一种可逆非线性混沌保密通信系统研究

朱灿焰[①] 郑毓蕃[②]
[①](苏州大学电子信息工程学院 苏州 215021)
[②](墨尔本大学电子电气工程系)

摘 要 该文分析了现有各类混沌保密通信技术的基本原理及其特点，并分别介绍了一些有实用价值的典型结构，比较了它们各自在实际应用中的性能和不足。在此基础上，提出了一种基于混沌驱动的零动态可逆离散非线性混沌通信系统。重点模拟分析了该系统的安全可靠性，防信息攻击能力，以及抗信道噪声干扰性能等，并指出了系统同步的必要性和解决途径。

关键词 混沌通信，加密，零动态，可逆非线性
中图分类号：TN918 **文献标识码**：A **文章编号**：1009-5896(2006)04-0721-07

Researching on Performances of an Invertible Nonlinear Chaotic Communication System

Zhu Can-yan[①] Zheng Yu-fan[②]
[①](*School of Electronics and Information Engineering*, *Soochow University*, *Suzhou* 215021, *China*)
[②](*Dept. of EEE*, *the Univ. of Melbourne*, *Parkville, VIC*3052, *Australia*)

Abstract All the existing chaotic communication techniques are simply classified into two catalogues，their implementation principles and characteristics are outlined，the corresponding valuable realizing schemes are introduced for comparing their advantages and disadvantages in application. Then a zero dynamical nonlinear invertible communication scheme with chaos driving is proposed. Its performances，such as encryption security，defending ciphertext attack， noise robust，etc. are extensively analysed by simulation. Its necessity to synchronization for application and the way to solve the problem are also discussed.

Key words Chaos communication，Encryption，Zero dynamics，Invertible nonlinearity

1 引言

混沌信号具有明显的宽带白噪声特点；可由非线性动态系统产生且很容易控制；动态系统不同初始状态所产生的混沌信号之间相互正交且独立[1]，因此，混沌信号在保密技术中得到了广泛应用[2-5]。在通信技术中应用混沌信号进行扩频、调制、加密等，自然而然地使通信系统继承了混沌信号的一些优点，故混沌保密通信也有着非常诱人的实际应用前景。然而，正是混沌信号表现出对系统初始状态的高度敏感性，使其作为通信信号的载体具有一定的困难，需要保证通信系统收发双方的严格混沌同步[1, 6]。直到 20 世纪 90 年代初，混沌同步试验取得初步成功[7]，并随着混沌同步技术研究的不断深入，混沌保密通信技术研究才得到强力关注。特别是近十多年来，由于计算机网络技术的不断发展，信息传播的速度和信息量越来越大，网络通信保密技术越来越受到重视；混沌保密通信作为一种有效的信息保密通信技术，必然成为了国际上发达国家争相研究的热点[8,9]。

本文首先分析了现有一些混沌通信技术及其特征，然后给出一种基于非线性零动态系统的可逆混沌通信方法。与众多现有数字混沌保密通信方法完全不同，该方法对原信息的加密过程是将原信息作为非线性混沌系统中的线性时变因子，自动改变和控制混沌加密信号的形成，这种变换是非线性时变的。原始信息既可以是数字符号信息也可以是数字量值信息，根据输出保密信息的编码结构决定。通过详细模拟分析，给出了有相当实用价值的结论。

2 混沌通信技术原理

尽管早在 60 年代初就已经知道混沌信号和系统的特点具有通信技术所要求的特征，但是混沌信号在通信技术中的应用主要局限在混沌编码技术上[2]。随着现代移动通信对具有自相关性随机码序列的不断需求，混沌信号产生技术、加密技术和同步技术得到了进一步研究，一些新的混沌通信系

2004-09-27 收到, 2005-04-07 改回
CSC，澳洲 ARC 和香港 CERG Grant CityU1115/03E 资助课题

统和方法不断涌现。它们主要分成二类，即混沌遮掩和混沌调制，以及这二种方法的混合。

2.1 混沌遮掩

混沌遮掩通信方法也称之为混沌覆盖[10]。混沌遮掩通信技术因其加密过程简单，是最早被研究的一种混沌保密通信技术。其基本思想是利用混沌信号的频域特性将其作为一个载体，将所要传输的信息特征掩盖起来一起传送，在接收端再将混沌信号消除，恢复出原信息。由于混沌信号的宽带白噪声特征，使得窃收者接收后很难从其频域或时域中分析出或找寻到信息特征，并被认为是噪声信号，从而起到保密通信效果。

尽管混沌遮掩加密技术原理简单，但加密信息的能量相对较小，因而噪声鲁棒性较弱，另外，实际混沌遮掩通信系统的具体电路一般比较复杂，用以满足收发双方严格混沌同步的解密要求[11]。事实上，因为信道噪声和信道衰落的不可避免，不可能满足这一理想要求，因此，这一技术主要应用在信道环境比较理想的光纤保密通信实验中。

2.2 混沌调制

混沌调制就是利用被传输信息来控制改变产生混沌信号的系统参数，以达到混沌保密通信的目的[6]。混沌调制方法主要以混沌开关技术和非线性动力学混沌系统调制技术为主。

2.2.1 *混沌开关* 最早提出混沌开关(CSK)技术是在 90 年代初[12]，其基本原理是将二进制信号映射成相应混沌基信号，并利用混沌基的相关独立性，实现混沌解调。该技术可以采用传统相干和非相干检测技术进行解调，从而避开了混沌遮掩技术所要求的严格混沌同步限制，但这类保密通信方法的抗破译性能较弱。此外，CSK技术还存在难以克服的两个问题: 即混沌基函数复原问题和位能估计问题[13, 14]。特别是位能估计问题，因为混沌函数的非周期性和随机性，使位能估计值是服从一定分布的随机量，其值是非零的，因而严重影响到相干解调的误码率[14]。另外，采用相干解调的CSK系统仍然存在混沌渐近同步问题。为了改善系统的位能估计问题，在CSK基础上提出了差分混沌开关(DCSK)技术[15]。虽然DCSK在理想状态下使位能估计值为常数，但信道存在噪声时，位能估计问题仍然存在。另外，DCSK在信噪比改善方面也存在一定的限制[14]。

考虑到传统调频(FM)信号中的瞬时功率与调制信号无关，相对于载波，调制信号对信号功率的影响是很小的[16]，由此提出了调频差分开关(FM-DCSK)技术[17]。该方法的基本原理是在DCSK之后再进行FM过程，而在接收端先行鉴频之后直接进行相干或非相干混沌解调。FM-DCSK方法克服了位能估计问题，较好地兼顾了系统误码率和传输速率的要求，对多径效应有较好的抑制效果。并随着混沌开关技术的进一步完善，其抗破译性能也将进一步加强。

2.2.2 *非线性动力学混沌调制* 非线性动力学混沌调制系统展示了混沌容易产生和控制的优越性，同时，系统对混沌初始状态的敏感性比前述系统强，因此，这类系统的混沌加密性能最好。混沌调制又称之为宽谱发射，其基本原理是将信息通过非线性映射，由此改变非线性混沌系统的动态特性，达到信息信号调制发射的目的，在接收端基于一定的同步或控制机制，并通过逆映射函数关系实现解调。采用不同的映射方法或不同的非线性动力学系统，以及建立不同的同步或控制机制，使这类方法的结构模型层出不穷。因此，这类调制方法的研究在混沌保密通信领域最为活跃。

根据信息调制方式，混沌动力学通信系统可以分成两类[18]，即基于混沌同步和基于混沌控制的非线性动力学系统．前者的关键是混沌同步技术，且需要另加激励信息能量控制，使发送信号的信噪比较低，干扰鲁棒性弱[19]。非线性动力学系统的同步问题实际上也是一个控制问题[20]。基于反馈控制的混沌动力学系统[18]，通过控制混沌轨迹可以使得混沌振子携带信息，以实现混沌调制。符号动力学的控制依赖于混沌振子的符号描述，通过坐标变换，可以在时间上实现从相空间到子变换空间上的抽象映射，而少量参数的反馈控制可以敏感地改变混沌轨迹。所以，将信息的变化映射为相空间上混沌振子坐标位置的变化，进而控制混沌轨迹。这样，非线性动力学相对应的混沌轨迹的变化，包含了需要传输的信息内容，从而实现了混沌调制。

3 可逆零动态混沌通信系统结构

不同于一般同步控制离散非线性动力学系统，基于混沌驱动的零动态离散非线性系统的一般形式如下:

$$\left.\begin{aligned} x_c[k+1] &= f(x_c[k]) \\ x[k+1] &= q(x_c[k], x[k]) + g(x_c[k], x[k], u[k]) \\ y[k+1] &= h(x_c[k], x[k]) \end{aligned}\right\} \tag{1}$$

式(1)中，$u[k]$为激励信息信号；$f(x_c[k])$包含一个或多个选定的混沌动态子系统，其状态$x_c[k]$作为非线性系统的另一激励；$x[k]$为零动态非线性加密系统状态。变换$f(.)$为混沌映射；变换$q(.)$和$g(.)$均为零动态过程，其中$g(.)$实现信息信号$u[k]$的非线性调制，从而实现混沌加密；函数$h(.)$则为混沌加密系统调制器，实现混沌加密信息调制输出。在$h(.)$满足正定和可观测条件下，该系统是稳定和左逆的[21]，故利用逆变换$h^{-1}(.)$，在系统同步条件下实现接收信号的混沌解调。基于可逆零动态混沌离散通信系统的基本结构如图 1 所示。

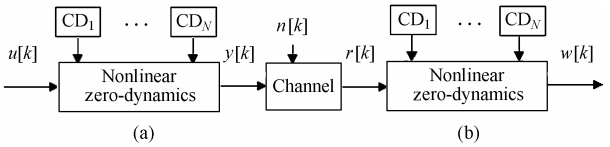

图 1 可逆零动态非线性混沌通信系统原理图

(a)发射部分 (b)接收部分

Fig.1 Principle of chaotic communication system with invertible nonlinear zero-dynamics

从图 1 中可以看出，发射部分的调制器与传统非线性调制器不同，它在信息信号和混沌动态子系统的共同驱动下进行非线性加密，实现混沌调制；由于零动态加密系统存在对应的零动态解密系统，且结构形式相似，因而在软硬件实现中均可进行模块化设计。为了检验上述方法的具体性能，我们构建了混沌通信系统，具体形式如下.

$$\left.\begin{aligned} &x_{c1}[k+1]=-3x_{c1}[k]+4x_{c1}^3[k]\\ &x_{c21}[k+1]=1+0.3x_{c22}[k]-1.4x_{c21}^2[k]\\ &x_{c22}[k+1]=x_{c21}[k]\\ &x[k+1]=\frac{1}{2}(x_{c1}[k]-x[k]x_{c1}[k])+\frac{1}{2}x_{c21}[k]u[k]\\ &y[k]=x[k] \end{aligned}\right\} \tag{2}$$

初始状态为 $x_{c1}[0],\begin{pmatrix}x_{c21}[0]\\ x_{c22}[0]\end{pmatrix}$。

很容易验证系统式(2)是左逆的。混沌驱动系统含有两个混沌动态系统，其状态变量分别是x_{c1}和 $x_{c2}=\begin{pmatrix}x_{c21}\\ x_{c22}\end{pmatrix}$。令 $z_{c1}[k]=x_{c1}[k]$，$\begin{pmatrix}z_{c21}\\ z_{c22}\end{pmatrix}=\begin{pmatrix}x_{c21}\\ x_{c22}\end{pmatrix}$，可得到式(2)的最小左逆系统具体形式如下：

$$\left.\begin{aligned} &z_{c1}[k+1]=-3z_{c1}[k]+4z_{c1}^3[k]\\ &z_{c21}[k+1]=1+0.3z_{c22}[k]-1.4z_{c21}^2[k]\\ &z_{c22}[k+1]=z_{c21}[k] \end{aligned}\right\} \tag{3}$$

$$w[k]=\frac{2r[k]-z_{c1}[k-1]\big(1-r[k-1]\big)}{z_{c21}[k-1]} \tag{4}$$

为了消除极值情况出现，逆动态系统模型式(4)修改为

$$w[k]=\begin{cases}\dfrac{2r[k]-z_{c1}[k-1]\big(1-r[k-1]\big)}{z_{c21}[k-1]}, & |z_{c21}[k-1]|>\varepsilon\\ w[k-1], & |z_{c21}[k-1]|\le\varepsilon\end{cases} \tag{5}$$

初始状态已知为 $z_{c1}[0],\begin{pmatrix}z_{c21}[0]\\ z_{c22}[0]\end{pmatrix}$。

系统式(2)和对应的最小左逆系统式(4)和式(5)中，$u[k]$和$x[k]$，k=0，1，2，…，分别表示原信息和加密激励信号，$y[k]$，$k\ge0$为需要传输的混沌加密信号。接收端接收到的混沌加密信号用 $r[k]$ 表示，通常它含有信道噪音等干扰信息。$w[k]$为混沌解密后的信息。$z_{c1}[k]=x_{c1}[k]$和$z_{c21}[k]=x_{c21}[k]$，$z_{c22}[k]=x_{c22}[k]$分别为Cubic和Henon混沌模型[22]。众所周知，当初始状态值$x_{c1}[0]$和$x_{c21}[0]$，$x_{c22}[0]$分别满足一定条件时，$x_{c1}[k]$和 $x_{c21}[k]$，$x_{c22}[k]$均表现出混沌现象。例如，$x_{c1}[0]$在区间(－1，1)上取值时，$x_{c1}[k]$，$k\ge0$为混沌波形；$x_{c2}[0]$处在图2所示的取值域时，则$x_{c2}[k]$，$k\ge0$也同样具有混沌现象[22, 23]。

根据系统式(2)和相应逆系统式(4)的结构形式，在知道混沌初始状态和系统同步之后，混沌驱动信号可以在本地直接产生，因而，解密系统相对简单；另外，零动态左逆系统具有最小递推阶数，因而其实现的实时性理想，硬件所需存储单元少；在通信系统设计中，由于激励系统(发射部分)和左逆系统(接收部分)中的混沌激励相同，故便于硬件标准模块化设计，从而简化通信系统构成，实现系统通信过程的有效性。

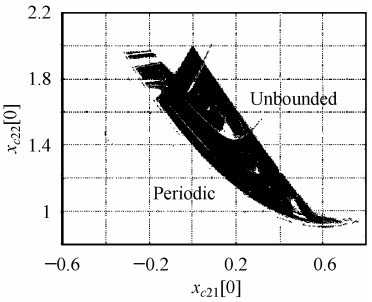

图 2　Henon 模型的混沌状态映射空间

Fig.2　Chaotic region for the Henon attractor

4　系统性能分析

4.1　加密安全可靠性分析

图 3 给出了原信息时域波形和频谱，以及根据本文方法所设计的混沌加密系统得到的混沌加密波形和频谱。图 3 中，原始信息是一段语音信号，该语音信号为标准的wav格式文件的记录. 其抽样速率为 22050Hz，即抽样点k之间的间隔为45.35147μs。加密信号为系统式(2)的输出，系统初始状态为$x_{c1}[0]$=0.15，$x_{c21}[0]$=0.1，$x_{c22}[0]$=0.1，以及初始值$x_1[0]$=0.15001。比较图 3(a)，3(c)和 3(b)，3(d)，可以看出加密信号的时域波形是混沌的，它的频谱为宽带白谱，具有白噪声特性。因而，一般侦听者会认为是噪声信号而将加密信号丢弃，从而起到了保密作用。

对照比较图3 (a)、3(c)和图3(b)、3(d)可以看出，无论是时域波形还是频谱分布，原信息在加密信号中的残留信息极少，时域和频域均难以被侦测到。因为语音信号主要能量分布在2kHz之内，进一步将原信息和加密信号的频谱在0~2kHz间放大，见图4。仔细比较不难发现，在原信息主要能量分布的频点及其周围，对应的加密信号频谱没有原信息的任何痕迹。因此，采用传统信号分析方法难以侦测到通信信号中原信息痕迹。

在众多现有数字混沌保密通信方法中，基本原理都是将数字符号变换成对应的混沌波形。而接收系统中，解密过程利用混沌基信号相互正交的特性，根据接收信号自相关结果的幅值来进行阀值判决，从而解密出原始信息。但是，本文方法所设计的零动态混沌激励模型对原信息的加密过程与传统方法完全不同，原信息作为非线性混沌系统中的线性时变因子，自动改变和控制混沌加密信号的形成，这种变换是非线性时变的。原始信息既可以是数字符号信息也可以是数字量值信息，根据输出保密信息的编码结构决定。在相同初始状态条件下所产生的加密信号其自相关函数具有显著的单线尖峰特性，不同初始状态条件下的加密信号是相互正交的，它们的互相关函数具有平缓的特性没有尖峰值出现。然而，系统式(2)在某一初始状态输入下，将递推出加密信号。图5(a)和图5(b)是利用系统式(2)所产生的加密信号的自相关函数和互相关函数。

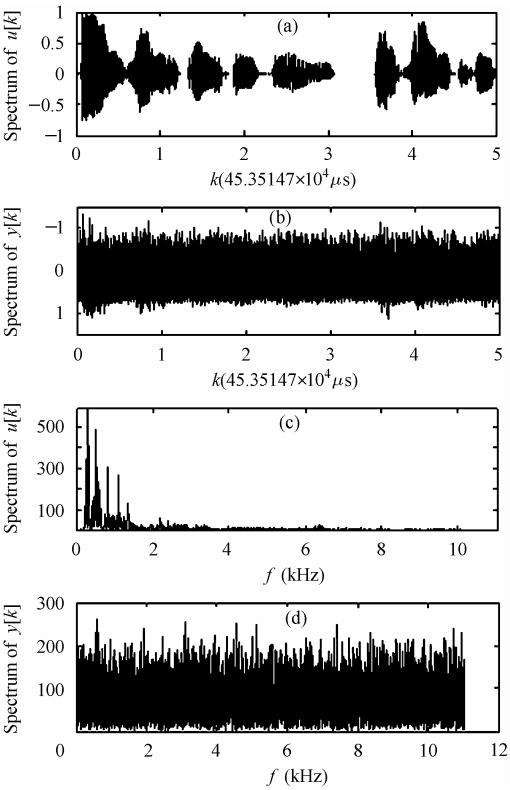

图3 原信息和加密信号的波形和频谱

(a), (b) 分别为原信息和加密信号的波形, 抽样点k之间的时间间隔为45.35147μs; (c), (d) 分别为原信息和加密信号的频谱

Fig.3 The original and encrypted waveform and their spectra

(a), (b) are respectively original and encrypted waveforms. The duration between sampling points k is about 45.35147μs; (c), (d) are spectra of correspondingly original and encrypted waveforms

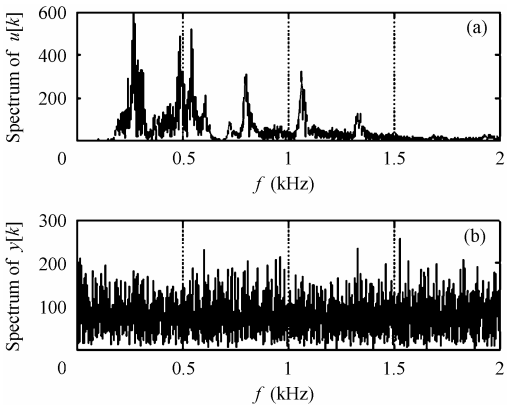

图4 原信息谱和加密信号谱的局部放大图

(a)和(b)分别是Fig. 3(c)和3(d)对应频段的放大图

Fig.4 The zoomed figures of corresponding spectra of original and encrypted waveforms.

(a), (b) are respectivelyzoomed figures of Fig.3 (c) and 3(d).

图5(a)是初始状态值$x_{c1}[0]=0.15$，$x_{c21}[0]=0.1$，$x_{c22}[0]=0.1$时加密信号的自相关特性；图5(b)是初始状态$x_{c1}[0]=0.15$，$x_{c21}[0]=0.1+10^{-11}$，$x_{c22}[0]=0.1$时的加密信号与图5 (a)所对应的加密信号之间的互相关特性，不同初始状态下加密的原始信息是一样的。其他初始状态值的测试模拟结果完全相同，因篇幅所限，在此省略。尽管初始状态仅仅只是$x_{c21}[0]$相差10^{-11}，但是，所得到的加密信号有明显的正交特性，即根据不同初始状态值所产生的加密信号是相互独立的。图5 所示的正交特性非常适用于多用户环境下的通信，如CDMA通信和WLAN无线接入[24]。与伪随机码扩频通信相比较，图5 的正交特性具有更好的保密安全，随着信号长度的增大，这种优越性更加明显。

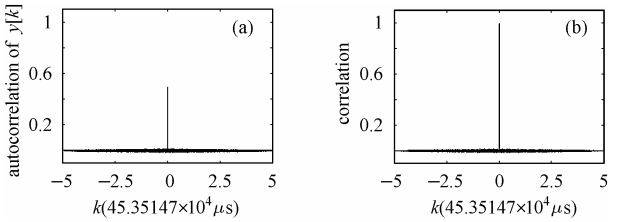

图5 加密信号的自相关函数和互相关函数

(a)是初始状态$x_{c1}[0]=0.15$, $x_{c21}[0]=0.1$, $x_{c22}[0]=0.1$时加密信号的自相关函数; (b)是(a)所对应加密信号与仅xc21[0]相差10^{-11}所对应加密信号之间的互相关函数

Fig.5 The autocorrelation and correlation of encrypted signals

(a) the autocorrelation of encrypted signal with initial states $x_{c1}[0]=0.15$, $x_{c21}[0]=0.1$, $x_{c22}[0]=0.1$; (b)the correlation between encrypted signal of (a) and that with 10^{-11} bias to $x_{c21}[0]=0.1$

事实上，混沌驱动模型对初始状态值是非常敏感的。尽管混沌激励信号模型和混沌保密通信模型可以公开获得，但是，在初始状态取值范围满足一定条件时，窃听者很难破译出原信息。所以，可以将初始状态值$x_{c1}[0]$， $x_{c21}[0]$， $x_{c22}[0]$作为不同加密过程的密钥，或者通信双方相互保持正确加解密的PIN码。图6是在无通道噪声时，左逆系统式(3),式(4)分别使用正确初始状态和非正确初始状态时解密出的信息波形和频谱。

图6(a)和图6(c)是在PIN码与加密过程的初始状态值完全相同时，即$z_{c1}[0]=0.15$， $z_{c21}[0]=0.1$， $z_{c22}[0]=0.1$时得到的解密信息的时域波形和频谱; 图6(b)和图6(d)则是左逆系统在初始状态值$z_{c1}[0]=0.15+10^{-11}$，$z_{c21}[0]=0.1$，$z_{c22}[0]=0.1$时解密出的信息波形及频谱。ε的取值均为10^{-12}。不难看出，尽管只有PIN码中初始状态$z_{c1}[0]$出现10^{-11}的偏差，但解密出的信号仍呈现混沌状态。因此，左逆系统使用的初始状态与激励系统存在任何微小的偏差，均会导致解密结果保持混沌现象不变。仿真结果说明，窃密者即使知道通信系统的模型或结构，但仍很难估测出准确的PIN码，从而无法威胁保密通信系统的安全。根据密码理论，加密密码空间至少需要10^{30}大小[23]。本文模拟结果是在16浮点数精度下取得的。以16位浮点数精度计算，因本系统具有3个初始状态，并根据对应的混沌区间范围，实际上本文系统的密码取值空间大于10^{100}，因此，足以对抗强力攻击。需要强调的是，图6是在保持激励系统和左逆系统中零动态混沌信号序列同步的情况下得到的。

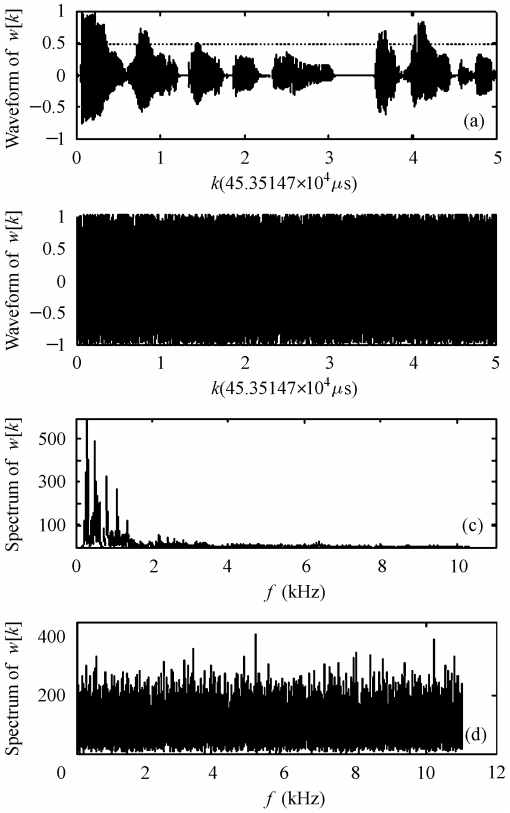

图6　无噪声时的解密信息(取$\varepsilon=10^{-12}$). (a)和(c)分别是用正确PIN码解密的信息波形和频谱; (b)和(d)是在初始状态$z_{c1}[0]$与原值存在$+10^{-11}$偏差时解密的信息波形和频谱.

Fig.6 Decryptions with no noise while $\varepsilon=10^{-12}$. (a) and (c) are decryption waveform and its spectrum with correct PIN codes; (b) and (d) are decryption waveform and its spectrum with $+10^{-11}$ bias of $z_{c1}[0]$ to its original state

4.2 抗信息攻击能力

加密信息的攻击者除采用密钥攻击外，还可对加密信息内容进行相关统计分析，从而找出原始信息的痕迹，经特殊滤波器破译有用信息。不同信息内容，相互之间不是完全独立的，特别是相同种类的原始信息之间存在较强的联系。

如图 7(a)所示为两段语音信号之间的互相关特性；图 7(b)为对应相同初始状态下不同原信息的加密信号的互相关特性。明显可以看出：原信息之间具有很强的相关性，有一定的语音信号特征。而加密信号之间的相关性完全独立。在初始状态完全相同时，其互相关性与加密信号的自相关函数相同；如果不同信息加密时的初始状态不同，则其互相关性与图 5(b)完全相同，因而不同加密过程之间具有高度的独立性．所以，信息经本文方法加密后，窃译者几乎不可能从信号之间的相关分析寻找到攻击点。

事实上，本文方法的加密过程，已将原始信息幅度分布的概率统计特性均匀化。图 8 所示为加密前后信号幅值分布统计特性曲线。从图 8 可以看出，原始信息的幅度概率统计分布特性呈现出明显的不均匀性，信息内容在低幅度上出现的概率高；而从加密信号的幅度统计特性可以看出，其信号幅值分布的平化状态已经大大改善，因而其信号特征不明显，从而达到了保密安全的目的。

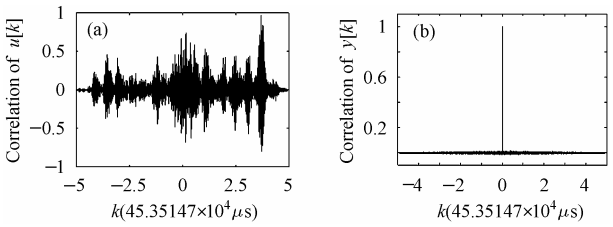

图7　原语音信息及其加密信号的相关统计分析结果
(a)是两段语音信息的相关统计特性
(b)为对应加密信号的相关统计特性

Fig.7 The correlations of original and corresponding encrypted messages (a) the correlation between two pieces of original message (b) the correlation between the two pieces of corres pondingly encrypted message

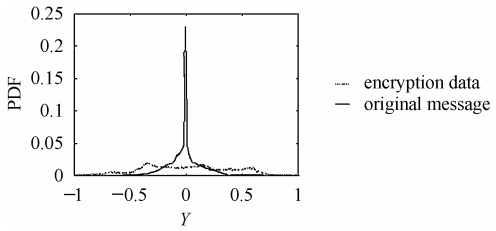

图8　原始信息和加密信号的幅度分布统计特性

Fig.8 The characteristics of amplitude statistical distribution for original and encrypted signals

4.3 抗噪声特性

作为通信系统，首先需要面对的是信道噪声问题。本文方法构造的可逆混沌通信系统是否具有噪声鲁棒性，体现在左逆接收部分对初始值$r[0]$是否敏感。事实上，信道中的噪声是无法避免的。在式(5)中，我们已经根据系统计算精度设定了界限，可以证明：只要$1/|z_{c21}[k]|$是有界的，则原信息$u[k]$总能从含有信道噪声的混沌加密信号 $r[k]$ 中有效恢复出来[21]。设接收信号存在信道加性高斯白噪声，则有

$$r[k]=y[k]+n[k] \tag{6}$$

代入式(4)，有

$$\begin{aligned} w[k]&=\frac{2r[k]-z_{c1}[k-1]\big(1-r[k-1]\big)}{z_{c21}[k-1]}\\ &=\frac{2(y[k]+n[k])-z_{c1}[k-1](1-y[k-1]-n[k-1])}{z_{c21}[k-1]}\\ &=\frac{2y[k]-z_{c1}[k-1](1-y[k-1])}{z_{c21}[k-1]}\\ &\quad+\frac{2n[k]+z_{c1}[k-1]n[k-1]}{z_{c21}[k-1]} \end{aligned} \tag{7}$$

所以，逆系统输出噪声为

$$e[k]=\frac{2n[k]+z_{c1}[k-1]n[k-1]}{z_{c21}[k-1]} \tag{8}$$

因为激励混沌信号的幅值范围在(－1，+1) ，则有

$$\varepsilon^{-1}n[k]<e[k]<3\varepsilon^{-1}n[k] \tag{9}$$

很显然，逆系统的噪声是有界的。但是，$\varepsilon^{-1}>>1$，故系统输出噪声得到了放大。然而，输出解密信号的信噪比为

$$\mathrm{SNR}_w = 20\lg\left|\frac{w[k]}{e[k]}\right| = 10\lg\frac{\mathrm{var}\{2y[k]-z_{c1}[k-1](1-y[k-1])\}}{\mathrm{var}\{2n[k]+z_{c1}[k-1]n[k-1]\}} \quad (10)$$

因为噪声与混沌激励信号是相互独立的，$\mathrm{var}\{z_{c1}[k]\}=1$，所以

$$\mathrm{SNR}_w = 10\lg\frac{3\sigma_y^2+1}{3\sigma_n^2} \quad (11)$$

式中σ_y是发射混沌加密信号$y[k]$的标准均方差; σ_n是信道加性高斯白噪声的标准均方差。故解密信息的信噪比并没有恶化，具有一定的鲁棒性。图9给出了其信噪比SNR为25dB时得到的解密信息波形。其中信噪比SNR定义为

$$\mathrm{SNR}=20\lg(\sigma_y/\sigma_n) \quad (12)$$

式中σ_y和σ_n的意义同式(10)。

图9(a)中解密信号是经过了截止频率为3kHz的低通滤波器的输出，尽管信息波形被背景噪声严重污染，但能够明显看出原语音信息波形的包络；图9(b)为解密信号的频谱分布，从中可以看出，本逆系统解密之后的频谱与原信息频谱特征非常吻合，只是存在较为严重的白噪声谱分布。对信道噪声本身而言，本逆系统输出噪声虽得到放大，但对解密信息而言，信噪比稍有改善，即通信系统对信道噪声不够敏感。

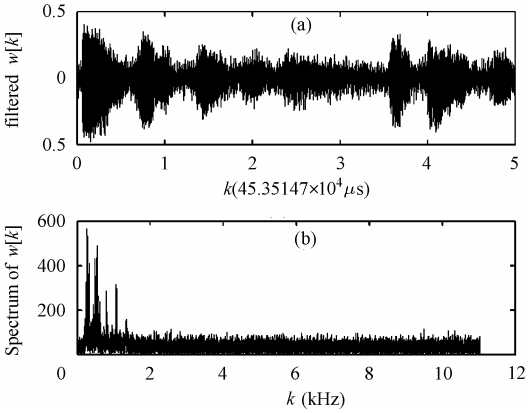

图9 通道噪声为*SNR*＝25dB时的解密信息波形和频谱

(a)解密信号经过低通滤波后的输出波形；(b) 解密信息的频谱

Fig.9 The decryption waveform and its spectrum with channel SNR=25dB.

(a) The lowpass filtered decryption waveform

(b) The spectrum of decryption signal.

4.4 系统同步特性

无论是模拟混沌加密系统还是数字加密系统，同步特性是混沌加密系统的非常重要的特性之一。在混沌激励系统式(2)和左逆系统式(5)中，保持零动态混沌信号序列的同步至关重要。如果在左逆解密过程中，不能保证混沌激励序列与接收信号序列在时间上的同步，就相当于左逆解密过程使用了一组完全不同的初始状态，其解密结果如图6(b)和图6(d)相似，仍为混沌信号。

因为本文提出的激励系统和左逆系统中零动态混沌序列，可以分别在发射端和接收端独立产生，且使用完全相同的零动态模型，所以，系统同步只需要保证零动态混沌信号$z_{c1}[k]$，$z_{c21}[k]$，$z_{c22}[k]$与接收到的加密信号序列$r[k]$实现同步一致。这样，知道接收端准确的时间序列号k和零动态混沌模型的初始状态$z_{c1}[0]$，$z_{c21}[0]$，$z_{c22}[0]$，就能够保证本系统的正确同步。而初始状态作为保密通信双方的PIN码是已知的，所以，只需要传输一个同步参数k，同步传输参数很少，系统存储容量需求也很少，有利于硬件实现和提高系统传输效率。研究如何传输同步序列号参数 k 编码方案和相关技术，是本方法所设计的保密通信系统能得到实际应用的关键，也是下一步的主要研究方向。

5 结束语

混沌保密通信在安全保密性能和通信有效性能上体现出了这一高新技术的实用性。本文所提出的可逆零动态非线性混沌通信系统模型，在实现结构上具有模块化特点，便于软硬件实现。同时，收发双方实现保密通信的关键是保持时序同步和混沌激励模型的初始状态参数一致。经过计算机详细模拟分析，信息加密输出保持了混沌信号特性，并且在预防传统时频域信号分析窃密方法和抗击常用信息攻击途径上，具有非常强的保密能力。可以认为本文方法所设计的保密通信系统是安全可靠的。另外，详细分析了本文通信系统抗信道加性噪声的特点，证明了左逆系统具有噪声鲁棒性。不足的是，本系统仍然存在一般数字混沌通信系统的同步问题，从而限制了本系统的实际应用。由于脉冲同步机制的有效性[25]，这一课题有望在进一步的研究工作中得到实际解决。此外，如何改善混沌激励信号的零动态非线性效果，如何进一步应用加密过程信号的混沌特征，以及改善抗噪声性能，也有待于进一步深入研究。

参 考 文 献

[1] Abel A, Schwarz W. Chaos communications: principles，schemes，and system analysis. *Proc. IEEE*，2002，90(5): 691－709.

[2] Liu Zhong，Tang Jun，Yu Juebang. An application of chaos: generating binary pseudorandom sequences. ISCAS 1988，California，May 31-June 3，1998，Vol.1: 1－3.

[3] Li Shujun, Chen Guanrong, Zheng Xuan. Chaos-Based Encryption for Digital Images and Videos. edited by Borko Furht and Darko Kirovski，Hong Kong，CRC Press LLC，2004，Chap. 4.

[4] Zhao D，Chen G，Liu W. A chaos-based robust wavelet domain watermarking algorithm. *Chaos，Solitons and Fractals*，2004, 22: 47－54.

[5] Cuenot J B，Larger L，Goedgebuer J P，*et al*.. Chaos shift keying with an optoelectronic encryption system using chaos in wavelength. *IEEE J. of Quantum Electronics*，2001，37(7): 849－855.

[6] Boccaletti S，Kurths J，Osipov G，*et al*. .The synchronization of chaotic systems. *Phys. ReportS*，2002，336: 1－101.

[7] Pecora L M，Carroll T L. Synchronization in chaotic system. *Phys. Rev. Lett*. 1990，64(8): 821－824.

[8] Aihara K, Katayama R. Chaos engineering in Japan. *Communications of the ACM*，1995，38(11): 103－107.

[9] Special issue on applications in modern communication systems. *IEEE Trans on CAS I*，2001，48(12): 1385－1527.

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

[11] 赵耿，郑德玲. 保密通信中数字流混沌产生器的同步. 电子学报，2002，30(4): 536－539.

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

[13] Kennedy M P，Kolumban G. Special issue on noncoherent chaotic communications. *IEEE Trans. on CAS I*，2000，47(12):1661－1662.

[14] Kolumban G，Kennedy M P，Chaotic communications with correlator receivers: theory and performance limits. *Proc.IEEE*，2002，90(5): 711－732.

[15] Kolumban G，Vizvari B，Schwarz W，*et al*.. Differential chaos shift keying: a robust coding for chaotic communication. Proc. NDES'96，Seville，Spain，1996: 87－92.

[16] Haykin S. Communication Systems. John Wiley & Sons，New York，3rd edition，1994, Chap.2

[17] Kolumban G，Kis G，Jako Z，*et al*.. FM-DCSK: a robust modulation scheme for chaotic communications. *IEICE Trans. on Fundametals*，1998，E81A: 1798－1802.

[18] Bollt E M. Review of chaos communication by feedback control of symbolic dynamics. *Int. J of Bifurcation and Chaos*, 2003, 13(2):269－285.

[19] Feki M，Robert B，Gelle G，*et al*. Secure digital communication using discrete-time chaos synchronization. Chaos，Solitons and fractals，2003，18: 881－890.

[20] Wu C，Chua L O. An unified framework for synchronization and control of dynamical systems. *Int. J of Bifurcation and Chaos*，1994, 4(4): 979－989.

[21] Zheng Yufan，Chen Guanrong，Zhu Canyan. A system inversion approach to chaos-based digital secure speech communication. *Int J of Bifurcation and Chaos*，Sept. 2005，15(3). to be published.

[22] Lau F C M，Tse C K. Chaos-Based Digital Communication Systems. Hong Kong: Springer-Verlag， 2003，Chap.3.

[23] Alvarez G，Li Shujun. Cryptographic requirements for chaotic secure communications. arXiv:nlin.CD/0311039，2003, vol.1.

[24] Chiaraluce F，Gambi E，Garello R，*et al*. .Performance of DCSK in multipath environments: a comparison with systems using Gold sequences. *IEICE Trans. on Fundamentals*，2002，E85A(10): 2354－2363.

[25] Yang T，Chua L O. Impulsive control and synchronization of nonlinear dynamical systems and applications to secure communications. *Int. J of Bifurcation and Chaos*，1997，7(3): 645－664.

朱灿焰:　男，1962 年生, 博士，教授，硕士生导师. 感兴趣的领域是混沌保密通信、软件无线电和实时信号处理.