一种增强混沌系统保密性能的新方法 [1]

谢 鲲 雷 敏* 冯正进

(上海交通大学机电控制研究所 上海 200030)
*(新加坡南洋理工大学 新加坡)

摘 要: 该文从研究混沌加密系统输出信号的保密性能角度出发,对典型的 Lorenz 系统进行了分析.研究发现,大采样间隔对增强混沌系统的保密性能有重要影响.然后用 Volterra-Wiener-Korengerg(VWK)模型非线性检验方法对上述结论进行了检验,最后通过计算机仿真得出相同的结论.

关键词: 混沌加密,时间序列分析, VWK 检验
中图分类号: TN918 **文献标识码**: A **文章编号**: 1009-5896(2004)09-1401-06

A New Method for Improving the Encryption Property of the Chaotic System

Xie Kun Lei Min* Feng Zheng-jin

(*Institute of Mechatronic Control, Shanghai Jiaotong Univ., Shanghai* 200052, *China*)

*(*Singapore Nanyang Technological University, Singapore*)

Abstract In this paper, the encryption property of the chaotic system in terms of the techniques developed in the analysis of chaotic time series is studied. Then, the typical Lorenz system is analyzed. It is found that the larger sampling interval is of huge help for improving the encryption property. The VWK(Volterra-Wiener-Korengerg) method is used to analyze and test. Finally, simulation on the computer gets the same result.

Key words Chaos encryption, Time series analysis, VWK(Volterra-Wiener-Korengerg) test

1 引言

混沌系统和密码学有着一些共同的特点,于是诱发了人们想要用混沌动力学系统对信息进行加密的思想.用于保密通信的混沌系统有两类:一类是连续的,如 Lorenz , Rossler 系统等.另一类是离散的,如 logistic 映射.在现代控制系统中,通常被控的对象是连续时间的 (物理) 子系统,而控制器是由逻辑控制器或计算机构成的离散子系统.随着计算机和逻辑控制器技术的不断发展,连续混沌系统越来越多地用于信息加密.这样就构成了连续-离散混合系统.那么,这就涉及到采样间隔的选取同系统加密安全性的问题.如何判定采样间隔是否合适,什么样的间隔更有利于增强系统的密码学特性呢?目前这方面的研究还很少.本文将从这一角度出发,以典型的 Lorenz 混沌系统为例,进行分析.进一步,应用非线性检验方法中的 VWK(Volterra-Wiener-Korengerg) 方法对所得结论进行验证.

2 典型混沌系统保密性能分析 [1]

在设计混沌保密通信系统时,需要考虑两个方面: (1) 所给的混沌系统在接受端能够获取信息信号; (2) 对于非法获取信号者很难从传输信道的背景噪声中提取有用的传输信号.后者

[1] 2003-05-09 收到, 2003-08-04 改回
985 工程子项目资助课题

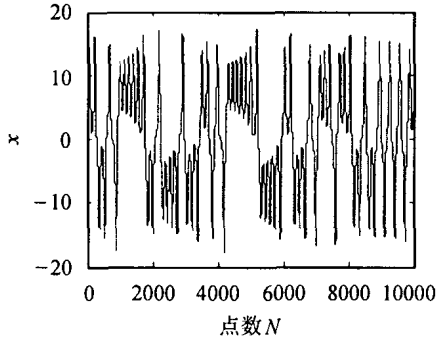
的问题也称为暴露性 (Unmasking)，即判断在传输信道中是否有传输信息。如果不能揭示信息的传输，那么在未知系统方程的情况下，就很难破译信息。

Lorenz 混沌系统为

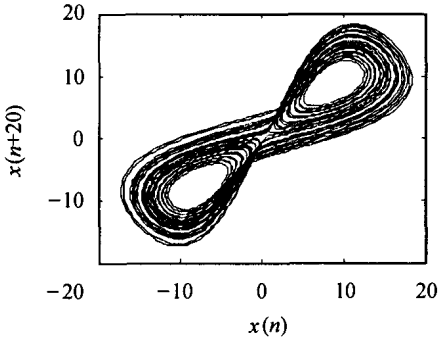
$$\left.\begin{aligned}\dot{x} &= \sigma(y-x)\\ \dot{y} &= \gamma x - y - xz\\ \dot{z} &= -bz + xy\end{aligned}\right\} \tag{1}$$

其中 $\sigma = 10, \gamma = 28, b = 8/3$，混沌信号 $x(t)$ 作为密钥序列对 $m(t)$ 进行加密编码。

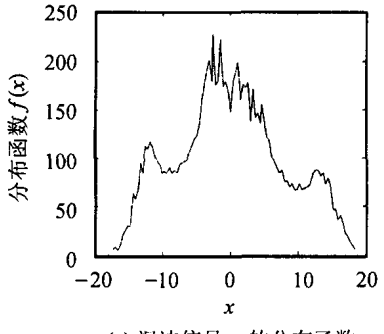
Lorenz 混沌系统所产生的混沌时间序列分析如图 1(a)-(j) 所示。当采样间隔较小时，如 t=0.005，从时间域上，可以看出 Lorenz 混沌系统所产生出的混沌信号 $x(t)$ 不完全类似于随机序列 (如图 1(a) 所示)。将 1 至 1000 点的曲线放大 (图 1(e))，可以看出，曲线有局部线性化的特点，故易受局部线性化的方法攻击，如用线性预测进行估计，如图 1(f)，这里仅用了 10 阶 AR 模型预测，可以看出预测的结果非常好。同时这一特点在系统的相空间 (图 1(b)) 上也可以看出，相空间上的曲线非常光滑，因此易受相空间重构方法的攻击 [2]。同时发现其自相关函数的随机性并不很好 (图 1(d))，这些说明在较小采样间隔下，Lorenz 混沌系统的密码学特性不好，不具有很好的加密特性。如果采样间隔较大时，情况就不同了，如 $t = 1$，从图 1(g) 可以看出，混沌信号 $x(t)$ 在时间域上完全类似于随机信号，相空间上的曲线也十分混乱 (图 1(h))，而且它的自相关特性图 1(i) 比图 1(d) 要好，这说明在较大采样间隔下，Lorenz 混沌系统的密码学特性要好了许多，同时用 AR 模型也很难对其进行预测。另外研究发现，该系统在不同的采样间隔下，所产生的混沌信号的分布函数基本一样，均如图 1(c) 所示，这说明采样间隔对混沌信号的分布基本上没有影响。



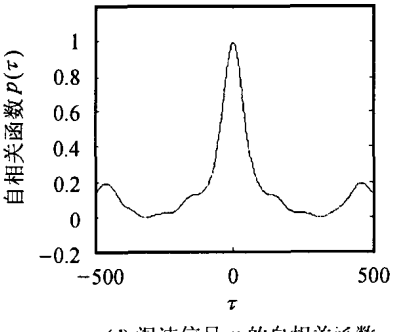
(a) 混沌信号x



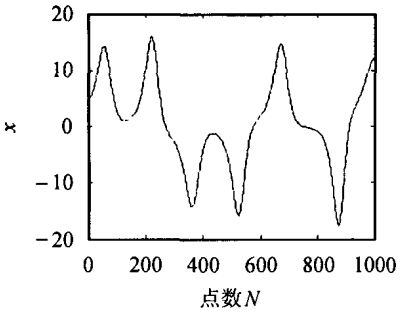
(b) 混沌信号x的相空间图



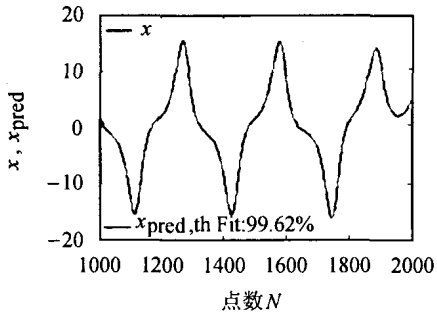
(c) 混沌信号 x 的分布函数



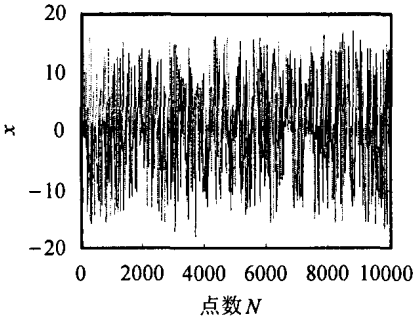
(d) 混沌信号 x 的自相关函数



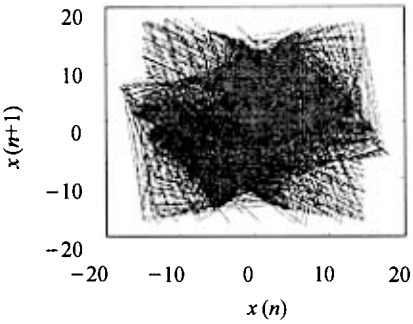
(e) 图(a)的局部放大图



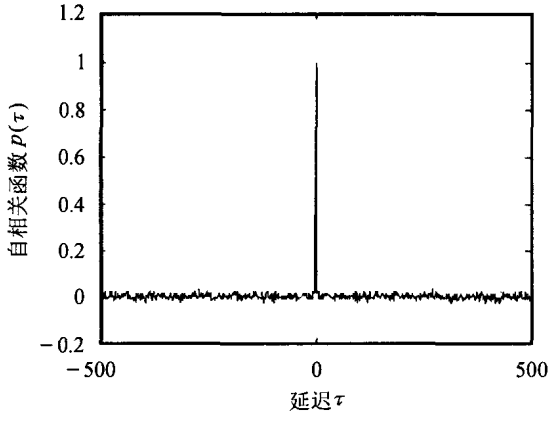
(f) 混沌信号 x 及其预测



(g) t=1 时的混沌信号 x



(h) t=1 时的相空间图



(i) 混沌信号 x 的自相关函数

图 1　Lorenz 混沌系统分析

进一步研究发现，即使是更高维数的混沌系统，如 Rossler 和 Lorenz 组合混沌系统还有 11 维或 101 维的超混沌系统，也都有类似的结果。这些结果都表明，较小的采样间隔如 $t = 0.01$，混沌信号曲线和相空间曲线都比较光滑，相应的自相关特性不好，说明在这样的情况下，混沌加密系统保密性不高，极易受到线性预测和相空间重构法的攻击 [2−4]。而当采样间隔较大时，如 $t = 1$，混沌信号在时间域上完全类似于随机序列，其相空间上的曲线也十分混乱，相应的自相关特性也好了许多，对于其它的系统也有类似的结果，这些都表明大采样间隔对增强混沌系统的密码学特性有帮助。

3 非线性检验研究

前面分析了混沌系统在欠采样间隔情况下，系统输出符合密码学特性，不易受到攻击，那

么是不是这样的系统一定安全呢？下面利用 VWK 非线性检验对 Lorenz 系统进行进一步的非线性检验研究.

3.1 VWK 检验方法原理

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 $x_n, x_{n-1}, \cdots, x_{n-k+1}$ ，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[5] 提出了一种利用 y_n 反馈 (即令 $x_n = y_{n-1}$) 的闭环 Volterra 序列，可通过下式来计算:

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

其中 $\{z_m(n)\}$ 是由嵌入空间坐标 $(y_{n-1}, y_{n-2}, \cdots, y_{n-k})$ 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功率:

$$\varepsilon(k,d)^2 \equiv \sum_{n=1}^{N} (y_n(k,d) - y_n)^2 \Big/ \sum_{n=1}^{N} (y_n - \bar{y})^2 \tag{3}$$

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

由式 (2) 和式 (3) 可知，该方法必须先给出合适的 k 和 d 二值，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:

$$C(r) = \log \varepsilon(r) + r/N \tag{4}$$

r 是模型阶次；当 $d = 1$ 时， VWK 模型是线性模型；当 $d > 1$ 时， VWK 模型是非线性模型.

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 ，尽量使得非线性信息准则 $C^{\text{nl}}(r)$ 小于线性准则 $C^{\text{lin}}(r)$ ，这时的 k 和 d 即为 k_{opt} 和 d_{opt} .

3.2 VWK 检验方法与采样间隔的关系

采样间隔对 VWK 检验方法的影响如图 2 所示. 由图 2 可见， $\tau = 0.0005$ 时，原始数据以线性模型为主，即 $C^{\text{lin}}(r) \approx C^{\text{nl}}(r)$ ，此时的原始时间序列总显示出线性特性，这说明若 τ 选择的过小，难以给出准确的检验结果，但对于破译者来说，则可利用这一特点，对其进行线性重构 (即线性建模) ，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 为欠采样间隔情况下，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， $C^{\text{nl}}(r)$ 明显地小于 $C^{\text{lin}}(r)$ ，可判断出原始序列是非线性时间序列，但这样的采样间隔是不行的，因为破译者可利用非线性重构的方法 (如吸引子重构 [3]) 对其进行破译.

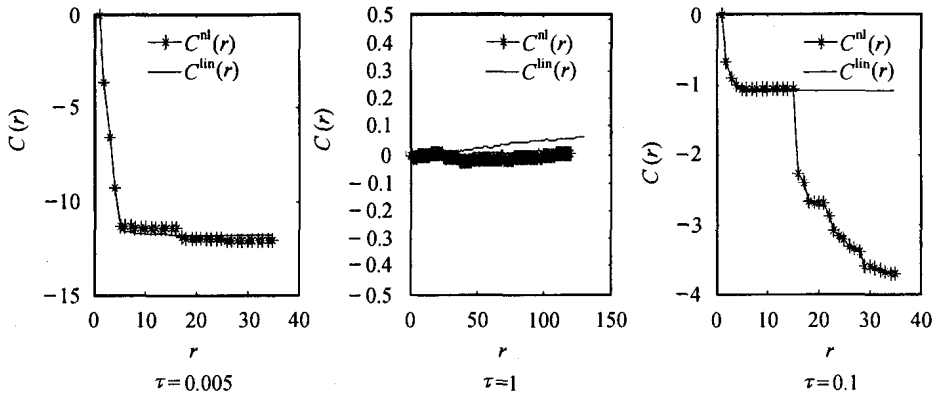
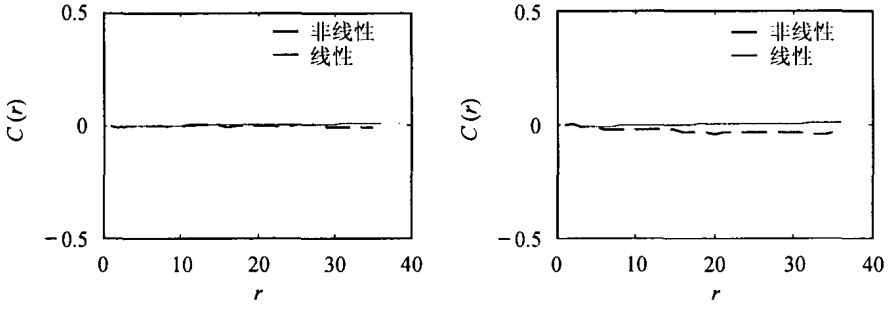


图 2　采样间隔对 VWK 检验方法影响的分析结果

考虑到在欠采样间隔下，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，我们可以利用 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的还是非线性的，则表明该混沌时间序列类似于噪声，更具有保密性。

4 基于 VWK 方法的混沌加密系统分析

图 3(a) 为 Lorenz 混沌时间序列的 VWK 检验结果，采样间隔 $\tau = 1$，$C^{\mathrm{nl}}(r)$ 和 $C^{\mathrm{lin}}(r)$ 均比较小，表明此时的 Lorenz 混沌时间序列很难用线性模型或非线性模型描述，该混沌时间序列类似于噪声。图 3(b) 为 Rossler 和 Lorenz 组合混沌系统所产生的混沌时间序列的 VWK 检验结果，采样间隔 $\tau = 1$，可以看出，$C^{\mathrm{nl}}(r)$ 和 $C^{\mathrm{lin}}(r)$ 也都比较小，该混沌时间序列同样难以用线性模型或非线性模型描述，更符合加密的要求。



(a) Lorenz 混沌时间序列,τ=1　　(b) Rossler 和 lorenz 混沌时间序列,τ=1

图 3　混沌加密系统时间序列 VWK 检验分析

5 结论

总之，当采样间隔较大时，混沌时间序列类似噪声，很难用模型方法描述，说明混沌加密系统的保密性在这种情况下被提高。尽管混沌同步是混沌保密通信的关键技术，但基于混沌动力学的信息加密安全性仍然是混沌系统本身的安全性。连续混沌系统，在采样间隔较小的情况下，它所产生的混沌时间序列不具有很好的密码学特性，只有当采样间隔较大时，期保密性才得到增强。本文从混沌时间序列分析的的非线性检验入手，介绍了 VWK 检验方法。研究了采样间隔对 VWK 检验方法的影响，发现当采样间隔为欠采样情况时，原始数据不仅表面上类似于噪声序列，而且本质上也表现为随机性，即很难用确定模型来描述，对于加密者来说，在该

情况下，其加密信息将几乎完全类似于噪声，从而使破译者不能进行有效的破解，并利用该方法对典型的 Lorenz 混沌加密系统进行了相应分析，进一步证实了在采样间隔较小时，混沌系统不具有保密性，因为该系统所产生的混沌时间序列存在确定性成分，而只有在欠采样情况下，其所生成的混沌时间序列才类似于噪声，保密性才得以提高。

参 考 文 献

[1] Yang T, Yang L B, Yang C M. Cryptanalyzing chaotic secure communications using return maps. *Physics Letters A*, 1998, 245: 495–510.

[2] Gibson J F, Farmer J D, Casdagli M, *et al*.. An analytic approach to practical state space reconstruction. *Physica D*, 1992, 57: 1–30.

[3] Palus M, Dvorak I. Singular-value decomposition in attractor reconstruction: Pitfalls and precautions. *Physica D*, 1992, 55: 221–234.

[4] Parlitz U. Nonlinear time series analysis. Proceedings of the 3rd International Specialist Workshop on Nonlinear Dynamics of Electronic Systems, Belgium, July 8–10, 1998: 179–192.

[5] Barahona M, Poon C H. Detection of nonlinear dynamics in short, noisy time series. *Nature*, 1996, 381: 215–217.

[6] 雷 敏. 混沌时间序列分析及其在混沌加密系统中的应用研究: [博士论文]. 上海: 上海交通大学, 2002.9.

谢 鲲: 男, 1976 年生, 博士, 研究方向: 混沌保密通信、机电系统的智能控制.

雷 敏: 女, 1968 年生, 博士后, 新加坡南洋理工大学访问学者. 研究方向: 非线性信号分析、混沌系统参数辨识.

冯正进: 男, 1938 年生, 博士生导师, 研究方向: 混沌保密通信.