

一种改进的基于混沌系统的数码防伪技术实现

朱海峰

(南通大学 电子信息学院, 江苏 南通 226019)

摘 要: 对文献[5]中提出的混沌加密系统进行仿真与分析, 通过分析可知该加密系统中所采用的混沌系统在随机性上有所欠缺. 在此基础上, 提出了将 Chebyshev 混沌系统应用到该混沌加密系统中, 并对改进后的混沌加密系统进行仿真与分析, 可知该混沌系统具有良好的随机性. 将混沌系统应用到数码防伪技术中, 使密钥空间增大, 使破译的难度增强, 使商品在市场流通中具有更强的防伪性能, 可以很好地弥补了数码防伪技术所存在的不足.

关键词: 混沌; 随机性; Chebyshev; 仿真; 数码防伪技术

中图分类号: TP309.7

文献标识码: A

文章编号: 1000-7180(2013)11-0006-03

An Improved Anti-counterfeiting Technology for Digital and Its Implementation Based on Chaotic Systems

ZHU Hai-feng

(School of Electronics and Information, Nantong University, Nantong 226019, China)

Abstract: Base on the literature [5] is proposed on the chaotic encryption system simulation and analysis, which was lacked in the randomness. On this basis, the Chebyshev chaotic applied to the chaotic encryption systems and that simulation and analysis of its improved were investigated. The results show that well randomness. If the chaotic systems applied to anti-counterfeiting technology for digital, the key space of algorithm will be bigger and the goods process of commodity circulation has a stronger function of anti-counterfeiting. This can be making up for insufficiency of the anti-counterfeiting Technology for Digital.

Key words: chaotic; randomness; Chebyshev; simulation; anti-counterfeiting technology for digital

1 引言

当今社会, 商品的伪造已经日益威胁着全球经济的发展^[1], 而数码防伪技术可以很大程度上抑制商品的假冒伪劣现象的发生, 从而保护了消费者和生产者的利益.

数码防伪技术依靠着防伪性能好、易于识别、代价小等优势得到了广大企业的青睐, 逐渐扩大了数码防伪技术在防伪领域的应用力度^[2]. 在数码防伪技术的发展过程中, 先后出现了基于随机条形码、加密有序的流水号、综合数码三种防伪技术^[3]; 其应用取得了较大的成果, 但是数码防伪技术仍然缺乏密码学技术的支撑, 使其生成的防伪码安全性不够高,

在应用过程中仍然存在一些漏洞.

混沌系统具有不可预测性、无周期性、不可分解性、对初始参数的敏感性等特性^[4], 因此混沌系统非常适合用到密码领域的. 将混沌系统应用到数码防伪技术中可以利用混沌所独有的一些性质很好的解决数码防伪技术中所存在的一些固有的难题.

2 前提

文献[5]中提出了一种基于双重混沌系统的数码防伪技术, 作者利用了混沌系统具有的初值敏感性、生成序列的随机性、无周期性等性质, 将混沌系统应用到了数码防伪技术当中.

在文献[6]中指出了戈龙布(Golomb)提出的假

收稿日期: 2012-12-28; 修回日期: 2013-02-25

基金项目: 中国交通运输部科技项目(2012-319-813-270); 江苏省高校自然科学基金项目(10KJB510021)

如序列可以称为随机序列所应该满足的三个随机性共设,在严格意义上全部满足这三个随机性共设条件的序列是很少的,所以笔者认为对所有用作加密的序列只需近似或者满足随机性共设条件的部分即可认为该序列是随机的.我们对文献[5]中用到的 Henon 混沌系统所生成的混沌序列进行随机性检测:

(1)频数检验:对混沌系统生成的二值序列进行如下测试:

$$\chi^2_1 = \frac{(n_0 - n_1)^2}{n} \tag{1}$$

式中, n 是混沌系统生成的二值序列数量的总和,其中 n_0 是序列中 0 的个数, n_1 是序列中 1 的个数,与 ‘1’ 的自由 χ^2 分布比较(随机性假设检验),假设对应 5% 的显著水平,可知 χ^2_1 的值为 3.84,所以只要二值序列的 χ^2_1 的上限为 3.84,就可以认为此二值序

列具有较好的随机性.

(2)序列检验:对混沌系统生成的二值序列进行分析计算,计算出此二值序列中 00,01,10,11 依次出现的次数,并计算出 00,01,10,11 各自的 χ^2 ,遵循的规则如式(2)所示:

$$\chi^2_2 = \frac{4}{n-1} \sum_{i=0}^1 \sum_{j=0}^1 (n_{i,j})^2 - \frac{2}{n} \sum_{i=0}^1 (n_i^2 + 1) \tag{2}$$

式中, $n_{i,j}$ 表示二值序列中 ij 的个数, $i,j \in \{0,1\}$,与 2 的自由度 χ^2 分布进行比较(随机性假设检验),假设对应 5% 的显著水平,并计算得出 χ^2_1 的值为 5.99,所以只要二值序列的 χ^2_2 值的上限为 5.99,就认为此序列具有较好的随机性.

结合上面的两个特性,对文献[5]中所用到的混沌系统进行测试,并得出表 1 的结果.

表 1 Henon 混沌系统的随机性检验

序列长度 n	1 000	4 000	8 000	15 000	30 000
‘0’的个数	496	1 984	4 006	7 470	14 869
‘1’的个数	504	2 016	3 993	7 530	15 131
‘00’的个数	148	610	1 218	2 271	4 423
‘01’的个数	349	1 393	2 765	5 186	10 416
‘10’的个数	349	1 393	2 765	5 186	10 416
‘11’的个数	154	604	1 252	2 357	4 745
频数检验 χ^2_1	0.064 0	0.256 0	0.018 0	0.240 0	2.288 1
序列检验 χ^2_2	157.978 0	618.711 7	1.173 9e+003	2.199 2e+003	4.600 2e+003

通过分析表 1 可知,在初值为 0.6,0.2,中间值为 0.4 的情况下,Henon 混沌系统的频数检验符合随机性,但是在通过序列检验的值可知,该系统生成的二值序列并不具备良好的随机性.所以用该系统进行加密的数码防伪系统并不具备绝对的不可攻击性,本文在此基础上对该加密系统进行改进,并进行测试.

3 混沌系统

文献[7]介绍了一种简单但是却十分有效的一维混沌系统—Chebyshev 混沌系统,其表达式为

$$x(n+1) = \cos(\arccos x(n)) \quad -1 \leq x(n) \leq 1 \tag{3}$$

当参数 $q \geq 2$ 时,该混沌系统迭代产生的序列 $\{x(n)\}$ 在值域 $[-1,1]$ 上遍历,且 Lyapunov 指数为正数,可知该序列是随机发散的.随着混沌系统的迭代次数的增加,产生的迭代序列值遍历整个值域,而且呈现无周期性和无规律性,这些特性使得 Chebyshev 系统生成的序列适用于对密钥的控制.本文取 Chebyshev 混沌系统的参数 $q = 4$,初值为 0.6,则该混沌系统的频数检验和序列检验,如表 2 所示.

表 2 Chebyshev 混沌系统随机性检验

序列长度 n	1 000	4 000	8 000	15 000	30 000
‘0’的个数	505	2 030	4 001	7 492	14 864
‘1’的个数	495	1 970	3 999	7 508	15 136
‘00’的个数	254	1 029	1 995	3 752	7 358
‘01’的个数	251	1 001	2 006	3 740	7 506
‘10’的个数	250	1 000	2 005	3 739	7 505
‘11’的个数	245	970	1 994	3 769	7 631
频数检验 χ^2_1	0.100 0	0.900 0	5.000 0e-004	0.017 1	2.466 1
序列检验 χ^2_2	1.065 2	1.841 7	1.060 1	1.139 0	3.518 7

通过分析表 2 可以发现 Chebyshev 混沌系统的频数检验和序列检验均符合条件,所以在一般情况下可以认为该混沌系统产生的序列为随机序列,可将该混沌系统应用到加密系统中.

4 算法描述

在每个商品的生产过程中,可以根据商品的出厂日期,生产厂家以及在生产线上的序列号等条件为商品赋予一个属于自身唯一的生产号,该生产号可由不同厂家不同的生产习惯灵活而定,本文中取该生产号为 12 位. 然后对生产号进行整合,使其整合成 8 位的身份码.

在本文中采用二维 logistic 映射对身份码进行置乱,置乱后可以得到一个 8 为的置乱码,然后将每一位的置乱码都转化为四位的二进制数.

将 Chebyshev 混沌系统按指定的初值与参数进行迭代 32 次,并将生成的混沌序列转化为二进制序列,得到二进制加密码,将得到的二进制加密码与置乱过后生成的二进制数进行异或运算,即可得到二进制的防伪码,将该二进制防伪码整合成八位的十六进制的数,该八位的十六进制数便是所要生成的商品的防伪码.

在该加密系统中,我们可以将两组混沌系统的参数值和初值作为该加密系统的密钥,并进行保护.

解密算法是加密算法的逆过程.

算法的流程图如图 1 所示.

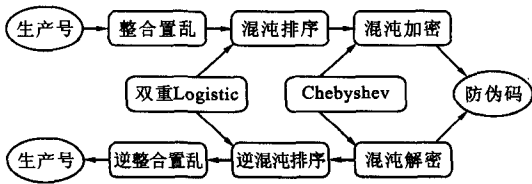


图 1 算法流程图

5 仿真结果

取 Chebyshev 混沌系统的参数 $q=4$, 初值为 0.6, 将该混沌加密算法在计算机中进行仿真, 本文取若干仿真结果进行比较. 表 3 是 Chebyshev 混沌系统初值为 0.6 时的仿真结果, 表 4 是 Chebyshev 混沌系统初值为 0.600 000 001 时的仿真结果.

通过分析表 3、表 4 可以发现, 在参数不变的情况下, 当初值发生 0.000 000 01 的变化, 则生成的防伪码完全不一样, 所以该混沌系统具有密码学特性, 可以用于数码防伪技术中.

表 3 $q=4$, 初值为 0.6 的仿真结果

商品的生产号	防伪码	解密后的生产号
120905010001	77bf4571	120905010001
121231051234	73ee7252	121231051234
140925253452	538c133f	140925253452
230116177892	6188d3f7	230116177892
250801210987	57dfc4e3	250801210987
320334121031	64be717e	320334121031
550919319987	47d6cfe4	550919319987

表 4 $q=4$ 初值为 0.600 000 01 的仿真结果

商品的生产号	防伪码	解密后的生产号
120905010001	3f84f5af	120905010001
121231051234	3bd5c28c	121231051234
140925253452	1bb7a3e1	140925253452
230116177892	29b36329	230116177892
250801210987	1fe4743d	250801210987
320334121031	2c85c1a0	320334121031
550919319987	0fed7f3a	550919319987

将混沌系统应用到数码防伪技术中, 可以利用混沌系统所具有的初值敏感性、生成序列随机性以及无周期性等特性很好的弥补数码防伪技术所存在的缺陷. 将混沌系统应用到数码防伪技术中可以防止假冒伪劣商品在市场的流通, 保护了消费者和生产者的权益, 维护了消费市场的秩序.

6 结束语

本文对文献[5]中的混沌系统进行测试, 提出了一个性能更好的混沌系统以用到数码防伪技术当中, 并验证了该算法具有良好的密码学特性. 同时利用混沌系统具有的初值敏感性、随机性等独有的性质, 满足了在数码防伪技术中对密钥的要求. 把混沌系统应用到数码防伪技术中, 实现了一个简单方便、快捷安全的数码防伪系统. 在今后的研究过程中, 我们将结合不同复杂程度的混沌系统, 通过测试不同混沌系统的敏感性、随机性等特性, 力争找到更加合适用于数码防伪技术中的混沌系统, 并将该系统应用到数码防伪技术当中.

参考文献:

[1] 徐大雄. 列入中华人民共和国国家标准的 10 项防伪技术[J]. 激光杂志, 1999, 10(4): 1-5.
[2] 甘光伟. 数码防伪技术[M]. 北京: 中国标准出版社, 2002.

工艺、更低的工作电压,虽然文献[9]功能略多,文献[10]采样率较高,但是本文通道数明显多于文献[9-10],系统的计算任务量仍可比于甚至多于文献[9-10],因此本文的流片结果比文献[9-10]的结果更具优势.

表 7 与已发表文献比较

	文献[9]	文献[10]	本文设计
功能	波束成形 反馈消除 NR WDRC	NR WDRC	NR WDRC
实现	ASIP	ASIC	ASIP
工艺/nm	65	90	130
采样率/kHz	16	24	16
通道数	17	18NR,3WDRC	32
时钟/MHz	11	3,6,8	8
电压/V	0.8	1.0	1.2
面积/mm ²	0.49	3.13	2.0
功耗/mW	0.334	1.095	0.963

4 结束语

专用指令集处理器提取算法特征,针对应用添加专用指令与硬件加速单元,兼具 ASIC 与 GPP 的低功耗、高性能与灵活性.本文提出的应用于数字助听器系统的专用指令集处理器结构,通过分析数字助听器系统中最广泛应用的语音处理算法,添加适用于语音处理的专用指令与加速单元,实现了数字助听器最核心的功能噪声消除与听力补偿,同时在设计的各个阶段综合采用低功耗的软硬件设计方法,ASIP 可以很好地满足系统低功耗以及灵活性的设计需求.本文的 ASIP 设计方法对其他低功耗应用的 ASIP 设计具有一定的借鉴意义.

参考文献:

- [1] James M K. Digital hearing aids[M]. Oxfordshire: Plural Publishing, 2008.
- [2] Jain M K, Balakrishnan M, Kumar A. ASIP design methodologies: survey and issues [C]// International Conference on VLSI Design. Bangalore: IEEE, 2001: 76-81.
- [3] 于增辉, 黑勇, 陈黎明, 等. 多通道数字助听器算法及低功耗 VLSI 设计[J]. 微电子学与计算机, 2012, 29(4): 14-18.
- [4] 于增辉, 黑勇, 薛金勇, 等. 助听器多通道宽动态范围压缩的低功耗硬件实现[J]. 哈尔滨工程大学学报, 2012, 33(1): 106-111.
- [5] Brennan R, Schneider T. A flexible filterbank structure for extensive signal manipulations in idigital hearing aids[C]// Proceedings of the 1998 IEEE International Symposium on Circuits and Systems. Monterey, CA: IEEE, 1998: 569-572.
- [6] James M K. Signal processing for hearing aids[M]. US: Springer, 2002: 235-277.
- [7] Crochiere R E, Rabiner L R. Multirate digital signal processing[M]. Englewood Cliffs: Prentice Hall, 1983.
- [8] Mitra S K. Digital signal processing - A computer-based approach[M]. 2nd ed. Beijing: Tsinghua University Press, 2006: 147-149.
- [9] Peng Qiao, Corporaal H, Lindwer M. A 0.964mW digital hearing aid system[C]// Design, Automation and Test in Europe Conference and Exhibition. Grenoble, France, 2011: 1-4.
- [10] Wei Chengwen, Kuo Yuting, Chang Kuochiang, et al. A low-power mandarin-specific hearing aid chip[C]// IEEE Asian Solid-State Circuits Conference. Beijing, 2010: 1-4.

作者简介:

薛金勇 男, (1985-), 博士研究生. 研究方向为数字集成电路设计.

(上接第 8 页)

- [3] 赵卓, 陈立杰. 密码技术在数字防伪系统中的应用[J]. 计算机工程与技术, 2005, 26(10): 2860-2862.
- [4] Zhang Xuefeng, Fan Jiulun. Digital image hiding technology based on chaos system[J]. Computer Engineering, 2007, 28(9): 134-136.
- [5] 魏旭, 陆国平, 陈秋琼. 基于双重混沌映射的数码防伪技术研究[J]. 微电子学与计算机, 2012, 29(8): 127-129.
- [6] 吴伟陵. 信息处理与编码[M]. 北京: 人民邮电出版社, 1997.

- [7] 石红芹, 吕方亮, 刘遵雄. 基于混沌加密的彩色图像盲数字水印算法[J]. 计算机工程, 2011, 37(20): 105-107.

作者简介:

朱海峰 男, (1979-), 硕士, 讲师. 研究方向为集成电路设计与数字加密.