A Chaotic Communication Scheme Based on Generalized Synchronization and Hash Functions *

XU Jiang-Feng(徐江峰)[1], MIN Le-Quan(闵乐泉)[1**], CHEN Guan-Rong(陈关荣)[2]

[1]*Department of Mathematics and Mechanics, University of Science and Technology Beijing, Beijing 100083*
[2]*Department of Electronic Engineering, City University of Hong Kong*

(Received 24 February 2004)

A new chaotic communication scheme based on generalized chaotic synchronization (GCS) and hash function transpositions is presented. The communication scheme has nonsymmetric secrete keys and its ability is similar to traditional digital signatures, i.e. a receiver can convince himself whether or not the sender's message contents have been modified. As a direct application of the scheme, a GCS system is designed by using Chen's chaotic circuit and is studied in some detail. The numerical simulation shows that this Chen GCS system has high security and is fast and reliable for secure Internet communications.

PACS: 05. 45. Xt, 05. 45. Vx, 05. 45. Pq

Cryptography was used as a tool to protect national secrets and strategies. Today, communication is widespread through wireless and fixed-wire networks. The proliferation of computers and communications systems create a demand from the private sector for means to protect information in digital form and to provide security services. Special attention has always been focused on on-line secure communications such as image and video transmission through the Internet, for which conventional encryption techniques are relatively slow and inefficient, and therefore difficult to apply on-line.

The chaos-based encryption methodology[1−9] differs from the traditional encryption approaches, and is faster but has a comparable degree of security: it has the required mixing, diffusion, and confusion properties, among others, and has high security. The parameter space can be as large as desired, and is used for chaotic keys; last but not least, it is fast and reliable. In particular, the research into chaos-synchronization-based communication has both received much attention and seen much improvement recently, for its potential in practical applications.[10−17] The idea of generalized synchronization has also been developed,[18−24] which offers new possibilities for various secure communication, especially in analogue settings. In Ref. [23], a theorem for constructing coupled GCS vector differential equations was presented, which was used to construct a system for encryption-based secure communication.[25]

Block ciphering is an important tool in the design of protocols for shared-key cryptography. This paper investigates GCS and the transposition-based secure communication, aiming to explore its further potential in practical applications of block ciphers. A new encryption scheme for digital block transposition is introduced, which can be practically used for on-line network communication. A six-dimensional Chen GCS system is designed and studied, with prototypes introduced as typical three-dimensional quadratic autonomous chaotic systems.[26] Applying the developed scheme to Chen's GCS system shows that the GCS source signals can successfully encrypt messages on-line. Numerical simulation shows that this system has high security and is fast and reliable for on-line Internet communications.

A chaotic system with GCS is decomposed into two parts:

$$\frac{d\boldsymbol{X}}{dt} = F(\boldsymbol{X}), \tag{1}$$

$$\frac{d\boldsymbol{Y}}{dt} = G(\boldsymbol{Y}, \boldsymbol{X}), \tag{2}$$

where $\boldsymbol{X} \in \mathbb{R}^n$ $\boldsymbol{Y} \in \mathbb{R}^m$,

$$F(\boldsymbol{X}) = (f_1(\boldsymbol{X}), f_2(\boldsymbol{X}), \ldots, f_n(\boldsymbol{X}))^T,$$
$$G(\boldsymbol{Y}, \boldsymbol{X}) = (g_1(\boldsymbol{Y}, \boldsymbol{X}), g_2(\boldsymbol{Y}, \boldsymbol{X}), \ldots, g_m(\boldsymbol{Y}, \boldsymbol{X}))^T.$$

Definition 1[18,19] The chaotic systems defined by (1) and (2) are said to be in GCS with respect to a transformation, $H : \mathbb{R}^m \longrightarrow \mathbb{R}^m$, if an open subset $B \subset \mathbb{R}^n \times \mathbb{R}^m$ exists such that $0 \in B$, and for any trajectory $(\boldsymbol{X}(t), \boldsymbol{Y}(t))$ of system (1) with initial conditions $(\boldsymbol{X}(0), \boldsymbol{Y}(0)) \in B$,

$$\lim_{t \to +\infty} \|\boldsymbol{X}_m(t) - H^{-1}\boldsymbol{Y}(t)\| = 0,$$

where $\boldsymbol{X} \in \mathbb{R}^n$, $\boldsymbol{X}_m = (x_1, x_2, \ldots, x_m)^T$, $\boldsymbol{Y} \in \mathbb{R}^m$.

Theorem 1[23] Let $\boldsymbol{X}, \boldsymbol{X}_m, \boldsymbol{Y}, F(\boldsymbol{X})$, and $G(\boldsymbol{Y}, \boldsymbol{X})$ be defined above. Suppose that $H : \mathbb{R}^m \longrightarrow \mathbb{R}^m$ is a C^1 diffeomorphism and $\boldsymbol{X}_m = V(\boldsymbol{Y})$ is the inverse function of H. If systems (1) and (2) are in GS via transformation $\boldsymbol{Y} = H(\boldsymbol{X}_m)$, then the function $G(\boldsymbol{Y}, \boldsymbol{X})$ in (2) takes the following form:

$$G(\boldsymbol{Y}, \boldsymbol{X}) = [\dot{V}(\boldsymbol{Y})]^{-1}[F_m(\boldsymbol{X}) - q(\boldsymbol{X}_m, \boldsymbol{Y})], \tag{3}$$

* Supported by the National Natural Science Foundations of China under Grant Nos 60074034 and 70271068, the Hong Kong Research Grants Council under CERG Grant No CityU 1115/03E, and the Research Fund for the Doctoral Programme of Higher Education by the Ministry of Education of China under Grant No 20020008004.

** Email: To whom correspondence should be addressed. Email:lqmin@sohu.com

©2004 Chinese Physical Society and IOP Publishing Ltd

$$\dot{V}(\boldsymbol{Y}) = \begin{bmatrix} \dfrac{\partial V_1}{\partial y_1} & \dfrac{\partial V_1}{\partial y_2} & \cdots & \dfrac{\partial V_1}{\partial y_m} \\ \dfrac{\partial V_2}{\partial y_1} & \dfrac{\partial V_2}{\partial y_2} & \cdots & \dfrac{\partial V_2}{\partial y_m} \\ \vdots & \vdots & \vdots & \vdots \\ \dfrac{\partial \dot{V}_m}{\partial y_1} & \dfrac{\partial \dot{V}_m}{\partial y_2} & \cdots & \dfrac{\partial \dot{V}_m}{\partial y_m} \end{bmatrix},$$

$$F_m(\boldsymbol{X}) = (f_1(\boldsymbol{X}), f_2(\boldsymbol{X}), \ldots, f_m(\boldsymbol{X}))^T,$$

and the function

$$q(\boldsymbol{X}_m, \boldsymbol{Y}) = (q_1(\boldsymbol{X}_m, \boldsymbol{Y}), q_2(\boldsymbol{X}_m, \boldsymbol{Y}), \ldots, q_m \cdot (\boldsymbol{X}_m, \boldsymbol{Y}))^T$$

ensures that the zero solution of the following error equation (4) is asymptotically stable:

$$\dot{\boldsymbol{e}} = \dot{\boldsymbol{X}}_m - \dot{V}(\boldsymbol{Y})\dot{\boldsymbol{Y}} = q(\boldsymbol{X}_m, \boldsymbol{Y}). \tag{4}$$

Assume that a plaintext to be sent is a block S with $k \times l$ (k rows and l columns) elements. If we first permute the columns of S, and then transpose the rows of S, then it can be verified that $k!l!$ possible arrangements exist. Consequently, the probability that someone obtains the correct transposition will be 1 out of $k!l!$. This implies that such a scheme is quite secure for one-pad communication. For instance, a plaintext with 1000 English alphabets in the binary format has about $10^{2572.2}$ possible permutations. Therefore, finding the correct permutation among them will be a very difficult task on-line.

Our chaos–hash-function-based transposition communication scheme is to realize such a tiny probability for detection. The scheme uses a GCS system to generate two hash functions, H_1 and H_2, such that $H_1 : S \longrightarrow H_1(S)$ results in column permutations for the block S, and $H_2 : H_1(S) \longrightarrow H_2(H_1(S))$ makes row transpositions for block $H_1(S)$. We describe the scheme in detail below.

Suppose that sender A wants to send receiver B a digital message, i.e. a block S with $k \times l$ elements over the Internet. Also we suppose that A has the GCS systems defined by (1) and (2), while B only has the drive system (1). Moreover, we assume that A and B agree on two prescribed sampling rules, T_{M_i} $(i = 1, 2)$, and two decrypting-code rules, T_B and T_σ related to the C^1 diffeomorphism, such that $y_1 = T_B(\boldsymbol{X})$ and $y_2 = T_\sigma(\boldsymbol{X})$. A secrete key λ is used to generate the transpositions of the rows and the columns of the block S by sampling the chaotic signals and using the hashing functions.

The proposed GCS–hash-function-based secure communication scheme is as follows:

1. Sender A uses an initial condition $(\boldsymbol{X}(0), \boldsymbol{Y}(0))$ to generate a chaotic signal $\{(\boldsymbol{X}(t), \boldsymbol{Y}(t)) : t \in [0, T]\}$ via the GCS systems (1) and (2), whose length is long enough so that it can be used to construct hash functions to permute the secret message block S. Sender A uses the sampling rule $T'_{M_i}s$ to extract source signals $M_{t_i}(j_i) = T_{M_i}(y_1)$ from y_1, and 'signature messages' $M_{s_i}(j_i) = T_{M_i}(y_2)$ from y_2, where $j_1 = 1, 2, \ldots, k$; $j_2 = 1, 2, \ldots, l$.

2. Sender A uses the secrete key λ to construct hash transposition functions:

$$\begin{aligned} H_{11} &= \mathrm{mod}(\mathrm{round}(\lambda M_{t_1}(j_1)), l), \\ H_{12} &= \mathrm{mod}(\mathrm{round}(\lambda M_{t_2}(j_2)), k), \\ H_{21} &= \mathrm{mod}(\mathrm{round}(\lambda M_{s_1}(j_1)), l), \\ H_{22} &= \mathrm{mod}(\mathrm{round}(\lambda M_{s_2}(j_2)), k). \end{aligned}$$

It is prescribed that if two transpositions are identical, for example if $\mathrm{mod}(\mathrm{round}(\lambda M_{t_1}(j')), k) = \mathrm{mod}(\mathrm{round}(\lambda M_{t_1}(j^*)), k)$, where $j' < j^*$, then position j^* will be, in order, replaced by a position in the entries $\{1, 2, \ldots, k\}$ that has not be used. Hence, the hash functions H_{ji} $(i, j = 1, 2)$ are transposition functions for l entries (if $i = 1$) and k entries (if $i = 2$), respectively, and are uniquely determined by the chaotic signals y_1, y_2.

3. Sender A uses the hash functions to encrypt (row and column transpositions) the secret message block S into a ciphertext, $c = H_{12}(H_{11}(S))$, as well as a 'signature message', $s = H_{22}(H_{21}(c))$. Then, he sends c with signature s and initial condition $\boldsymbol{X}(0)$ to receiver B.

4. Receiver B uses $\boldsymbol{X}(0)$ to solve system (1) and then obtains a message $\boldsymbol{X}(t)$. He then uses the decrypting-rules T_σ and the sampling rule T_B to find the source signal $M_{t_i}(j_i) = T_{M_i}(T_B(\boldsymbol{X}))$ from y_1, and 'signature messages' $M_{s_i}(j_i) = T_{M_i}(T_\sigma(\boldsymbol{X}))$. Therefore, the receiver can obtain the inverse hash functions H_{ij}^{-1}.

5. If the received signature s makes the calculated value $H_{22}^{-1}(H_{21}^{-1}(s)) - c \neq 0$, then at least one value among $\{c, \boldsymbol{X}(0), s\}$ had been modified by an intruder; otherwise, c is valid and receiver B continues the following step.

6. Receiver B uses the inverse hash functions H_{1j}^{-1} to decrypt S by computing $S = H_{11}^{-1}(H_{12}^{-1}(c))$.

Remarks: (a) An intruder finds it difficult to forge a signature of message based on the value of $s_1 + s_2$, even if he knows the signatures s_1 and s_2 of S_1 and S_2, respectively, because a legal signature for message $S_1 + S_2$ will be produced via GCS on systems (1) and (2) with different initial conditions. (b) Clearly, using the proposed secure communication scheme, receiver B can recognize efficiently existing attacks of a possible intruder without communicating with user A. (c) Since receiver B cannot construct the GCS system (2) from the two decrypting-code rules T_B and T_σ, the 'secrete keys' used in the scheme are nonsymmetric.

Chen's system with the GCS property is constructed as follows. The drive system is a smooth quadratic autonomous chaotic system[26] given by

$$\begin{aligned} \dot{x}_1 &= a_1 x_1 + a_2 x_2 + a_3 x_3, \\ \dot{x}_2 &= x_1 x_3 + b, \\ \dot{x}_3 &= c_1 x_1 + c_2 x_2 x_3 + c, \end{aligned} \tag{5}$$

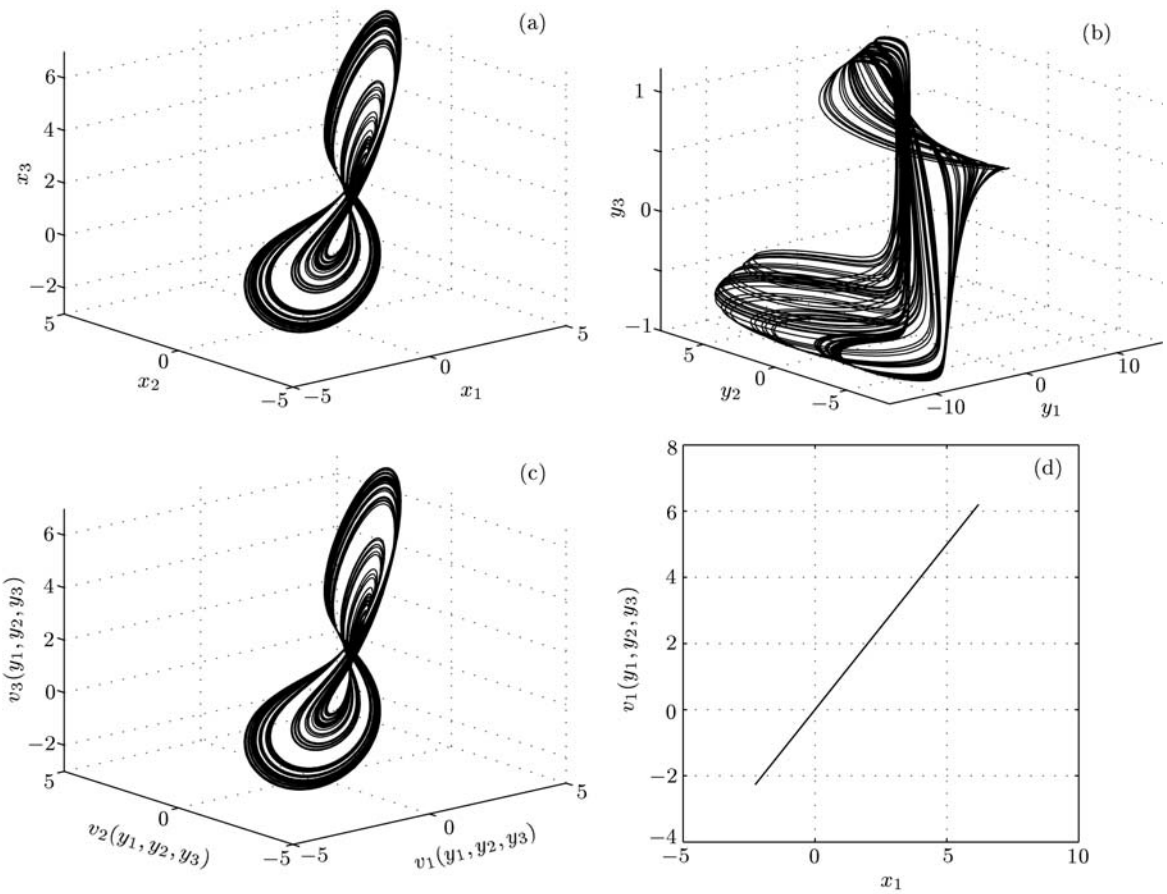

Fig. 1. GCS trajectories of the state variables: (a) x_1, x_2, and x_3; (b) y_1, y_2, and y_3; (c) the decoded trajectory; (d) the variables x_1 and y_1 are in GCS via a transformation v_1.

where $a_1 = -1.44$, $a_2 = 1.5$, $a_3 = 2$, $b = -1.3$, $c_1 = -1.5$, $c_2 = -1$, $c = -\dfrac{a_1 c_2}{a_2} b$. In vector form, system (5) is expressed as

$$\frac{d\boldsymbol{X}}{dt} = F(\boldsymbol{X}). \tag{6}$$

Let a C^1-diffeomorphism, $H : \mathbb{R}^3 \longrightarrow \mathbb{R}^3$, be given by

$$\begin{aligned} H(x_1, x_2, x_3) &= \Big(\frac{5x_2}{x_1^2 + x_2^2}, \frac{5x_1}{x_1^2 + x_2^2}, \arctan(x_3) \Big) \\ &= (y_1, y_2, y_3). \end{aligned} \tag{7}$$

Then,

$$\dot{V}(\boldsymbol{Y})^{-1} = \begin{bmatrix} \dfrac{-2y_1 y_2}{5} & -\dfrac{y_1^2 - y_2^2}{5} & 0 \\ \dfrac{y_1^2 - y_2^2}{5} & \dfrac{-2y_1 y_2}{5} & 0 \\ 0 & 0 & \cos^2(y_3) \end{bmatrix}.$$

Let

$$\begin{aligned} q(\boldsymbol{X}, \boldsymbol{Y}) &= [q_1(\boldsymbol{X}, \boldsymbol{Y}), q_2(\boldsymbol{X}, \boldsymbol{Y}), q_3(\boldsymbol{X}, \boldsymbol{Y})]^{\mathrm{T}} \\ &= \Big[\frac{5y_2}{y_1^2 + y_2^2} - x_1, \frac{5y_1}{y_1^2 + y_2^2} - x_2, \tan y_3 - x_3 \Big]^{\mathrm{T}} \\ \boldsymbol{e} &= \Big[x_1 - \frac{5y_2}{y_1^2 + y_2^2}, x_2 - \frac{5y_1}{y_1^2 + y_2^2}, x_3 - \tan y_3 \Big]^{\mathrm{T}}. \end{aligned}$$

Then, $q(\boldsymbol{X}, \boldsymbol{Y})$ ensures that the zero solution of the error equation (3) is asymptotically stable.

From Eq. (3), Eq. (2) has the form

$$\frac{d\boldsymbol{Y}}{dt} = \dot{V}(\boldsymbol{Y})^{-1} [F(\boldsymbol{X}) - q(\boldsymbol{Y}, \boldsymbol{X})]. \tag{8}$$

The GCS trajectories of Chen's systems (6) and (8) are shown in Fig. 1, in which the following initial condition is selected:

$$\begin{aligned} (\boldsymbol{X}(0), \boldsymbol{Y}(0)) = [&1.0377 \quad -0.4014 \quad -2.0630, \\ &-1.6212 \quad 4.1913 \quad -1.1194]. \end{aligned} \tag{9}$$

It can be seen that the trajectories in Fig. 1(a) display prominent chaotic behaviour, which is different from those of the original chaotic system (see Fig. 1(b) in Ref. [26]) because of taking different initial condition. On the other hand, the chaotic trajectories shown in Fig. 1(b) of the state variables y_1, y_2 and y_3 are difficult to be seen graphically in the process of GCS with state variables x_1, x_2 and x_3. Figures 1(c) and 1(d) show that the state variables $\boldsymbol{X}(t)$ and $\boldsymbol{Y}(t)$ are in GCS with respect to the C^1 diffeomorphism (7).

Chen's GCS system is now applied to secure communication as a possible Internet application. Assume that sender A wants to send a message S—the first two paragraphs in this paper—to receiver B via email over the Internet. This message has 1546×8

blocks in binary form. The sampling rule T_{M_1} takes the first 1546 values in x_i or y_i $(i = 1, 2)$ whose 'positions' $l's$ satisfy $\mathrm{mod}(l, 25) = 0$. The sampling rule T_{M_2} takes the first 8 values in x_i or y_i $(i = 1, 2)$ whose 'positions' $l's$ satisfy $\mathrm{mod}(l, 6614) = 0$. The two decrypting-code rules T_B and T_σ are the diffeomorphisms $T_B(\boldsymbol{X}) = h_1(\boldsymbol{X})$, $T_\sigma(\boldsymbol{X}) = h_2(\boldsymbol{X})$ defined by Eq. (7). Let the secrete key be $\lambda = 1034$.

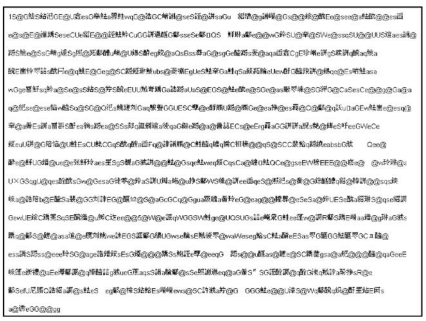

Fig. 2. Ciphertext c that masks the message S.

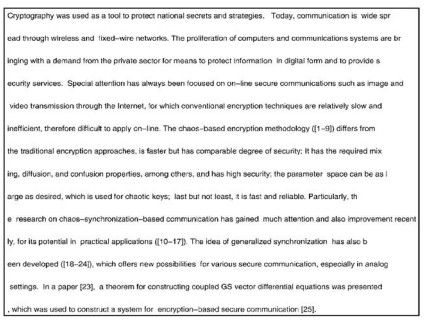

Fig. 3. Paragraphs are decrypted by receiver B.

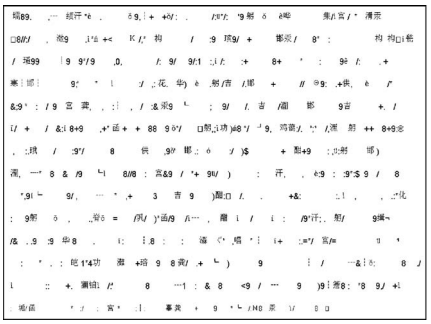

Fig. 4. Meaningless characters decrypted by an intruder using a nearly exact but approximate transformation, $\tilde{T}_B$.

• Sender A uses Chen's GCS system (5) and (6), with initial condition (9), to generate chaotic trajectories $(\boldsymbol{X}(t), \boldsymbol{Y}(t))$, as shown in Fig 1.

• Sender A follows steps 2–4 described above to encrypt the block S into a ciphertext c and a 'signature message' s. Figure 2 shows that the ciphertext c masks the message S successfully.

• Receiver B follows the steps 5–7 described above to decrypt the ciphertext c and compute the message S. Figure 3 displays that the two paragraphs have been successfully recovered.

Since sender A can use different initial conditions to generate the chaotic signals, an intruder will find it very difficult to decrypt the permuted message S on-line.

On the other hand, assume that an intruder knows the system (5) but only knows the decrypting-code rule T_B approximately (even nearly exactly). He will then use, for example, an approximate transformation, say

$$\tilde{T}_B(x_1, x_2) = \frac{(5 + 0.005)x_2}{x_1^2 + x_2^2},$$

to decrypt y_1. The decoding result is shown in Fig. 4, in which the meaningless characters cannot provide any useful information about the true message S (shown in Fig. 3.) Therefore, practically speaking, the intruder is unable to attack this secure communication on-line.

In summary, this chaotic GCS-based encryption scheme provides a new approach to chaotic communications for practical applications.

References

[1] Mao Y B and Chen G 2003 *Chaos-Based Image Encryption* in *Handbook of Computational Geometry for Pattern Recognition, Computer Vision, Neurocomputing and Robotics* (Berlin: Springer)
[2] Baptista M S 1998 *Phys. Lett.* A **240** 50
[3] Andrecut M 1998 *Int. J. Mod. Phys.* **8** 921
[4] Fridrich J 1998 *Int. J. Bifur. Chaos* **8** 1259
[5] Jakimoski G and Kocarev L 2001 *IEEE Trans. Circuits Systems I* **48** 163
[6] Kocarev L and Jakimoski G 2001 *Phys. Lett.* A. **289** 199
[7] Kotulski Z, Szczepanski J, Gorski K, Paszkiewicz A and Zugaj A 1000 *Int. J. Bifur. Chaos* **6** 1121
[8] Masuda N and Aihara K 2002 *IEEE Trans. Circuits Systems I* **49** 28
[9] Matthews R 1989 *Cryptologia* **XIII** 29
[10] Pecora L M and Carroll T L 1990 *Phy. Rev. Lett.* **64** 821
[11] Cuomo K M and Oppenheim A V 1993 *Phys. Rev. Lett.* **71** 65
[12] Kocarev L and Parlitz U 1995 *Phys. Rev. Lett.* **74** 5028
[13] Kawata J, Nishio Y and Ushida A 1999 *IEICE Trans. Fund.* E **82-A** 1322
[14] Kolumbán G, Kennedy M P and Chua L O 1998 *IEEE Trans. Circuits Systems I* **45** 1129
[15] Kolumbán G and Kennedy M P 2000 *IEEE Trans. Circuits Systems I* **47** 1673
[16] Feng J and Lu R 2002 *Chin. Phys. Lett.* **19** 302
[17] Carroll T 2003 *Phys. Rev.* E **67** 026207-1
[18] Kocarev L and Parlitz U 1996 *Phys. Rev. Lett.* **76** 1816
[19] Yang T and Chua L O 1996 *Int. J. Bifur. Chaos* **6** 2653
[20] Hunt B R, Ott E and York J A 1997 *Phys. Rev.* E **55** 4029
[21] Murali K and Lakshmanan M 1998 *Phys. Lett.* A **241** 302
[22] Yang T and Chua L O 1999 *Int. J. Bifur. Chaos* **9** 215
[23] Zhang X and Min L 2000 *J. Univ. Sci. Technol. Beijing* **7**(3) 225
[24] Zhang X, Zhang L and Min L 2003 *Chin. Phys. Lett.* **20** 2114
[25] Min L, Zhang X and Yang M 2003 *J. Univ. Sci. Technol. Beijing* **10**(2) 74
[26] Zhou T and Chen G and Yang Q 2004 *Chaos, Solitons Fractals* **19** 985