关于数字混沌系统保密通信的探讨 [1]

周 红 罗 杰 凌燮亭

(复旦大学电子工程系 CAT 室 上海 200433)

摘 要 本文对 D. R. Frey(1993) 提出的基于非线性递归数字滤波器的混沌保密通信系统的参数选取、适用条件、抗噪声能力以及保密能力等进行了分析，并采用混沌密码序列来提高该通信系统的保密性。模拟结果表明，该系统具有一定的可靠性和保密性，而且结构简单、容易实现。

关键词 混沌信号，自同步，保密通信，非线性数字滤波器，有限字长效应

中图号 TN918

1 引 言

近几年来， Pecora 和 Carroll[1−4] 的研究结果表明，在一个混沌信号的驱动下，两个混沌系统之间可能达到自同步状态。在这个基础上，利用混沌的自同步特性来实现保密通信的方法得到越来越多的研究，其中主要有混沌掩埋技术 [5−6] 、混沌开关技术 [7−8] 、混沌调制技术 [9] 以及数字混沌通信技术 [10] 等等。尽管如此，混沌保密通信方法还存在下面一些问题：(1) 对连续混沌系统而言，由于电路元件的生产精度有限，参数不可能完全一致，必然导致收发双方混沌系统的差异，从而影响通信的性能。(2) 采用在混沌信号中加入小幅度的原始信号的混沌保密通信技术，为了实现有效的自同步，往往需要原始信号功率相对混沌信号功率很弱，这样，经混沌解密后的信噪比大大降低 [6,11] ；同时，这种方案在原则上可以通过线性滤波器来实现解密，因而还不够保密。(3) 混沌系统的自同步特性允许收发系统的参数存在一定的不同，使得在系统参数大致了解的情况下就可能基本恢复出信号，这必然会降低通信的保密性。

文献 [10] 指出，采用混沌数字编码的系统来进行保密通信，比连续混沌系统更易于实现，而且具有较高的保密性。本文根据文献 [10] 提出的方法，以简单的二阶非线性递归数字滤波器构成了数字混沌保密通信系统，并在这个基础上，分析了通信的各项性能 (包括相关性、抗噪声性、参数灵敏性以及有限字长效应等) 与系统参数的关系，随后引入新的结构来提高通信的保密性能，最后给出了模拟结果。

2 数字混沌保密通信系统

这里的保密通信系统根据 Frey[10] 所给出的结构，用非线性递归数字滤波器实现。对于一般的非线性递归数字滤波器，由于有限字长效应使得其状态数目有限，从而系统表现出有限的周期。然而随着字长的增加，其周期迅速增长，以至超出我们的考虑范围 [12,13] ，这样，在我们的计算能力和存储能力之内，可以将这样的信号看为拟混沌信号。数字混沌加密采用这样一个二阶非线性递归数字滤波器 [10]:

[1] 1994-08-21 收到， 1995-03-08 定稿
国家自然科学基金和上海市重点学科基金资助课题

$$x_s(n) = f(a_s x_s(n-1) + b_s x_s(n-2) + u(n)), \tag{1}$$

这里 $u(n)$ 为原始信号序列，$x_s(n)$ 为滤波输出，函数 $f(\cdot)$ 为非线性函数，其特性如图 1，图中 L 代表字长。

混沌加密的过程在于通过由 (1) 式所构成的非线性滤波混沌系统，将原始信号 $u(n)$ 编码为类似白噪声的混沌加密信号 $x_s(n)$。Chua[12] 指出，对于这类滤波器，在图 2 所示的参数区域 I 内，该滤波器是稳定的；在区域 I 和区域 II 的边界上，滤波的结果表现出自相似的分形状态。通过数值模拟发现，在区域 II 中，特别是其中远离区域 I 的地方，滤波器的输出类似白噪声。

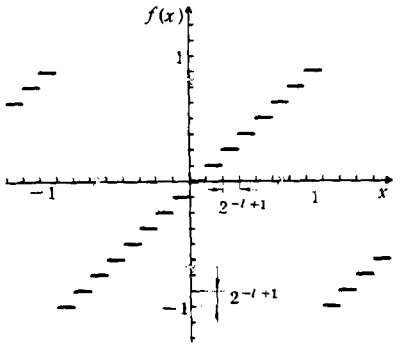

图 1　非线性滤波器的特性函数

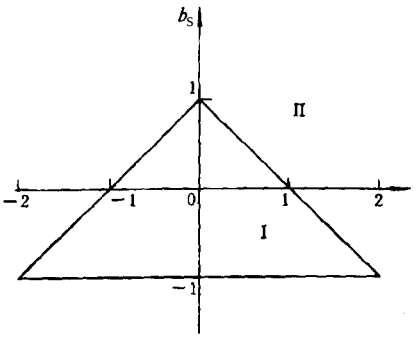

图 2　非线性滤波器的参数区域

解密时采用 (1) 式的逆滤波器：

$$\left.\begin{aligned} u_c(n) &= f(x_r(n) - a_s x_r(n-1) - b_s x_r(n-2)), \\ x_r(n) &= x_s(n) + s(n), \end{aligned}\right\} \tag{2}$$

这里 $x_r(n)$ 为接收信号，$u_c(n)$ 为解密输出，$s(n)$ 为通道的接收噪声。显然，当 $x_r(n) = x_s(n)$，$-1 \le u(n) < 1$ 时，$u_c(n) = u(n)$。这就是数字拟混沌保密通信基本原理。

3　保密通信的各项性能

为了分析和衡量该保密通信的各项性能，将所有信号按发送的最大信号幅度进行归一，得到的原始信号幅度为 A，通信中叠加的噪声的幅度为 B。$(A < 1, B < 1)$

3.1　加密信号的保密性能

为了达到加密的目的，希望加密后的信号自身具有噪声的特性而且与原始信号互不相关，因此我们用相关性来度量通信的保密程度。在 8 位字长下，设输入信号幅度为 0.5、周期为 50 的正弦波，滤波器的初始状态 $x(0) = -0.6135, x(1) = 0.6135$。数值模拟结果表明，在区域 I 内，自相关值和互相关值都很大；从区域 I 的边界向外进入区域 II，相关性逐渐降低；到区域 II 中远离区域 I 的地方，相关性已很弱。为从数量上进行统一的考察，以归一化自相关函数的第二高峰来度量加密输出信号的自相关性，同时以归一化最大互相关值来度量加密前后信号的互相关性，得到图 3 所示结果。另一方面，从系统 $x(n)$—$x(n-1)$ 的相图 (图 4(b)) 来看，在参数区域 I 中，加密后的信号表现得与加密前的信号极为相似；而在 I 与 II 的边界上，加密前后信号仍大致相似 (图 4(c))；区域 II 中，加密后信号的在相图上几乎均匀分布，类似白噪声 (图 4(d))。

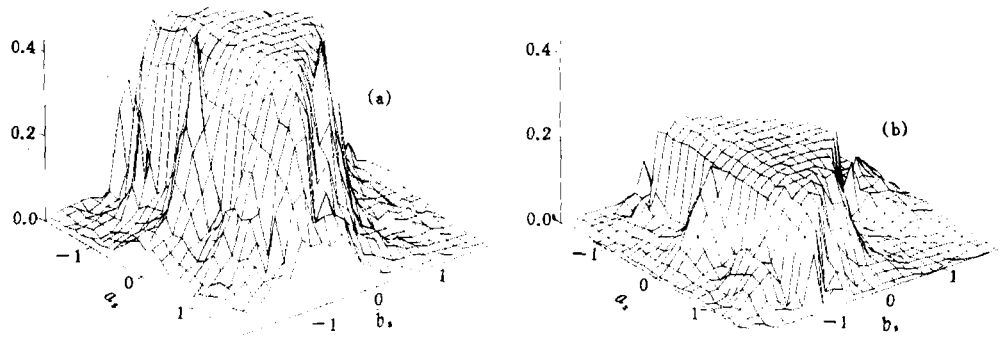

图 3 (a) 加密后信号自相关函数的第二高峰值，(b) 加密前后信号的最大互相关值

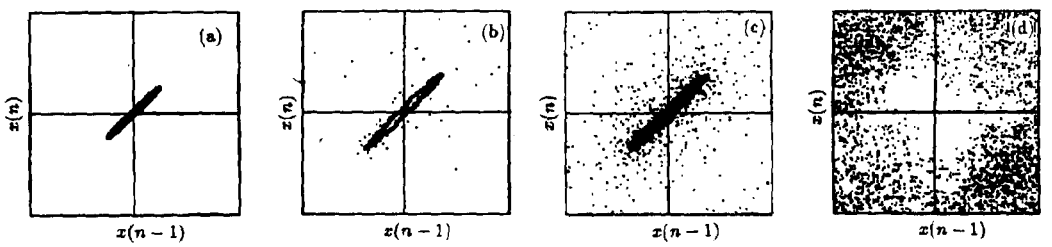

图 4 (a) 原始信号的相图，(b) 区域 I 中加密信号的相图 a_s=0.5,b_s=−0.9,
(c) 区域边界上加密信号的相图 a_s=0.5,b_s=−1.0, (d) 区域 II 中加密信号的相图 a_s=0.5,b_s=−1.1

对于相关性的度量还与不同的输入信号、滤波器的初始状态有关。从 (1) 式可知，当输入信号是短周期序列时，对于某些特殊的初始状态和滤波器参数，加密后的信号可能也是周期的并且与加密前信号强相关。但对于一般非特定的信号和随机的初态而言，这样的情况发生概率很小。从实验结果得出，在 8 位字长下，为了使加密输出具有较好的保密性，滤波器的参数应选择在区域 II 中，必须满足

$$\|a_s\| + \|b_s\| > 1 \quad 或 \quad b_s < -1. \tag{3}$$

3.2 通信的抗噪声能力

对 (1) 式和 (2) 式组成的系统中，不同的参数选取直接影响通信的抗噪声能力，严重的情况下甚至导致 (2) 式与 (1) 式不可逆——这在数字拟混沌保密通信方法的研究中被忽视了 (见文献 [10]) 。这里，将噪声项加入 (2) 式

$$u_c(n) = f(x_s(n) - a_s x_s(n-1) - b_s x_s(n-2) + s(n) - a_s s(n-1) - b_s s(n-2)).$$

结合 (1) 式，即有 $u_c(n) = f(u(n) + s(n) - a_s s(n-1) - b_s s(n-2))$，得

$$\begin{aligned} u_c(n) &= f(u(n) + c + 2i), \\ c + 2i &= f(s(n) - a_s s(n-1) - b_s s(n-2)), \\ c &= s(n) - a_s s(n-1) - b_s s(n-2), \end{aligned}$$

其中 i 为整数，易知 $c \in [-B(1+\|a_s\|+\|b_s\|), B(1+\|a_s\|+\|b_s\|)]$. 为使 (2) 式与 (1) 式可逆，要求当噪声幅度 B 趋于零时 $u_c(n)=u(n)$, 因此必须有 $-1 \le u(n)+c<1$，由此可以得出这类保密通信的实用条件：

$$A+B(1+\|a_s\|+\|bs\|)<1. \tag{4}$$

可以推知，混沌解密过程中导致噪声幅度被放大为 $B(1+\|a_s\|+\|b_s\|)$，为了达到最大信噪比，应满足：

$$\mathrm{SNR}_{\max}=\max\left\|\frac{A}{(1+\|a_s\|+\|b_s\|)B}\right\|. \tag{5}$$

结合保密条件 (3) 式、可逆条件 (4) 式和最大信噪比要求 (5) 式，可以得出，这类保密通信的最大信噪比的上界为 $(1-2B)/2B$ 。从 (2) 式中还可以得知，这类保密通信方法有很好的自同步性能，传输过程中的任何一个瞬时噪声都只影响两个数据。

3.3　对参数的灵敏性

如果解密变换 (2) 式的参数与加密变换 (1) 式的参数存在一定的差异，则会导致通信的系统误差。设加密、解密变换的参数分别为 a_s 、 b_s 和 a_r 、 b_r ，在无噪声情况下，若条件 (4) 式得到满足，同时不存在信号衰落，则可以推知解密误差幅度为 $\|a_s-a_r\|+\|b_s-b_r\|$ 。由此可见，系统参数的微小差异不会对通信的性能影响很大。这种情况下，尽管可以认为该保密通信方式具有较强的鲁棒性；但在另一方面，它降低了通信的保密程度：在 (2) 式参数大致接近原始变换 (1) 式的情况下，就可以基本恢复出原始的信号，如果再采用适当的自适应分析技术，就有可能相当准确地实现破译，甚至还能进一步实施有效的干扰。

3.4　受信号衰落的影响

若在传输过程中存在信号衰落，则从 (2) 式中知，在满足 (4) 式的情况下，它完全等效于参数的减小，因此这里不专门分析由于信号衰落而对通信性能产生的影响。另外，也可以看出，在满足 (4) 式的情况下，由于信号衰落而导致的解密误差只与 (2) 式的参数有关，与原始信号的幅度无关。

3.5　受有限字长效应的影响

从 Chua[12] 的工作中我们看到，在零输入情况下，若滤波器的参数选择在区域 I 的边界，则其输出在相空间出现如图 5(a) 那样的分形现象，其周期随着字长的增加而迅速增大，由此产生的序列类似噪声，Chua 认为当字长达到 16 位时就可以满足需要。在我们的通信方式中，由于工作在区域 II，而不是在 I 的边界，所得到的相关特性比前者更好 (见图 5(b)) 。事实上，为达到同样的相关特性，在混沌区域中产生的序列比在分形区域中产生的序列需要的有效位数更少，因此在混沌区域下进行的保密通信实现起来更为容易。

4　保密性能的改进

根据前面的分析可知，建立在数字混沌系统及其逆系统基础上的加密和解密方案，可以使得变换前后的信号接近线性不相关，从而具有很好的保密作用。然而，这种通信方式由于对参数变化较强的鲁棒性而使得它仍不够保密。对于这种状况，可以在自同步混沌加密的同时采用外加的密码序列，如文献 [10] 中采用的固定周期码。为了达到保密的目的，往往需要外加很长的密码序列，由此又带来密码保存和发送的困难。因此我们考虑在 (1) 式的非线性滤波器中加入另一独立数字混沌信号作为密码序列。根据前面的分析，这类序列可以表现出近噪声的特性，

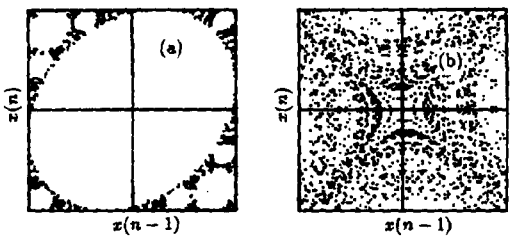

图 5 (a) 分形状态下加密信号的相图 a_s=0.5, b_s=−1.0, A=0
(b) 混沌状态下加密信号的相图 a_s=−0.5, b_s=1.0, A=0

又具有一定的保密性，即使非常小的初始状态的差异也会导致外加混沌密码序列的很大不同；同时，对确定的数字混沌系统而言，以它的初始状态作为密钥，可以完全决定随后的混沌密码序列，因而也不存在序列存储、传送的困难。

5 实验模拟

作为一个例子，我们设原始信号是周期为 50， A=0.5 的正弦波，而所有数字混沌系统，包括加密变换、解密变换和外加混沌密码产生，都采用同样的 8 位字长的二阶非线性递归数字滤波器，其参数为 a_s=0.3,b_s=1.0 。图 6— 图 8 分别表示通信的相关特性、抗噪声特性以及对于外加混沌密码的密钥的敏感性。

6 结 论

通过以上的分析和实验模拟可以看出，建立在有限字长数字混沌系统下的保密通信方法，与目前基于连续信号的方法相比，具有明显的优点：在数字系统实现中，不必考虑连续系统中

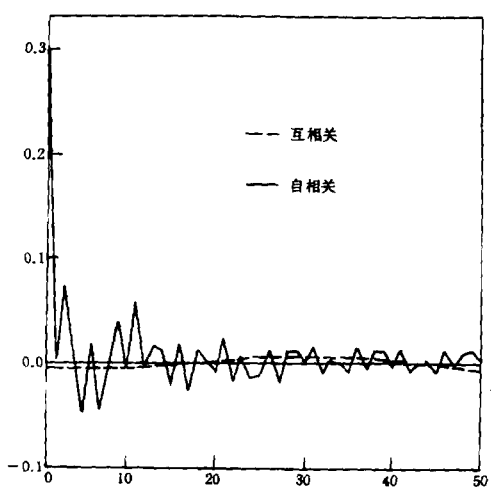

图 6 加密后信号的自相关函数和信号加密前后的互相关函数

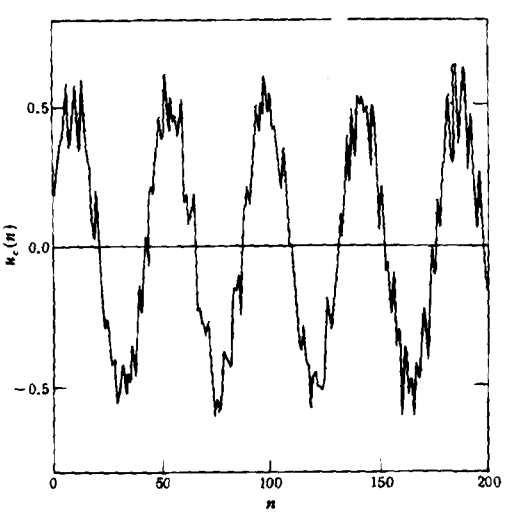

图 7 噪声对解密的影响 B=0.10

存在的参数离散的问题；其次，它不必象连续混沌系统中那样，为了同步条件而苛求很小的信号幅度，因此解密端可以得到较大的信噪比；同时，它具有很强的自同步能力，对于任何瞬时噪声，只会影响极为有限的时间。此外，根据前面的数值模拟，我们还可以看到，在特定的参数区域中，通过数字混沌系统加密前后的信号可以达到弱相关，再结合由简单密钥产生的非自同步混沌密码，能提高通信的保密能力，克服目前在自同步混沌保密通信中普遍存在的潜在不保密性。

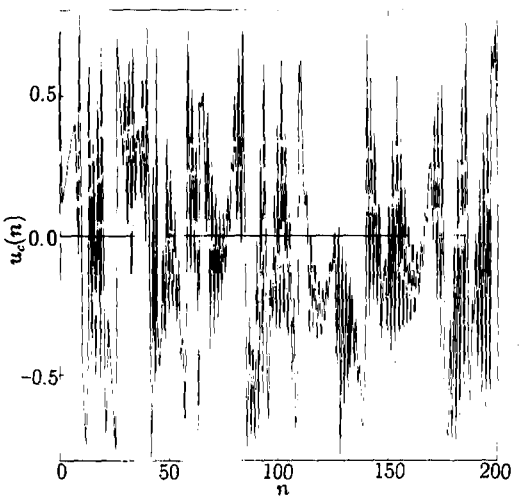

图 8　在外加混沌密码的密钥与加密密钥存在微小差异下的解密信号
加密初态 (密钥) $x_s(1)$=0.5, $x_s(0)$=0;
解密初态 (密钥) $x_s(1)$=0.5, $x_s(0)$=0.008

参　考　文　献

[1] Pecora L M, Carroll T L. Synchronization in chaostic systems. Phys. Rev. Lett., 1990, 64(8): 821–824.

[2] Pecora L M, Carroll T L. Driving systems with chaostic signals. Phys. Rev. A., 1991, 44(4): 2374–2382.

[3] Pecora L M, Carroll T L. Synchronized chaotic signal and systems. in Proc. 1992, IEEE ICASSP.

[4] Carroll T L, Pecora L M. Synchronization in chaotic circuits. IEEE Trans. on CAS, 1991, CAS-38(4): 453–456.

[5] Cuomo K M, Oppenheim A V, Strogatz S. H. Synchronization of Lorenz-based chaotic circuits with applications to communications. IEEE Trans. on CAS, 1993, CAS-40(10): 626–633.

[6] Kocarev L, Halle K S, Eckert K, *et al.* Experimental demonstration of secure communications via chaotic synchronization. Int. J. Bifurcation & Chaos, 1992, 2(3): 709–713.

[7] Parlitz U, Chua L O, Kocarev L, *et al.* Transmission of digital signals by chaotic synchronization. Int.J. Bifurcation & Chaos, 1992, 2: 973–977.

[8] Dedieu H, Kennedy M P, Hasler M. Chaos shift keying: Modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuits. IEEE Trans. on CAS, 1993, CAS-40(10): 634–643.

[9] Halle K S, Wu C W, Itoh M, *et al.* Spread spectrum communication through modulation of chaos. Int. J. Bifurcation & Chaos, 1993, 3(2): 469–477.

[10] Frey D R. Chaotic digital encoding: An approach to secure communication. IEEE Trans. on CAS, 1993, CAS-40(10): 660–666.

[11] Cuomo K M, Oppenheim A V. Chaotic signals and systems for communications. Proc. IEEE ASSP Conf., Minneapolis, MN: 1993, III:137–140.

[12] Lin T, Chua L O. On chaos of digital filters in the real world. IEEE Trans. on CAS, 1992, CAS-38(5): 557–558.

[13] Chua L O, Lin T. Chaos in digital filters. IEEE Trans. CAS, 1988, CAS-35(6): 648–658.

RESEARCH ON DIGITAL CHAOTIC SYSTEM FOR SECURE COMMUNICATION

Zhou Hong Luo Jie Ling Xieting

(*Dept. of Electronic Engineering, Fudan University, Shanghai* 200433)

Abstract The chaotic secure communication method proposed by D. R. Frey (1993) is studied. The system is composed of regressive nonlinear digital filters. Several practical aspects of the communication are analyzed, such as the correlation functions, the tolerance to noise, the sensitivity to parameter mismatches and the effect of finite word length, etc. Another chaotic system is introduced to increase the security of the communication. Simulation result shows that the method is secure and easy to realize.

Key words Chaotic signal, Self-synchronization, Secure communications, Nonlinear digital filter, Effect of finite word length

周 红： 男，1969 年生，博士，从事于神经网络、模糊控制、时间序列分析以及混沌理论及应用等领域的研究.

罗 杰： 男，1972 年生，硕士，从事于混沌理论及应用研究.

凌燮亭： 男，1932 年生，博士生导师，从事模拟 VLSI 系统设计、神经网络、电路 CAD 和参数容差分析与设计方面的研究.