Soft Comput (2006) 10: 224–229
DOI 10.1007/s00500-005-0475-y

ORIGINAL PAPER

C. L. Liu · K. Xie · Y. Miao
X. F. Zha · Z. J. Feng · J. Lee

Study on the communication method for chaotic encryption in remote monitoring systems

Published online: 1 August 2005

Abstract In chaotic cryptosystems, it is recognized that using (very) high dimensional chaotic attractors for encrypting a given message may improve the privacy of chaotic encoding. In this paper, we study a kind of hyperchaotic systems by using some classical methods. The results show that besides the high dimension, the sub-Nyquist sampling interval (SI) is also an important factor that can improve the security of the chaotic cryptosystems. We use the method of time series analysis to verify the results.

Keywords Remote monitoring · Time series analysis · Surrogate data

1 Introduction

For the last decade synchronization of chaotic systems has been explored very intensively by many researchers in various fields ranging from physics, mathematics to engineering for possible applications in communication systems [1, 13–15]. Typical examples include engineering systems for e-maintenance and e-manufacturing where mass data /information transmitted on-line or real-time is regarded [16]. Parlitz and Kocarev [1] used the surrogate data analysis to unmask chaotic communication systems. Their research result shows that one possibility to improve the privacy of chaotic encoding is to use (very) high dimensional chaotic attractors for encrypting a given message [2].

C. L. Liu (✉) · K. Xie · Y. Miao · Z. J. Feng
Institute of Mechatronics Control
Shanghai Jiao Tong University
Shanghai 200030, P.R.China
E-mail: chlliu@sjtu.edu.cn

X. F. Zha
Manufacturing Engineering Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899, USA
E-mail: zha@cme.nist.gov

J. Lee
Center for Intelligent Maintenance
University of Wisconsin at Milwaukee
Milwaukee, WI 53211, USA

First, based on the active-passive decomposition method, a hyperchaotic system is decomposed into the transmitter and receiver.

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

where, m is the embedded dimension, M is the total dimension, $a = 0.29, b = 4, d = 2$, and $\varepsilon = 0.1$. For $M = 11$, its chaotic attractor has $D_L = 10.02$ Lyapunov dimension; for $M = 101$, the dimension is $D_L = 100.02$. The transmitter and receiver are expressed as follows:

transmitter:

$$\begin{aligned} \dot{x}_1 &= -x_2 + (a-1)x_1 + s \\ \dot{x}_m &= x_{m-1} - x_{m+1} \\ \dot{x}_M &= \varepsilon + bx_M\,(x_{M-1} - d) \quad 1 < m < M, \end{aligned} \tag{2}$$

transmitted signal: $s = x_1 + i, i(t) = 0.2\sin(t)$;
receiver:

$$\begin{aligned} \dot{y}_1 &= -y_2 + (a-1)y_1 + s \\ \dot{y}_m &= y_{m-1} - y_{m+1} \\ \dot{y}_M &= \varepsilon + by_M\,(y_{M-1} - d) \quad 1 < m < M, \end{aligned} \tag{3}$$

with a sampling interval $t_s = 1.4$, four cases are compared and simulated: (a) i=0, M=1; (b) $i = 0.2\sin(t)$, M=11; (c) i=0, M=101; and (d) $i = 0.2\sin(t)$, M=101. In these four cases, the phase graphs possess no discernible structure and thus may not be easily distinguished from a linear stochastic process.

Second, to investigate the efficiency of the hyperchaotic system in masking the sinusoidal information, two surrogate data tests are applied for deterministic nonlinearties to the transmitted signals. The analysis showed that the system described in Eq. (1) exhibits nonlinear noise-like dissipative dynamics. It is therefore necessary to use (very) high dimensional chaotic carriers to achieve a satisfactory degree of privacy.

However, their method only used surrogate data to validate the security of the hyperchaotic system. This kind of system is not absolutely safe. It cannot stand up other test methods. Through our research, we find that when using the Volterra-Wiener-Korengerg test (VWK) method to verify

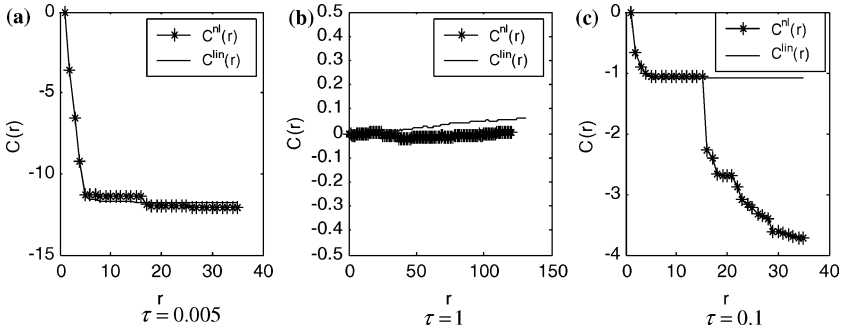

Fig. 1 The analysis effects of SI on VWK test

it there will be not the same security as the surrogate data method. In this paper, we study why this hyperchaotic system is vulnerable in the VWK test and propose a solution to improving its security. We use both the VWK method and the surrogate data method to make comparison.

2 Nonlinear test based on the VWK method

2.1 The theory

For a dynamic system, we assume let input and output sampling points be $\{x_n\}_{n=1}^N$, $\{y_n\}_{n=1}^N$, sampling interval (SI) be τ, and the length of the data be N . If $x_n, x_{n-1}, \ldots, x_{n-k+1}$ are used, the discrete Volterra series can be expanded by the Taylor polynomial of y_n. k is the order of the system. Barahona [4] presented a kind of the closed loop Volterra series using y_n feedback ($x_n = y_{n-1}$), which can be calculated through the following formula:

$$\begin{aligned} y_n^{\text{calc}} &= a_0 + a_1 y_{n-1} + a_2 y_{n-2} + \cdots + a_k y_{n-k} + a_{k+1} y_{n-1}^2 \\ &\quad + a_{k+2} y_{n-1} y_{n-2} + \cdots + a_{M-1} y_{n-k}^d \\ &= \sum_{m=0}^{M} a_m z_m(n), \end{aligned} \tag{4}$$

where $\{z_m(n)\}$ is an all-different combination composed of embedding space coordinates $(y_{n-1}, y_{n-2}, \ldots, y_{n-k})$, d is the highest combination degree, k is the model order. Since the total dimension is $M = (k+d)!/(d!k!)$, k is equal to the embedding dimension, and d is equal to the nonlinear degree of the model. By using one step forecasting error, the short time forecast power could be calculated as:

$$\varepsilon(k,d)^2 \equiv \frac{\sum_{n=1}^{N} (y_n^{\text{calc}}(k,d) - y_n)^2}{\sum_{n=1}^{N} (y_n - \bar{y})^2}, \tag{5}$$

where, $\bar{y} = \frac{1}{N} \sum_{n=1}^{N} y_n$, $\varepsilon(k,d)^2$ is the regularization variance of the residual.

From formula (4) and (5), we know that an appropriate k and d must be given before using this method. And the most appropriate k_{opt} and d_{opt} are just k and d, which can make the information criterion $C(r)$ be the least.

$$C(r) = \log_\varepsilon(r) + r/N, \tag{6}$$

where, N is the number of data, and r is the order of model. If $d = 1$, VWK is the linear model; if $d > 1$, VWK is the nonlinear model. It is noted that the larger k_{opt} is, the larger M is. If $d > 1$, the count quantum will be enhanced. We should adjust k and d to make $C^{nl}(r)$ be less than $C^{\text{lin}}(r)$, $k = k_{\text{opt}}$ and $d = d_{\text{opt}}$.

2.2 The effect of sampling interval

Here, we take the Lorenz chaotic system as an example to explain the relationship between the sampling interval and the VWK test. The Lorenz chaotic system is:

$$\begin{cases} \dot{x} = \sigma(y - x) \\ \dot{y} = \gamma x - y - xz \\ \dot{z} = -bz + xy, \end{cases} \tag{7}$$

where, $\sigma = 10, \gamma = 28, b = 8/3$, and the chaotic signal $x(t)$ is the encryption key.

Sampling interval is as large as possible in the case of which can keep the synchronization of the crypto system. The effect of the sampling interval on the VWK test method is shown in Fig. 1. When $\tau = 0.005$, most of the original data are linear, i.e. $C^{nl}(r) \approx C^{\text{lin}}(r)$. The initial time series has linear properties, which indicates that if the sampling interval is too small, it will be difficult to get the test result. However, the attackers can make use of this weakness to accomplish the linear reconstruction (linear modeling) [5,6]. If $\tau = 1$, the information of the linear model and nonlinear model are very similar, and they both are so small that we could assure that the original data have nonlinear properties. If we enlarge the sampling interval, the original data will be more like noise. In this case, according to the VWK test method, we can't figure out whether or not there are nonlinear elements in signals. Attackers can't identify if it is accurate signal or random noise either. If $\tau = 0.1$, it is obvious that $C^{nl}(r)$ is less than $C^{\text{lin}}(r)$. In this situation, the initial series is nonlinear time series. However, this kind of the SI isn't good enough because it can be attacked by the nonlinear reconstruction method (attractor reconstruction) [7,8].

In the case of sub-Nyquist sampling interval, according to the VWK test method, we do not know that if there are

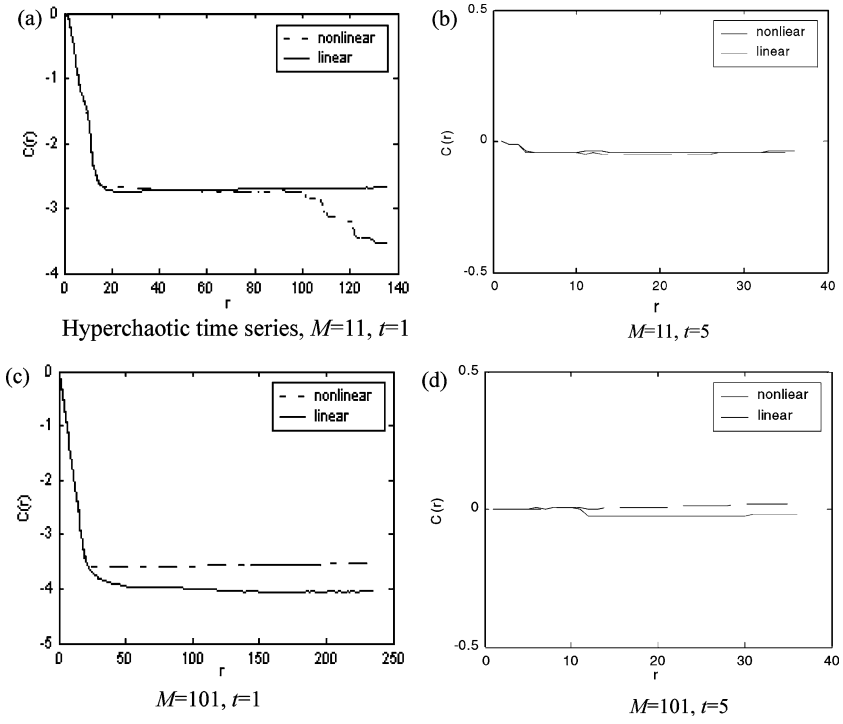

Fig. 2 The VWK test analysis for the chaotic time series given by the chaotic encryption system

accurate elements in the time series and the initial time series are much like random noises. From that point of view, we can use the VWK test method to analyze the time series of the chaotic system.

2.3 Application

Fig. 2a is the hyperchaotic system time series generated by formula (1) whose dimension is 11 and $t = 1 C^{nl}(r)$ is obviously less than $C^{\text{lin}}(r)$. Though it looks like a random noise, the analysis result shows that it can be depicted using a nonlinear model and it has no security as we desire. Fig.2b is the test result of the situation $t = 5$. $C^{nl}(r)$ and $C^{\text{lin}}(r)$ are both small. We also studied higher dimension (M=101) system. Fig.2c shows the time series graph when $t = 1$. Both $C^{nl}(r)$ and $C^{\text{lin}}(r)$ are large, which means that the system is not secure. When $t = 5$, $C^{nl}(r)$ and $C^{\text{lin}}(r)$ become small, the pseudo-randomicity of the system is improved, as shown in Fig.2b and d. We can see that if the sampling interval is the same, the hyperchaotic system still put up the assured elements. Therefore, not only the dimension but also the sampling interval determines the security of the system. Because of the calculation ability, we only give out the greatest count results in this paper when $k \leqslant 50$ and $d \leqslant 3$.

3 The cryptanalysis

The time series analysis graphs for the hyperchaotic system (1) are shown in Fig. 3a–o. First, we study the situation with a small sampling interval. Let $t = 1$, we can find from Fig. 3a–h that no matter how high is M, 11 or 101, there are no difference for the results. The chaotic curves have local linearzation charteristics. The phase space curves are very smooth and the corresponding δ specialties of the autocorrelation functions are bad. This indicates that if the SI is small, even if the hyperchaotic system is very complex, it is still menaced by the method of linear forecasting and the phase space reconstruction [6]. In other words, this kind of chaotic system has no enough security. While, if we enlarge the SI, and let t=5, the situation will be totally different (see Fig.3i–p). The autocorrelation property of the cryptosystem becomes better. In addition, with the same data length (N=1000), the higher the chaotic system dimension is, the better the autocorrelation property of the chaotic time series is, i.e., with the better encryption property. Fig 3 c, g, k and n show that the dimension M and SI do not have any effect on the distribution of the chaotic signal.

Through the above analysis on the hyperchaotic system, we can conclude that the sub-Nyquist sampling interval is more suitable for chaotic systems to be encrypted as it has better encryption properties. We also use the surrogate data method to verify our conclusion. In certain condition, the pseudo- randomness of chaotic time series can be determined. Thus it can be used to analyze the pseudo-randomicity of chaotic signal generated from the chaotic encryption system.

4 Nonlinear test study based on the surrogate data

We choose 1000 points from the hyperchaotic system time series. If the sampling interval is $t = 5$ then according to the zero supposition in [1] we can produce 39 sets of surrogate

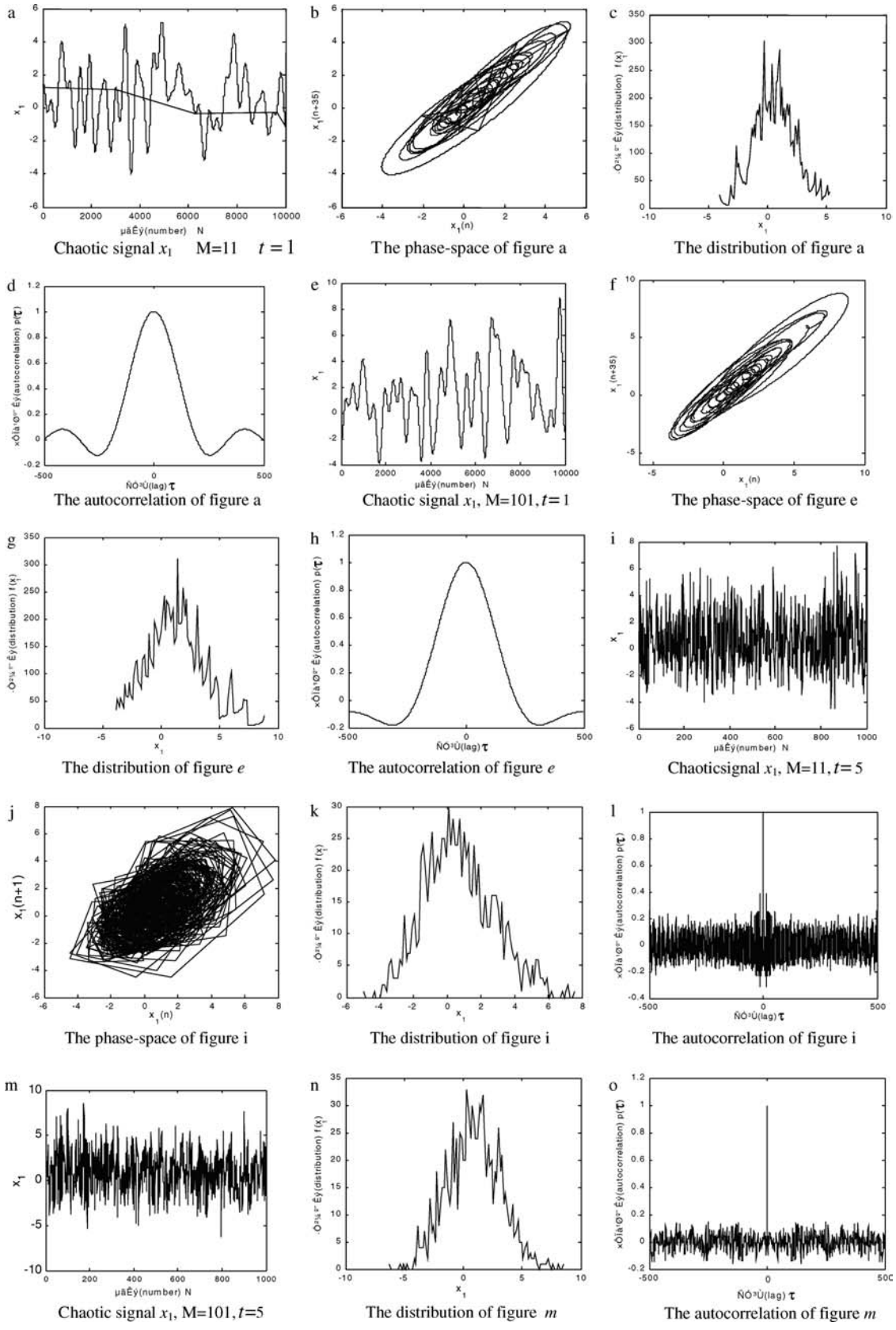

Fig. 3 The analysis of hyperchaotic system

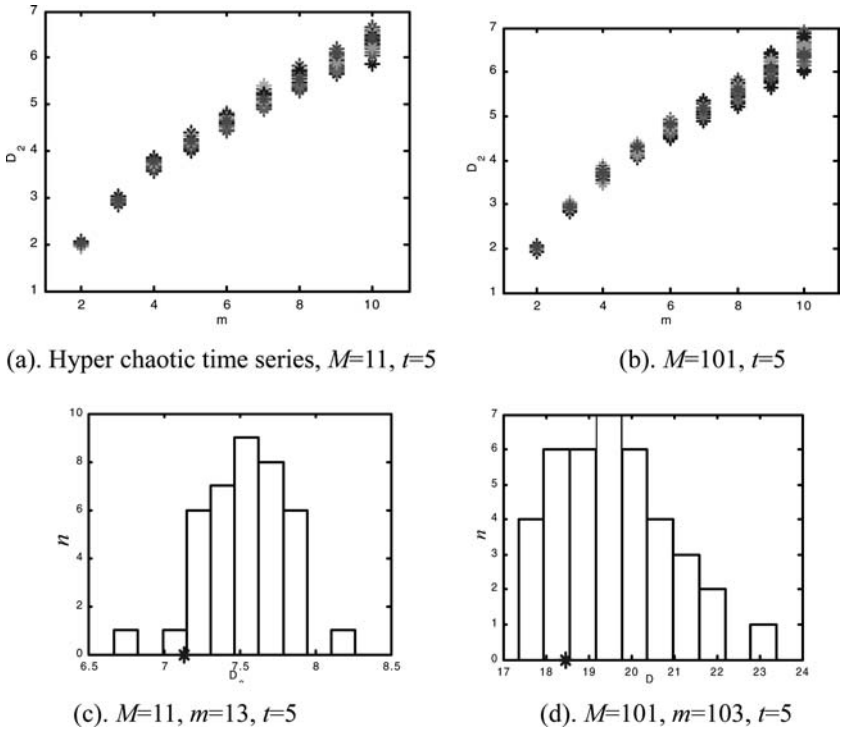

Fig. 4 The results of chaotic encryption system by surrogate data test

data by the algorithms in [9]. If the credibility is p then the surrogate data collection is $B_{\min} = 2/(1-p) - 1$. Therefore, when $p = 95\%$ and $B_{\min} = 39$, the test statistics has the correlation dimension: $D = \lim_{l \to 0} \frac{\ln C(l)}{\ln(l)}$.

For the hyperchaotic system with M=11 dimensions (see Fig. 4a), if $m = 2$–10 then the surrogate data and the original data have no significant difference and the zero supposition is accepted. If m is bigger than 11, what will be the situation? Looking at Fig. 4c, $m = 13$, we still can't find any difference between the original data and the surrogate data. This indicates that if the decrypter does not know the structure of the system it will be impossible to find useful information in the background noises. Even if the dimension is higher, $M = 101$, the results are the same (see Fig. 4b and d). The vertical axes of the Fig. 4c and 4d are the number of the surrogate data.

5 Conclusion

In this paper, we first pointed out the disadvantages of the method discussed in [1] and then proposed a new method to improve the security of the chaotic cryptosystems. Through studying the effect of the sampling interval on the VWK test, we found that when the SI is a sub-Nyquist sampling, the original data appear like noise apparently and they can express randomness in nature. It is therefore very difficult to depict the time series by a model method so that attackers can't decrypt information effectively. Based on the VWK test method, the analysis result for the hyperchaotic system referred in [1] proved that if the sampling interval is too small the hyperchaotic system still has no enough security even though the dimension of the system is very large. The time series generated by the chaotic system has accurate elements. In addition, if the SI is too large the security of the hyperchaotic system is bad too. Only when the SI is the sub-Nyquist sampling, the chaotic time series is similar to be the random noise and the security will be high. We also used the surrogate data method to analyze the hyperchaotic system in [1] in the sub-Nyquist sampling. In conclusion, when designing a chaotic cryptosystem with high security, the designer should consider not only adding the dimension of the system but also taking a suitable sampling interval.

Acknowledgement and Disclaimer This work is supported by the National Natural Science Foundation of China (Grant No.50128504). No approval or endorsement by the National Institute of Standards and Technology, USA is intended or implied.

References

1. Parlitz U, Kocarev L (1997) Using surrogate data analysis for unmasking chaotic communication systems. Int J Bifurcation Chaos 7(2):407–413
2. Parlitz U(1998) Nonlinear time series analysis. In: Proceedings of the 3rd international specialist workshop on nonlinear dynamics of electronic systems, pp. 179–192
3. Abarbanel HDI, Brown R, Sidorowich JJ et al. (1993) The analysis of observed chaotic data in physical systems. Rev Modern Phys 65(4):1331–1392
4. Barahona M, Poon Shi-Sang (1996) Detection of nonlinear dynamics in short, noisy time series. Nature 381:215–217

5. Hilborn RC, Ding MZ (1996) Optimal reconstruction space for estimating correlation dimension. Int J Bifurcation Chaos 6(2):377–381
6. Gibson JF, Farmer JD, Casdagli M et al. (1992) An analytic approach to practical state space reconstruction. Physica D 57: 1–30
7. Kennel M, Brown R, Abarbanel HDI (1992) Determining embedding dimension for phase-space reconstruction using a geometrical construction. Phys Rev A 45(5):3403–3411
8. Palus M, Dvorak I (1992) Singular-value decomposition in attractor reconstruction: pitfalls and precautions. Physica D 55: 221–234
9. Sakaguchi Hidetsugu (2002) Parameter evaluation from time sequences using chaos synchronization. Phys Rev E 65 p 027201-1-4
10. Theiler J, Prichard D (1996) Constrained-realization Monte-Carlo method for hypothesis testing. Physica D 94:221–235
11. Lei M, Wang ZZ, Feng ZJ (2001) Detecting nonlinearity action surface EMG signal. Phys Let A 290:297–303
12. Lei M (2002) Chaotic time series analysis and its application study on chaotic encryption system. PhD Thesis, Shanghai Jiao Tong University, China
13. Parlitz U, Chua LO, Kocarev Lj, Halle KS, Shang A (1992) Transmission of digital signals by chaotic synchronization. Int J Bifurcation Chaos 2(4):973–977
14. Parlitz U, Kocarev L, Stojanovski T, Preckel H (1996) Encoding messages using chaotic synchronization. Phys Rev E53:4351–4361
15. Pecora LM, Carroll TL (1990) Synchronization in chaotic systems. Phys Rev Let 64:821–824
16. Koc Muammer, Lee J (2001) A system framework for next-generation e-maintenance systems. http://www.umw.edu/ceas/ims/