第 5 卷第 1 期 2007 年 3 月
1672-6553/2007/05(1)/039-5

动 力 学 与 控 制 学 报
JOURNAL OF DYNAMICS AND CONTROL

Vol. 5 No. 1
Mar. 2007

两种混沌加密方式的计算分析

孙志华　郝建红

（华北电力大学 信息工程系，北京　102206）

摘要　利用加性掩盖和函数调制两种混沌加密方式对模拟信号进行加密，分别从幅值和频率两方面分析加性掩盖方式和函数调制方式，对比两种加密方式加密效果，了解两种加密方式的差异. 计算结果表明：函数调制方式在幅值和频率的范围上都好于加性掩盖方式的幅值和频率范围，函数调制方式比加性掩盖方式更具安全性.

关键词　混沌加密，加性掩盖，函数调制，模拟信号

引 言

在 1990 年，佩考拉，卡罗尔等人提出控制与同步混沌后，利用控制与同步混沌来实现保密通信的思想，激发了人们研究混沌应用的热情. 混沌序列的类随机和宽带功率谱的特性十分适合于通信系统中的噪声伪装调制，同时通过混沌系统对初始值的敏感依赖性，又可以提供数量众多，非相关，类随机而又确定性的，易于产生和再生的混沌信号，此信号可作为密钥来设计混沌保密通信系统. 根据实际通信需要可以采用低维混沌系统，高维混沌系统，甚至可以是时空混沌系统；同步方式也可以是驱动同步，反馈同步等等；而常用的调制解调方式有加性掩盖的方式，函数调制解调方式和乘性扩频方式等等. 由于混沌现象的普遍性和混沌序列容易产生，加之控制与同步混沌也能很方便地实现，混沌加密系统具有很广阔的研究空间和极大的研究价值[1-2].

本文以混沌加密认知理论为基础，采用驱动同步方式，研究了模拟信号上加性掩盖加密方式和函数调制加密方式，表明了两种混沌加密方式在信号加密上应用情况的差异.

1　加性掩盖加密方式

利用加性掩盖方式[1]进行混沌加密通信，是指将消息信号直接叠加到混沌序列上，利用混沌输出的随机性将信号掩盖起来. 下面以罗伦兹混沌系统来进行研究，假是传输消息信号.

调制信号：

$$s(t)=m(t)+x(1) \tag{1}$$

发射端系统方程：

$$\begin{aligned}\dot{x}(1)&=\sigma(x(2)-x(1))\\ \dot{x}(2)&=\rho x(1)-x(2)-20x(1)x(3)\\ \dot{x}(3)&=5x(1)x(2)-\beta x(3)\end{aligned} \tag{2}$$

用 $s(t)$ 代替(3)中的 $x(1)$，来驱动接收端混沌系统

接收端系统方程：

$$\begin{aligned}\dot{y}(1)&=\sigma(y(2)-y(1))\\ \dot{y}(2)&=\rho s(t)-y(2)-20s(t)y(3)\\ \dot{y}(3)&=5s(t)y(2)-\beta y(3)\end{aligned} \tag{3}$$

解密信号：

$$s(t)-y(1)=m'(t) \tag{4}$$

其中取系统参数 $\sigma=16,\rho=45.6,\beta=4$.

模拟信号：$m(t)=A\sin\omega t$ 其中信号幅值分别为 $A=0.5$ 和 $A=1$，$\omega\in(15.4,15.5)$kHz 时，将其代入上述混沌加密系统，数值计算结果如图 1 所示，传输信号、混沌加密信号、解密后信号分别为图 1 的(a)、(b)、(c)三组对比图. 从图上对比结果可得幅值大的信号用该系统加密解密效果不好.

图 1 所示 $A=0.5$，信号频率分别为 $\omega=500$Hz，$\omega\in(15.4,15.5)$kHz 时，传输信号、混沌加密信号、解密后传输信号分别为图 1 的(a)、(b)、(c)三组对比图.

2006-06-12 收到第 1 稿，2006-09-21 收到修改稿.

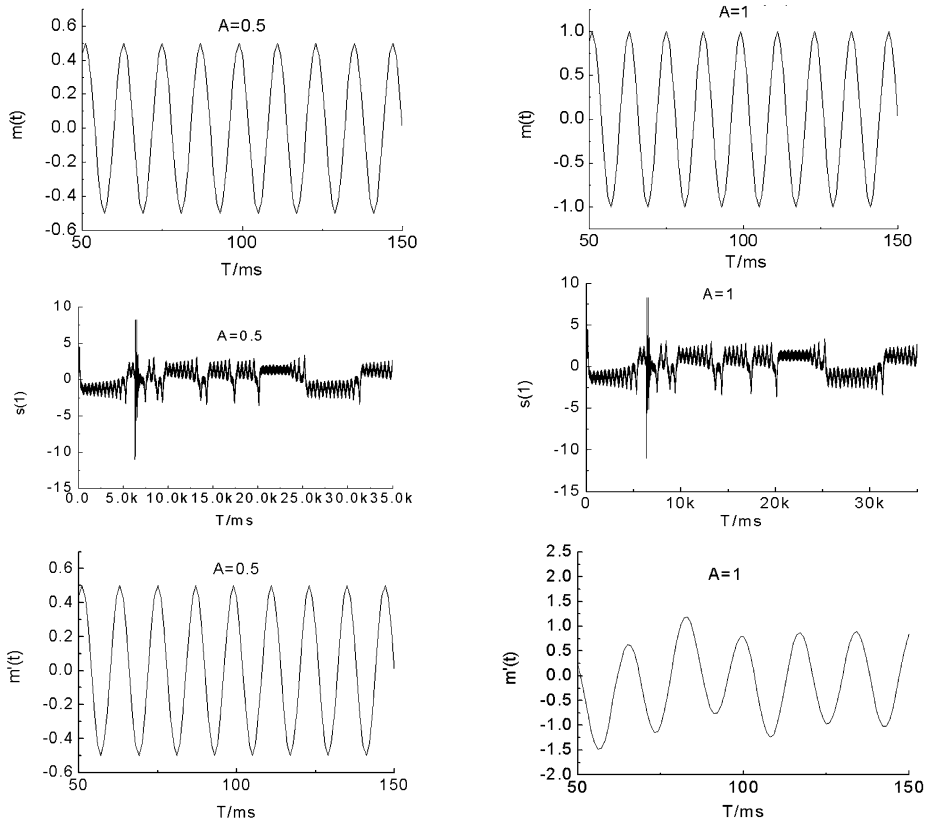

图 1 幅值不同的情况(a)传输信号;(b)经混沌序列加密后的传输信号;(c)解密后信号

Fig. 1 Scale different(a)input information signal (b)encrypted information signal(c)output information signal

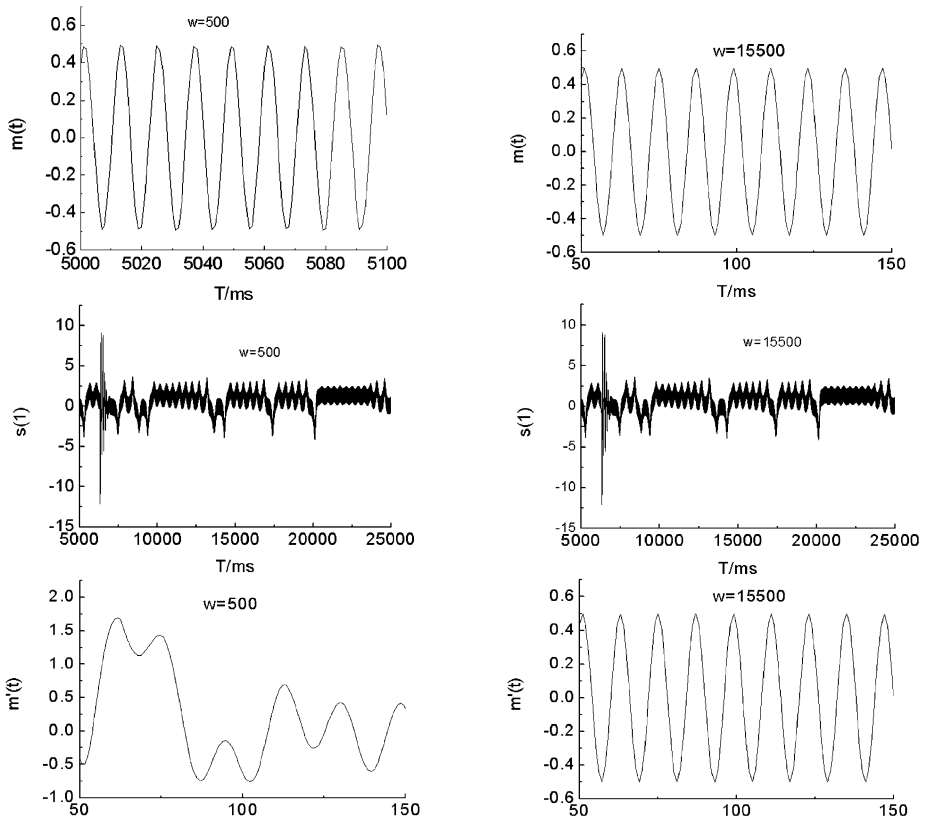

图 2 频率不同(a)传输信号;(b)经混沌序列加密后的传输信号;(c)解密后信号

Fig. 2 Frequency different(a)input information signal (b)encrypted information signal(c)output information signal

从图上对比结果可得运用该系统加密解密的信号频率范围很窄. 从图 1 到图 2 的分析发现,频率对加密性的影响要大于幅值对加密性的影响,这是由于频率变化引起同步误差加大.

为了使混沌信号完全遮掩住传输信号,使它很难从混沌时间序列上直接解出,所以传输信号的幅度要比混沌信号的幅度小,同时传输信号的功率谱强度小于混沌信号的功率谱强度,从而在频谱上很难窃取信息. 从图 2 可看到该系统对频率的要求很苛刻,用该系统的加密的传输信号是有限的,即通过该混沌系统的模拟信号,是一种频率范围窄,幅值不超过 1 的小幅度的信号.

2　函数调制解调加密方式[1]

为了增强通过的安全性、抗干扰性和准确性,需要提高混沌序列的维数,以防止攻击者重构动力学,增加信号强度同时又增加信号的隐蔽性以增强抗干扰和抗非法破译的能力,同时又要确保混沌同步准确性. 为此,通过函数调制解调超混沌加密通信系统来研究有用信号的加密过程. 下面将处于混沌态的洛斯勒系统与罗伦兹系统耦合起来,形成大系统作为发射端

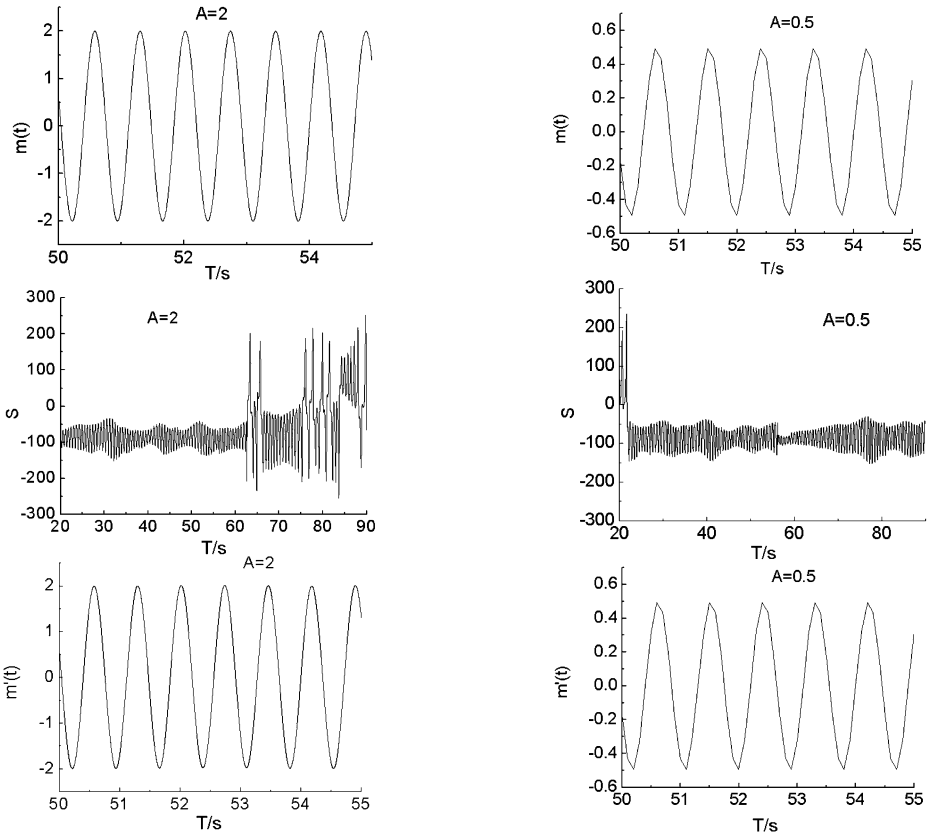

图 3　幅值不同(a)传输信号;(b)经混沌序列加密后的传输信号;(c)解密后信号

Fig. 3　Scale different(a)input information signal (b)encrypted information signal(c)output information signal

$$\dot{x}(1)=\eta+x(1)(x(2)-c);\qquad \dot{x}(2)=-x(1)-\xi x(3)$$
$$\dot{x}(3)=\xi x(2)-ax(3)+s(1);\qquad \dot{x}(4)=\sigma x(4)+s$$
$$\dot{x}(5)=\rho x(4)-x(5)-x(4)x(6);\qquad \dot{x}(6)=x(4)x(5)-\beta x(6)$$
$$s(1)=m(t)+3x(3);\qquad s=10x(5)+30s(1)/x(6)$$

其中 $m(t)$ 为传输信号,混沌序列 s 为高维的超混沌序列加密信号又是信道的传输信号. $x(1)$、$x(2)$、$x(3)$为洛斯勒方程,$x(4)$、$x(5)$、$x(6)$为罗伦兹方程,信号 $s(1)$与 s 将两个不同的混沌耦合起来. 接收端由信号 s 驱动,使发射端与接收端同步[3].

$$\dot{y}(1)=\eta+y(1)(y(2)-c);\qquad \dot{y}(2)=-y(1)-\xi y(3)$$
$$\dot{y}(3)=\xi y(2)-ay(3)+\hat{s}(1);\qquad \dot{y}(4)=\sigma y(4)+s$$
$$\dot{y}(5)=\rho y(4)-y(5)-y(4)y(6);\qquad \dot{y}(6)=y(4)y(5)-\beta y(6)$$
$$\hat{s}(1)=(s-10y(5))y(6)/30$$

解密信号:

$$\hat{m}(t)=(s(1)-10y(5))y(6)/30-3y(3)$$

其中取系统参数 $\eta=2$, $c=5$, $\sigma=10$, $\rho=28$, $\beta=2.666$, $a=2$, $\xi=1$.

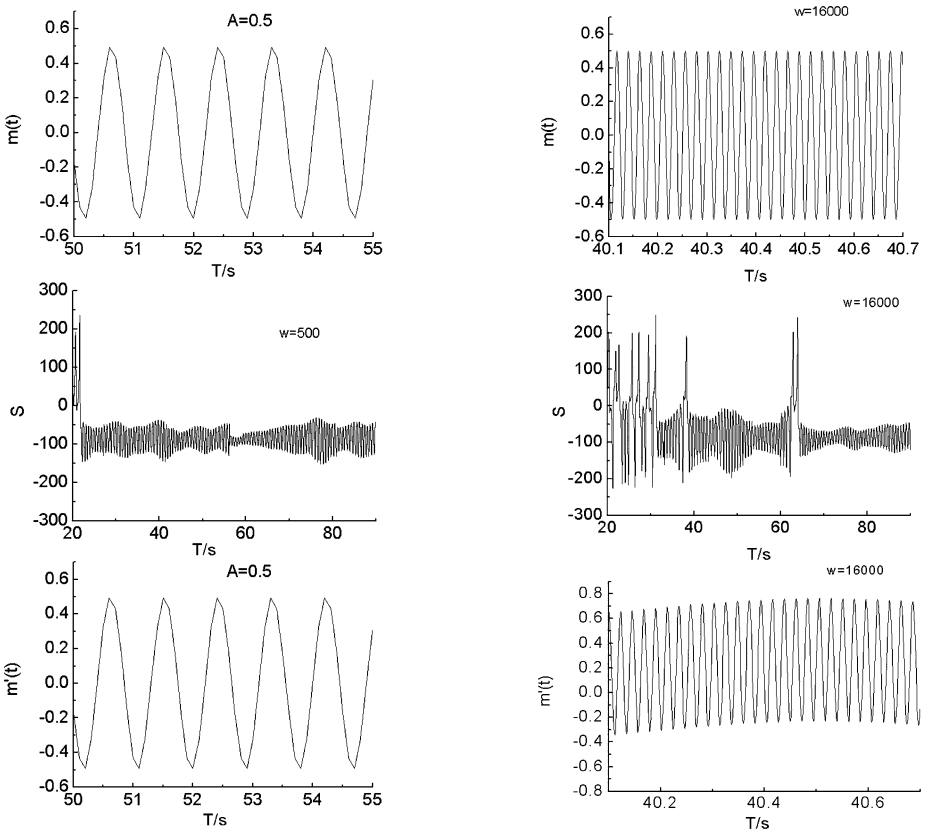

图 4 频率不同(a)传输信号;(b)经混沌序列加密后的传输信号;(c)解密后信号

Fig. 4 Frequency different (a)input information signal (b)encrypted information signal(c)output information signal

模拟信号 $m(t)=A\sin\omega t$;其中信号幅值分别 $A=0.5$ 和 $A=2$,$\omega=500$Hz 时,将其代入上述混沌加密系统,数值计算可得幅值在(0.3,2)的范围上,频率最大不超过 15.5kHz. 如图 3 所示,传输信号、混沌加密信号、解密后传输信号分别为图 3 的(a)、(b)、(c)对比图. 因此,对比图 1 可知:在相同的频率信号上函数调制加密方式更适合于幅值大的信号加密.

如图 4 为 $A=0.5$,其信号频率分别为 $\omega=16$kHz 和 $\omega=500$Hz 时,传输信号、混沌加密信号、解密后传输信号分别为图 4 的(a)、(b)、(c)对比图. 从图 4 的(c)可看到 $\omega=16$KHz 时,解密后信号的幅值出现明显的误差,说明同步误差加大. 而对比图 2 可知:给相同幅值的信号加密,函数调制方式允许的频率变化范围要大于加性掩盖方式允许的频率范围.

从图 3 至图 4 可看到该加密方式在频率、幅值上范围都比加性掩盖加密方式的要大,并且加密信号也更好. 但是当频率超过 15.5kHz 时,从图 4 中的解密后的图形看到幅值恢复出现了不准确.

3 小结

通过两种的混沌加密方式分别对模拟信号进行加密解密,计算结果表明:函数调制加密方式的频率可在小于 15.5kHz 范围上变化,幅值的变化范围可在小于 2 的范围上;加性掩盖加密方式的频率可在(15.4,15.5)kHz 范围上变化,幅值的变化范围小于 1;因此函数调制加密方式在频率、幅值的变化范围上都优于加性掩盖加密方式,而且两种加密方式对频率的敏感性要好于它们对幅值的敏感性;从而进一步验证了函数调制方式的加密比加性掩盖方式的加密更具安全性,在解密上更具准确性.

参 考 文 献

1 胡岗等. 混沌控制. 上海:科技教育出版社,2000(Hu Gang. chaos control. ShangHai: science and technology & education publishing company,2000(in Chinese))

2 李祥飞等. 混沌控制及其优化应用. 北京:国防科技大学

出版社,2002(Li XiangFei. chaos control & optimize applications. BeiJing:national defence science and technology university publishing company,2002(in Chinese))

3 王琳,等. 一种新的类 Lorenz 系统的混沌行为与形成机制. 动力学与控制学报,2005,3(4):1~6(Wang Lin. chaos and its forming mechanism of a new lorenz-like system. *Journal of dynamics and control*,200,3(4):1~6(in Chinese))

4 J Z Yang, G Hu, J H Xiao. Chaos synchronization in coupled chaotic oscillators with multiple positive Lyapunov exponents. *Phys. Rev. Lett*,1998,80: 496~499

5 G V Osipov, B V Shulgin, J J Collins. Controlled movement and suppression of spiral waves in excitable media. *Phys. Rev. E*,1998,58: 6955~6958

6 K Konishi, H Kokame. Decentralized delayed – feedback control of a one – way coupled ring map lattice. *Physica D*, 1999,127:1~12

7 M J Bunner. The control of high – dimensional chaos in time – delay systems to an arbitrary goal dynamics. *Chaos*, 1999,9:233~237

8 Z H Liu, S G Chen, B Hu. Coupled synchronization of spatiotemporal chaos. *Phys. Rev. E*,1999,59: 2817~2821

9 Pecora L M, Carroll T L. Synchronization in chaotic systems. *Phys. Rev. Lett*,1990,64 (8):821~824

10 Pecora L M, Carroll T L. Driving systems with chaotic signals. *Phys. Rev. A*,1991,44 (4):2374~2378

11 Cuomo KM, Oppenheim A V. Circuit implementation of synchronized chaos with applications to communication. *Phy. Rev. Lett*,1993 ,71(1):65~68

12 Perez G, Cerdeira H A. Extracting messages masked by chaos. *Phys. Rev. Lett*,1995,74 (11):1970~1973

13 Short K M. Steps toward unmasking secure communications. *Int . J. Bifur. & Chaos*,1994,4 (4):959~977

14 TelrLu Liao, Nan Sheng Huang. An observed based approach for chaotic synchronization with applications to secure communications. *IEEE Trans. on CAS2I*,1999,46(9):1144~1150

15 Changsong Zhou, C lai. Extracting messages masked by chaotic signalsof time delay systems. *Phys. Rev. E*,1999,60 (1):320~323

ANALYSIS ON TWO KINDS OF CHAOTIC ENCRYPTING MODES

Sun Zhihua　Hao Jianhong

(*Department of Information Engineering, North China Electric Power University ,Beijing* 102206,*China*)

Abstract This paper adopted respectively the additive masking mode and the functional encoding and decoding mode to encrypt analog signals. The comparative experiment indicates that the functional encoding and decoding mode is better than the additive masking mode in value & frequency range, and has higher security than the additive masking mode.

Key words chaos secure systems, additive masking mode, functional encoding and decoding mode, analog signals

Received 12 June 2006, revised 21 September 2006.