第 56 卷 第 12 期 2007 年 12 月
1000-3290/2007/56(12)/6857-08

物 理 学 报
ACTA PHYSICA SINICA

Vol.56,No.12,December,2007

干扰信号对两种混沌加密系统的影响及分析

郝建红[1)] 孙志华[1)] 许海波[2)]

1)(华北电力大学电气与电子工程学院,北京 102206)

2)(北京应用物理与计算数学研究所,北京 100088)

(2006 年 9 月 29 日收到;2007 年 5 月 17 日收到修改稿)

通过加入高斯白噪声干扰,对 Lorenz 和 Liu 两种混沌加密系统进行噪声干扰的分析和计算.结果表明:Liu 混沌系统抗噪声干扰能力好于 Lorenz 混沌系统,连续信源的抗干扰能力好于离散信源的抗干扰能力.

关键词:Lorenz 系统,Liu 系统,抗干扰性,信噪比

PACC:0545,4260B

1. 引 言

1963 年,Lorenz 提出了描述热对流不稳定性的模型,在三维自治系统中发现了第一个混沌吸引子,建立了 Lorenz 混沌系统[1],从此混沌科学得到迅速的发展.在短短的几十年里,混沌的概念已经渗透到数学、物理、化学、天文、地学、生物学、工程控制、信息技术、生命科学等自然科学领域以及一些社会科学领域.混沌同步在保密通信、信号处理和生命科学等方面有着广阔的应用前景和巨大的潜在价值.信号的混沌加密所要考虑的主要问题就是信号加密、解密以及信号的传输.混沌加密的方式有多种多样,但基本思路是类似的[2—4]:在发射端利用混沌信号掩盖有用信息,使之在公开信道传输中得以保密,然后在接收端采用同步装置再生用于掩盖信号的混沌信号,借此恢复传输信息.为了能对各种高频信号进行有效加密,高维宽谱的混沌同步系统应是首选.

自从 Lorenz 混沌系统和蔡氏混沌系统实现了同步控制电路之后,人们对各种混沌系统进行了大量的研究,相继出现了 Duffing 系统、Rössler 系统、Chua 系统等.最近,刘崇新等[5]提出了一种新的混沌系统——Liu 系统.由于 Lorenz 系统的带宽在 15 kHz 附近,所以它能够完全掩盖小于 15 kHz 的信源信号[6—8],但对高频(大于 15 kHz)信号,其加密效果较差.而 Liu 系统的带宽约为 40 kHz,因此 Liu 系统的频带宽于 Lorenz 系统的频带,这样 Liu 系统比 Lorenz 系统能更好地对高频率范围的信号进行加密.

在实际采集的信号以及信号的传输过程中,噪声的存在是不可避免的.噪声“污染”了信号,影响了信息加密和解密的效果,使得接收端信号发生失真甚至完全不能识别,所以研究信息混沌加密必须考虑噪声的影响[9—12].本文通过 Lorenz 和 Liu 两种混沌系统在函数调制加密方式下的加密效果进行计算和模拟,探讨了高斯白噪声干扰对两种混沌系统的加密和解密效果的影响,分析了 Liu 混沌系统在抗噪声性能上与 Lorenz 混沌系统间的差异,并进一步说明 Liu 混沌系统在混沌保密可靠性中的应用.

2. 干扰信号对混沌加密系统的影响

2.1. 干扰信号对 Liu 系统的影响

设 Liu 系统发射端系统归一化方程为

$$\dot{x}(1) = a(x(2) - x(1)), \tag{1}$$

$$\dot{x}(2) = bx(1) - kx(1)x(3), \tag{2}$$

$$\dot{x}(3) = hx^2(1) - cx(3), \tag{3}$$

其中取系统参数 $a = 10, b = 40, k = 1, c = 2.5, h = 4$.

我们采用函数调制加密方式,分别讨论信噪比为 9 dB 时干扰对信源信号加密效果的影响,其中干扰信号取图 1 所示的高斯白噪声.加密前的信源信号分别选取图 2 所示的连续信号和图 3 所示的离散信号.

2.1.1. 连续信源信号分析

考虑到任意连续信号均可通过傅里叶分析将其变换为各种频率的正弦信号的叠加,所以计算中我们选择连续信源信号为

$$m(t) = A\sin\omega t,$$

其中无量纲幅值 $A = 0.5$,频率 $f = 400$ Hz,如图 2

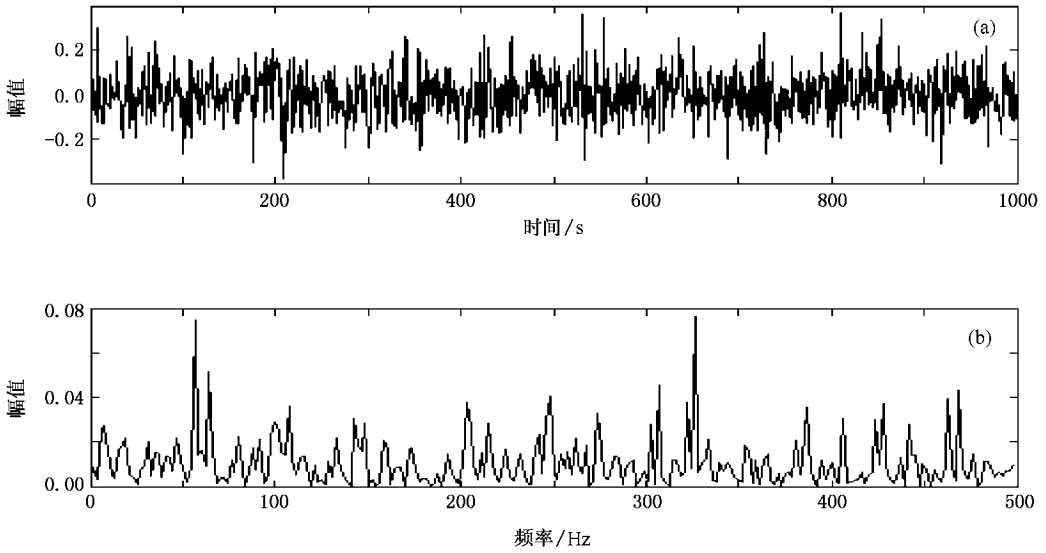

图 1 白噪声 $n(t)$及其频谱 $n(\omega)$ (a)噪声信号,(b)噪声频谱

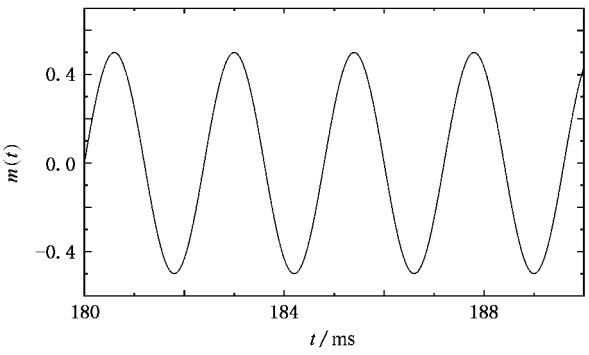

图 2 加密前输入的连续信号

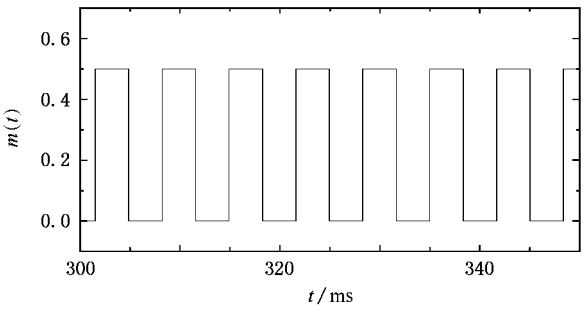

图 3 加密前输入的离散信号

所示.

为了分析干扰对信息加密的影响,考虑在传输信号过程中加入如图 1 所示的白噪声干扰信号 $n(t)$,即函数调制加密方式同步混沌系统输出端调制信号为

$$s(1) = m(t) + x(1) + n(t), \tag{4}$$

$$s(t) = 10x(2) + 30s(1)/x(3). \tag{5}$$

用调制信号驱动输出端方程,接收端系统归一化方程为

$$\dot{y}(1) = a(y(2) - s(t)), \tag{6}$$

$$\dot{y}(2) = bs(t) - ks(t)y(3), \tag{7}$$

$$\dot{y}(3) = hs^2(t) - cy(3). \tag{8}$$

图 4 给出了无噪声和有噪声两种情况下 Liu 系统对连续信号的加密和解密结果.从图 4 可以看出,有噪声干扰时,虽然系统解密后信号 $m'(t)$波形能够恢复,但在波形顶部出现了某些局部微小畸变,曲线变得不够光滑,这是由于传输过程中的加性噪声干扰使同步误差增加.对于一个混沌系统,其混沌吸引子的束缚能力越强,表征系统越不容易偏离混沌目标态转向其他的轨道.计算结果表明,在信噪比为 9 dB 时,噪声对解密信号 $m'(t)$的恢复影响不是很大,说明由于 Liu 系统混沌吸引子的束缚能力,使得低噪声干扰对信息加密过程的影响不是很大.

2.1.2. 离散信源信号分析

下面考虑信噪比仍为 9 dB 时,白噪声干扰 $n(t)$对离散信号(如图 3)加密的影响,离散信号取幅值为 0.5 的数字信号.图 5 是 Liu 系统对离散信号的加密结果.

从图 5 可以看出 在没有考虑干扰时,混沌系统输出端能很好恢复信源信号.若考虑传输中的干扰影响,输出端的解密信号顶部出现不光滑失真.

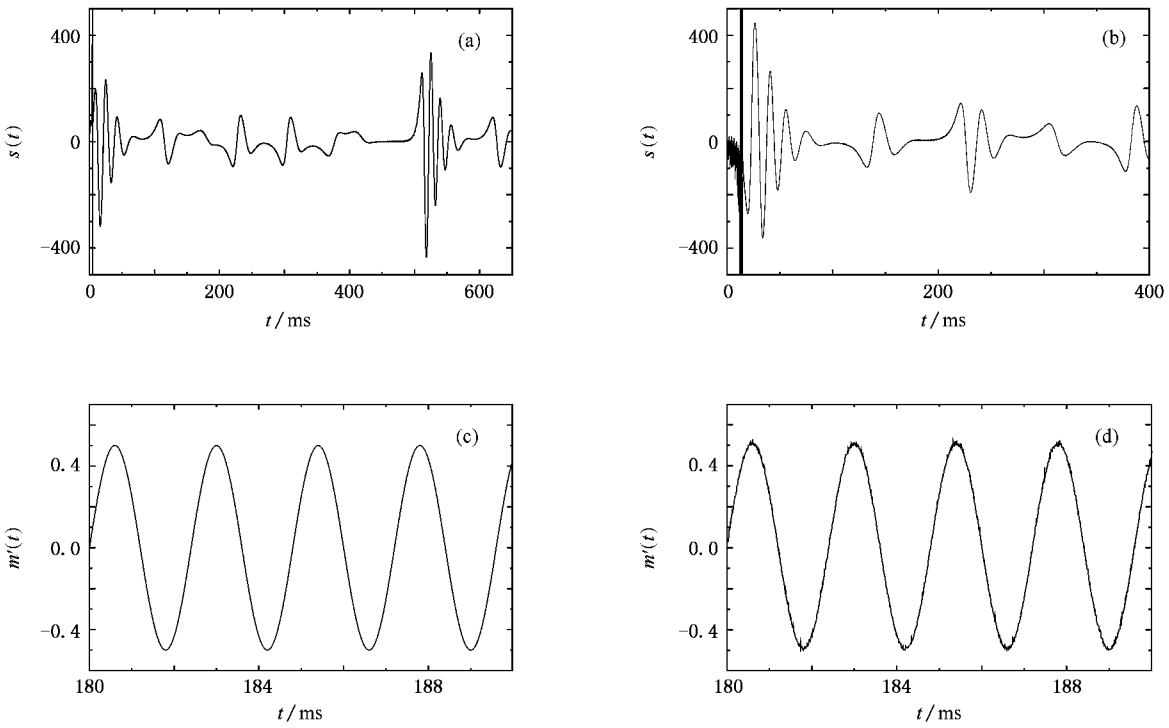

图 4　Liu 系统对连续信号进行加密时的抗干扰性　(a)无噪声情况的加密信号，(b)有噪声情况的加密信号，(c)无噪声情况的解密信号，(d)有噪声情况的解密信号

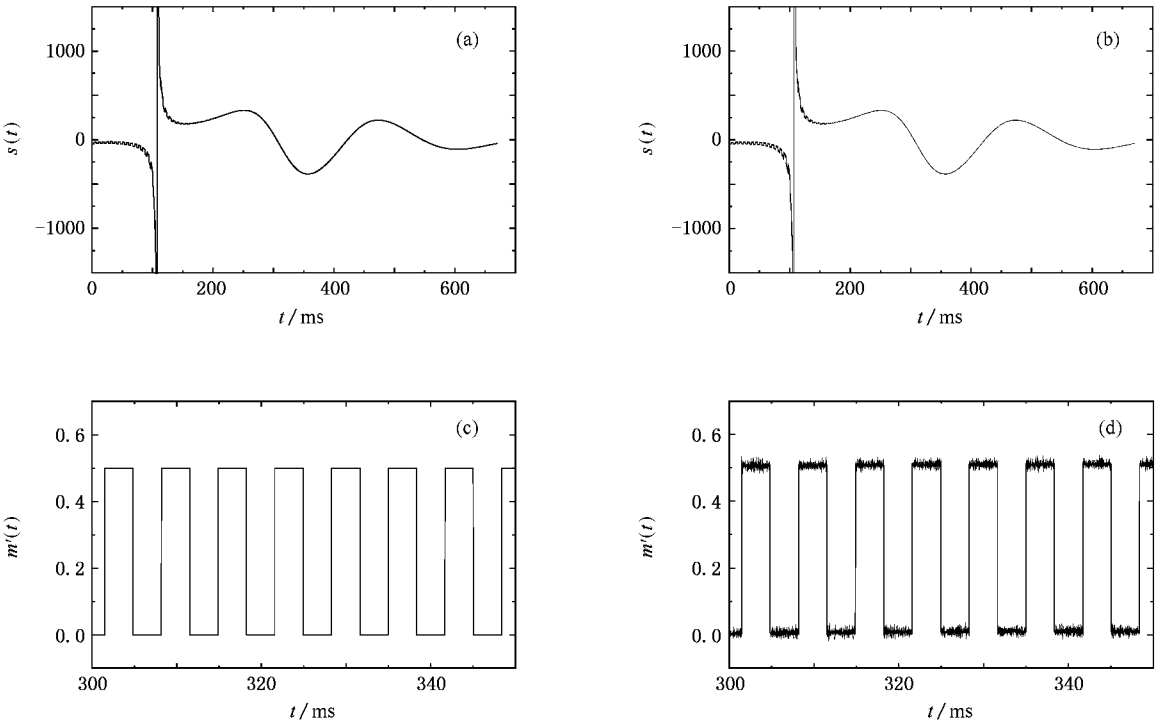

图 5　Liu 系统对离散信号进行加密时的抗干扰性　(a)无噪声情况的加密信号，(b)有噪声情况的加密信号，(c)无噪声情况的解密信号，(d)有噪声情况的解密信号

2.2. 干扰信号对 Lorenz 系统的影响

Lorenz 系统方程参数可参阅文献[13—15]，信源信号和干扰信号的选择与上相同.

白噪声干扰 $n(t)$ 对 Lorenz 系统的连续信号和离散信号的加密影响如图 6 和图 7 所示.

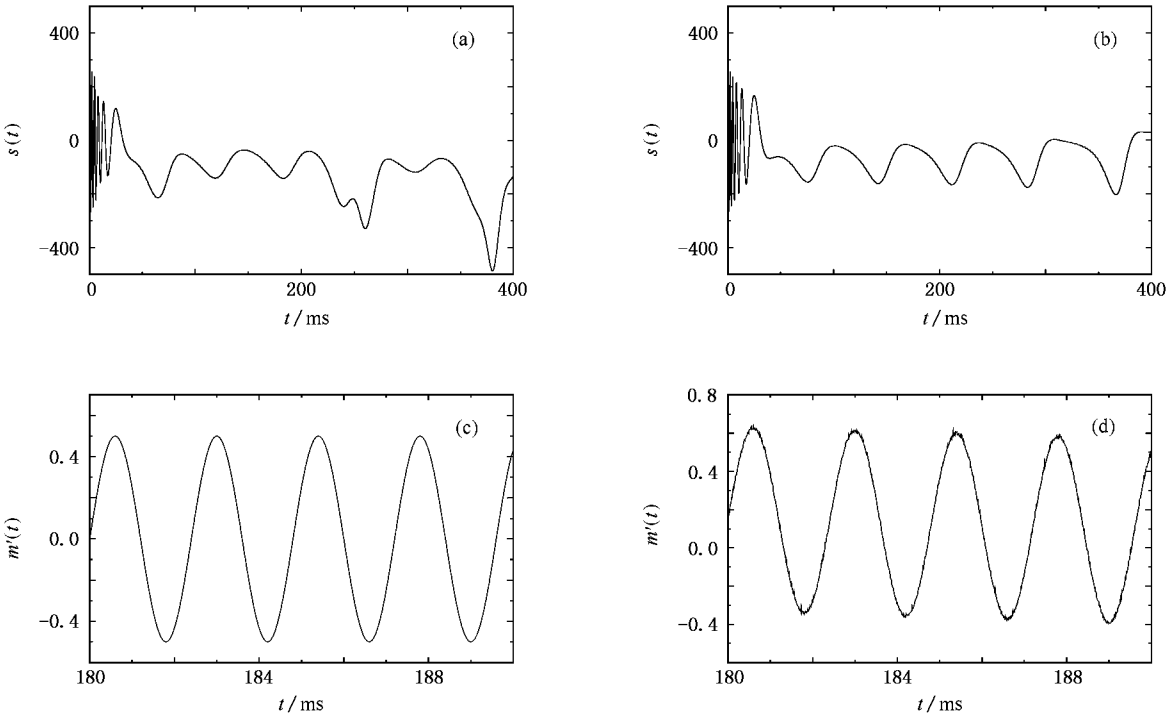

图 6 Lorenz 系统对连续信号进行加密时的抗干扰性 (a)无噪声情况的加密信号，(b)有噪声情况的加密信号，(c)无噪声情况的解密信号，(d)有噪声情况的解密信号

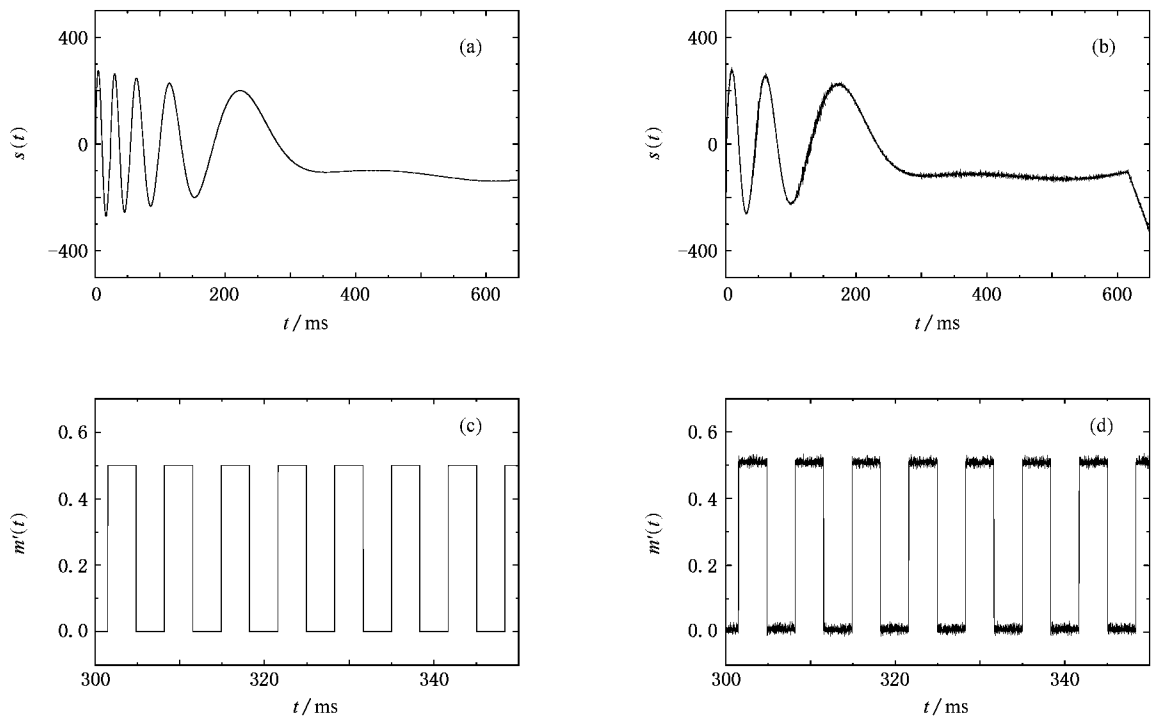

图 7 Lorenz 系统对离散信号进行加密时的抗干扰性 (a)无噪声情况的加密信号，(b)有噪声情况的加密信号，(c)无噪声情况的解密信号，(d)有噪声情况的解密信号

从图 6 和图 7 可以看出，考虑噪声影响时解密后的信号出现时间延迟(误码率)和幅值跳动．与 Liu 系统相同，Lorenz 系统对离散信号进行加密时的抗干扰性不如连续信号好，表明 Lorenz 吸引子对离散信号的束缚能力不如对连续信号的束缚能力．

3. Lorenz 系统和 Liu 系统的抗噪声能力比较

下面我们分析比较噪声对两种系统加密效果的影响，其中干扰仍考虑高斯白噪声，信源信号选取图 2 所示的连续信号．在连续信号功率一定的情况下，通过改变高斯白噪声的功率来调节信噪比，比较不同信噪比时两种混沌加密系统的加密和解密效果的变化，以此考察两种系统抗噪声能力的强弱．

3.1. Lorenz 系统的抗干扰分析

图 8 是 Lorenz 系统在信噪比分别是 7.9，7.2 和 6.8 dB 时抗干扰能力的计算结果．

我们知道，混沌吸引子内涵丰富，内嵌有无穷多不稳定周期轨道，且对微小的外部扰动极为敏感．因此在噪声的干扰下混沌系统的随机性有所增加，导致混沌系统内部不稳定轨线走出混沌吸引域的概率增大，混沌吸引子的束缚能力将有所减弱．从图 8 可以看出：当信噪比为 7.9 dB 时，解密后的信源信号曲线较光滑，较好地恢复了信源信号．当信噪比为 7.2 dB 时，解密后的信源信号曲线粗糙，出现明显的杂波畸变．当信噪比继续减小到 6.8 dB 时，解密后

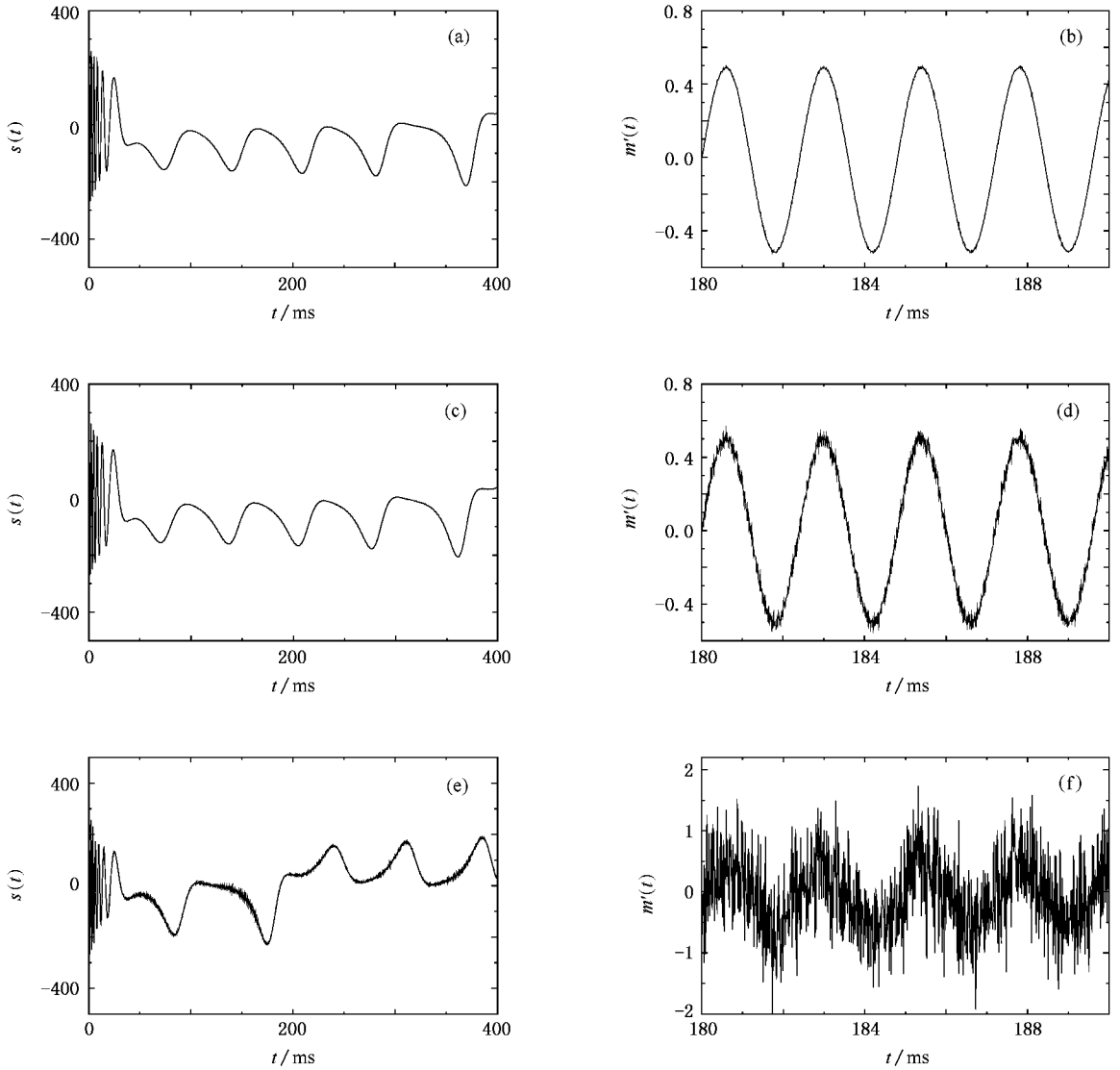

图 8　Lorenz 系统在不同信噪比下的抗干扰性　(a)和(b)分别是信噪比为 7.9 dB 时的加密信号和解密输出信号，(c)和(d)分别是信噪比为 7.2 dB 时的加密信号和解密输出信号，(e)和(f)分别是信噪比为 6.8 dB 时的加密信号和解密输出信号

图形虽保留了正弦曲线的信息,但波形失真严重.噪声信号是一种加性干扰,噪声干扰越大,它对混沌吸引子束缚能力的破坏力也越大.上述结果表明,当噪声干扰比较小时,其 Lorenz 混沌吸引子仍能将相点束缚在轨道内,但当噪声干扰增大到一定程度后干扰信号就会从混沌载体中浮现出来,对混沌吸引子的束缚能力产生明显的影响,进而影响信号的恢复.通过对比可知,当信噪比大于 7.9 dB 时,Lorenz 系统对连续信号有较好的抗噪声干扰能力.

3.2. Liu 系统的抗干扰分析

图 9 是 Liu 系统在信噪比分别是 7.2,6.4 和 6 dB 时的计算结果.从图 9 可以看出:当信噪比为 7.2 dB 时,解密后的信源信号曲线较光滑,较好地恢复了信源信号.当信噪比为 6.4 dB 时,解密后的信号曲线出现不光滑,有小的扰动.这是由于噪声使系统在达到控制目标的过程中出现小扰动,对解密效果造成影响.当信噪比为 6 dB 时,解密后图形也出现类似正弦的曲线,但幅值失真严重.这说明在没有噪声的情况下,系统的混沌吸引子能很好将其相点控制在混沌不稳定轨道上,不会出现扰动.在有噪声的情况下,由于噪声是随机变化和毫无规律的,混沌吸引子在混沌系统内不稳定轨道上控制其相点的能力受噪声影响,易出现扰动.结果表明,当信噪比大于 7.2 dB 时,Liu 系统对连续信号有较好的抗噪声干扰能力.

对于离散信号,用同样的方法可以分析不同信噪比情况下两种系统的抗干扰能力,数值计算结果

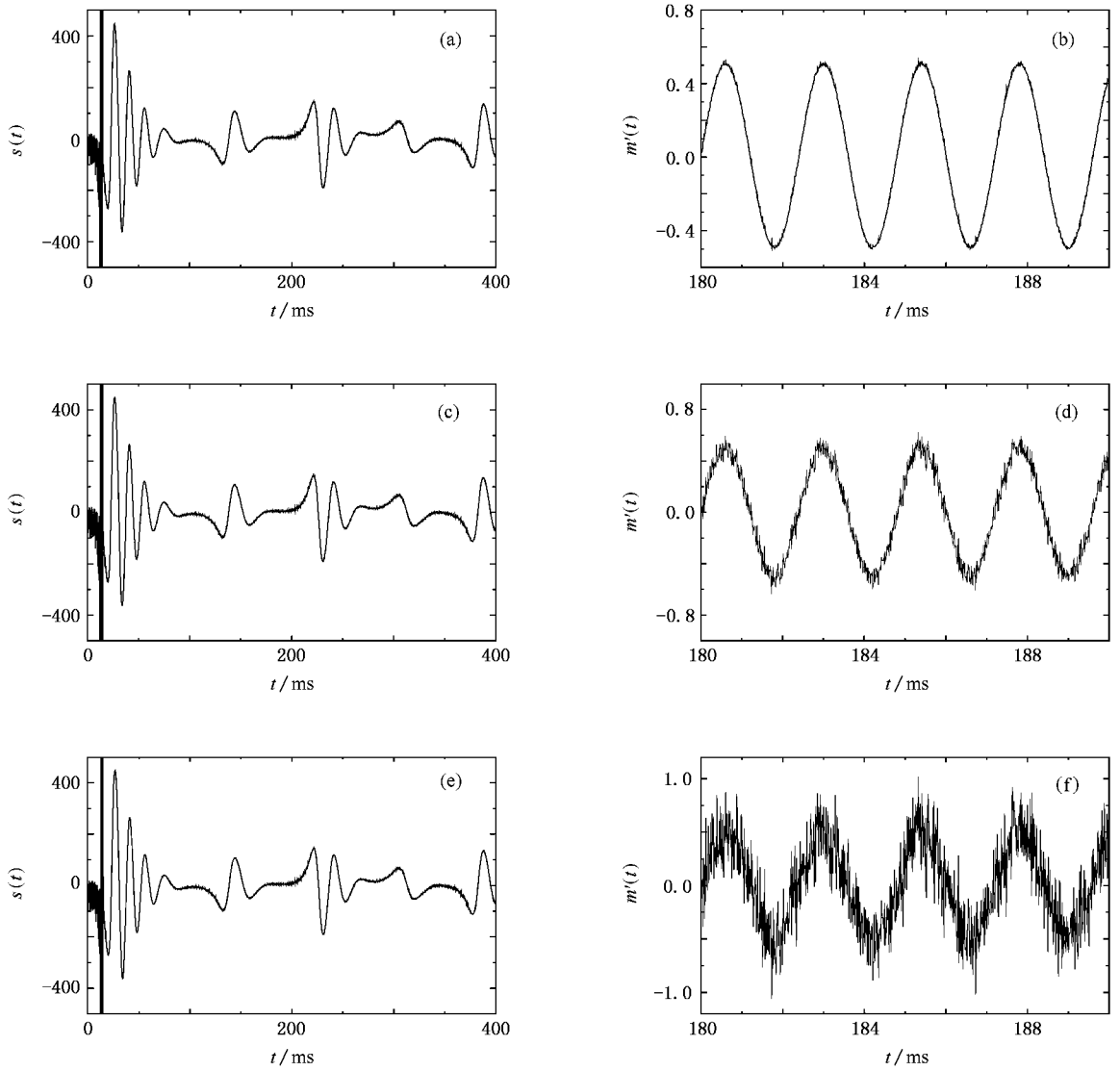

图 9 Liu 系统在不同信噪比下的抗干扰性 (a)和(b)分别是信噪比为 7.2 dB 时的加密信号和解密输出信号,(c)和(d)分别是信噪比为 6.4 dB 时的加密信号和解密输出信号,(e)和(f)分别是信噪比为 6 dB 时的加密信号和解密输出信号

如下：(1) Liu 系统在信噪比大于 8.7 dB 时具有良好的抗噪声能力，而 Lorenz 系统在信噪比大于 10 dB 时才具有良好的抗噪声能力.这是因为噪声相当于在信道中加上了一个随机信号，而 Liu 系统的带宽比 Lorenz 系统要宽 20 kHz 以上，这样加性干扰信号对 Lorenz 系统的影响就要比对 Liu 系统的影响大得多.(2) 对比连续信号与离散信号上的信噪比临界值，表明无论是 Liu 系统还是 Lorenz 系统，噪声干扰对连续信号的加密效果影响小于噪声干扰对离散信号的加密效果影响.

离散信号可以看成是很窄的矩形波，由傅里叶分析可以知道矩形波是由各种成分的谐波组成，而频率越高的谐波强度也越小.这样，一些高频谐波(大于系统频宽)成分与干扰信号叠加就会浮在混沌载体之外，对加密和解密效果产生较大的影响.另一方面，这些强度弱小的高频谐波极易受到加性噪声信号的干扰，产生较大的误码率.

4. 结　论

通过对 Liu 系统和 Lorenz 系统的混沌加密效果计算，分析了信号传输过程中的噪声干扰对加密解密效果的影响.结果表明：无论是 Liu 系统还是 Lorenz 系统，噪声干扰对离散信号的解密效果影响比对连续信号的解密效果影响要大，这大概是由于离散信号出现的无限多个奇异点对混沌吸引子的束缚力有较大破坏力的缘故.Liu 系统在连续信号的抗干扰能力方面与 Lorenz 系统相差不多，但在离散信号上的抗干扰能力方面 Liu 系统比 Lorenz 系统更好.与 Liu 系统相比，Lorenz 系统的误码率较大，这是由于 Liu 系统比 Lorenz 系统频谱宽，能遮掩离散信号中较多的高频谐波成分.

[1] Lorenz E N 1963 *J. Atoms. Sci.* **20** 130

[2] Liu Z H, Chen S G, Hu B 1999 *Phys. Rev. Lett.* **46** 2817

[3] Bunner M J 1998 *Phys. Rev. Lett.* **44** 233

[4] Pecora L M, Carroll T L 1990 *Phys. Rev. Lett.* **64** 821

[5] Liu C X, Liu T, Liu L, Liu K 2004 *Chaos Solitons Fract.* **22** 1031

[6] Perez G, Cerdeira H A 1995 *Phys. Rev. Lett.* **74** 1970

[7] Short K M 1994 *Int. J. Bifur. Chaos* **4** 959

[8] Liao T L, Huang N S 1999 *IEEE Trans. Circuits Syst.* Ⅰ **46** 1144

[9] Pecora L M, Carroll T L 1991 *Phys. Rev.* A **44** 2374

[10] Yang J Z, Hu G, Xiao J H 1998 *Phys. Rev. Lett.* **80** 496

[11] Boutayeb M, Darouach M, Rafaralahy H 2002 *IEEE Trans. Circuits Syst.* Ⅰ **49** 345

[12] Cuomo K M, Oppenheim A V 1993 *Phys. Rev. Lett.* **71** 65

[13] Hu G, Xiao J H, Zheng Z G 2000 *Chaos Control* (Shanghai: Shanghai Scientific and Technological Publishing House) (in Chinese) [胡　岗、萧井华、郑志刚 2000 混沌控制(上海：上海科技教育出版社)]

[14] Yan S L, Chi Z Y, Chen W J, Wang Z N 2004 *Acta Phys. Sin.* **53** 1704 (in Chinese) [颜森林、迟泽英、陈文建、王泽农 2004 物理学报 **53** 1704]

[15] Tang G N, Luo X S 2004 *Acta Phys. Sin.* **53** 15 (in Chinese) [唐国宁、罗晓曙 2004 物理学报 **53** 15]

Analyzing the noise resistance effect for two chaos secure systems

Hao Jian-Hong[1)] Sun Zhi-Hua[1)] Xu Hai-Bo[2)]

1)(*School of Electric and Electronic Engineering*, *North China Electric Power University*, *Beijing* 102206, *China*)

2)(*Institute of Applied Physics and Computational Mathematics*, *Beijing* 100088, *China*)

(Received 29 September 2006; revised manuscript received 17 May 2007)

Abstract

In consideration of interfering Gauss noise, the results of encoding and decoding are simulated and analyzed for the Lorenz chaotic system and Liu chaotic system. It was shown that the capacity of Liu chaotic system resisting noise is better than that of Lorenz chaotic system, and the capacity of the continuous signal resisting noise is superior to that of the discrete signal resisting noise during the encoding and decoding processes.

Keywords: Lorenz chaotic system, Liu chaotic system, resisting noise performance, signal-to-noise ratio

PACC: 0545, 4260B