第 54 卷 第 3 期 2005 年 3 月
1000-3290/2005/54(03)/1267-06

物 理 学 报
ACTA PHYSICA SINICA

Vol.54,No.3,March,2005

一种超混沌系统的加密特性分析

谢 鲲[1)] 雷 敏[2)] 冯正进[1)]

[1)](上海交通大学机电控制研究所,上海 200030)

[2)](新加坡南洋理工大学,新加坡)

(2003 年 6 月 30 日收到;2004 年 7 月 10 日收到修改稿)

把欠采样的思想用于混沌保密通信系统的设计中,对 Lorenz 系统及一种典型的超混沌系统的时间序列进行了分析. 研究发现,加密系统的安全性不仅取决于系统维数,而且还与采样间隔的选取有关. 用 VWK 非线性检验方法和替代数据检验方法对上述混沌加密系统在不同采样间隔时的输出信号进行了检验.

关键词:混沌加密,时间序列分析,VWK 非线性检验,替代数据检验

PACC:4610,0350D,0530

1. 引 言

混沌系统以其类噪声及对初值高度敏感性的特点,越来越多地被应用到保密通信系统的设计中. 然而,研究者大多关注的是如何采用高维混沌系统[2],增加破译的难度. 实际上,高维混沌系统不仅给设计带来很多麻烦,而且研究证实有些系统已被现有的破解方法所破译[3]. 研究发现,混沌加密系统在不同采样间隔时的输出信号的类随机性不同. 根据这一特点,本文对一种典型的超混沌系统进行了分析,得出欠采样间隔有助于提高混沌加密系统的安全性的结论.

2. 基于 Volterra-Wiener-Korengerg (VWK)检验的非线性分析

2.1. 采样间隔的影响

以 Lorenz 系统[4] 为例,来分析采样间隔对 VWK 方法的影响.

Lorenz 系统:

$$\begin{cases} \dot{x} = \sigma(y - z), \\ \dot{y} = \gamma x - y - xz, \\ \dot{z} = -bz + xy, \end{cases} \tag{1}$$

式中 $\sigma = 10$,$\gamma = 28$,$b = 8/3$,混沌信号 $x(t)$ 为加密密钥.

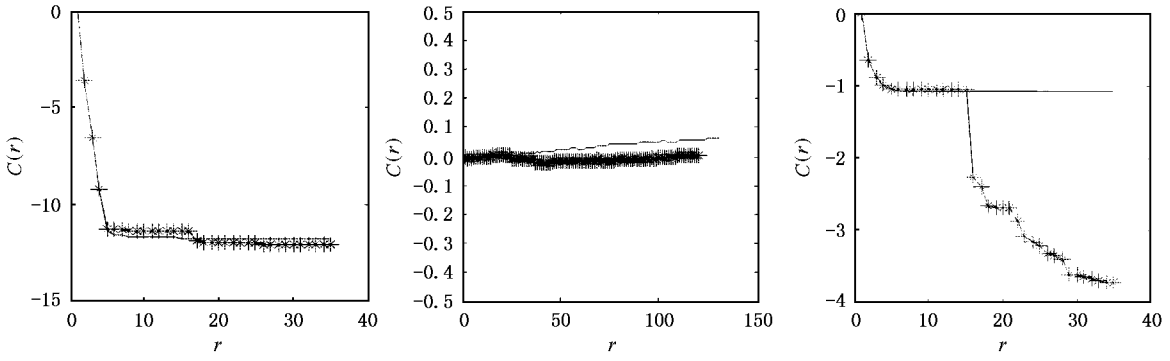
采样间隔对 VWK 检验方法的影响如图 1 所示. 由图 1 可见,$\tau = 0.005$ 时,原始数据以线性模型为主,即 $C^{\mathrm{lin}}(r) \approx C^{\mathrm{nl}}(r)$,此时的原始时间序列总显示出线性特性,这说明若 τ 选择得过小,难以给出准确的检验结果,但对于破译者,则可利用这一特点,对其进行线性重构(即线性建模[3,5]),达到破译的目的;$\tau = 1$ 时,线性模型和非线性模型的信息准则很相似,都是很小的值,不足以得出原始数据有非线性特性的结论,说明在 τ 为欠采样间隔时,原始数据更类似于噪声,该检验方法不能确定原始数据中存在非线性成分,使破译者不能分清楚是确定性信号还是噪声,进而不能达到破译的目的;$\tau = 0.1$ 时,$C^{\mathrm{nl}}(r)$ 明显地小于 $C^{\mathrm{lin}}(r)$,可判断出原始序列是非线性时间序列,但这样的采样间隔不可靠,因为破译者可利用非线性重构的方法(如吸引子重构[6,7])对其进行破译.

考虑到在欠采样间隔时,VWK 检验方法不能判断出时间序列中是否存在确定性成分,说明此时的原始时间序列与噪声完全类似. 从这个角度来看,可以利用 VWK 检验法来分析混沌系统所产生的时间序列,若不能检验出是线性或非线性,则表明该混沌时间序列类似于噪声,更具有保密性.

2.2. 超混沌系统非线性检验分析

$$\begin{cases} \dot{x}_1 = -x_2 + ax_1, \\ \dot{x}_m = x_{m-1} - x_{m+1}, \quad m = 2,\cdots,M-1, \\ \dot{x}_M = \varepsilon + bx_M(x_{M-1} - d), \end{cases} \tag{2}$$

式中 $a = 0.29$,$b = 4$,$d = 2$,$\varepsilon = 0.1$. 当 $M = 11$,系统



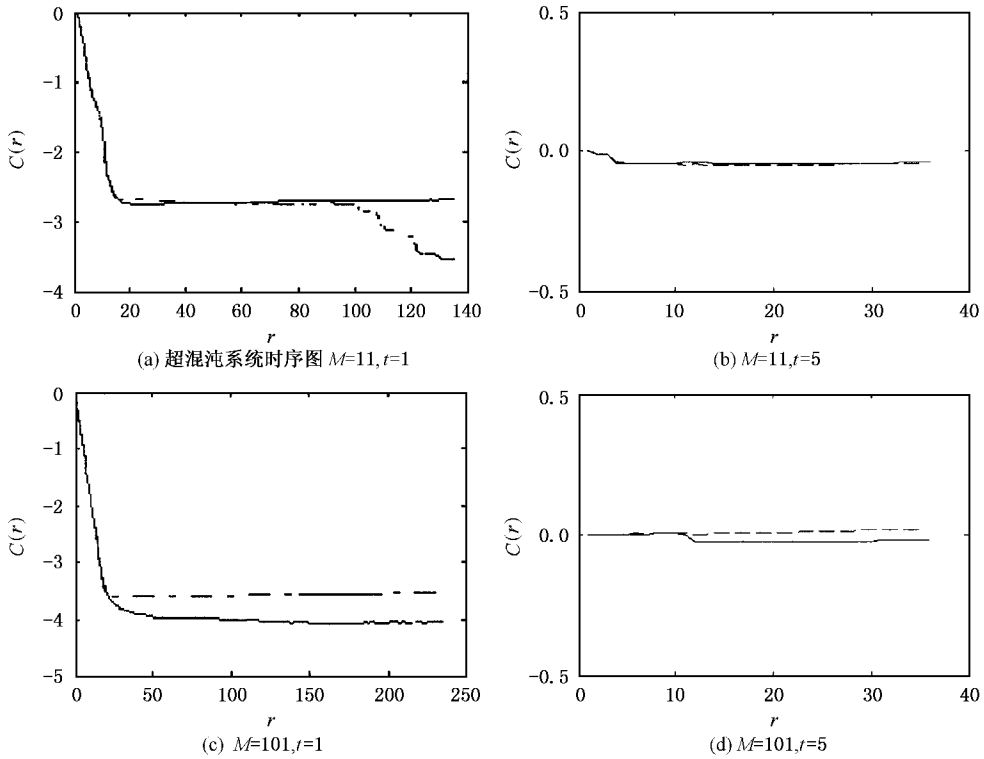
(a) τ=0.005 (b) τ=1 (c) τ=0.1

图 1 采样间隔对 VWK 检验法的影响 * 为 $C^{nl}(r)$，——为 $C^{lin}(r)$

的混沌吸引子维数 $D_L = 10.02$；当 $M = 101$，$D_L = 100.02$[8]．

图 2(a)为 11 维超混沌时间序列(由(2)式产生)，其中采样间隔 $t = 1$，可以看出，$C^{nl}(r)$明显地小于 $C^{lin}(r)$，说明尽管此时的混沌时间序列从表面上看类似于噪声，但却可以用非线性模型描述，即此时的混沌时间序列同样不具有保密性，那么采样间隔再增大一些时，情况是否会好一些呢？图 2 (b)为采样间隔 $t = 5$ 时的相应检验结果，可以看出，$C^{nl}(r)$和 $C^{lin}(r)$均较小，表明此时的混沌时间序列类似于噪声，很难用线性模型或非线性模型描述．还研究维数高达 101 维的超混沌系统的情况，如图 2 (c)和(d)所示．图 2 (c)为采样间隔 $t = 1$ 时的相应结果，可以看出，$C^{nl}(r)$和 $C^{lin}(r)$均较大，说明此时的混沌时间序列同样不具有安全性，因为它能够用确定模型描述．同样当采样间隔 $t = 5$ 时，$C^{nl}(r)$和 $C^{lin}(r)$也均较小，表明增大采样间隔后，该混沌信号的随机性增强，从而保密性得以提高．

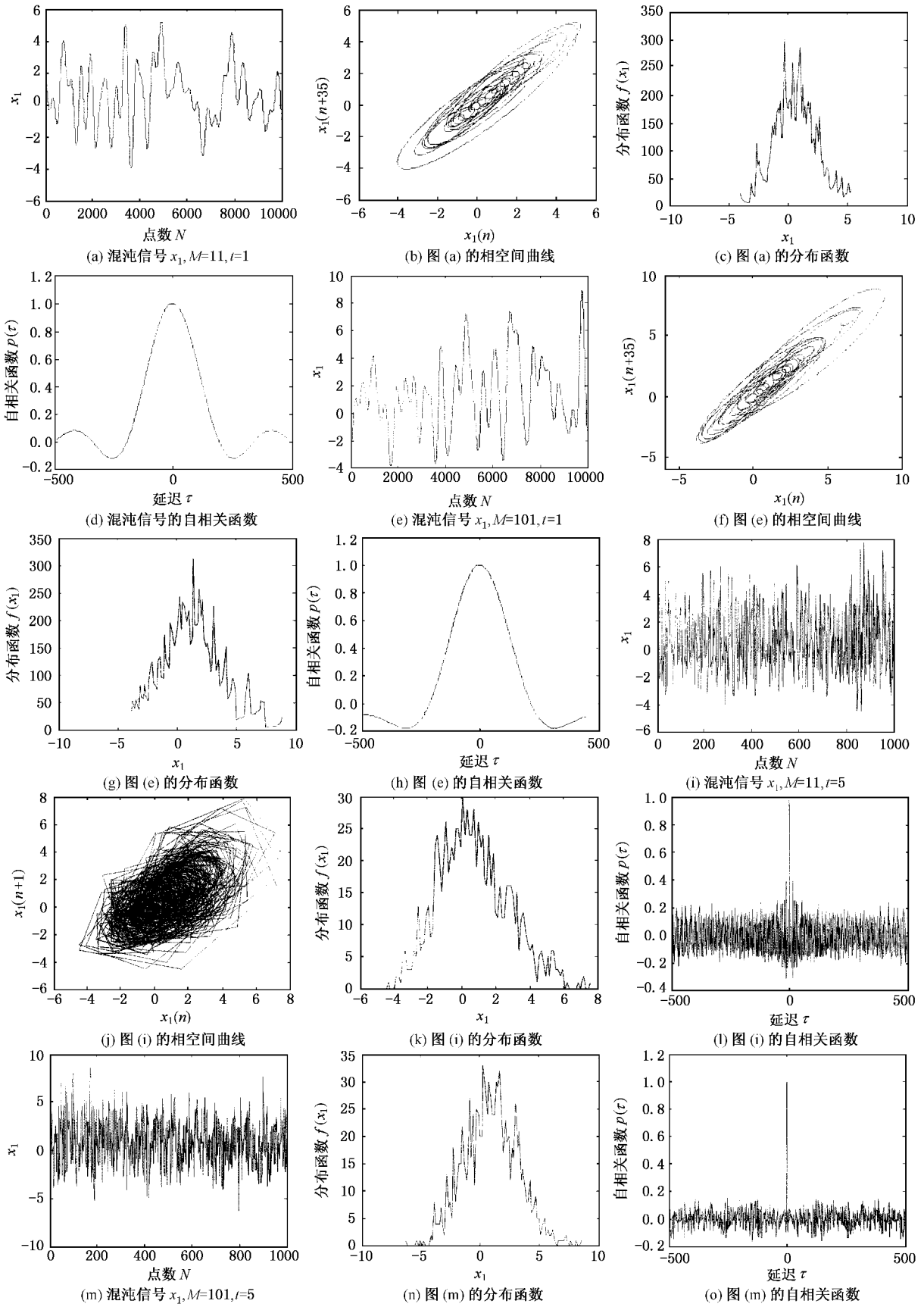
从图 2(b)和(d)，看到在同样的采样间隔下，超混沌系统仍然表现出了确定性成分，因此说加密系统的安全性不单单由系统维数决定，更主要的是采样间隔的选取．由于计算能力的限制，这里只给出



(a) 超混沌系统时序图 M=11, t=1 (b) M=11, t=5

(c) M=101, t=1 (d) M=101, t=5

图 2 超混沌加密系统时间序列的 VWK 检验 - - - 为非线性，——为线性



(a) 混沌信号 $x_1, M=11, t=1$　(b) 图 (a) 的相空间曲线　(c) 图 (a) 的分布函数

(d) 混沌信号的自相关函数　(e) 混沌信号 $x_1, M=101, t=1$　(f) 图 (e) 的相空间曲线

(g) 图 (e) 的分布函数　(h) 图 (e) 的自相关函数　(i) 混沌信号 $x_1, M=11, t=5$

(j) 图 (i) 的相空间曲线　(k) 图 (i) 的分布函数　(l) 图 (i) 的自相关函数

(m) 混沌信号 $x_1, M=101, t=5$　(n) 图 (m) 的分布函数　(o) 图 (m) 的自相关函数

图 3　超混沌系统分析图

了 $k \leqslant 50, d \leqslant 3$ 时的最佳结果.

3. 超混沌系统的密码学特性分析

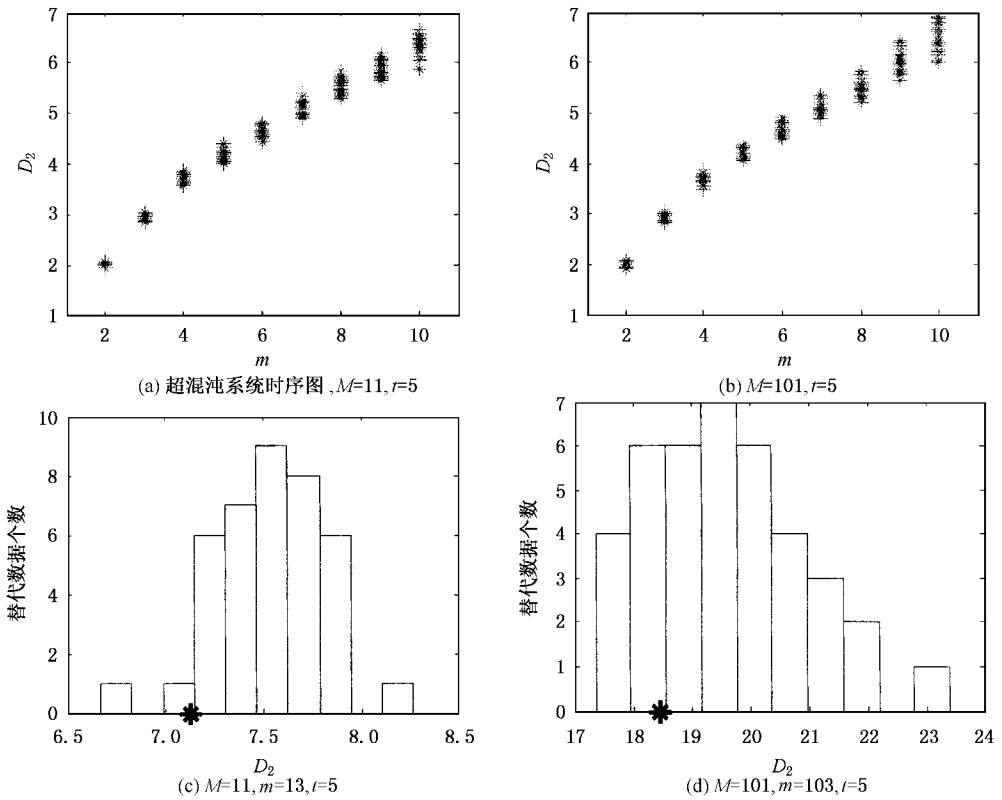
超混沌系统(2)的时间序列分析如图 3(a)—(o)所示. 首先研究小采样间隔的情况. 当 $t = 1$ 时,从图 3(a)—(h)发现无论 M 有多高,11 或者 101,结果都是一样,混沌曲线均存在局部线性化的特征. 相空间曲线非常光滑,且其自相关函数的 δ 特性不好. 这些分析表明在小采样间隔时,即使超混沌系统结构再复杂,它仍易受到线性预测和相空间重构方法的攻击[9]. 换言之,这种混沌系统不具有足够的加密特性. 如果加大采样间隔,令 $t = 5$,情况则完全不同(图 3(i)—(o)),加密系统的自相关特性好了许多. 另外,在同样的数据长度下($N = 1000$),混沌系统维数越高,它的时间序列的自相关性就越好,亦即系统的加密特性越强. 图 3(c),(g),(k),(n) 表明系统维数和采样间隔对混沌信号的分布不会造成太大的影响.

通过上面对超混沌系统的分析,基本上可以得出结论:混沌系统在欠采样间隔时更适合加密,具有更好的加密特性. 以上采用的是 VWK 检验方法对该超混沌在欠采样间隔时的密码学特性进行了分析. 下面采用非线性检验方法中另外一种方法——替代数据检验对该系统在同样欠采样间隔时的特性进行分析.

4. 基于替代数据方法的非线性检验分析

从超混沌系统(2)的时间序列中选择 1000 个点. 令采样间隔 $t = 5$,然后根据文献[11]中零假设,基于文献[9]中提出的算法,产生 39 组替代数据. 如果置信度是 p,那么替代数据集 $B_{\min} = 2/(1 - p) - 1$. 因此,如果 $p = 95\%$,$B_{\min} = 39$[12],检验统计量是相关维:$D = \lim\limits_{l \to 0} \dfrac{\ln C(l)}{\ln(l)}$.

对于 $M = 11$ 的超混沌系统(图 4(a)),当 $m = 2$—10,替代数据和原始数据没有明显的差异,零假设被接受. 如果 $m > 11$,情况会怎样?如图 4(c),$m = 13$. 仍然不能在原始数据和替代数据间找出不同点,这表明如果解密者在不知道系统结构的情况下,想从背景噪声中提取有用信息基本上不可能. 在系统维数更高,M 达到 101 时,结果与上面相同(图 4(b) 和 (d)).



(a) 超混沌系统时序图,M=11, t=5 (b) M=101, t=5

(c) M=11, m=13, t=5 (d) M=101, m=103, t=5

图 4 基于替代数据检验的混沌加密系统的分析结果

5. 结　论

本文提出一有效方法来提高混沌加密系统的安全性. 首先,通过研究采样间隔对 VWK 检验方法的影响,发现在欠采样间隔时,原始数据不仅明显类似于随机噪声,而且它本质上也表现出随机性. 对于攻击者而言,用模型方法预测混沌系统的时间序列非常难,不能进行有效破译[10]. 其次,基于 VWK 检验方法,对一种典型的超混沌系统进行了分析. 结果表明,如果采样间隔太小,即使加密系统维数再高,系统本身仍表现出确定性特征,不具有安全性. 另外,如果采样间隔过大,系统的加密特性同样不好. 只有在欠采样间隔时,系统输出才类似随机. 运用替代数据检验方法对上述超混沌系统在欠采样间隔时进行了分析,得出了与 VWK 方法检验相同的结论. 因此,在设计混沌加密系统时,不仅应该考虑采用高维系统,还要考虑合适的采样间隔.

附录　VWK 检验原理

对于一个动态系统,设其输入、输出的采样点分别为 $\{x_n\}_{n=1}^{N}$, $\{y_n\}_{n=1}^{N}$,采样间隔为 τ, N 为数据长度. 若利用 x_n, x_{n-1}, …, x_{n-k+1},则其离散 Volterra 序列可由 y_n 的 Taylor 多项式展开,其中 k 为系统阶次. Barahona[1] 提出了一种利用 y_n 反馈(即令 $x_n = y_{n-1}$)的闭环 Volterra 序列,可通过下式计算:

$$\begin{aligned} y_n^{\mathrm{cala}} &= a_0 + a_1 y_{n-1} + a_2 y_{n-2} + \cdots + a_k y_{n-k} + a_{k+1} y_{n-1}^2 \\ &\quad + a_{k+2} y_{n-1} y_{n-2} + \cdots + a_{M-1} y_{n-k}^d \\ &= \sum_{m=0}^{M} a_m z_m(n), \end{aligned} \tag{A1}$$

式中 $\{z_m(n)\}$为由嵌入空间坐标($y_{n-1}, y_{n-2}, \cdots, y_{n-k}$)的所有不同组合,$d$ 为其最高组合度,k 为模型阶次,整体维数 $M = (k+d)!/(d!\,k!)$. k 相当于嵌入空间的维数,d 相当于模型的非线性度. 于是利用一步预报误差,就可计算出上述模型的短期预报误差功率,即

$$\varepsilon(k,d)^2 \equiv \frac{\sum_{n=1}^{N} (y_a^{\mathrm{calc}}(k,d) - y_n)^2}{\sum_{n=1}^{N} (y_n - \bar{y})^2}, \tag{A2}$$

式中 $\bar{y} = \frac{1}{N}\sum_{n=1}^{N} y_n$, $\varepsilon(k,d)^2$ 为残差的正规化方差值.

由(A1)和(A2)式可知,该方法必须先给出合适的 k 和 d 值,最佳值 k_{opt}和 d_{opt}是使信息准则 $C(r)$最小的 k 和 d, $C(r)$可由下式计算:

$$C(r) = \log\varepsilon(r) + r/N. \tag{A3}$$

当 $d = 1$ 时,VWK 模型为线性模型;当 $d > 1$ 时,VWK 模型为非线性模型. 需要指出的是,当 k_{opt}较大时,M 会很大,从而导致 $d > 1$ 时计算量巨增,为此,可以适当地同时调整 k 和 d 值,尽量使 $C^{\mathrm{nl}}(r)$小于 $C^{\mathrm{lin}}(r)$,这时的 k 和 d 即为 k_{opt}和 d_{opt}.

[1] Barahona M 1996 *Nature* **381** 215

[2] Cheng L 2003 *Acta Phys. Sin.* **52** 536 (in Chinese) [程　丽 2003 物理学报 **52** 536]

[3] Gibson J F *et al* 1992 *Physica* D **57** 1

[4] Guan X P 2001 *Acta Phys. Sin.* **50** 26 (in Chinese) [关新平 2001 物理学报 **50** 26]

[5] Robert C 1996 *Int. J. Bifurc. Chaos* **6** 377

[6] Kennel M 1992 *Phys. Rev.* A **45** 3403

[7] Palus M 1992 *Physica* D **55** 221

[8] Abarbanel H D I 1993 *Rev. Mod. Phys.* **65** 1331

[9] Lei M 2001 *Phys. Lett.* A **290** 297

[10] Lei M 2002 *Chaotic Time Series Analysis and Its Application Study on Chaotic Encryption System* (Shanghai: Shanghai Jiaotong University Press)

[11] Parlitz U 1997 *Int. J. Bifurc. Chaos* **7** 407

[12] Theiler J 1996 *J. Physica* D **94** 221

A study of a kind of hyper chaotic cryptosystem security

Xie Kun[1)] Lei Min[2)] Feng Zheng-Jin[1)]

[1)] (*Institute of Mechatronic Control*, *Shanghai Jiaotong University*, *Shanghai* 200030, *China*)

[2)] (*Singapore Nanyang Technological University*, *Singapore*)

(Received 30 June 2003; revised manuscript received 10 July 2004)

Abstract

In this note, we apply the sub-sampling idea to the design of the chaotic secure communication system and analyze the Lorenz system and a kind of hyper chaotic system. The result obtained indicates that the security of the cryptosystem is not only determined by the dimension, but also related with the sampling interval. Then, we verify these two systems using the VWK (Volterra-Wiener-Korengerg) nonlinear test and surrogate data test methods.

Keywords: chaotic encryption, time series analysis, VWK nonlinear test, surrogate data

PACC: 4610, 0350D, 0530