doi:10.11959/j.issn.1000-436x.2016252

基于细胞神经网络的伪随机数生成方法

董丽华，药国莉
（西安电子科技大学通信工程学院，陕西 西安 710071）

摘 要：为了克服有限精度效应对混沌系统的退化影响，改善所生成随机序列的统计性能，设计了一种新的基于六维 CNN（细胞神经网络）的 64 bit 伪随机数生成方法。在该方法中，通过控制六维 CNN 在每次迭代过程中的输入输出，改善了混沌退化对随机数的性能影响，同时，通过与 Logistic 映射所生成的随机序列和可变参数进行异或处理，有效避免了生成序列的重复出现，扩大了密钥空间和输出序列的周期。以新方法设计的 PRNG（伪随机数生成器）易于在软件中实现，每次可生成 64 bit 的伪随机数，生成速率快。测试结果表明，该方法生成的伪随机序列可以完全通过随机数检测标准 NIST SP800-22，因而具有很好的随机性，可用于保密通信等信息安全领域。
关键词：混沌系统；6-CNN；Logistic 映射；PRNG
中图分类号：TN918 **文献标识码**：A

Method for generating pseudo random numbers based on cellular neural network

DONG Li-hua, YAO Guo-li
(School of Telecommunications Engineering, Xidian University, Xi'an 710071, China)

Abstract: To overcome the degradation characteristics of chaos system due to finite precision effect and improve the statistical performance of the random number, a new method based on 6th-order cellular neural network (CNN) was given to construct a 64-bit pseudo random number generation (PRNG). In the method, the input and output data in every iteration of 6th-order CNN were controlled to improved the performance of the random number affected by chaos degradation. Then the data were XORed with a variable parameter and the random sequences generated by a Logistic map, by which the repeat of generated sequences was avoided, and the period of output sequences and the key space were expended. Besides, the new method was easy to be realized in the software and could generate 64 bit random numbers every time, thus has a high generating efficiency. Test results show that the generated random numbers can pass the statistical test suite NIST SP800-22 completely and thus has good randomness. The method can be applied in secure communication and other fields of information security.
Key words: chaotic systems, 6-CNN, Logistic map, PRNG

1 引言

随机数生成器作为流密码中的一个重要部件，在信息安全领域中有着广泛的应用，如对文本或图像信息的加密、数字签名和身份认证等，因而研究如何构造高性能的随机数生成器已成为密码安全中的重要课题。随着科学技术的不断发展，人们对随机数的性能要求也越来越高，许多学者开始研究真随机数生成器（TRNG），并涌现了大量基于振荡环构造的 TRNG[1,2]。这些 TRNG 利用数字电路中的物理噪声来产生随机源，通过采样来获得所需的随机数，具有很好的不可预测性。但在实际应用中，TRNG 通常需要基于硬件中的数字电路去实现，生成速度相对较慢且花费较高，而物理噪声易受到周围环境的影响，导致随机数的生成并不稳定。

为了将随机数生成器更好地应用到实际中，对

收稿日期：2016-09-31
基金项目：国家重点研发计划基金资助项目（No.2016YFB0800601/02/03/04/05）
Foundation Item: The National Key Research and Development Program (No.2016YFB0800601/02/03/04/05)

伪随机数生成器（PRNG）的研究也变得至关重要。PRNG 通常是基于算法和初始化种子来实现，可通过调整算法来改进随机数的统计性能和生成速度，易于软件实现，且其生成速率高并可控[3]。一些常见算法，如取中法、移位法和同余法[4]的复杂度相对较低，生成的序列周期对初始值具有很大的依赖性，因而产生随机数的统计性能并不理想。而 *m* 序列因其易于在软硬件中实施且算法简单，在 PRNG 构造中也得到了广泛的应用[5,6]，但其生成的序列线性复杂度低，且通过 BM 攻击很容易得到序列的特征多项式[7]，在实际的应用中存在安全隐患。

混沌是确定的非线性系统中一种杂乱无序的状态，具有对初值敏感性、不可预测性和遍历性等特点，因而在密码学中得到了广泛的应用，尤其适用于构造伪随机数生成器。在现有文献中，有许多基于低维混沌映射构造的 PRNG，如 Wang[8]提出了一种基于离散混沌迭代的耦合映像格子（CML）构造伪随机数生成器的方法；Francois[9]通过混沌方程对向量内部比特数的位置进行置换，生成了统计性能良好的伪随机序列；LUI[10]用一个 Rényi 映射控制另外 4 个 Rényi 映射设计得到了长周期的伪随机数生成器，但这些方法的密钥空间小，且由于低维混沌系统的复杂度相对较低，使整个系统的安全性不够好；此外，也有一些 PRNG 是基于高维混沌映射设计生成伪随机数，如 Wang[11]利用三维连续 Lorenz 系统生成了随机性良好的伪随机数；齐迎宾[12]用离散超混沌映射 Folded-tower 设计伪随机数生成器，这些设计大大地增加了密钥空间，但却未能避免混沌退化对系统安全性的影响。在实际应用中，由于数字系统的有限精度效应，在数字化过程中出现的量化误差将会导致混沌系统随机性能的退化，进而出现序列短周期、线性复杂度低等缺陷，降低了 PRNG 的安全性能[13]。

为避免混沌退化对 PRNG 的影响，提高生成序列的随机性能，本文提出了一种基于细胞神经网络的伪随机数生成方法，在该方法中利用超混沌连续系统六维 CNN 和一维离散混沌 Logistic 映射设计生成伪随机序列。该方法首先用超混沌生成随机性好的序列，随后通过对序列中的数据进行处理，每次循环生成 64 bit 的伪随机数，生成速率快且具有足够大的密钥空间。在序列数据的处理过程中，通过控制每次六维 CNN 迭代后的输入输出，有效地避免了混沌的退化特性，并通过与 Logistic 映射所生成的随机序列和可变参数的异或，使处理后的数据很难出现重复现象，扩大了序列的周期。测试结果表明：本方法生成的随机数具有初值敏感性，同时，满足国际随机数检测标准 NIST SP800-22 的要求，易于在软件中实现，可在保密通信等领域得到很好的应用。

2 相关混沌映射

混沌是一种无序的、不可预测的运动状态，同时对初始值具有很高的敏感性。

所谓敏感性是指对于混沌系统，给定相差很小的 2 个初始值，经过一段时间的运动后，会产生 2 种截然不同的运动轨道，而 Lyapunov 指数可以定量地描述这种轨道分离的程度。

所谓 Lyapunov 指数是指在相空间中相互靠近的 2 条轨道随着时间的推移产生的分离程度，当指数小于零时，表明该系统的相空间是收缩的，此方向的运动趋于稳定；当指数大于零时，表明该系统的相空间在某方向上不断膨胀和折叠，进而使 2 个轨道之间的相关性越来越小，即初态的微小差异导致了系统长时间运动后的不可预测[14]。因而一个系统要进入混沌状态，至少要有一个大于零的 Lyapunov 指数，且正的 Lyapunov 指数越多，系统的混沌特性越好。为了构造随机性更加复杂的 PRNG，本文利用超混沌系统——六维 CNN 来生成伪随机序列。

2.1 六维 CNN

CNN 是由 Chua 和 Yang 于 1988 年首先提出的一种神经网络模型[15]，该模型具有复杂的混沌动力学特性和快速并行处理能力，可以提供复杂的随机序列。在 CNN 基础上，Wang 等[16]提出了一种连续超混沌系统——六维 CNN，六维 CNN 具有更复杂的混沌特性，如式(1)所示。

$$\begin{cases} x_1' = -x_3 - x_4 \\ x_2' = 2x_2 + x_3 \\ x_3' = 14x_1 - x_2 \\ x_4' = 100x_1 - 100x_4 + 100(|x_4 + 1| - |x_4 - 1|) \\ x_5' = 18x_2 + x_1 - x_5 \\ x_6' = 4x_5 - 4x_6 + 100x_2 \end{cases} \tag{1}$$

当时间 *t* 趋于无穷时，Wang 等计算得到该混沌系统的 6 个 Lyapunov 指数分别为：$\lambda_1 = 2.748\ 1$，$\lambda_2 = -2.984\ 4$，$\lambda_3 = 1.241\ 1$，$\lambda_4 = -14.454\ 9$，$\lambda_5 = -1.412\ 3$，

$\lambda_6 = -83.228\ 2$，即有 2 个大于零的 Lyapunov 指数，该系统是一个超混沌系统。

图 1 是该系统的超混沌吸引子在三维空间上的投影，由图 1 可知，六维 CNN 超混沌吸引子的投影有复杂的折叠轨迹，因而六维 CNN 具有非常复杂的动力学特性，可以很好地应用于通信保密系统。

2.2 Logistic 映射

Logistic 映射[17]是一种常用的离散混沌系统，如式(2)所示。

$$x_{n+1}=\mu x_n(1-x_n) \tag{2}$$

其中，迭代状态值 x_n 的取值范围是(0, 1), n=0, 1, 2, …；控制参数 μ 的取值范围是(0, 4)，当 μ 的取值不同时，该 Logistic 映射的迭代效果也会发生很大的改变。

图 2 是初始值 $x_0 = 0.422\ 12$ 时的 Logistic 映射分岔，其中，横轴为控制参数 μ，纵轴为多次迭代输出序列的状态值 $x(n)$。由图 2 可以看出，随着控制参数 μ 的增大，序列的状态值从稳定不动点到出

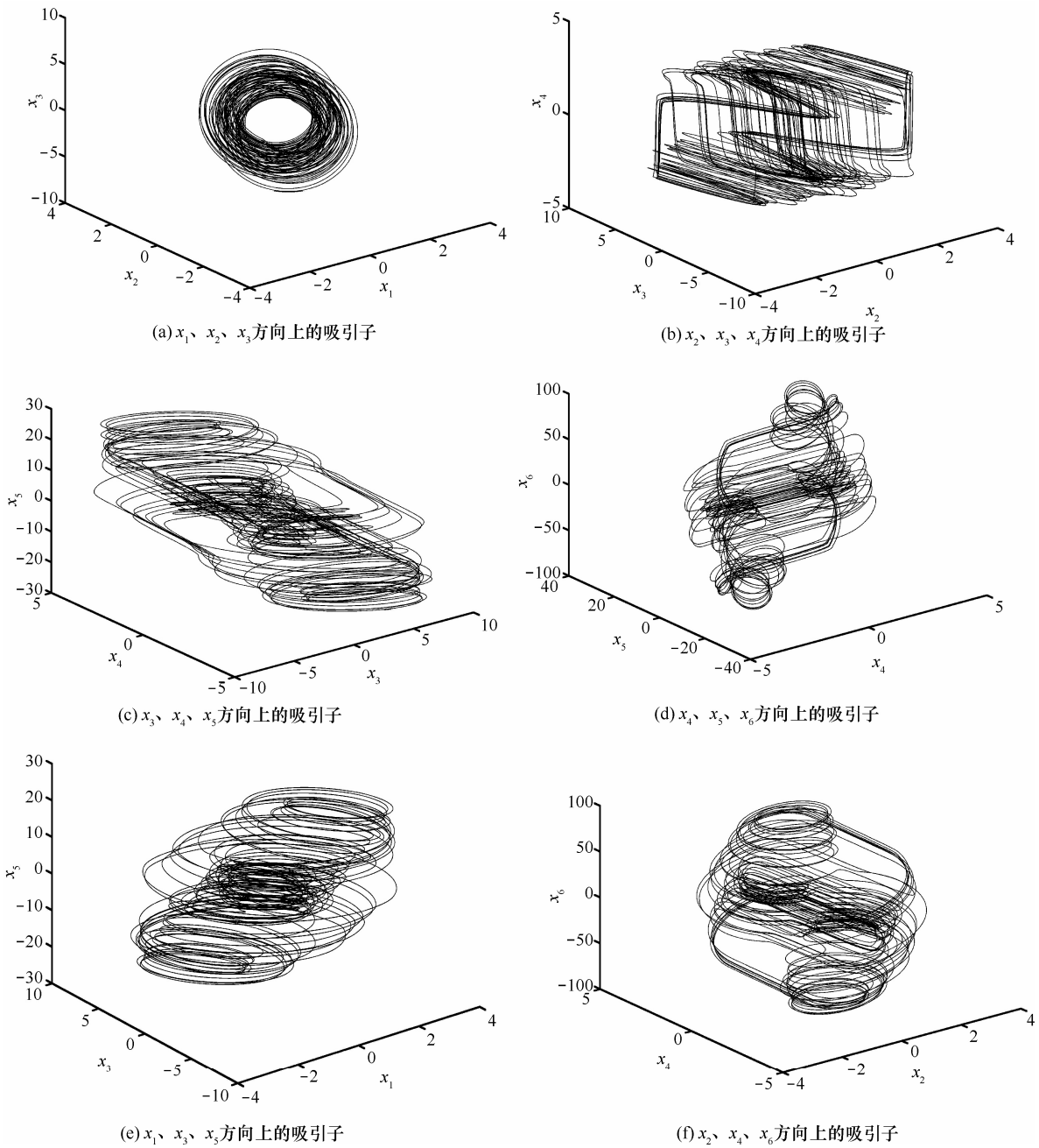


图 1　六维 CNN 的超混沌吸引子在三维空间中的投影

现倍周期分叉，最后进入混沌状态。当 μ 的值在(2, 3)时，该系统的状态值始终是一个稳定不动点；当 μ 的值在(3, 3.449)时，该系统出现周期 2，状态值在 2 个值之间跳跃；当 μ 的值在(3.449, 3.544)时，该系统出现周期 4，状态值在 4 个值之间跳跃；当 μ 的值大于 3.57 时，该系统可由倍周期分叉进入混沌状态。此外，μ 的值越接近 4，其输出序列的状态值范围越广，混沌特性也越好。在本文设计的方法中，为使所生成的序列获得更好的随机性，控制参数 μ 的取值设为 3.999 9。

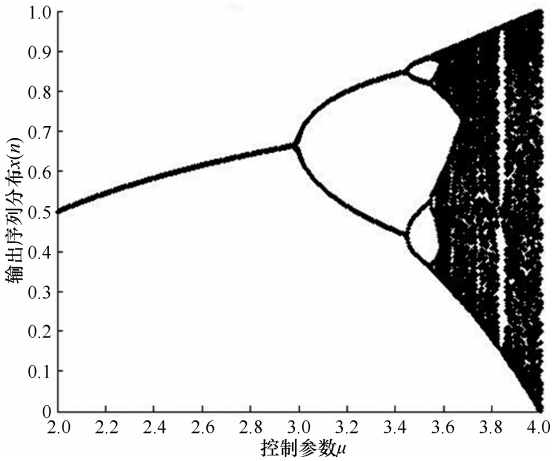


图 2 Logistic 映射分岔

3 伪随机数生成方法

超混沌系统有多个大于零的 Lyapunov 指数，生成的序列具有很好的随机性，用超混沌系统构造的伪随机数生成器的安全性也会更高。为避免有限精度效应带来的混沌退化，每次都对六维 CNN 迭代生成的 6 个输出值进行处理，以获得下一次的输入；同时将 Logistic 映射生成的随机序列和可变参数加入运算，以避免生成序列的重复出现，进而扩大序列的周期。

本文用密钥设置六维 CNN 的 6 个初始值 x_1、x_2、x_3、x_4、x_5、x_6 和 Logistic 映射的初始值 x_n，伪随机数的生成方法步骤如下。

步骤 1 迭代式(1)和式(2)1 000 次，消除初始效应，继续迭代 Logistic 映射，生成的数据记为随机序列 X；继续迭代六维 CNN，生成的数据记为随机序列 P，每次迭代前对六维 CNN 生成的 6 个数据做如下处理。

$$x'_k=\frac{f(xk)+f_{(x(k+1) \bmod 6)}}{2} \tag{3}$$

其中，k=1，2，3，4，5，6，f()表示取()中数据的小数部分。

步骤 2 将随机序列 P 中的数据按照从左到右、从上到下的顺序依次存入数组 p[6][6]，对 p[6][6]中数据做处理，如式(4)所示。

$$p'[i][j]=|p[i][j]|\times 2^{15} \bmod N \tag{4}$$

其中，i 和 j 是[0, 5]的整数，N=256。

步骤 3 将随机序列 X 中的数据按照从上到下、从左到右的顺序依次存入数组 x[6][6]，对 x[6][6]中数据做处理，如式(5)所示。

$$x'[i][j]=x[i][j]\times 2^{15} \bmod N \tag{5}$$

步骤 4 生成新数组 r[6][6]，设其初始值均为 0。

$$r'[i][j]=p[i][j]\text{^}x[i][j]\text{^}K\text{^}r[i][j] \tag{6}$$

其中，^为异或运算，K 是由密钥 c_1 和 c_2 控制的可变参数，$K=(G+c_2K^2) \bmod N$。

步骤 5 用数组 r[6][6]生成 8 个 8 bit 的数据。

第 1 个数据是数组中心 r[2][2]、r[2][3]、r[3][2]、r[3][3]的异或和。

第 2 个数据是数组外圈所有数据的异或和。

第 3 个数据是数组除中心和外圈外所有数据的异或和。

第 4 个数据是数组两条对角线上所有数据的异或和。

矩阵的对角线将数组分成了 4 个区域。

第 5 个数据是上三角形区域所有数据的异或和。

第 6 个数据是右三角形区域所有数据的异或和。

第 7 个数据是下三角形区域所有数据的异或和。

第 8 个数据是左三角形区域所有数据的异或和。

步骤 6 将 8 个数据依次输出，得到 64 bit 的伪随机数。

将步骤 1 到步骤 5 循环多次，得到所需长度的伪随机数序列。每次循环前，六维 CNN 和 Logistic 映射的初始值即为上一次的输出值；参数 α 和 β 均更新为其与 r[6][6]中所有数据的异或和，数组 r[6][6]更新为上次循环后所得数据。

4 安全性分析

4.1 密钥空间分析

为使本文所构造的 PRNG 有足够大的密钥空间来抵抗穷举攻击[17]，本文方法采用双混沌映射来构造 PRNG，以增加所需的密钥空间。在本文方法中，用 7 个 16 bit 的密钥分别设置 Logistic 映射的初始

值 x_0 和六维 CNN 的初始值($x_1, x_2, x_3, x_4, x_5, x_6$)，用 2 个 8 bit 的密钥分别设置参数 c_1 和参数 c_2 的初始值，用 16 bit 的密钥设置参数 K 的初始值，共 144 bit 的密钥，即本文方法的密钥空间为 2^{144}，远大于 2^{128}，因而可有效地抵抗穷举攻击。

4.2　密钥敏感性分析

混沌对初值具有很高的敏感性，因而基于混沌构造的 PRNG 也应该对密钥较为敏感，才能产生性能良好的随机数。对于 PRNG，可以采用位变化率[18]来衡量其对密钥的敏感程度，即观察密钥做微小改变时，该 PRNG 生成的序列中比特数不同的程度。理想的位变化率的值为 50%，通过仿真所得的位变化率越接近 50%，该 PRNG 对初值的敏感性越好。

在仿真过程中，给定 3 组有微小差异的密钥，生成同等长度的 3 组序列，以一组为基准计算位变化率，进而分析 PRNG 对初值的敏感性。

给定第一组密钥为：0x532a42d2,0x78a12bc4, 0x30b571f2,0xd32954c3,0x4a2f，以此生成长度为 1 073 741 824 bit 的序列 a，以序列 a 为基准进行比较。如表 1 所示，任意改变第一组密钥的 1 bit，如将 0x532a42d2 改为 0x432a42d2，其余密钥保持不变，得到第二组密钥，再用本文方法生成长度为 1 073 741 824 bit 的序列 b，比较序列 a 和序列 b，有 536 856 263 bit 的不同，即得到的位变化率为 49.998 6%；如将第一组密钥的 0x78a12bc4 改为 0x78a12bc5，其余密钥保持不变，得到第三组密钥，用本方法生成长度为 1 073 741 824 bit 的序列 c，比较序列 a 和序列 c，有 536 898 975 bit 的不同，即得到的位变化率为 50.002 6%。这些位变化率都非常地接近理想值 50%，由此可知，密钥的微小改变会对生成的序列有很大的影响，因而本文方法对密钥具有很高的敏感性。

表 1　　伪随机序列的初值敏感性分析

密钥变化	位变化率
0x532a42d2→0x432a42d2	49.998 6%
0x78a12bc4→0x78a12bc5	50.002 6%

4.3　NIST 随机性检测

美国国家标准与技术研究院(NIST)[19]提供的 SP800-22 测试分组是用来对任意长的二进制序列进行随机性检测的一种重要方法，该测试分组包括 15 个测试项，有些测试项包含多个子测试项，每个测试项的结果中均有 P-value 值和通过率 Propotion 这 2 个指标。

对于 P-value 值，若该值大于设定的显著性水平 α，则说明序列是随机的，通常 α 的取值为[0.001, 0.01]；对于通过率的值 Propotion，若该值在置信区间内，表示序列通过该项检测，设 β 是被测序列的组数，则置信区间[13]为

$$\left[1-\alpha-3\sqrt{\frac{\alpha(1-\alpha)}{\beta}}\beta, 1-\alpha+3\sqrt{\frac{\alpha(1-\alpha)}{\beta}}\right] \quad (7)$$

用上述 NIST 随机性测试方法对本方法生成的 1 000 组 1M bit 的序列进行测试，即 $\beta=1\,000$，设置显著性水平 $\alpha=0.01$，计算得到置信区间为[0.980 6, 1]。由表 2 中测试结果可知：每一项的测试结果中，P-value 值都大于显著性水平 α，且通过率 Propotion 的值都在置信区间内，因而生成的序列可完全通过 NIST 测试，即序列是随机的，其中，“*”表示该项包含多个子项，表 2 中所给数据为最坏结果值。

表 2　　NIST SP800-22 测试结果

统计测试	P-value	Propotion	结果
Frequence	0.693 581	0.990 7	Pass
BlockFrequence	0.832 273	0.984 2	Pass
CumulativeSums*	0.251 036	0.987 0	Pass
Runs	0.509 353	0.987 0	Pass
LongestRun	0.509 906	0.981 4	Pass
Rank	0.582 379	0.986 0	Pass
FFT	0.251 349	0.986 0	Pass
OverlappingTemplate	0.149 171	0.985 1	Pass
Universal	0.703 826	0.987 9	Pass
LinearComplexity	0.122 987	0.988 8	Pass
ApproximateEntropy	0.150 973	0.987 0	Pass
Serial*	0.376 366	0.984 2	Pass
NonOverlappingTemplate*	0.214 120	0.983 2	Pass
RandomExcursions*	0.301 571	0.985 2	Pass
RandomExcursionsVariant*	0.811 644	0.986 7	Pass

4.4　加密效果分析

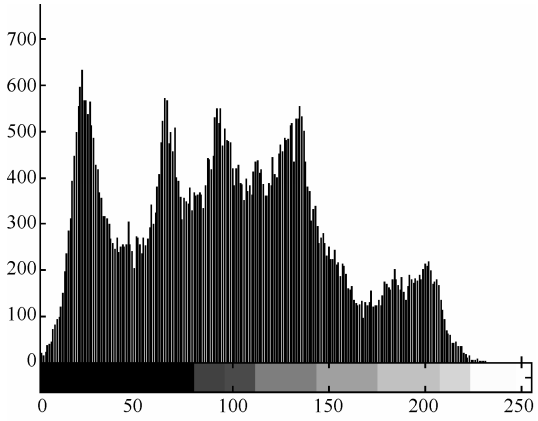
PRNG 在保密通信中有着很广泛的应用，常见的如对数字图像的加密。图 3(a)所示是标准的 8 bit 灰度图 Lena，将其用作明文图像来进行实验，具体操作为用产生的伪随机序列直接与明文图像的像素值进行异或，得到密文图像如图 3(b)所示，通过分析密文图像的直方图和信息熵来进一步对生成

的伪随机数进行性能检测。

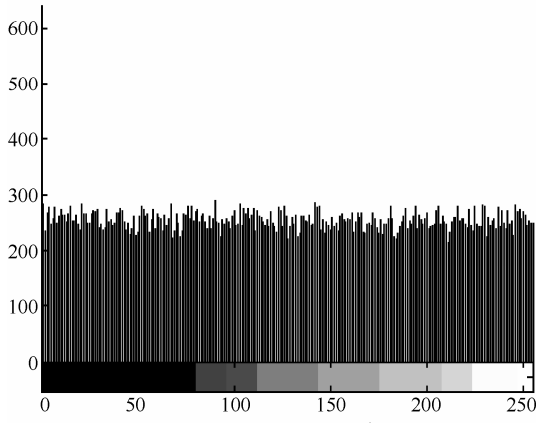
(a) Lena 图像　　(b) Lena 图像加密

图 3　实验明文和密文图像

图 4(a)和图 4(b)分别是明文图像和密文图像对应的直方图，由图 4 可知：明文图像的像素值分布有一定的规律，相邻像素间有密切的关系；经过伪随机序列异或加密得到的密文图像的像素值分布均匀，接近于白噪声的直方图分布。除此之外，加密后 Lena 图像的信息熵为 7.997 4，非常接近于理想的信息熵值 8。表 3 通过与其他文献中用生成序列对图像加密后的信息熵比较，进一步说明用本文方法生成的伪随机序列对图像加密后，可以很好地抵抗统计攻击。



(a) Lena原图直方图



(b) Lena加密图直方图

图 4　实验明文和密文图像直方图

表 3　　信息熵比较结果

方法	信息熵
本文方法	7.997 4
文献[20]方法	7.989 1
文献[21]方法	7.989 0

5　结束语

本文用连续超混沌系统六维 CNN 和离散混沌系统 Logistic 映射设计了一种新的伪随机数生成方法，该方法通过控制六维 CNN 每次迭代的输入输出和设计可变参数参与运算，有效地改善了混沌退化对 PRNG 安全性的影响，在很大程度上减少了序列出现周期的可能性，提高了随机数的统计性能。通过对其性能进行仿真分析，表明了本文方法具有很大的密钥空间和很好的密钥敏感性，每次可生成 64 bit 的伪随机数，且生成的随机数序列可以通过 NIST 随机性检测，因而具有良好的统计性能，可以很好地应用于诸如图像加密等信息安全领域，丰富了混沌在密码学中的应用。

参考文献：

[1] KILLMANN W, SCHINDLER W. A design for a physical RNG with robust entropy estimators[C]//International Workshop on Cryptographic Hardware and Embedded Systems. Springer Berlin Heidelberg, 2008: 146-163.

[2] MA Y, LIN J, CHEN T, et al. Entropy evaluation for oscillator-based true random number generators[C]//International Workshop on Cryptographic Hardware and Embedded Systems. Springer Berlin Heidelberg, 2014: 544-561.

[3] KELSEY J, MCKAY K A, TURAN M S. Predictive models for min-entropy estimation[C]//International Workshop on Cryptographic Hardware and Embe dded Systems. Springer Berlin Heidelberg, 2015: 373-392.

[4] 杨自强, 魏公毅. 综述:产生伪随机数的若干新方法[J]. 数值计算与计算机应用, 2001, 22(3): 201-216.
YANG Z Q, WEI G Y. Review: several new methods of generating pseudo random numbers[J]. Numerical Calculation and Computer Applications, 2001, 22(3): 201-216.

[5] GU X C. Multi-output LFSR based uniform pseudo random number generator[J]. Geomatics & Information Science of Wuhan University,2010, 35(5): 566-569.

[6] FOKHRULISLAM M, A M A M, YEOP M B. FPGA implementation of an LFSR based pseudo random pattern generator for MEMS testing[J]. International Journal of Computer Applications, 2013, 75 (11): 30-34.

[7] SINGLA P, SACHDEVA P, AHMAD M. A chaotic neural network based cryptographic pseudo-random sequence design[C]//2014 Fourth International Conference on Advanced Computing & Communication

Technologies. 2014: 301-306.

[8] WANG X Y, QIN X. A new pseudo-random number generator based on CML and chaotic iteration[J]. Nonlinear Dynamics, 2012, 70(2): 1589-1592.

[9] FRANCOIS M, GROSGES T, BARCHIESI D, et al. A new pseudo-random number generator based on two chaotic maps[J]. Informatica, 2013, 24(2): 181-197.

[10] LUI O Y, YUEN C H, WONG K. A pseudo-random number generator employing multiple rényi maps[J]. International Journal of Modern Phys ics C, 2013, 24(11).

[11] WANG X, LIU L. Cryptanalysis of a parallel subimage encryption method with high-dimensionalchaos[J].Nonlinear Dynamics, 2013, 73(1-2): 795 -800 .

[12] 齐迎宾, 孙克辉, 王会海,等. 超混沌伪随机序列生成器设计与性能分析[J]. 计算机工程与应用, 2015.
QI Y B, SUN K H, WANG H H, et al. The design and performance analysis of hyper-chaotic pseudo-random sequence generator[J]. Computer Engineer and Applications, 2015.

[13] 许栋, 崔小欣, 王田,等. 基于 Logistic 映射的混沌随机数发生器研究[J]. 微电子学与计算机, 2016(2):1-6.
XU D, CUI X X, WANG T, et al. The study of chaotic random number generator based on Logistic map[J]. Microelectronics & Computer, 2016(2):1-6.

[14] 姚勇. 熵、分维、李雅普诺夫指数与混沌[J]. 自然杂志, 1987(5): 41-47.
YAO Y. Entropy, fractal dimension, Lyapunov exponent and chaos[J]. Nature, 1987(5): 41-47.

[15] CHUA L O, YANG L. Cellular neural networks: theory[J]. IEEE Transactions on Circuits & Systems, 1988, 35(10): 1257-1272.

[16] WANG X, BING X, ZHANG H. A multi-ary number communication system based on hyperchaotic system of 6th-order cellular neural network[J]. Communications in Nonlinear Science & Numerical Simulation, 2010, 15(1): 124-133.

[17] LI Y, XIAO D, LI H, et al. Parallel chaotic Hash function construction based on cellular neural network[J]. Neural Computing & Applications, 2011, 21(7): 1563-1573.

[18] 张雪锋, 范九伦. 基于线性反馈移位寄存器和混沌系统的伪随机序列生成方法[J]. 物理学报, 2010, 59(4): 2289-2297.
ZHANG X F, FAN J L. The method of generating pseudo random sequence based on LFSR and chaos[J]. Acta Physica Sinica, 2010, 59(4): 2289-2297.

[19] RUKHIN A, SOTO J, NECHVATAL J, et al. A statistical test suite for random and pseudorandom number generators for cryptographic applications[J]. Andrew Rukhin Juan Soto James Nechvatal Miles Smid Elaine, 2010, 59(4): 2289-2297.

[20] 王亚红. 基于 Henon 映射参数扰动的伪随机数发生器设计及应用[J]. 中文信息, 2010, 59(4): 2289-2297.
WANG Y H. The design and applications of PRNG based on Henon map with parameter perturbation[J]. Journal of Chinese Information Processing, 2010, 59(4): 2289-2297.

[21] HOSSAIN M B, RAHMAN M T, RAHMAN B M S, et al. A new approach of image encryption using 3D chaotic map to enhance security of multimedia component[C]//International conference on Informatics, Electronics & Vision. 2014: 1-6.

作者简介：

董丽华（1997-），女，辽宁盘锦人，博士，西安电子科技大学副教授，主要研究方向为信息安全、密码学。

药国莉（1992-），女，山西临汾人，西安电子科技大学硕士生，主要研究方向为流密码。