

CNN超混沌系统伪随机序列发生器设计

张琴,林达,许理

(四川理工学院自动化与信息工程学院,四川 自贡 643000)

摘要:基于CNN超混沌系统,设计了一种混沌伪随机序列发生器。通过对细胞神经网络系统的理论分析及仿真实验可知,该系统具有复杂的动力学特性,具有初值敏感性、密钥空间大等特点,非常适合作为伪随机序列发生器。基于该系统的发生器能够产生两种不同的序列,一种为二进制序列,另一种为十进制序列,并且通过该发生器产生的伪随机序列具有良好的性能,如序列值的均匀分布性、尖锐的自相关特性和良好的互相关特性。除此之外,利用NIST标准对序列发生器进行性能检验,检验结果表明该序列满足伪随机序列的要求,具有较高的安全性和保密性,具有较好的应用前景。

关键词:超混沌;细胞神经网络;伪随机序列发生器

中图分类号:TN918

文献标志码:A

引言

混沌理论在确定性与随机性之间架起了互通的桥梁,是经典力学的一次革命突破^[1]。混沌是确定性的非线性动力系统,由于它具有伪随机性、对初值敏感性等特性,使得它非常适合保密通信、信息加密等工程领域^[2]。而混沌的应用需要产生混沌信号、混沌序列,而混沌序列的产生需要混沌伪随机序列发生器^[3-5]。文献[6]中,Rafik Hamza提出了一种基于陈氏混沌系统的伪随机序列生成算法。文献[7]中,Franois等人提出了一种随机序列产生算法,该随机序列是由混合的三个混沌映射产生的,该序列发生器能够抵抗一些攻击,如差分攻击、穷举攻击。文献[8]中,Hu等人提出了一种基于陈混沌系统的伪随机序列发生器,该系统具有较高的承受攻击的能力。

目前,一些基于混沌系统的加密方案存在一些安全性问题^[9-10],主要存在的问题有:密钥空间、算法的构造、一些低维的混沌映射,如文献[11]中提到的一维Logistic映射,在有限精度计算中存在周期退化的问题。事实上,一个复杂的高维混沌映射要比任何低维的混沌映射安全^[6],而且复杂的高维混沌系统能提高伪随机序列生成器的安全性。因此,基于高维混沌系统的伪随机序列发生器适合产生密钥流。

1 细胞神经网络(CNN)超混沌系统

细胞神经网络(CNN)的神经元激活函数是非线性函数,因此细胞神经网络是高度非线性动力系统,四阶CNN系统能够产生超混沌行为。本文所采用的超混沌系统模型为^[12]:

收稿日期:2017-07-29

基金项目:国家自然科学基金项目(61640223);人工智能四川省重点实验室开放基金(2016RZJ02)

作者简介:张琴(1989-),女,江苏扬州人,硕士生,主要从事混沌保密通信与图像加密方面的研究,(E-mail)820441750@qq.com;

林达(1974-),男,山东日照人,教授,博士,硕士生导师,主要从事混沌保密通信、非线性系统的智能控制与化与无人机运动协调控制方面的研究,(E-mail)971244320@qq.com

$$\begin{cases} \frac{dx_1}{dt} = -x_3 - x_4, \\ \frac{dx_2}{dt} = bx_2 + x_3, \\ \frac{dx_3}{dt} = cx_1 - dx_2, \\ \frac{dx_4}{dt} = 96x_1 - 90x_4 + 2ey_4, \end{cases} \quad (1)$$

其中: $y_4 = \frac{1}{2}(|x_4 + 1| - |x_4 - 1|)$; b, c, d, e 为系统的控制参数,当 $b = 2, c = 12, d = 13, e = 99$ 时,系统(1)呈现为超混沌状态。

系统(1)的超混沌细胞神经网络的混沌吸引子相图如图1所示,为在 Matlab 中仿真得到的各个相平面上的混沌吸引子。

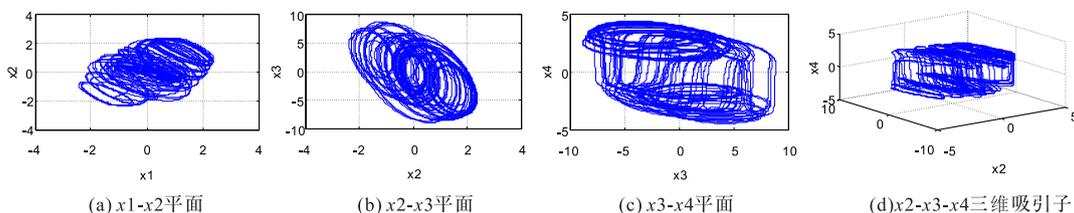


图1 超混沌细胞神经网络的吸引子相图

为了能够更直观地看到不同的初值对混沌系统的影响,建立对应值的时间序列图和直方图,如图2~图3所示。图2(a)与图2(b)是 $x_1 = 1.0$ 对应的的时间序列图与直方图;图2(c)与图2(d)是 $x_1 = 1.0 + 10^{-11}$ 对应的的时间序列图与直方图。图3是 x_4 分别取值 4.0 与 $4.0 + 10^{-11}$ 对应的的时间序列图与直方图。从这些图中,可以看

出由超混沌细胞神经网络系统直接产生的序列不是均匀分布的。换言之,由超混沌细胞神经网络系统产生的序列不能直接用于图像密码学中,它需要经过适当的量化处理之后才可以使用,常见的量化方法有:二值量化、中间多比特量化等^[13-14]。

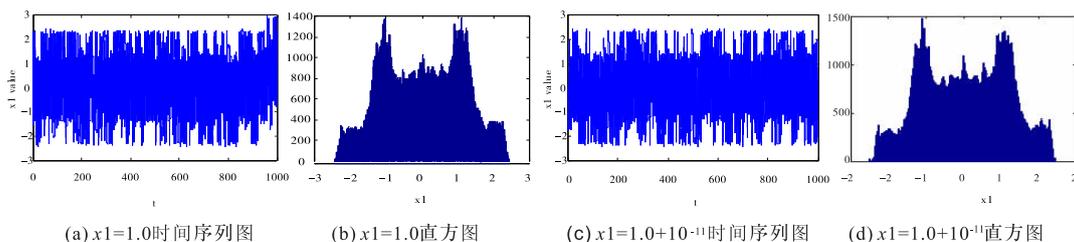


图2 不同初值时的 x_1 值分布

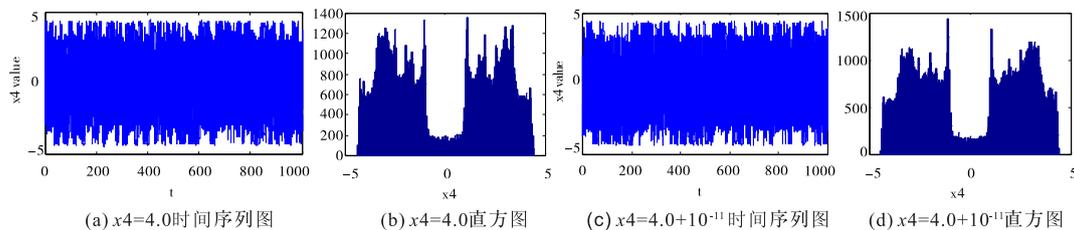


图3 不同初值时 x_4 值分布

2 基于 CNN 超混沌系统的伪随机序列发生器设计

量化是生成混沌伪随机序列非常重要的一个环节,该环节直接影响生成序列的复杂性和随机性^[2]。量化

算法的好坏最终会影响到其应用的安全性,随机性是衡量量化算法优劣的主要指标之一,因此选择合适的量化算法是至关重要的。

基于大量的实验,提出了一种量化算法,该算法生成的序列是均匀分布的,并且具有随机统计的特征。该

量化算法如下:

$$\begin{cases} P(4 \cdot i) = \alpha \cdot p \cdot x \\ P(4 \cdot i + 1) = \beta \cdot p \cdot y \\ P(4 \cdot i + 2) = \gamma \cdot p \cdot z \\ P(4 \cdot i + 3) = \delta \cdot p \cdot w \\ i = 0, 1, 2, 3, \dots, k \end{cases} \quad (2)$$

其中:

$$\begin{cases} \alpha = \frac{\sum |x(i)|}{n} \\ \beta = \frac{\sum |y(i)|}{n} \\ \gamma = \frac{\sum |z(i)|}{n} \\ \delta = \frac{\sum |w(i)|}{n} \\ p = 800 \cdot \alpha \cdot \beta \cdot \gamma \cdot \delta \\ S = \text{round}(|P| \bmod l) \end{cases} \quad (3)$$

$$S = \text{round}(|P| \bmod l) \quad (4)$$

其中:round为四舍五入符号,mod为取余符号, S 为该算法产生的一维序列。序列 S 的输出是二进制数还是十进制数,主要取决于 l 的取值。 l 的值可以取2或256,当 $l=2$ 时,序列 S 为二进制输出,当 $l=256$ 时,序列 S 为十进制整数输出。

$x(i)$ 、 $y(i)$ 、 $z(i)$ 、 $w(i)$ 为神经网络系统的样本, α 、 β 、 γ 、 δ 为样本绝对值之和的平均值, k 为轨道 x 、 y 、 z 、 w 中任意一个的长度,换句话说,假设序列的长度为 n ,那么 k 的长度为 n 的1/4倍。利用公式(2)产生一个长度为 n 的一维向量序列 P ,且 P 为实数。最后,利用公式(4)产生序列 S 。

具体的伪随机发生器设计步骤如下:

步骤1:选取四阶CNN超混沌系统的初始值及系统控制参数。

步骤2:将初始值及系统控制参数带入CNN系统中,进行多次迭代,产生一系列一定范围内的实数值。

步骤3:产生的实数值不能直接作为伪随机序列,需将这些实数值进行量化处理。

步骤4:将公式(3)带入公式(2)中,利用公式(2)得到4组长度相等的实数值,并将这4组数据按一维向量排好序。

步骤5:利用公式(4)可以产生两种伪随机序列,当 $l=2$ 时,产生的 S 为二值序列,当 $l=256$ 时,产生的 S 序列范围为0~255, S 序列即为所需要的伪随机序列。

根据上述步骤设计的伪随机序列发生器,相比于一一般的二值量化算法,具有较好的伪随机特性,并且基于CNN超混沌系统设计的伪随机发生器产生的序列具有较高的安全性。除此以外,利用该伪随机发生器能够产生两种不同的伪随机序列,一种为二进制序列,另一种为十进制序列,实现一物多用功能。

该量化算法是基于4个混沌轨道坐标的结合,这样可以确保伪随机序列发生器的安全性。该发生器的输入即为密钥,密钥的构成有:初始值,控制参数及序列的长度 n 。当 $l=256$ 时,该算法产生的序列如图4所示,从图中可以看出序列值具有均匀分布性。

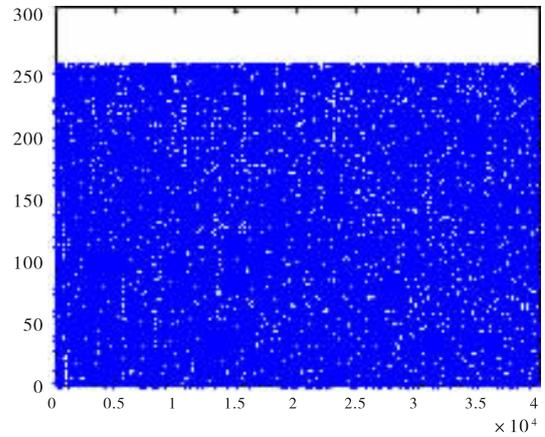


图4 伪随机序列值的分布图

3 混沌伪随机序列的分析

3.1 密钥空间分析

伪随机序列发生器的一个重要用途就是用来产生加密密钥,为了保证加密的安全性^[15],其密钥空间应不小于 2^{128} 。本文以细胞神经网络混沌系统的初始值和控制参数作为密钥,密钥空间的大小取决于混沌系统的初值和控制参数的敏感性。经过实验证明,该算法精确到小数点后11位,密钥空间为 $10^{11 \times 8} = 10^{88} \approx 2^{290}$,远大于 2^{128} 的密钥空间,足以抵抗穷举密钥攻击^[16]。

3.2 初值敏感性分析

为了保证系统的安全性,一个好的加密系统必须对

密钥有敏感性^[8]。对本文提出的算法的密钥的敏感性进行了测试,通过轻微改变密钥的初始值,来观察产生的序列与原始序列是否变化,从而达到测试的目的。利用本文提出的伪随机算法产生两组序列,其中一组为原始序列 S_1 ,另一组序列为 S_2 , S_2 是在细微改变任意一个初始值(相差 10^{-11}),迭代 10 000 次后产生的序列,从图 5 可以看出 S_1 和 S_2 是两个不同的序列,说明该算法对密钥初始值具有敏感性。

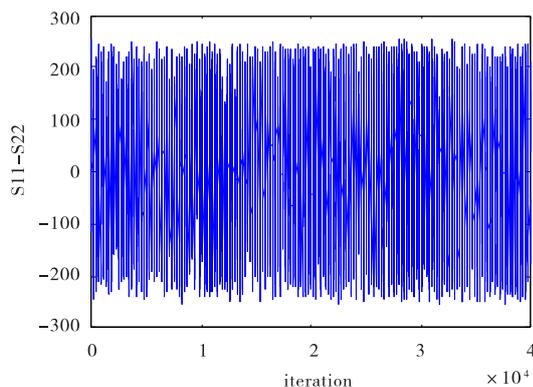


图 5 S_1 与 S_2 的差异图

3.3 相关性分析

相关性是混沌序列重要的性质,良好的相关性是系统能够可靠运行的保证之一。相关性包括自相关和互相关,对于理想的随机序列,自相关函数应为 δ 函数,互相关函数应为 0。当系统参数 $b = 2$ 、 $c = 12$ 、 $d = 13$ 、 $e = 99$,系统初值 $x(0) = 1$ 、 $y(0) = 2$ 、 $z(0) = 3$ 、 $w(0) = 4$ 时,系统迭代 10 000 次后,产生如图 6 与图 7 所示的二进制序列的自相关和互相关特性。从图 6 和图 7 可以看出,二进制序列具有类似 δ -like 的性质,有尖锐的自相关特性和良好的互相关特性。

3.4 随机性测试

本文采用 NIST 标准中部分测试方法对文中所产生的二进制序列进行测试,该测试标准为美国国家标准技术研究所制定的随机序列测试标准,即 SP800-22 标准。该标准从不同角度检验伪随机序列在统计特性上相对于理想随机序列的偏离程度,一般认为通过了该检验标准的伪随机序列具有好的随机性能^[5]。

3.4.1 频率测试

频率测试的目的是检验整个序列中 0 和 1 的比例,即测试序列中 0 和 1 的比例是否近似相等,约为 50%。

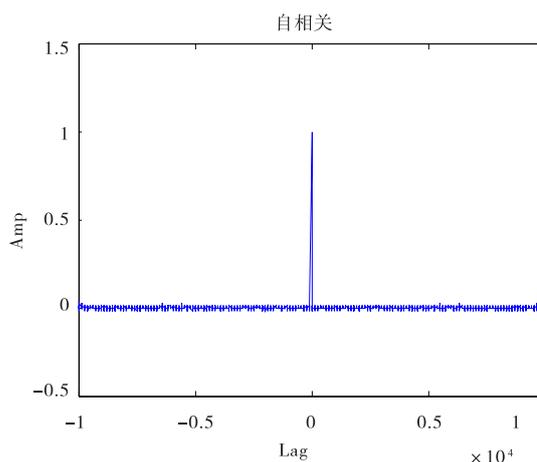


图 6 序列的自相关特性

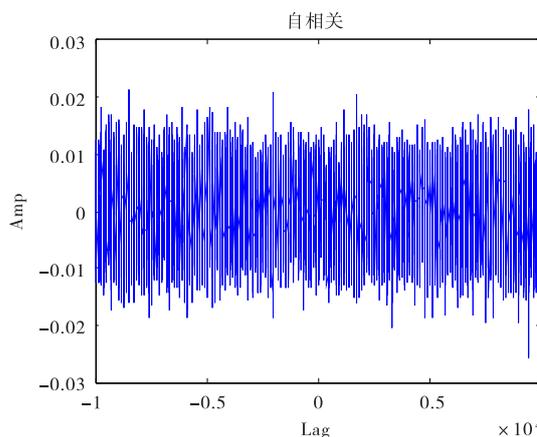


图 7 序列的互相关特性

具体的测试方法如下^[17]:

(1) 将由 0 和 1 组成的序列转换为由 -1, 1 组成的序列,转换方式为 $x_i = 2\varepsilon - 1$ 。其中, ε 、 x_i 为转换前后的比特值。计算转换后的序列的和 S_n , 即 $S_n = x_1 + x_2 + x_3 + \dots + x_n$ 。

(2) 计算统计值 s_{obs} , 即

$$s_{obs} = \frac{|S_n|}{\sqrt{n}} \quad (5)$$

(3) 计算判断标准 P -Value 的值:

$$P\text{-Value} = \text{erfc}\left(\frac{|S_{obs}|}{\sqrt{n}}\right) \quad (6)$$

其中, $\text{erfc}()$ 为互补误差函数,即

$$\text{erfc}(z) = \frac{2}{\sqrt{\pi}} \int_z^{\infty} e^{-u^2} du \quad (7)$$

若 P -Value 的值小于 0.01,则认为测试的序列不为随机序列;反之,则认为序列是随机序列。

取迭代初值 $x(0) = 1, y(0) = 2, z(0) = 3, w(0) = 4$, 系统参数 $b = 2, c = 12, d = 13, e = 99$, 迭代次数 $N = 10\ 000$, 生成长度为 40 000 的二进制序列, 通过统计, 二进制混沌序列中‘0’的个数 $N_0 = 19\ 973$, ‘1’的个数 $N_1 = 20\ 027$, 0-1 之比为 $N_0/N_1 = 0.9973$, 由上述测试方法得 $P - Value = 0.7872 > 0.01$, 故可认为序列是随机序列。

3.4.2 游程测试

游程是指序列中由相同比特所构成的不间断的子序列。游程测试的目的是计算序列中游程的个数, 并判断 0 和 1 的游程个数是否与随机序列一致。同时, 该项测试还可以用于判断序列在 0 和 1 之间的振荡快慢^[18]。

在这里, 只关心序列是否是随机的, 不关心序列是否具有某种倾向, 故采用双侧假设检验, 在假设为真的情况下, 0 和 1 出现的可能性相等, 其在序列中应是交互的。相对于一定个数的‘0’和‘1’, 序列游程的总数应在一定范围内。若游程总数过少, 表明某一游程的长度过长, 意味着有较多的 0 或 1 相连, 序列存在成群倾向; 若游程总数过多, 表明某一游程的长度过短, 意味着‘0’和‘1’频繁交替, 序列具有混合倾向。因此无论游程总数过多或过少, 都表明序列不是随机的。

同样, 取迭代初值 $x(0) = 1, y(0) = 2, z(0) = 3, w(0) = 4$, 系统参数 $b = 2, c = 12, d = 13, e = 99$, 迭代次数 $N = 10\ 000$, 生成长度为 40 000 的二进制序列, 利用双侧假设检验测试游程, 得到游程数为 20 014, 在显著性水平 0.05 下的检验结果为 0.1438, 小于显著水平 0.05 下的正态上 0.025 分位点的值 1.9600, 接受独立假设。故可认为序列是随机序列。

4 结束语

本文基于超混沌细胞神经网络系统设计了一种伪随机序列生成算法, 该算法能同时生成两种伪随机序列。通过理论分析和仿真验证可知, 该序列生成器能够产生均匀分布的序列, 并且具有良好的自相关和互相关特性。除此之外, 本文还利用 NIST 标准中部分指标对序列发生器进行性能检验, 检验结果表明该序列发生器能够产生良好的伪随机序列, 该发生器产生的伪随机序

列可以作为密码系统的密钥, 具有较高的安全性和保密性, 具有较好的应用前景。

参考文献:

- [1] 马英杰, 于航如. Tent 混沌伪随机序列发生器设计与实现[J]. 北京电子科技学院学报, 2015, 23(4):61-64.
- [2] 孙克辉, 叶正伟, 贺少波. 混沌伪随机序列发生器的 FPGA 设计与实现[J]. 计算机应用与软件, 2014, 31(12):7-11.
- [3] LEE W B, CHEN T H. A public verifiable copy protection technique for still images[J]. Journal of Systems & Software, 2002, 62(3):195-204.
- [4] GARCIA-MARTINAZ M, CAMPOS-CANTON E. Pseudo-random bit generator based on lag time series[J]. Int J Mod Phys C, 2014, 25(4):822-836.
- [5] WANG X Y, QIN X, XIE Y X. Pseudo-random sequences generated by a class of one-dimensional smooth map[J]. Chinese Physics Letters, 2011, 28(28):080501.
- [6] HAMZA R. A novel pseudo random sequence generator for image-cryptographic applications[J]. Journal of Information Security and Applications, 2017, 35(1):119-127.
- [7] FRANOIS M, GROSGES T, BARCHIESI D, et al. Pseudo-random number generator based on mixing of three chaotic maps[J]. Communications in Nonlinear Science & Numerical Simulation, 2014, 19(4):887-895.
- [8] HU H P, LIU L F, DING N D. Pseudo-random sequence generator based on the Chen chaotic system[J]. Computer Physics Communications, 2013, 184(3):765-768.
- [9] WANG X, LUAN D, BAO X. Cryptanalysis of an image encryption algorithm using Chebyshev generator[J]. Digital Signal Processing, 2014, 25(1):244-247.
- [10] WANG Q, YU S, LI C, et al. Theoretical design and FPGA-based implementation of higher-dimensional digital chaotic systems[J]. IEEE Transactions on Circuits & Systems I Regular Papers, 2015, 63(3):401-412.
- [11] 冯汉, 索宇, 朱培勇. 基于 Logistic 映射的迭代式的混沌特性及混沌控制[J]. 四川理工学院学报: 自然

- 科学版,2011,24(1):24-26.
- [12] 朱艳平.初始值对细胞神经网络混沌特性的影响[J].赤峰学院学报:自然科学版,2016,32(1):38-40.
- [13] 张严平,陆锐敏.一种改进的混沌序列量化算法[J].通信技术,2016,49(3):278-281.
- [14] 唐立法,周健勇,董斌辉,等.混沌量化算法研究及测试分析[J].微型机与应用,2010,29(19):13-24.
- [15] AKHSHANI A, AKHAVAN A, MOBARAKI A, et al. Pseudo random number generator based on quantum chaotic map[J]. Communications in Nonlinear Science and Numerical Simulation, 2014, 19(1): 101-111.
- [16] 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,2017,53(4):135-139.
- [17] 李红燕,杨万利.时空混沌二值化方法研究[J].计算机工程与应用,2013,49(21):65-69.
- [18] 刘金.无线传感器网络密钥管理与信息加密研究[D].沈阳:东北大学,2014.

Design of Pseudo-Random Sequence Generator Based on CNN Hyperchaotic System

ZHANG Qin, LIN Da, XU Li

(School of Automation & Information Engineering, Sichuan University of Science & Engineering, Zigong 643000, China)

Abstract: A design of pseudo random sequence generator is proposed based on CNN hyperchaotic system. Theory analysis and simulation show that the cellular neural network is good with complex dynamic characteristics, such as great sensitivity to initial values, large key space, which is quite adequate to be the pseudo random sequence generator. This generator based on hyperchaotic system can generate two different sequences, one is the binary and the other is decimal, and the sequence is good with performance such as uniform distribution, sharp autocorrelation characteristics and good cross-correlation. Furthermore, the generated pseudo random sequence passed NIST test successfully. It is good in practical applications.

Key words: hyperchaotic; cellular neural network; pseudo random sequence generator