fuyan. sum@ gmail. com