文章编号:1001 - 893X(2011)04 - 0069 - 06

一种改进的数字混沌编码器*

肖利丽,何世彪, 田 东,吴永彬

(重庆通信学院,重庆 400035)

摘 要:针对解码器在解码前不需要初始化,攻击者容易重构出解码器结构这一缺陷,提出了一种新的编解码方法。改进后的解码器只有当编、解码器的初始状态相同时,解码器才能正确地恢复出原始信息序列。仿真结果表明,改进后的混沌编解码器结构比原结构具有更好的保密性能。

关键词:保密通信;混沌编码;数字滤波器

中图分类号:TN918;TN762 **文献标识码**:A doi:10.3969/j.issn.1001 - 893x.2011.04.015

A Novel Digital Chaotic Encoder

XIAO Li-li, *HE Shi-biao*, *TIAN Dong*, *WU Yong-bin*

(Department of Communication and Information System, Chongqing Communication Institute, Chongqing 400035, China)

Abstract: Aiming at the shortcoming that initial value is not required before decoding of the decoder, an improved en-decoder is proposed. To restore the original signal exactly, the state of the decoder must be initialized to that of the encoder. Simulation results show that the new en-decoder possesses much better security performance compared with original chaotic en-decoder.

Key words: secure communication; chaos code; digital filter

1 引 言

随着知识经济、信息产业的发展,信息安全问题日益突出,受到社会的广泛关注。对信息安全新理论与技术的研究已经成为高新技术发展中一个重要的热点问题。近年来,混沌方法在保密通信中的应用受到越来越多的关注,将混沌方法应用于保密通信最初是由 Tang 等人提出的[1]。Tang 在文章中指出:一个混沌电路可以通过输入信号同步驱动。后来,Chua 和 Newcomb[2-5]等人对混沌电路的同步进行了研究,他们一致确认了混沌用于保密通信的可能性。

混沌信号的隐蔽性、不可预测性、高度复杂性和易于实现等特性特别适合于保密通信[11-13]。Frey 提出的数字混沌保密通信方案结构简单,易于实现。但是在一些要求较高的保密通信环境下,这种简单的方法明显存在不足。为了提高通信保密性能,本文对 Frey 原有结构进行了改进。

2 数字滤波器的混沌现象

在构造一个实际的离散混沌系统时,首先遇到的问题是"字长效应"(或"有限精度")的影响。Chua 和 Lin[4-6]曾对有限字长效应的非线性递归数字滤波器进行了研究,其中数字滤波器如图 1 所示,其有限字长效应由一个非线性函数 $f_L(\cdot)$ 表示,如图 2 所示。研究和仿真实验显示,由于有限字长效应的

* **收稿日期**:2010 - 11 - 11;**修回日期**:2011 - 02 - 23
基金项目:重庆市科委自然科学基金资助项目(2007ba2017)
Foundation Item: The Natural Science Foundation of Chongqing Science and Technology Commission(No.2007ba2017)

存在,非线性数字递归滤波器在一定初始条件和参数下会呈现混沌行为。图 1 中,$x(n)$和 $y(n)$分别为滤波器的输入和输出,z^{-1}为延时器,a、b 为滤波器参数。

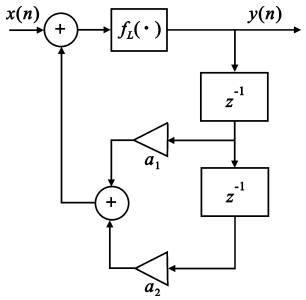


图 1 一个二阶数字滤波器
Fig.1 A second-order digital filter

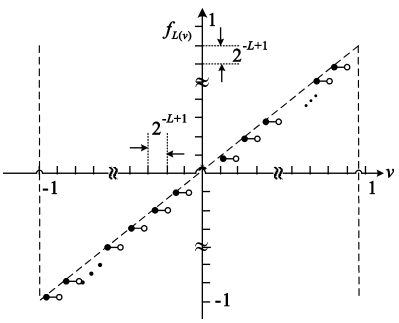


图 2 有限字长效应的非线性函数特性
Fig.2 Characteristic of nonlinear function with the finite word length effect

利用数字滤波器产生混沌现象面临的一个重要问题是对混沌映射的参数和状态只能用有限的精度来表示,这使得一个理论上的混沌系统实际上总可以表达成一个有限状态机,并且该系统具有有限的周期。随着字长的增加,非线性滤波器的周期将会迅速增长,同时,非性线数字滤波器的混沌行为基本上被保存了下来,这种情况被称为准混沌(Quasi-Chaotic,QC)现象,如图 3 所示。Frey[7,8]在 Chua 等人工作基础上,给出了准混沌应满足的一组特性,并将它作为数字混沌滤波器是否产生混沌的检验标准。这组特性包括:

(1)对几乎所有初始条件,零输入具有宽带噪声谱的响应,并且在相同的初始条件下,该响应的自相关函数与不相关的噪声相似;

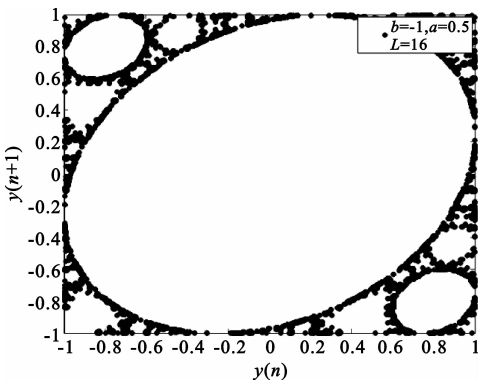
(2)对几乎所有初始条件,任意输入通过滤波器都具有宽带噪声谱的响应,并且在相同的初始条件下,该响应的自相关函数与不相关的噪声序列相似;

(3)对几乎所有初始条件,任意输入通过滤波器所产生的响应与其输入是不相关的;

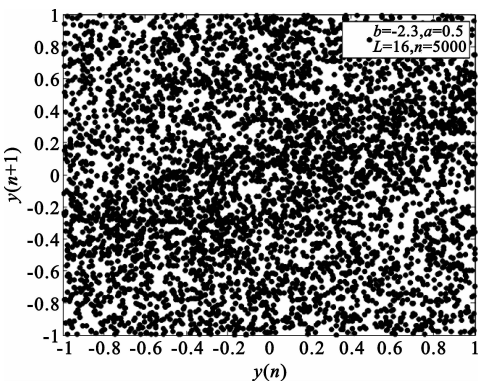
(4)对不相同的初始条件,相同输入通过滤波器所产生的响应之间是不相关的;

(5)对两个结构相同的滤波器,即使它们具有非常接近的初始状态,任意相同的输入总会使两个滤波器中的状态分离。

满足这组特性要求的数字滤波器可以认为具有一定的混沌特性,能够产生准混沌现象,可以用于混沌编码或其它保密通信。



(a) $b=-1, a=0.5$



(b) $b=-2.3, a=0.5$

图 3 非线性数字滤波器的混沌特性
Fig.3 Chaotic characteristic of nonlinear digital filter

3 混沌编码器结构和性能分析

3.1 基于非线性数字滤波器的混沌编解码器

根据文献[7]给出的非线性递归数字混沌编码器的原理和一般性方程,数字混沌编码器的编码过程可以表示为

$$\begin{cases} x(n) = h_1(n) * u(n) + h_2(n) * F(x(n), \\ \qquad x(n-1), \cdots, x(n-M)) \\ e(n) = d(n) * x(n) \end{cases} \tag{1}$$

式中,$u(n)$为信息信号,$F(\cdot)$为非线性映射函数,+、* 分别为加法和卷积运算,在有限精度的硬件实现中,也可认为是一种广义的非线性运算;$x(n)$为内部状态,$h_1(n)$和 $h_2(n)$是 IIR 或 FIR 滤波器的脉冲响应,$e(n)$为加密后的序列,被传送到接收端。混沌加密的过程就是经过由式(1)构成的非线性递归滤波器系统,将信息信号 $u(n)$变换为类似白噪声的混沌信号 $e(n)$。

解码时,采用与式(1)相对应的逆系统来对 $e(n)$进行直接逆滤波。解码过程为

$$\begin{cases} x(n) = \overline{d}(n) * e(n) \\ y(n) = \overline{h_1}(n) * x(n) + \overline{h_2}(n) * F(x(n), \\ \qquad x(n-1), \cdots, x(n-M)) \end{cases} \tag{2}$$

式中,$\overline{d}(n)$、$\overline{h_1}(n)$、$\overline{h_2}(n)$是根据式(1)求得的逆系统中的滤波器。由于解码系统是编码系统的直接逆系统,所以 $u(n)$将被准确地恢复出来,即 $y(n) = u(n)$。

图 4 就是满足式(1)和式(2)的一个简单的编解码器结构,其编解码方程为

$$\begin{cases} e(n) = u(n) + \{e(n-1) + f[e(n-2)]\} \\ y(n) = e(n) - \{e(n-1) + f[e(n-2)]\} \end{cases} \tag{3}$$

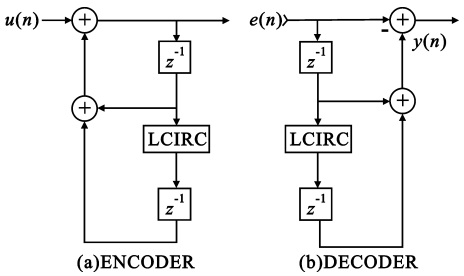
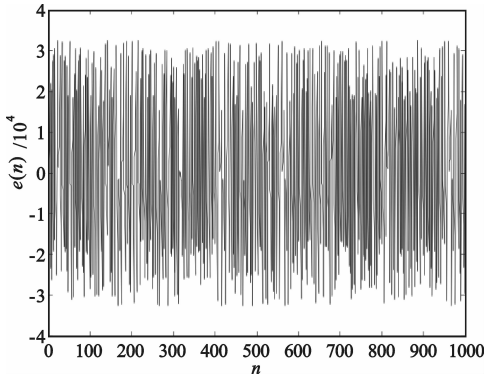


图 4　基于非线性数字滤波器的混沌编解码器

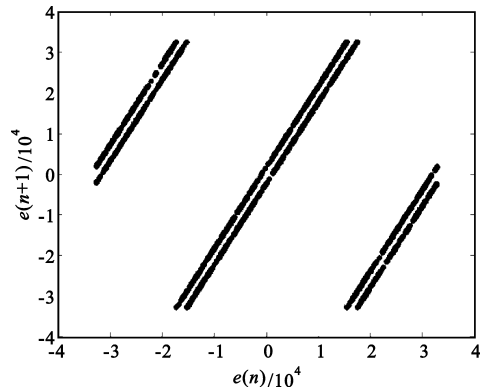
Fig.4 Chaotic digital en-decoder based on nonlinear digital filter

图 4 中左循环移位函数(LCIRC)为 $F(\cdot)$,即乘以 2 并加进位项;所有加、减都以模 2^m 进行运算(m 为字长)。下面对该结构生成的编码信号进行性能分析。

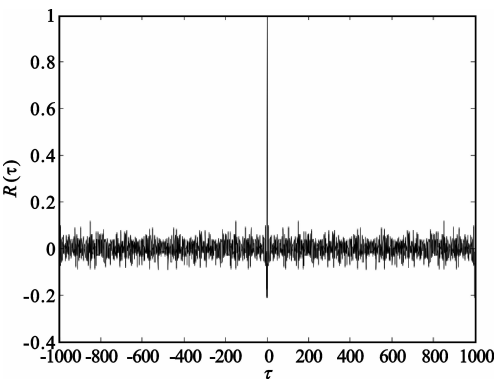
假设输入信号 $u(t) = 5\sin(n\pi/25)$,初始条件 $e(-1) = 0, e(-2) = 1\,000, a_1 = 1, a_2 = 1$,字长 $L = 16$,仿真点数为1 000点。我们可以得到编码器的加密序列、编码信号的相图、自相关函数和互相关函数分别如图 5(a)、(b)、(c)、(d)所示。



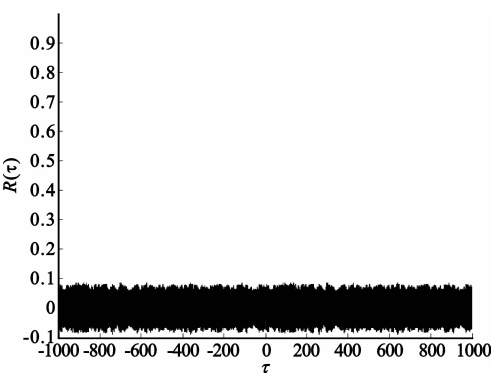
(a)加密序列



(b)编码信号的相图



(c)编码信号自相关函数



(d)编码信号互相关函数

图 5　编码信号的特性

Fig.5 Characteristic of encoded signal

Frey 用频谱、自相关函数和互相关函数等方法深入研究了这一类结构的数字滤波器后指出:该类编码器明显具有 QC 特性,适用于保密通信的需要。并且由于解码器是 FIR 滤波器,所以突发错误不会传播。编码输出传送过程中的一个误码,在解码器端只会引起 3 个突发误码,所以不管起始状态如何,解码器总能锁定到 $e(n)$上,也就是说,即使解码器没有被初始化,经过一个较短的突发误码后,解码器也能精确地恢复出输入序列 $u(n)$,如图 6 所示。

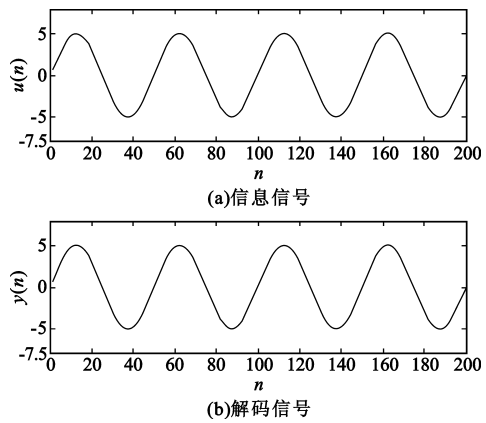


图 6 解码信号与信息信号的比较

Fig.6 Comparison between decoded and original signal

3.2 改进后的数字混沌编解码器

上述数字混沌保密通信方案结构简单,易于实现。但是在一些要求较高的保密通信环境下,这种简单的方法明显存在不足[7-10]。由于解码器在解码前不需要初始化,因此攻击者利用这一特点可以有效地重构出解码器的结构。针对这一缺陷,对上述编 - 解码结构进行了改进,如图 7 所示。改进后的解码器输出 $y(n)$不仅与输入 $e(n)$有关,而且还与初始状态有关。下面对改进的数字混沌编码器的性能加以分析,并与原有结构编码器性能进行比较,仿真条件与上述相同。

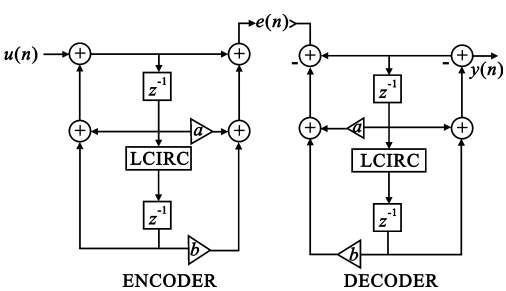


图 7 改进的编解码器

Fig.7 Enhanced encoder and decoder

3.2.1 自相关特性

对于一个性能良好的加密系统,其输出的编码信号应该具有 δ - like 自相关特性,而且编码信号与原始信号的互相关应接近 0。图 8 显示了在相同输入下原有结构和改进结构的归一化自相关函数比较结果,从图中可以看出,改进结构编码信号的自相关特性优于原有结构。

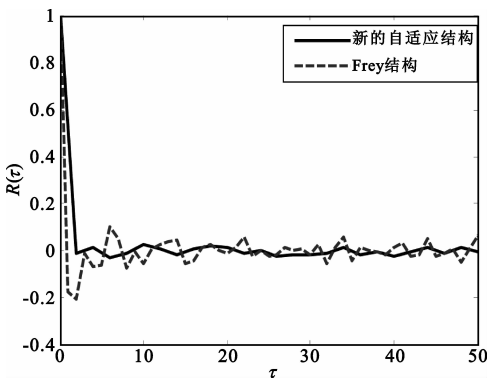


图 8 自相关函数比较

Fig.8 Comparison of autocorrelation function of the encoded sequence

3.2.2 互相关特性

两种结构的编码信号互相关函数比较结果如图 9 所示,从图中可以看出,两者的互相关函数都非常接近于 0。从图 8 和图 9 我们可以知道,改进结构具有更类似噪声的相关特性,更利于保密通信的应用。

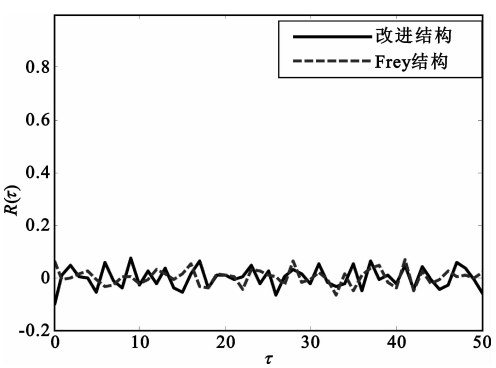


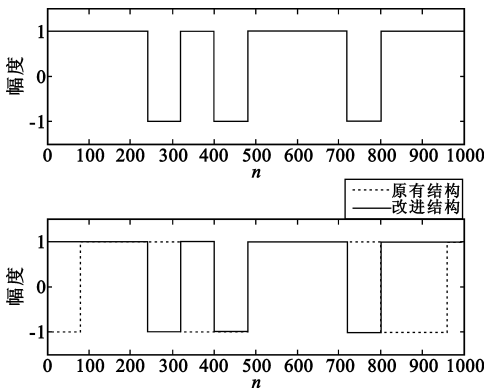
图 9 互相关函数比较

Fig.9 Comparison of crosscorrelation function of the encoded sequence

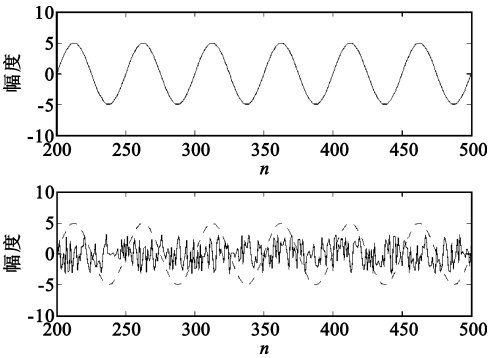
3.2.3 编码器对参数的敏感性

图 10 显示了在解码器初始状态失配时两种结构的解码结果。从图中我们可以看出,原有结构在一小段时间后确实恢复出了原始的信号,而改进结构却得到了完全不同于原始信号的杂乱的解码信

号,这说明改进结构的数字混沌编码器具有更高的安全性。



(a)信息信号为随机序列时的解码效果



(b)信息信号为一正弦信号时的解码效果

图 10　初值不匹配时的解码结果
Fig. 10 Decoding result with no-match of initial value

仿真结果表明,只有当编、解码器的初始状态相同时,解码器才能正确地恢复出信息序列。可以看出,改进后的加密、解密结构比原结构的保密性能更好。

4　结　论

本文首先介绍了数字滤波器中的混沌现象,然后研究了 Frey 建议的数字混沌编码器。在分析 Frey 编码器不足的基础上,提出了改进的数字混沌编码器。仿真实验表明,通过调整解码器的初始状态,只有当解码器的初始条件和编码器的相同时,才能进行正确地解码,使编码器具有更高的保密性。因此,改进后的编码器具有更好的保密性能,更适用于保密通信。但是在加入噪声信号的情况下,数字混沌编码器的解码效果非常不理想,从仿真实验中得到,只有在噪声极其小的情况下方可正确译码。下一步主要就是针对大噪声情况下的解码效果进行研究。

参考文献:

[1] TangY S, Chua L O. Synchronization and Chaos[J]. IEEE Transactions on Circuits and Systems,1983,30(9):620 – 626.

[2] 李辉. 混沌数字通信[M]. 北京:清华大学出版社, 2006:93 – 94.
LI Hui. Chaos digital communication[M]. Beijing: Tsinghua University Press, 2006:93 – 94.(in Chinese)

[3] Newcomb R W. Chaotic generation using binary hysteresis [J]. Circuits System and Signal Processing, 1986,5(3):321 – 341.

[4] Chua L O. Chaos and fractals from third – order digital filters [J]. International Journal of Circuit Theory Applications, 1990,10(18):245 – 255.

[5] Chua L O. Chaos in digital filters[J]. IEEE Transactions on Circuits and Systems,1988,35(6):648 – 658.

[6] Lin T, Chua L O. On chaos of digital filters in the real world [J]. IEEE Transactions on Circuits and Systems, 1991, 38 (5):557 – 558.

[7] Frey D R .Chaotic Digital Encoding: An Approach to Secure Communication[J]. IEEE Transactions on Circuits and Systems,1993,40(10):660 – 666.

[8] Frey D. On adaptive chaotic enclding[J]. IEEE Transactions on Circuits and Systems, 1998,45(11):1200 – 1205.

[9] Zhang J G, Dai X C, Xu P X. Improvement to Frey's Adaptive Chaotic Encoder[C]//Proceedings of the 3rd World Congress on Intelligent Control and Automation. Hefei, China: IEEE,2000:2479 – 2483.

[10] 袁新峰. 刘嘉勇. 一种混沌密码序列的产生及其改进[J]. 电讯技术, 2003,43(2):87 – 90.
YUAN Xin – feng, LIU Jia – yong. Generation and Improvement of a Chaotic Cipher Sequence[J]. Telecommunication Engineering, 2003,43(2):87 – 90.(in Chinese)

[11] 王亚东,张辉,高帆. 混沌跳频序列的设计及其性能检验[J]. 电子元器件应用,2007,9(3):59 – 62.
WANG Ya-dong, ZHANG Hui, GAO Fan. Design and Performance examination of Chaotic Hopping Sequence[J]. Electronic Component & Device Applications,2007, 9(3): 59 – 62.(in Chinese)

[12] 蒋国平,万冬东,薛龙. 超宽带通信中一种新的伪混沌编码器及其解码方法[J].通信学报,2005,26(10): 72 – 76.
JIANG Guo-ping, WAN Dong-dong, XUE Long. New realization scheme of pseudo-chaotic-based encoder and decoder for UWB communications[J]. Journal on Communications, 2005,26(10):72 – 76.(in Chinese)

[13] 覃玉祝, 谢进. 用 MATLAB 进行混沌动力系统的分析[J]. 机械设计与制造, 2010, 7(7): 73 – 75.
QIN Yu-zhu, XIE Jin. Analyse dynamic systems of chaos with MATLAB[J]. Machinery Design & Manufacture,

2010,7(7):73 – 75. (in Chinese)

作者简介:

肖利丽(1984—),女,广西南宁人,2008 年于重庆通信学院获工学学士学位,现为硕士研究生,主要研究方向为抗干扰通信;

XIAO Li-li was born in Nanning, Guangxi Zhuang Autonomous Region, in 1984. She received the B.S. degree from Chongqing Communication Institute in 2008. She is now a graduate student. Her research direction is anti – jamming communication.

Email:610399345@qq.com

何世彪(1963—),男,安徽安庆人,1985 年获解放军工程技术学院工学学士学位,1990 年获南京通信工程学院工学硕士学位,2003 年获重庆大学通信工程学院获工学博士学位,2007 年博士后出站,现为教授、博士生导师,主要研究方向为混沌扩频通信;

HE Shi-biao was born in Anqing, Anhui Province, in 1963. He received the B.S. degree from PLA College of Engineering and Technology, the M.S. degree from Nanjing Communication Engineering Institute, the Ph.D. degree from Communication Engineering Institute of Chongqing University in 1985, 1990 and 2003, respectively. He is now a professor and also the Ph.D. supervisor. His research direction is chaotic spread spectrum communication.

Email: hdoctor@vip.sina.com

田 东(1984—),男,四川渠县人,2007 年于重庆通信学院获工学学士学位,现为硕士研究生,主要研究方向为抗干扰通信;

TIAN Dong was born in Quxian, Sichuan Province, in 1984. He received the B.S. degree in Chongqing Communication Institute in 2007. He is now a graduate student. His research direction is anti-jamming communication.

吴永彬(1984—),男,重庆人,2007 年于安徽电子工程学院获工学学士学位,现为硕士研究生,主要研究方向为军事通信学。

WU Yong-bin was born in Chongqing, in 1984. He received the B.S. degree from Anhui Electronic Engineering University in 2007. He is now a graduate student. His research direction is military communication.