基于 SC 混沌同步方法的一种保密通信方案

宋志平,于洪洁

上海交通大学船舶海洋与建筑工程学院工程力学系,上海 200240

摘要 混沌掩盖通信方案是最基础、最容易实施的保密通信方法,但要求传输信息的幅值要相当小,所以传输信息易受信道噪声影响,导致还原信息的解码精度降低。本文利用基于线性稳定性准则的混沌同步方法,提出一种进行信息保密通信的混沌掩盖方案。通过对混沌系统线性项与非线性项的适当分离,构造一个特殊的混沌状态变量的非线性驱动向量函数,将要传递的信息加入其中一个分量上,提高信息掩盖的复杂度和进行破解的困难度。以 Lorenz 吸引子和陈氏吸引子为例进行数值模拟,应用混沌掩盖技术传输正弦信息。雅克比矩阵的配置是灵活、多选的,文分析并给出简单、最优的混沌掩盖方案。数值分析证明,即使传输的正弦信息的振幅很大,也没有对解码信息的精度产生影响,同步效果很好。

关键词 保密通信;混沌掩盖;雅克比矩阵;稳定性准则

中图分类号 O322,TN918 **文献标识码** A **doi** 10.3981/j.issn.1000-7857.2011.23.006

A Technical Scheme of Secure Communication Based on SC Chaotic Synchronization Method

SONG Zhiping, YU Hongjie

Department of Engineering Mechanics, School of Naval Architecture, Ocean and Civil Engineering, Shanghai Jiao Tong University, Shanghai 200240, China

Abstract Chaotic masking communication program is the basic method and it is also easy to implement, however the required amplitude for the transmitted message is rather small. Therefore the transmitted message is sensitive to the channel noise, and then the decoding message has a lower accuracy. A method of chaotic synchronization based on the linear stability criterion is utilized, and a technical scheme of chaotic masking for secure communication is proposed. A nonlinear drive vector function of special chaotic state variable is constructed by a proper separation of the linear and nonlinear terms in a chaotic system. The transmitted message is injected into one element of the state vector. Thus the scheme increases the complexity of masking message and the decoding difficulty. Lorenz attractor and Chen attractor are used as an example to simulate the application of sinusoidal information transmitted by chaotic masking technique. The configuration of the Jacobi matrix is flexible and multiple choices. A simple and optimal chaotic masking scheme is given through comparative analysis. Numerical analysis shows that even if the amplitude of sine function information for transmission is quite large, there is no effect on the decoding accuracy of the information. The proposed scheme is effective.

Keywords secure communication; chaotic-masking; Jacobi matrix; stability criterion

0 引言

自从 Pecora 等[1]提出两个耦合的混沌系统可以实现同步的方法, 混沌同步和控制的研究引起了科研工作者的兴趣。目前,主要的混沌同步方法有 P-C 方法[1]、主动-被动方法[2]和变量反馈同步法等。有些混沌同步方法是两个系统单向耦合,其中一个是驱动系统,而另一个是响应系统,从驱动系统中输出一个信号驱动响应系统,从而使两个耦合的系统达到同步。判定耦合混沌系统同步的方法主要是计算误差系统的

收稿日期:2011-04-20;修回日期:2011-07-21

基金项目:国家自然科学基金青年基金项目(11002087);高等学校博士学科点专项科研基金项目(20100073110007)

作者简介:宋志平,研究方向为非线性动力学混沌同步与控制,电子信箱:songzhiping@126.com;于洪洁(通信作者),副教授,研究方向为神经动力学、混沌同步与控制,电子信箱:yuhongjie@sjtu.edu.cn

李雅普诺夫指数，或者是构造误差系统的李雅普诺夫函数，如果误差系统在零点是稳定的,就可以判定两个耦合系统是同步的。由于同步方法实验上证明完全可行,而且可以通过蔡氏电路等构造同步的耦合混沌系统,所以基于混沌同步的实际应用成为当前研究热点[3]。特别的,因为混沌信号的类噪声性以及频谱分布比较宽，所以混沌信号可以用于保密通信。1993 年,Cuomo 和 Oppenheim 等[4]基于 Lorenz 混沌系统构造出一种基于混沌掩盖技术的保密通信模拟试验电路,但是所传输的信息信号要比载波信号小 20—30dB,容易受到信道噪声干扰，适用于慢变信号的保密通信，而且安全性低。1993—1995 年,混沌调制方法被提出,分为混沌参数调制和混沌非自治调制[5-7]。混沌参数调制是把传输信息(一般是数字信息)调制进发送端系统参数中,混沌非自治调制是用传输信息改变混沌发送端的相空间,理论上讲,混沌非自治调制是零误差方案。混沌调制较之混沌掩盖技术,改善了系统的安全性。此后,陆续有各种基于混沌的保密通信方案被提出,例如自适应方法和控制方法等[8-11]。

Yu 和 Liu 在 2003 年提出一个基于线性系统稳定性准则的混沌同步方法(SC 方法)[12-13],该方法是基于线性系统的稳定性判据实现混沌同步的,而不需要繁琐的计算李雅普诺夫指数和构造李雅普诺夫函数。通过对驱动混沌系统的线性项与非线性项的适当分离,构造一个受驱动系统的非线性项驱动的响应混沌系统,利用线性系统稳定性准则保证两个系统的同步。SC 方法适用于自治、非自治混沌系统以及超混沌系统的同步。只要配置的雅克比矩阵 $\boldsymbol{A}$ 的特征值都有负实部,就可以判定混沌系统是同步的,而且选取雅克比矩阵 $\boldsymbol{A}$ 的范围、灵活性很大,所以这是一种简单有效的混沌同步方法。

本文将采用上述基于线性系统稳定性准则的混沌同步方法对正弦信息进行加密解密。通过对驱动混沌系统的线性项与非线性项的适当分离配置,线性项部分配置的雅克比矩阵 $\boldsymbol{A}$ 的特征值都有负实部,以非线性部分作为传输的正弦信息的载波信号组,并作为掩盖信息的驱动信号传输给响应系统,接收端响应系统经同步、解密过程恢复出要传递的正弦信号。与传统保密通信方案不同的是,在这里混沌发送端传输的信号为不少于一项的信号向量,因此在实际应用中的电路设备,在发射信号端要引出一个向量输出,而不是以往中的一个单项输出。同样,在传输信道中,要由一组电缆传输混沌载波,因此任何破解信息的第三方都不知道所要传输的有用信息到底隐藏或被调制在哪一组混沌载波中,无疑这将增加信息破解的难度,因此也达到了保密通信的目的。此外,本文所用的混沌同步方法输出的是非线性信号向量,因此第三方不可能用一个返回回路破解信号,而在通常的混沌掩盖技术中有可能通过一个返回回路破解信号。再者,传输的非线性混沌信号通常是混沌状态变量的线性与非线性函数的组合,更增加了破解的困难度与复杂度。本文第 1 节给出该同步方法的理论描述;第 2 节说明基于此同步方法的混沌掩盖通信方案,并给出数值仿真的例子和结果分析。

1　基于线性稳定性准则的混沌同步方法

首先考虑一个连续的混沌系统

$$\dot{\boldsymbol{x}}(t)=\boldsymbol{f}(\boldsymbol{x}(t)) \tag{1}$$

其中 $\boldsymbol{x}(t)\in R^n$ 为混沌系统的 n 维状态向量,$\boldsymbol{f}:R^n\to R^n$ 定义了一个 n 维向量场。将函数 $\boldsymbol{f}(\boldsymbol{x}(t))$ 分解为线性和非线性两部分,即

$$\boldsymbol{f}(\boldsymbol{x}(t))=\bar{\boldsymbol{g}}(\boldsymbol{x}(t))+\bar{\boldsymbol{h}}(\boldsymbol{x}(t)) \tag{2}$$

在 $\boldsymbol{f}(\boldsymbol{x}(t))$ 的右端部分加上并减去一个经过适当配置的线性函数 $\bar{\boldsymbol{A}}\boldsymbol{x}(t)$,则

$$\begin{aligned}\boldsymbol{f}(\boldsymbol{x}(t))&=\bar{\boldsymbol{g}}(\boldsymbol{x}(t))+\bar{\boldsymbol{A}}\boldsymbol{x}(t)+\bar{\boldsymbol{h}}(\boldsymbol{x}(t))-\bar{\boldsymbol{A}}\boldsymbol{x}(t)\\&=\boldsymbol{g}(\boldsymbol{x}(t))+\boldsymbol{h}(\boldsymbol{x}(t))\\&=\boldsymbol{A}\boldsymbol{x}(t)+\boldsymbol{h}(\boldsymbol{x}(t))\end{aligned} \tag{3}$$

其中,$\boldsymbol{A}$ 为满秩的常数矩阵,通过适当的分离配置 $\boldsymbol{A}\boldsymbol{x}(t)=\boldsymbol{g}(\boldsymbol{x}(t))=\bar{\boldsymbol{g}}(\boldsymbol{x}(t))+\bar{\boldsymbol{A}}\boldsymbol{x}(t)$,可使矩阵 $\boldsymbol{A}$ 的所有特征值均具有负实部。函数 $\boldsymbol{h}(\boldsymbol{x}(t))$ 为函数 $\boldsymbol{f}(\boldsymbol{x}(t))$ 的非线性部分:

$$\boldsymbol{h}(\boldsymbol{x}(t))=\bar{\boldsymbol{h}}(\boldsymbol{x}(t))-\bar{\boldsymbol{A}}\boldsymbol{x}(t)=\boldsymbol{f}(\boldsymbol{x}(t))-\boldsymbol{g}(\boldsymbol{x}(t)) \tag{4}$$

因此,系统(1)作为驱动系统可以表述为

$$\dot{\boldsymbol{x}}(t)=\boldsymbol{g}(\boldsymbol{x}(t))+\boldsymbol{h}(\boldsymbol{x}(t)) \tag{5}$$

然后,构造一个新的系统作为响应系统:

$$\dot{\boldsymbol{w}}(t)=\boldsymbol{g}(\boldsymbol{w}(t))+\boldsymbol{h}(\boldsymbol{x}(t)) \tag{6}$$

$\boldsymbol{w}(t)\in R^n$ 为所构造新系统的状态向量,响应系统接收来自驱动系统的非线性混沌信号 $\boldsymbol{h}(\boldsymbol{x}(t))$。定义 $\boldsymbol{e}(t)=\boldsymbol{x}(t)-\boldsymbol{w}(t)$ 为同步误差,$\boldsymbol{e}(t)$ 满足如下微分方程:

$$\dot{\boldsymbol{e}}(t)=\dot{\boldsymbol{x}}(t)-\dot{\boldsymbol{w}}(t)=\boldsymbol{A}(\boldsymbol{x}(t)-\boldsymbol{w}(t))=\boldsymbol{A}\boldsymbol{e}(t) \tag{7}$$

显然 $\boldsymbol{e}(t)$ 的零点即为其平衡点。因为经过特殊配置的矩阵 $\boldsymbol{A}$ 的特征值都有负实部,由线性系统的稳定性准则可知,$\boldsymbol{e}(t)$ 的零点是渐近稳定的,可判定 $\boldsymbol{w}(t)$ 和 $\boldsymbol{x}(t)$ 能实现完全同步。

2　利用 SC 方法进行混沌掩盖的技术方案及数值仿真

2.1　混沌掩盖的技术方案

利用第 1 节所述 SC 混沌同步方法进行传输信息的混沌掩盖。把所要传输的信息 $i_m(t)$ 直接加到驱动系统的混沌信号 $\boldsymbol{h}(\boldsymbol{x}(t))$ 第 j 项 $h_j(\boldsymbol{x}(t))$ 中,得到混沌信号与有用信息 $i_m(t)$ 的混合驱动信号 $\boldsymbol{s}(t)$

$$\boldsymbol{s}(t)=\boldsymbol{h}(\boldsymbol{x}(t))+\boldsymbol{i}(t)=\begin{bmatrix}s_1\\\vdots\\s_j\\\vdots\\s_n\end{bmatrix}=\begin{bmatrix}h_1(\boldsymbol{x}(t))\\\vdots\\h_j(\boldsymbol{x}(t))\\\vdots\\h_n(\boldsymbol{x}(t))\end{bmatrix}+\begin{bmatrix}0\\\vdots\\i_m(t)\\\vdots\\0\end{bmatrix} \tag{8}$$

其中,$\boldsymbol{s}(t)\in R^n$ 是将信息加密的混沌信号向量,包含 n 个传输的分量 $s_j(t)$,这和以往的仅传输一个混沌信号的混沌掩盖方法不同,可以将信息加密任意一个分量 $s_j(t)$ 中,增加了第三方解码的难度。再通过信道传输到接收端,驱使响应系统与驱动系统同步,响应系统输出同步的混沌信号 $\boldsymbol{h}(\boldsymbol{w}(t))$,最后用驱动信号 $\boldsymbol{s}(t)$ 直接减去同步的混沌信号 $\boldsymbol{h}(\boldsymbol{w}(t))$ 就可以在

接收端恢复出有用信息$\hat{i}_m(t)$。信号加密传输、同步解码过程示意如图 1 所示。

接收端受混合驱动信号驱使微分方程为

$$\dot{\boldsymbol{w}}(t)=\boldsymbol{g}(\boldsymbol{w}(t))+\boldsymbol{s}(t) \tag{9}$$

同步后的解码信息为

$$\hat{i}_m(t)=\boldsymbol{s}(t)-\boldsymbol{h}(\boldsymbol{w}(t)) \tag{10}$$

因为$\boldsymbol{h}(\boldsymbol{x}(t))$是驱动系统的非线性部分,故$\boldsymbol{s}(t)$也是非线性的,这是很关键的。以往利用混沌同步方法进行信息掩盖的传输信号都是状态变量的一个线性组合,很明显混沌状态变量的非线性函数组合的信号更不容易被破解,因此安全性也更高。

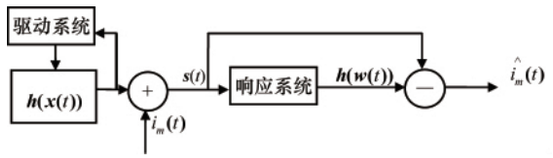


图 1　混沌掩盖加密解密过程示意图

Fig. 1　Scheme of encryption and decryption process of chaotic masking

2.2　数值仿真

2.2.1　Lorenz 吸引子

作为进行数值仿真的例子,考虑如下描述的 Lorenz 混沌系统

$$\begin{aligned}\dot{x}_1&=\sigma(x_2-x_1)\\ \dot{x}_2&=-x_1x_3+rx_1-x_2\\ \dot{x}_3&=x_1x_2-bx_3\end{aligned} \tag{11}$$

其中,取 σ=16,r=45.92,b=4 时,该系统是混沌的。将系统(11)右端函数按照式(2)—式(4)适当分离配制成函数$\boldsymbol{g}(\boldsymbol{x}(t))$和$\boldsymbol{h}(\boldsymbol{x}(t))$

$$\begin{aligned}\boldsymbol{g}(\boldsymbol{x}(t))&=\boldsymbol{A}\begin{bmatrix}x_1\\x_2\\x_3\end{bmatrix}=\begin{bmatrix}-\sigma & & \\ & -1 & \\ & & -b\end{bmatrix}\begin{bmatrix}x_1\\x_2\\x_3\end{bmatrix}\\ \boldsymbol{h}(\boldsymbol{x}(t))&=\begin{bmatrix}\sigma x_2\\-x_1x_3+rx_1\\x_1x_2\end{bmatrix}\end{aligned} \tag{12}$$

雅可比矩阵$\boldsymbol{A}$的特征值为−16、−1、−4,均为负实数。此处$\boldsymbol{A}$矩阵按照对角线配置,在分离过程中保留 Lorenz 吸引子函数$\boldsymbol{f}$的 3 个相应的线性项$-\sigma x_1$,$-x_2$,$-bx_3$,因为这 3 项的系数都为负,将另外的线性项σx_2,rx_1配置到非线性函数中,矩阵上三角和下三角的元素都为 0,对角线上的元素就是其对应的特征值,这是最简单的一种配置。传输信息取正弦信息$i_m(t)=a\sin\omega t$。将传输信息$i_m(t)$加入到非线性传输信号$\boldsymbol{h}(\boldsymbol{x}(t))$的第 1 项$h_1(\boldsymbol{x}(t))$中,构成发送端混合驱动信号

$$\boldsymbol{s}(t)=\begin{bmatrix}\sigma x_2\\-x_1x_3+rx_1\\x_1x_2\end{bmatrix}+\begin{bmatrix}i_m(t)\\0\\0\end{bmatrix} \tag{13}$$

按照式(5)和式(6),构造接收端系统

$$\begin{aligned}\dot{w}_1&=-\sigma w_1+s_1(t)\\ \dot{w}_2&=-w_2+s_2(t)\\ \dot{w}_3&=-bw_3+s_3(t)\end{aligned} \tag{14}$$

则在接收端解码信息为

$$\hat{i}_m(t)=s_1(t)-h_1(\boldsymbol{w}(t))=[\sigma x_2+i_m(t)]-\sigma w_2 \tag{15}$$

若将传输信息$i_m(t)$分别加入到非线性传输信号$\boldsymbol{h}(\boldsymbol{x}(t))$的第 2 项$h_2(\boldsymbol{x}(t))$和第 3 项$h_3(\boldsymbol{x}(t))$中,则接收端解码信息分别为

$$\hat{i}_m(t)=s_2(t)-h_2(\boldsymbol{w}(t))=(-x_1x_3+rx_1+i_m(t))-(w_1w_3+rw_1) \tag{16}$$

$$\hat{i}_m(t)=s_3(t)-h_3(w(t))=(x_1x_2+i_m(t))-w_1w_2 \tag{17}$$

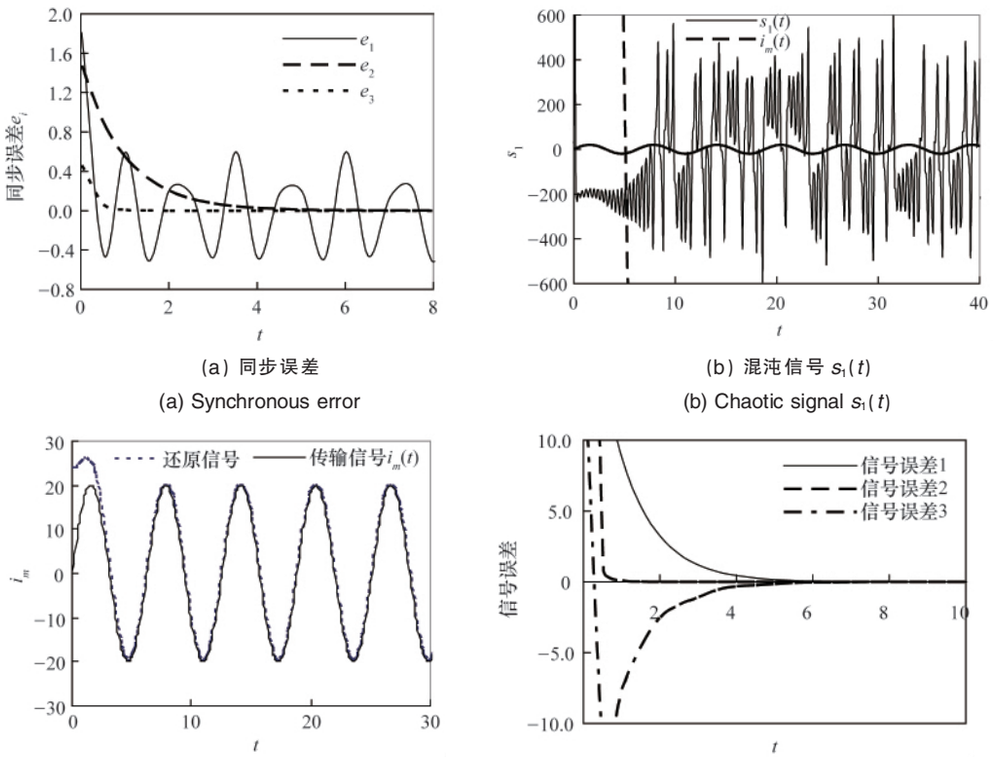
按照式(7)列出同步误差的微分方程

$$\begin{bmatrix}\dot{e}_1\\\dot{e}_2\\\dot{e}_3\end{bmatrix}=\begin{bmatrix}-\sigma & & \\ & -1 & \\ & & -\mathrm{b}\end{bmatrix}\begin{bmatrix}e_1\\e_2\\e_3\end{bmatrix}=\boldsymbol{A}\begin{bmatrix}e_1\\e_2\\e_3\end{bmatrix} \tag{18}$$

由于雅可比矩阵$\boldsymbol{A}$的特征值实部均为负,满足线性系统稳定性准则,系统(11)和系统(14)的同步误差具有渐近稳定性。

初值采用$\boldsymbol{x}$=[5.0　2.5　1.5]$^{\mathrm{T}}$,$\boldsymbol{w}$=[2.5　1.0　1.0]$^{\mathrm{T}}$。本文采用正弦信号$i_m(t)=a\sin\omega t$作为要进行掩盖传输的信号。图 2 给出了利用混沌掩盖进行信号加密解密的结果,a=20,ω=1。图 2(a)显示状态变量$\boldsymbol{w}$和$\boldsymbol{x}$的同步误差$e_1(t)$、$e_2(t)$、$e_3(t)$随时间发展的变化图,其中$e_2(t)$和$e_3(t)$随时间变化迅速收敛为 0,而$e_1(t)$却并不收敛,这是因为正弦信号$i_m(t)$被掩盖在$\boldsymbol{s}(t)$3 组传输混沌信号的第 1 组$s_1(t)$中,信号$i_m(t)$的振幅a=20 比较大,破坏了w_1和x_1的同步结果。但是注意到式(15),解码信息中不包含w_1和x_1,所以不影响信号的解码恢复。图 2(b)显示的是进行混沌掩盖传输的混合信号$s_1(t)$,从图中可以看出混合信号是毫无规律的混沌信号,正弦信号很好地隐藏其中。图 2(c)显示的是信号$i_m(t)$=20sin$t$和经接收端系统还原后的正弦信号$\hat{i}_m(t)$,可以看出恢复信号迅速收敛到原始传输信号而且此后相当稳定。图 2(d)显示的是正弦信号分别加到$s(t)$的 3 个传输分量中,在接收端还原信息与原始正弦信号的同步误差图,从图中看出当正弦信息加到第 2 个传输的混沌信号$s_2(t)$中时,还原信号$\hat{i}_m(t)$的收敛时间最短,而加到第1个分量$s_1(t)$和第 3 个分量$s_3(t)$时的收敛时间一致,在t=10.1 时,信号同步误差$\hat{i}_m(t)-i_m(t)=9.86\times10^{-4}$,已小于$1\times10^{-3}$。因此在解码精度相同的情况下,将正弦信息加到第 2 个传输信号中是最好的选择。

分别将正弦信号的振幅a与角频率ω作为控制参数,在$a\in[0.001,900]$,$\omega\in[0.01,500]$参数组合的范围内,利用上述混沌掩盖技术数值模拟传输与解码过程,发现解码的精度和收敛速度均一致,不受$i_m(t)$的振幅与频率变化的影响。信号同步误差图与图 2(d)一致,说明利用这种方法,可供选择的正弦信号非常多,不管是低频还是高频、振幅大或小,都能采



(a) 同步误差　(b) 混沌信号 $s_1(t)$

(a) Synchronous error　(b) Chaotic signal $s_1(t)$

(c) $i_m(t)$和 $\hat{i}_m(t)$　(d) 信号同步误差 $\hat{i}_m(t)-i_m(t)$

(c) $i_m(t)$ and $\hat{i}_m(t)$　(d) Synchronous error of signal: $\hat{i}_m(t)-i_m(t)$

图 2　利用混沌掩盖技术传输及还原正弦信号数值模拟

Fig. 2　Transferring and restoring sinusoidal signal using chaotic masking technology

用这种混沌掩盖方式传输解码,而且解码速度快精度高。

由于雅克比矩阵 $\boldsymbol{A}$ 是按对角线配置的,由式(18)可以看出,3 个同步误差方程是彼此独立的,故当在其中一个传输信号 $s_j(t)$中因加入正弦信号而使相应的状态变量 w_j 和 x_j 同步失效时,其余两组状态变量的同步效果不会改变。注意到式(12)—式(13)的非线性驱动函数 $\boldsymbol{h}(\boldsymbol{x}(t))$及 $\boldsymbol{s}(t)$的第 j 项分量 $h_j(x(t))$、$s_j(t)$(j=1,2,3)中都不包含对应的第 j 个状态变量 x_j,因此解码信息式(15)—式(17)中不包含相应不同步的 w_j 和 x_j,解码信息是由同步的状态变量构成的,所以不论正弦信号加到哪一个传输信号中,都不会影响在接收端解码信息的精度和收敛性,如图 2(d)所示。

但是如果稍改变一下雅克比矩阵 $\boldsymbol{A}$ 的配置,使得在驱动信号 $\boldsymbol{s}(t)$中的第 j 项含有 x_j,由于信号 $i_m(t)$的振幅 a=20 比较大,则在接收端就不会解码出原来的正弦信号。例如在方程组(11)第一个方程等号右边加上 $\beta x_1-\beta x_1$,得

$$\begin{aligned}\dot{x}_1&=\sigma(x_2-x_1)+\beta x_1-\beta x_1\\ \dot{x}_2&=-x_1x_3+rx_1-x_2\\ \dot{x}_3&=x_1x_2-bx_3\end{aligned}\tag{19}$$

其中,$-\sigma-\beta<0$,配置雅可比矩阵 $\boldsymbol{A}=\begin{bmatrix}-\sigma-\beta & & \\ & -1 & \\ & & -b\end{bmatrix}$,雅可比矩阵 $\boldsymbol{A}$ 的特征值为$-\sigma-\beta$,-1,-4,均为负实数,相应的驱动信号为

$$\boldsymbol{s}(t)=\begin{bmatrix}\sigma x_2+\beta x_1\\ -x_1x_3\\ x_1x_2\end{bmatrix}+\begin{bmatrix}i_m(t)\\ 0\\ 0\end{bmatrix}\tag{20}$$

则还原信息表达如下:

$$\begin{aligned}\hat{i}_m(t)&=s_1(t)-\sigma w_2-\beta w_1=\sigma(x_2-w_2)+\beta(x_1-w_1)+i_m(t)=\\ &\sigma e_2+\beta e_1+i_m(t)\end{aligned}\tag{21}$$

在这种情况下 w_1 和 x_1 不同步,所以 $\hat{i}_m(t)$和 $i_m(t)$也是不同步的,信息解码失败。因此,在实际应用中应当选择合适的载波信号以确保在接收端解码成功。

下面考虑雅克比矩阵 $\boldsymbol{A}$ 的另外一种配置,将 Lorenz 方程右端函数适当分离配置,得到新的 $\boldsymbol{g}(\boldsymbol{x}(t))$和 $\boldsymbol{h}(\boldsymbol{x}(t))$

$$\boldsymbol{g}(\boldsymbol{x}(t))=\begin{bmatrix}-\sigma x_1+\sigma x_2\\ -x_2+rx_3\\ -bx_3\end{bmatrix}=\boldsymbol{A}\begin{bmatrix}x_1\\ x_2\\ x_3\end{bmatrix}=\begin{bmatrix}-\sigma & \sigma & \\ & -1 & r\\ & & -b\end{bmatrix}\begin{bmatrix}x_1\\ x_2\\ x_3\end{bmatrix}\tag{22}$$

$$\boldsymbol{h}(\boldsymbol{x}(t))=\begin{bmatrix}0\\ -x_1x_3+rx_1-rx_3\\ x_1x_2\end{bmatrix}\tag{23}$$

雅克比矩阵 $\boldsymbol{A}$ 的下三角元素均为 0,特征值仍与对角线配置时的特征值一致,为-16、-1、-4,均为负数。

按照式(6)构造接收端系统

$$\begin{aligned}\dot{w}_1&=-\sigma w_1+\sigma w_2\\ \dot{w}_2&=-w_2+rw_3-x_1x_3+r(x_1-x_3)\\ \dot{w}_3&=-bw_3+x_1x_2\end{aligned}\tag{24}$$

按照式(7)同步误差微分方程

$$\begin{bmatrix}\dot{e}_1\\ \dot{e}_2\\ \dot{e}_3\end{bmatrix}=\begin{bmatrix}-\sigma & \sigma & \\ & -1 & r\\ & & -b\end{bmatrix}\begin{bmatrix}e_1\\ e_2\\ e_3\end{bmatrix}=\boldsymbol{A}\begin{bmatrix}e_1\\ e_2\\ e_3\end{bmatrix}\tag{25}$$

由于雅克比矩阵 $\boldsymbol{A}$ 的特征值全为负,满足线性系统稳定性准则,故系统(24)和系统(11)可以达到同步。依然取传输信息 $i_m(t)=20\sin t$,将其加入驱动信号的第二项 $h_2(x)$ 中进行混沌信号掩盖

$$\boldsymbol{s}(t)=\begin{bmatrix}0\\ -x_1x_3+rx_1-rx_3\\ x_1x_2\end{bmatrix}+\begin{bmatrix}0\\ i_m(t)\\ 0\end{bmatrix}\tag{26}$$

恢复信息

$$\hat{i}_m(t)=s_2(t)-h_2(\boldsymbol{w}(t))=i_m(t)-x_1x_3+re_1-re_3+w_1w_3\tag{27}$$

图 3 给出了 $\boldsymbol{A}$ 这样配置下加密解密的结果。图 3(a)为 $\boldsymbol{w}$ 与 $\boldsymbol{x}$ 的同步误差随时间的变化图,可以看出 $e_1(t)$ 和 $e_2(t)$ 几乎完全重合在一起,没有收敛性,只有 $e_3(t)$ 迅速收敛为0,并一直稳定下去。图 3(b)显示的是传输信号 $s_2(t)=-x_1x_3+rx_1-rx_3+i_m(t)$,信息 $i_m(t)$ 隐藏在混沌载波信号中,这样传输信息被加密。图 3(c)是系统接收端被还原出来的信息信号,很明显与原始的正弦信息相差甚远。在这里正弦信息 $i_m(t)$ 加到了第 2 项混沌信号 $s_2(t)$ 中,由于 $i_m(t)$ 的振幅较大,从而破坏了变量 x_2 和 w_2 的同步,而在式(25)中 $\dot{e}_1=-\sigma e_1+\sigma e_2$,因为 e_2 不收敛,所以 e_1 也不收敛,故 x_1 和 w_1 也不同步,从式子 $\dot{e}_3=-be_3$ 可以看出,e_3 收敛为 0,式(27)中包含不同步的状态变量 x_1 和 w_1,所以在接收端不可能恢复出原始信息 $i_m(t)$。

可以预知,当正弦信息加到第 3 个混沌信号 $s_3(t)$ 中,系统的同步会被完全破坏,自然在接收端也不可能恢复出原始信息了。

再者,将雅克比矩阵 $\boldsymbol{A}$ 配置为上三角元素均为 0 的矩阵,如取

$$\boldsymbol{A}=\begin{bmatrix}-\sigma & & \\ r & -1 & \\ & & -b\end{bmatrix}$$

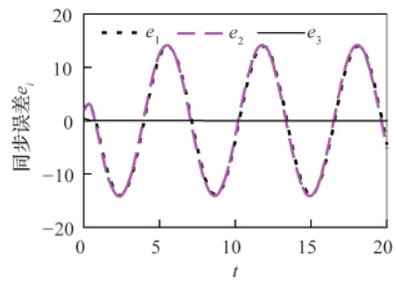
依然取传输信息 $i_m(t)=20\sin t$,将其加入驱动信号的第 2 项 $h_2(\boldsymbol{x})$ 中进行混沌信号掩盖得到

$$\boldsymbol{s}(t)=\begin{bmatrix}\sigma x_2\\ -x_1x_3\\ x_1x_2\end{bmatrix}+\begin{bmatrix}0\\ i_m(t)\\ 0\end{bmatrix}$$

恢复信息:

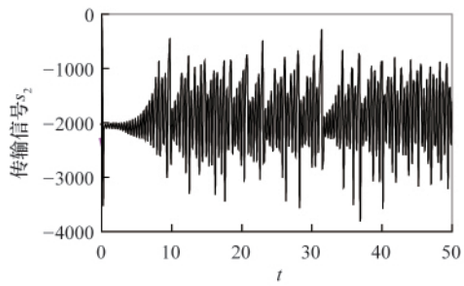
$$\hat{i}_m(t)=s_2(t)-h_2(\boldsymbol{w}(t))=i_m(t)-x_1x_3+w_1w_3$$

因为恢复信息中不含有不同步的状态变量 x_2 和 w_2,故传输信息 $i_m(t)$ 在接收端可以无误差的还原出来。从雅克比矩阵 $\boldsymbol{A}$ 的特征可以看出,即使把传输信息 $i_m(t)$ 隐藏在驱动信号的第 3 项 $h_3(\boldsymbol{x})$ 中,$i_m(t)$ 和 $\hat{i}_m(t)$ 的同步精度依然很好。



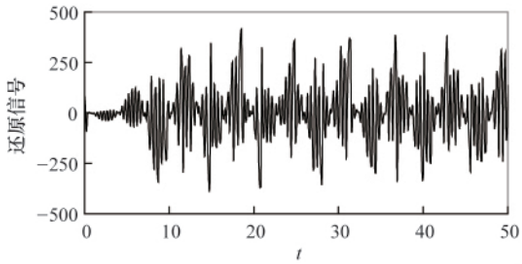
(a) w 和 x 的同步误差

(a) Synchronous error between w and x



(b) 传输信号 $s_2(t)$

(b) Transmission signal $s_2(t)$



(c) 接收端的还原信息

(c) Restored signal of receiver

图 3　非对角矩阵 A 情况下的混沌掩盖数值模拟

Fig. 3　Chaotic masking numerical simulation in the case of non-diagonal matrix A

2.2.2　陈氏吸引子

作为对比,下面以陈氏吸引子为例。陈氏吸引子的微分方程为

$$\begin{aligned}\dot{x}_1&=a(x_2-x_1)\\ \dot{x}_2&=(c-a)x_1-x_1x_3+cx_2\\ \dot{x}_3&=x_1x_2-bx_3\end{aligned}\tag{28}$$

当系统参数 $a=35,b=3,c=28$ 时,系统处于混沌状态。依然按照式(2)—式(4)对系统(28)进行分解,在此配置雅克比矩阵 $\boldsymbol{A}$ 和非线性函数 $\boldsymbol{h}(\boldsymbol{x}(t))$

$$\boldsymbol{A}=\begin{bmatrix}-a & a & 0\\ c-a & \alpha & 0\\ 0 & 0 & -b\end{bmatrix},\boldsymbol{h}(t)=\begin{bmatrix}0\\ 23x_2-x_1x_3\\ x_1x_2\end{bmatrix} \tag{29}$$

其中,α 为一个可调参量且 $\alpha<7$,$\boldsymbol{A}$ 的特征向量[−27.45 −2.55 −3.00]$^{\mathrm{T}}$。依然选取传输信息 $i_m(t)=20\sin t$,将其加入驱动信号的第 3 项 $h_3(\boldsymbol{x})$中进行混沌信号掩盖得到

$$\boldsymbol{s}(t)=\begin{bmatrix}0\\ 23x_2-x_1x_3\\ x_1x_2\end{bmatrix}+\begin{bmatrix}0\\ 0\\ i_m(t)\end{bmatrix} \tag{30}$$

构造接收系统

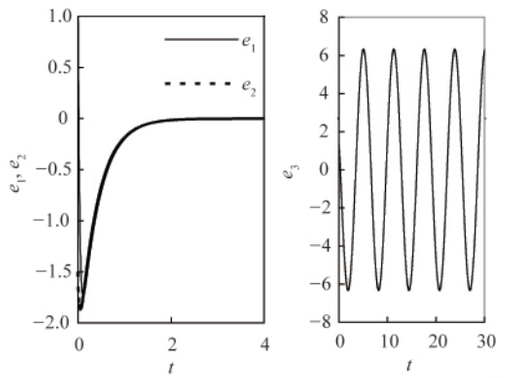
$$\begin{aligned}\dot{w}_1&=-aw_1+aw_2\\ \dot{w}_2&=(c-a)w_1+5w_2+s_2(\boldsymbol{x})\\ \dot{w}_3&=-bw_3+s_3(\boldsymbol{x})\end{aligned} \tag{31}$$

恢复信息

$$\hat{i}_m(t)=s_3(t)-h_3(\boldsymbol{w}(t))=i_m(t)+x_1x_2-w_1w_2$$

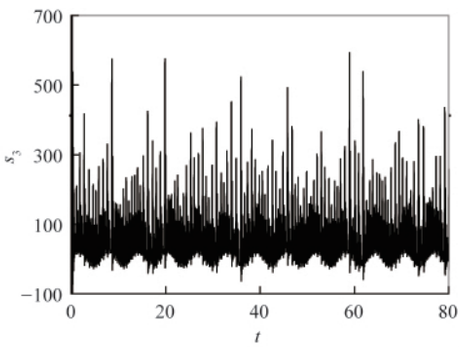
取初值 $\boldsymbol{x}$=[0.5 −0.5 2]$^{\mathrm{T}}$,$\boldsymbol{w}$=[−1 1 0.5]$^{\mathrm{T}}$。图 4 给出了基于陈氏吸引子的混沌掩盖通信结果。从图 4(a)可以看出,状态变量 x_1 和 w_1,x_2 和 w_2 迅速同步,但是 x_3 与 w_3 却始终不能同步,正如在前面讨论的那样,由于正弦信息加载到第 3 项传输信号而影响了状态变量 x_3 与 w_3 的同步。图 4(b)显示的是第 3 项传输信号,正弦信息 $i_m(t)$很好地隐藏在混沌信号中,起到加密效果。图 4(c)显示了在极短的瞬态过程后信息误差 $i_m(t)-\hat{i}_m(t)$收敛为 0,说明信息的恢复性和保真度极好,如图 4(d)所示还原正弦信息。与 Lorenz 系统相同的是,这种配置的陈氏吸引子也对所要传输的正弦信息的振幅和频率限制很小,且解码速度与解码精度几乎是不受影响的。但是有别于 Lorenz 系统,此处陈氏吸引子的配置矩阵 $\boldsymbol{A}$ 可用一个参量 α 控制,只要满足 $\alpha<7$ 即可得到允许的雅克比矩阵,相较 Lorenz 系统而言配置比较方便,而且可以用 α 作为控制器进行二次加密。

雅克比矩阵的非对角形式使得误差微分方程组中的各方程不再独立,因此相对于雅克比矩阵是对角形式的误差微分方程组而言,在传输信息时要注意适当选择配置,使掩盖信息的混沌信号中不包含不同步的状态变量,从而确保信息在接收端的解码精度。在传统的混沌掩盖技术中是将传输的有用信息加载到一项混沌载波中,其误差微分方程组彼此不独立,因此由于有用信息的加入使驱动系统和接收系统同步误差较大,如果要消除误差就要使传输信息的振幅相当小,当振幅为 0 时,驱动系统和接收系统完全同步。这样的问题在



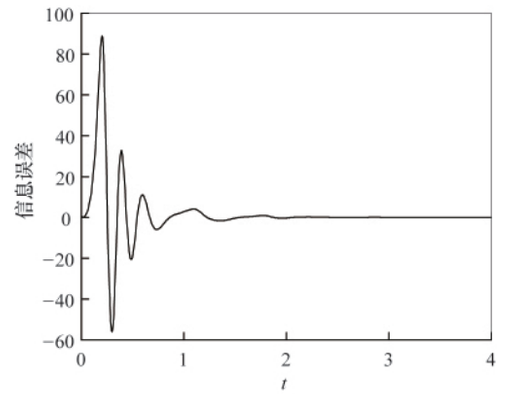
(a) 状态变量同步误差

(a) Synchronous error of each state variable



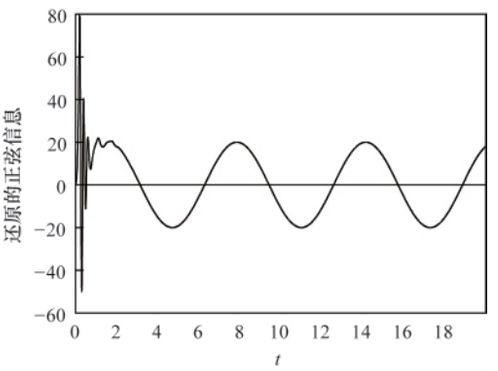
(b) 传输的混沌信号 $s_3(t)$

(b) Transmission chaotic signal $s_3(t)$



(c) 信号同步误差 $i_m(t)-\hat{i}_m(t)$

(c) Synchronous error of signal $i_m(t)-\hat{i}_m(t)$



(d) 还原的正弦信息 $\hat{i}_m(t)$

(d) Restored sinusoidal signal $\hat{i}_m(t)$

图 4　基于陈氏吸引子的混沌掩盖数值分析结果

Fig. 4　Numerical analysis results of chaotic masking on the basis of Chen attractor

传统的混沌掩盖技术中没有得到解决,而在本文中只要配置合适的雅克比矩阵 $\boldsymbol{A}$,就可以传输振幅相对大的正弦信号。

3 结论

利用一种新的混沌同步方法对要传输的正弦信息进行掩盖处理并在接收端精确地将其还原出来。以 Lorenz 吸引子、陈氏吸引子为例,验证了雅可比矩阵 $\boldsymbol{A}$ 在不同配置时,通过选择合适的混沌载波,使得还原信息 $\hat{i}_m(t)$ 中不含有非同步项,在接收端还原的正弦信息的精度与正弦信息的振幅 a 和频率 ω 无关,在陈氏吸引子的雅克比矩阵 $\boldsymbol{A}$ 中还使用可调参量 α,可以对系统进行二次加密。利用 SC 混沌同步方法进行安全保密通信的优点是所要传输的正弦信息的选择范围很宽,指出 Lorenz 系统最优化的雅可比矩阵是对角形矩阵。

参考文献(References)

[1] Pecora L M, Corroll T L. Synchronization in chaotic system [J]. *Physical Review Letters*, 1990, 64(1): 821–824.

[2] Parlitz U, Kocarev L, Stojanovski T, *et al*. Encoding messages using chaotic synchronization [J]. *Physical Review E*, 1996, 53(5): 4351–4361.

[3] 阮炯. 混沌应用研究的动态及分析[J]. 自然杂志, 1995, 17(6): 318–322.
Ruan Jiong. *Chinese Journal of Nature*, 1995, 17(6): 318–322.

[4] Cuomo K M, Oppenheim A V. Circuit implementation of synchronized chaos with applications to communications [J]. *Physical Review Letters*, 1993, 71(1): 65–68.

[5] Chee C Y, Xu D. Chaos-based M-ary digital communication technique using controlled projective synchronization [J]. *IEE Proceedings Circuits, Devices & Systems*, 2006, 153(4): 357–360.

[6] Yu W W, Cao J D, Wong K W, *et al*. New communication schemes based on adaptive synchronization [J]. *Chaos*, 2007, 17(3): 1–13.

[7] Parlitz U. Estimating model parameters from time series by autosynchronization[J]. *Physical Review Letters*, 1996, 76(8): 1232–1235.

[8] 李国辉, 徐得名, 周世平. 基于状态观测器的参数调制混沌数字通信[J]. 物理学报, 2004, 53(3): 706–708.
Li Guohui, Xu Deming, Zhou Shiping. *Acta Physica Sinica*, 2004, 53(3): 706–708.

[9] Raju B V S S N, Rao K D. Robust multiuser detection in synchronous chaotic modulation systems [J]. *IETE Journal of Research*, 2009, 55(2): 54–62.

[10] Millerioux G, Amigo J M, Daafouz J. A connection between chaotic and conventional cryptography [J]. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 2008, 55(6): 1695–1703.

[11] Alonge F, Branciforte M, Motta F. A novel method of distance measurement based on pulse position modulation and synchronization of chaotic signals using ultrasonic sensors [J]. *IEEE Transactions on Instrumentation and Measurement*, 2009, 58(2): 318–329.

[12] Yu H J, Liu Y Z. Chaotic synchronization based on stability criterion of linear systems[J]. *Physics Letters A*, 2003, 314(4): 292–298.

[13] Xing G J, Huang D B. Encoding-decoding message for secure communication based on adaptive chaos synchronization [J]. *Journal of Shanghai University*, 2008, 12(5): 400–404.

(责任编辑　刘志远)