DOI: 10.7641/CTA.2014.30791

参数扰动下的混沌同步控制及其保密通信方案

李震波†, 唐驾时

(湖南大学 机械与运载工程学院, 湖南 长沙 410082)

摘要: 研究了变参数混沌系统的同步控制问题及其保密通信方案设计. 主要创新点可归结如下: 第一, 提出了利用混沌系统状态变量来构造变参数系统参数扰动项的思想, 研究了混沌系统参数在另一组混沌序列持续扰动下的同步控制问题. 混沌系统对参数具有敏感依赖性, 当混沌系统的参数被另一组混沌序列持续扰动时, 系统将产生更加难以预测的混沌行为. 第二, 对加密后的信息信号再进行一次非线性叠来生成加密端与解密端之间的通信信号, 而不是直接以加密信号作为通信信号, 使得实际传输的通信信号具有更复杂的形式从而难以被破译. 此外, 该方案只需向接收系统发送一路信号, 且同步控制器简单, 实用性较强. 数值模拟和理论分析表明该方案具有良好的通信、保密特性和较广的适用范围.

关键词: 混沌同步; 参数扰动; 单向耦合; 保密通信

中图分类号: TN914. 2 **文献标识码**: A

Chaotic synchronization with parameter perturbation and its secure communication scheme

LI Zhen-bo†, TANG Jia-shi

(College of Mechanical and Vehicle Engineering, Hunan University, Changsha Hunan 410082, China)

Abstract: The synchronization of chaotic system with variable parameters is investigated; the corresponding secure communication scheme is also proposed. The main innovations can be listed as follows. First, the parameter perturbation items adopted in this paper are not periodical signals but chaotic signals. This process can make a chaotic system present more complicated dynamical behavior. Secondly, a unidirectional couple controller is designed to realize the present synchronization. On the other aspect, a nonlinear superposition procedure is introduced to generate the transmitted signal. In many existing chaos-based secure communication schemes, the encrypted signal plays the role of the transmitted signal directly. However, in this paper, the transmitted signal is obtained by adding the encrypted signal with several chaotic signals. This procedure enhances the security of the algorithm. Besides, only one signal is needed to be transmitted in this algorithm and the controller is also simple; this means that the proposed algorithm is feasible and practical. Numerical simulations and theoretical analysis show that this algorithm is secure, efficient and generally applicable.

Key words: chaos synchronization; parameter perturbation; unidirectional couple; secure communication

1 引言(Introduction)

自1990年Pecora和Carroll实现混沌同步以来[1], 由于混沌同步在保密通讯、信号处理和生命科学等方面有着十分广泛的应用前景, 十几年来它一直是研究非线性科学的热点课题之一, 引起了人们极大地关注并对此进行了广泛而深入的研究[2–3]. 由于混沌信号具有非周期性、连续宽带频谱、类噪声的特性以及异常复杂的运动轨迹和不可预测性, 使得混沌信号十分适合作为保密通信的载体. 近年来混沌控制理论趋于成熟也为混沌保密通信奠定了理论基础, 使得近年来混沌保密通信研究取得了较丰富的成果. Zhang和An等研究了一种完全错位混合投影同步及其保密通信方案设计[4], Mengue和Essimbi研究了基于耦合半导体激光的混沌保密通信方案[5], Sun和Shen等研究了一个带有4个忆阻器的振子的复合同步及其保密通信应用[6], Luo和Wang基于三维混沌系统的随机复合同步设计保密通信方案[7], Nguimdo和Colet等为基于时间延迟系统的混沌光通信设计了新的数字密钥[8], Lemos和Benenti研究了混沌在量子保密通信中的应用[9], Ren和Baptista等则研究了利用混沌进行无线通信[10]. 此外, 基于复杂网络的混沌保密通信也受到了较大的关注[11–12].

收稿日期: 2013−07−28; 录用日期: 2014−02−25.

†通信作者. E-mail: lizhenbo126@126.com; Tel.: +86 731-85527054.

基金项目: 国家自然科学基金资助项目(11172093, 11032004); 湖南省研究生科研创新基金资助项目(CX2012B159).

众所周知, 对参数的敏感依赖性是混沌系统的一大特性. 在研究常参数混沌系统保密通信的同时, 人们渐渐对利用变参数混沌系统进行保密通信产生了兴趣, 如果对混沌系统的参数施加一定的扰动使其在一定范围内进行变化, 同时确保系统依然处于混沌状态, 则系统将产生更加难以预测的混沌行为. 混沌调制之所以被认为是保密性最强的通信方案, 也正是由于其利用信息信号作为扰动项来对系统的状态变量或者参数进行了扰动. 然而混沌调制方法也有一些不足之处, 如需要传输多路信号、对慢变信号的恢复存在误差以及要求信息信号是可微的等[13]. 如果利用变参数混沌系统进行保密通信, 则可以在保持强保密性的同时弥补混沌调制的上述不足. Grzybowski构造了基于单参数扰动的混沌保密通信方案[14], 王兴元等研究了混沌系统在三角周期函数扰动下的混沌同步控制问题[15], 本文则提出利用混沌序列来构造参数扰动项的思想, 即在驱动系统中引入另一混沌系统的状态变量作为参数扰动, 并对响应系统在同一扰动下施加控制从而实现驱动与响应系统的同步. 基于该同步思想设计了一种保密通信方案: 首先, 在加密端将信息信号注入加密系统, 则系统的输出信号与信息信号有关; 然后利用非线性叠加对驱动信号进行掩盖并生成通信信号, 使得通信信号具有更复杂的形式从而难以被破译. 在解密端, 先将通信信号还原成驱动信号, 然后利用基于Lyapunov稳定性理论设计的单向耦合控制器, 使解密系统与加密系统实现完全同步从而不失真的恢复出信息信号. 该方案的优点在于: 1) 加密和解密系统为变参数系统, 且参数变化律也是混沌的, 使得该方案的保密强度大大提高; 2) 只需向接收系统发送一路信号即可实现同步和解密, 且同步控制器简单, 实用性较强; 3) 信道中不是直接传输同步驱动信号, 而是传输通过非线性叠加后的混合信号, 从而使该方案可有效对抗基于噪声削减、回归映射、相空间重构等方法的攻击, 进一步提高了该方案的保密性.

2 参数扰动下的混沌同步及其单向耦合控制器(Chaotic synchronization with parameter perturbation and its unidirectional couple controller)

考虑如下方程描述的两个混沌系统:

$$\dot{x} = f(x; a + \sigma z), \tag{1}$$

$$\dot{z} = g(z), \tag{2}$$

其中: $x \in \mathbb{R}^n$, $z \in \mathbb{R}^n$是n维状态变量, $f(\cdot)$和$g(\cdot)$为非线性函数, a为系统(1)的参数, σz为参数扰动, σ称为扰动强度. $f(\cdot)$满足Lipschitz条件, 即

$$\|f(x; a + \sigma z) - f(y; a + \sigma z)\| \leqslant L\|x - y\|, \tag{3}$$

其中: $\|\cdot\|$为欧式空间2范数, $L > 0$称为Lipschitz常数. 选取适当的σ可使系统(1)保持混沌状态. 考虑以系统(1)为驱动系统, 系统(2)为参数扰动系统的自结构同步问题. 设响应系统为

$$\dot{y} = f(y; a + \sigma z) - Ku, \tag{4}$$

其中: $y \in \mathbb{R}^n$是n维状态变量, 参数扰动项σz依然由系统(2)提供. $u = y - x$为单向耦合控制器, $K = \mathrm{diag}\{k_1, k_2, \cdots, k_n\}$为耦合强度矩阵. 令同步误差向量$e = y - x$, 则由式(4)减去式(1)可得误差系统为

$$\dot{e} = f(y; a + \sigma z) - f(x; a + \sigma z) - Ke. \tag{5}$$

适当选取耦合强度K的值, 使得误差系统(5)是Lyapunov稳定的, 则系统(1)和(4)实现在系统(2)扰动下的同步. 若耦合强度矩阵K中至少有两个元素不为零, 则驱动系统须向响应系统传送多路信号才能实现同步, 这显然在保密通信的实际应用中并不适用. 现考虑耦合强度矩阵有且仅有一个非零元素的情形, 即$K = \mathrm{diag}\{0, \cdots, k_i, \cdots, 0\}$. 文献[16]对类似的单向耦合控制器进行了讨论, 并指出对于满足Lipschitz条件的n维混沌系统, 存在正整数$i(i \leqslant n)$和$k_i(k_i > Ln)$, 使得当耦合强度为$K = \mathrm{diag}\{0, \cdots, k_i, \cdots, 0\}$时, 该系统可实现单驱动变量单向耦合自结构同步. 虽然上述结果保证了当系统满足一定条件时, 单变量单向耦合控制器的存在性. 然而在实际应用中, 要确定控制器非零项所在的维数, 即正整数i的值, 仍需具体问题具体分析. 通常可先假设i为某一确定的正整数, 然后针对具体系统进行Lyapunov函数分析或Lyapunov指数计算, 来讨论所作之假设是否正确. 现以经典的Lorenz系统作为驱动系统, Chen系统作为扰动系统来实现上述同步.

Lorenz系统由如下方程描述[17]:

$$\begin{cases} \dot{x}_1 = (a_1 + \sigma z_1)(x_2 - x_1), \\ \dot{x}_2 = (b_1 + \sigma z_2)x_1 - x_1x_3 - x_2, \\ \dot{x}_3 = x_1x_2 - (c_1 + \sigma z_3)x_3, \end{cases} \tag{6}$$

其中: $x_i(i = 1, 2, 3)$为系统状态变量, a_1, b_1, c_1为系统参数, $z_i(i = 1, 2, 3)$为参数扰动, σ称为扰动强度. z_i由如下Chen系统提供[18]:

$$\begin{cases} \dot{z}_1 = a(z_2 - z_1), \\ \dot{z}_2 = -z_1z_3 + (c - a)z_1 + cz_2, \\ \dot{z}_3 = z_1z_2 - bz_3, \end{cases} \tag{7}$$

其中: $z_i(i = 1, 2, 3)$为系统状态变量, a, b, c为系统参数. 为了确保系统(6)在系统(7)的扰动下依然保持混沌, 需要确定扰动强度σ的取值. 本文利用文献[19–20]提出的方法计算了系统(6)在系统(7)扰动下的最大Lyapunov指数, 如图1所示. 当$-0.16 < \sigma < 0.18$时, 系统(6)的最大Lyapunov指数为正, 即系统保

持混沌状态. 特别的, 当$\sigma = 0$时, 系统(6)的最大Lyapunov指数为0.497, 与文献[19–20]中的结果一致. 为了更直观说明扰动强度σ的取值对系统(6)的影响, 分别在$\sigma = 0, \sigma = 0.1$和$\sigma = 0.3$时, 绘制了系统(6)的相图, 如图2–4所示. 图2为扰动强度$\sigma = 0$时系统(6)的相图, 图3为扰动强度$\sigma = 0.1$时系统(6)的相图, 图4为扰动强度$\sigma = 0.3$时系统(6)的相图. 可见当$\sigma = 0$和$\sigma = 0.1$时, 系统依然保持混沌运动, 当$\sigma = 0.3$时, 奇怪吸引子消失, 系统不处于混沌运动, 这一结果与图1所示的结果一致.

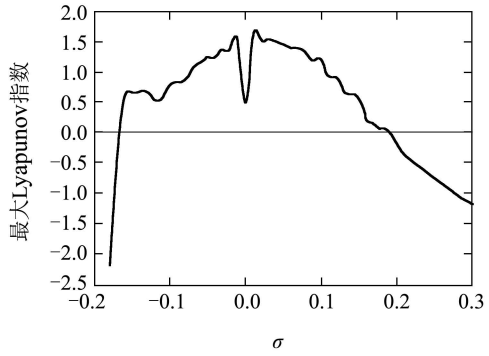
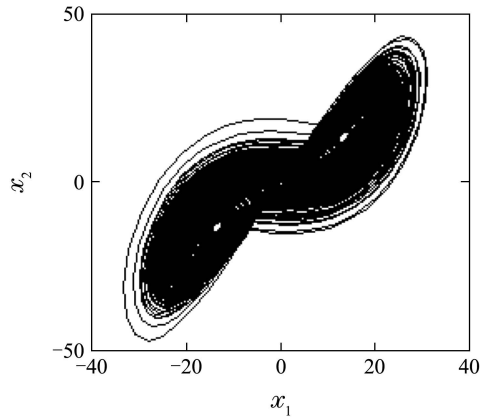
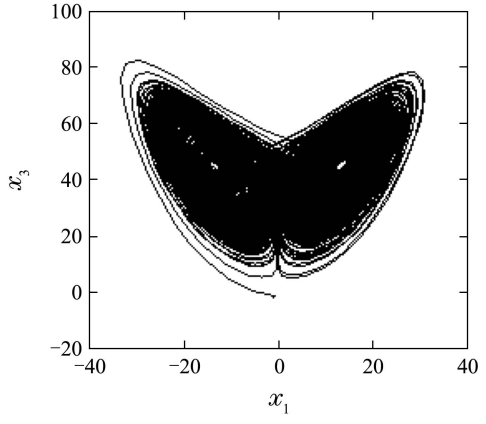


图 1 系统(6)的最大Lyapunov指数随扰动强度σ变换的曲线图

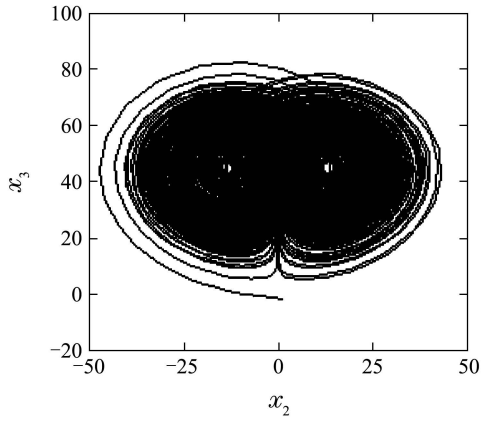
Fig. 1 The variation of the biggest Lyapunov exponent vesus the pertubation parameter σ of system (6)



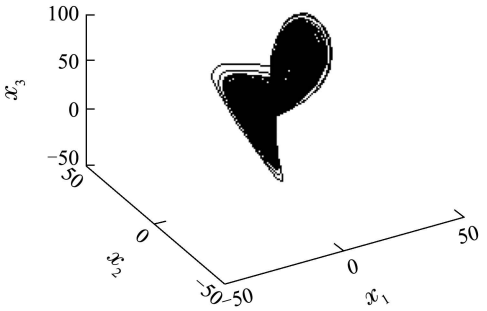
(a)



(b)



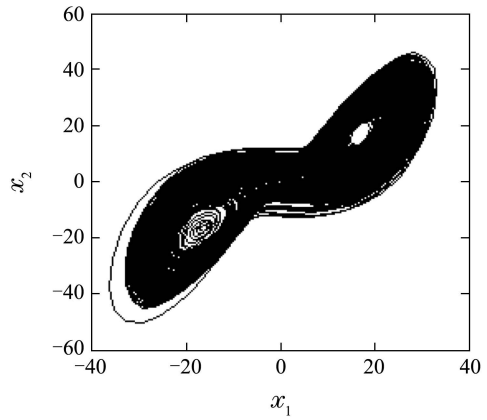
(c)



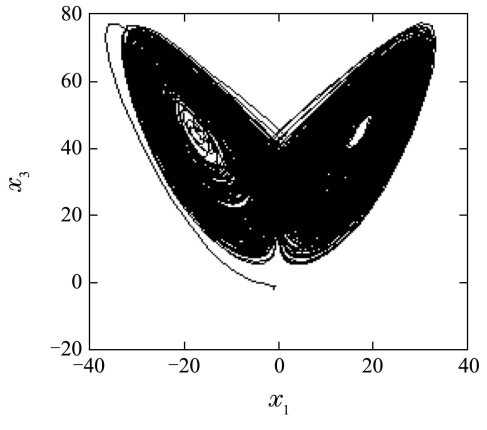
(d)

图 2 扰动强度$\sigma = 0$时系统(6)的相图

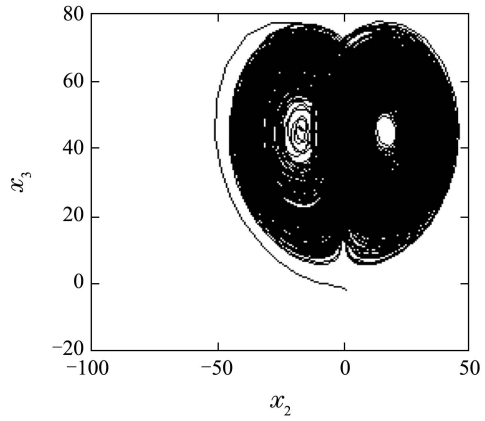
Fig. 2 The phase portrait of system (6) when $\sigma = 0$



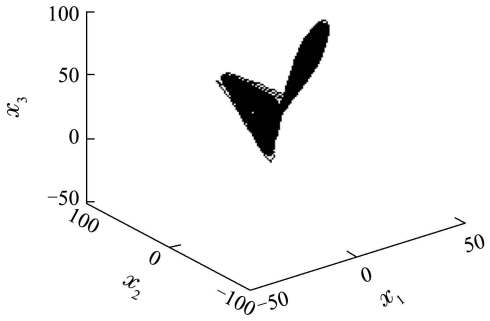
(a)



(b)



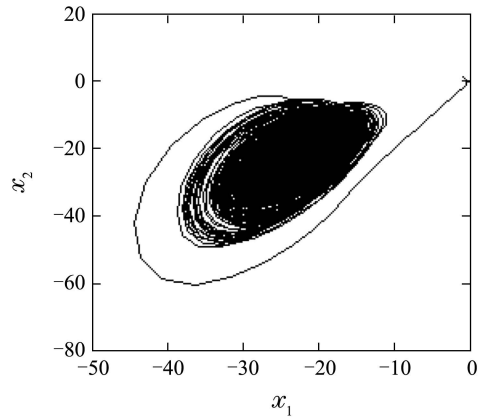
(c)



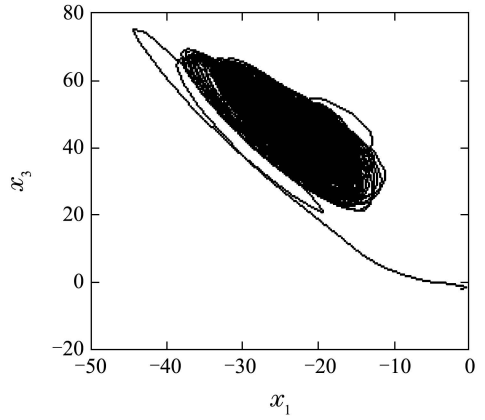
(d)

图 3 扰动强度$\sigma = 0.1$时系统(6)的相图

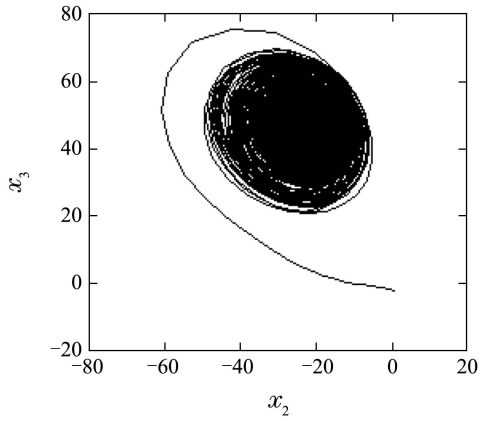
Fig. 3 The phase portrait of system (6) when $\sigma = 0.1$



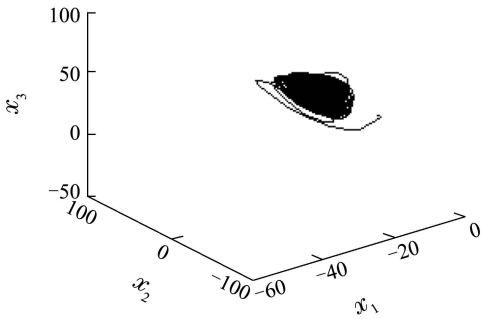
(a)



(b)



(c)



(d)

图 4 扰动强度$\sigma = 0.3$时系统(6)的相图

Fig. 4 The phase portrait of system (6) when $\sigma = 0.3$

现考虑系统(6)的同步问题, 设耦合强度矩阵$K = \mathrm{diag}\{k_1, 0, 0\}$, 即$i = 1$, 则响应系统为

$$\begin{cases} \dot{y}_1 = (a_1 + \sigma z_1)(y_2 - y_1) - k_1 u_1, \\ \dot{y}_2 = (b_1 + \sigma z_2) y_1 - y_1 y_3 - y_2, \\ \dot{y}_3 = y_1 y_2 - (c_1 + \sigma z_3) y_3, \end{cases} \tag{8}$$

其中: $y_i (i = 1, 2, 3)$为系统状态变量, a_1, b_1, c_1为系统参数, $z_i (i = 1, 2, 3)$为参数扰动, σ称为扰动强度. z_i依然由系统(7)提供. $u_1 = y_1 - x_1$为单向耦合控制器, k_1为耦合强度. 令系统(8)减去系统(6), 得到如下同步误差系统:

$$\begin{cases} \dot{e}_1 = -(k_1 + a_1 + \sigma z_1) e_1 + (a_1 + \sigma z_1) e_2, \\ \dot{e}_2 = (b_1 + \sigma z_2 - x_3) e_1 - e_2 - x_1 e_3 - e_1 e_3, \\ \dot{e}_3 = x_2 e_1 + x_1 e_2 - (c_1 + \sigma z_3) e_3 + e_1 e_2, \end{cases} \tag{9}$$

其中$e_i = y_i - x_i (i = 1, 2, 3)$为同步误差. 为了讨论所选择的$i$值是否可行以及确定耦合强度$k_1$的值, 选取如下Lyapunov函数:

$$V(t) = \frac{1}{2}(e_1^2 + e_2^2 + e_3^2). \tag{10}$$

显然$V(t) \geqslant 0$, 对上式求导得

$$\dot{V}(t) = e_1 \dot{e}_1 + e_2 \dot{e}_2 + e_3 \dot{e}_3. \tag{11}$$

将式(9)代入上式并整理得

$$\dot{V}(t) = -[k_1 + (a_1 + \sigma z_1) - \frac{x_2^2}{4(c_1 + \sigma z_3)} - \frac{1}{4}(a_1 + \sigma z_1 + b_1 + \sigma z_2 - x_3)^2]e_1^2 - [e_2 - \frac{1}{2}(a_1 + \sigma z_1 + b_1 + \sigma z_2 - x_3)e_1]^2 - (\sqrt{c_1 + \sigma z_3}e_3 - \frac{x_2}{2\sqrt{c_1 + \sigma z_3}}e_1)^2.$$

若k_1满足

$$k_1 > \frac{x_2^2}{4(c_1 + \sigma z_3)} + \frac{1}{4}(a_1 + \sigma z_1 + b_1 + \sigma z_2 - x_3)^2 - (a_1 + \sigma z_1), \tag{12}$$

则$\dot{V}(t) \leqslant 0$. 由Lyapunov稳定性理论可知, 误差系统(9)渐进稳定, 即驱动系统(6)与响应系统(8)在系统(7)的扰动下实现同步. 因为混沌系统的状态变量总是有界的, 所以只要取足够大的k_1即可满足式(12). 由于满足上述条件的k_1一定存在, 表明所作之假设$i = 1$成立; 反之, 若无法确定k_1或k_1不存在, 则假设不成立, 需继续讨论i为其他值的情形. 由于一些混沌系统在进行耦合同步时很难找到合适的Lyapunov函数来讨论, 因此对于i和k_i的确定, 除了利用上述Lyapunov函数分析之外, 还可以通过计算Lyapunov指数来确定, 即先假设i和k_i为某一确定值, 然后计算误差系统(9)的Lyapunov指数, 若所得的Lyapunov指数全为负, 则假设成立; 反之, 需计算i和k_i为其他值时误差系统(9)的Lyapunov指数. 为了说明控制器的有效性, 现进行数值模拟. 令驱动和响应系统参数为: $a_1 = 16$, $b_1 = 45.92$, $c_1 = 4$, 初值分别为: $x_1(0) = -1$, $x_2(0) = 1$, $x_3(0) = -2$, $y_1(0) = 4$, $y_2(0) = -2$, $y_3(0) = 3$. 扰动系统的参数为: $a = 35$, $b = 3$, $c = 28$, 初值为: $z_1(0) = 2$, $z_2(0) = 1$, $z_3(0) = -1$. 扰动强度$\sigma = 0.1$, 耦合强度k取250. 图5表示驱动系统(6)与响应系统(8)的同步误差曲线, 误差很快的收敛于零, 表明系统(6)和(8)实现同步. 同时也验证了本节所设计的单向耦合控制器是有效的.

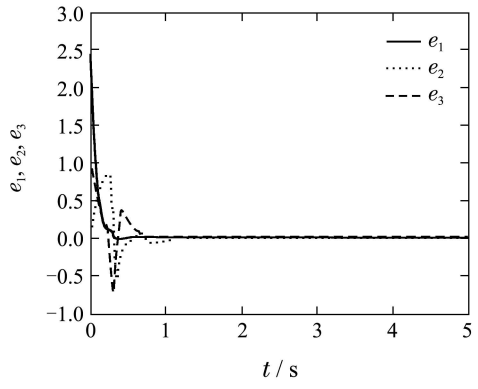


图 5 驱动系统(6)与响应系统(8)的同步误差曲线

Fig. 5 The synchronization error between the driven system (6) and respone system (8)

3 保密通信方案设计(Design the secure communication scheme)

上一节讨论了当混沌系统参数在另一组混沌序列持续扰动下的同步控制问题, 并针对Lorenz系统被Chen系统扰动的情形设计了相应的单控制变量单向耦合控制器. 现基于该同步思想和控制器设计相应的保密通信方案. 设待加密的信息信号为$m(t)$, 加密系统为

$$\begin{cases} \dot{x}_1 = (a_1 + \sigma z_1)(x_2 - x_1) + \varepsilon m(t), \\ \dot{x}_2 = (b_1 + \sigma z_2)x_1 - x_1 x_3 - x_2, \\ \dot{x}_3 = x_1 x_2 - (c_1 + \sigma z_3)x_3, \end{cases} \tag{13}$$

其中ε为信息信号的振幅控制因子. 将信息信号注入加密系统可使加密系统的输出信号与信息信号有关, 有利于提高保密性. 加密系统中的参数扰动仍由系统(7)即Chen系统提供, 混沌系统是对参数敏感依赖的, 利用变参数混沌系统来进行保密通信有着比利用常参数系统更高的保密性从而受到极大关注. 上节中, 讨论了利用混沌序列来构造参数扰动的思想, 并设计了相应的同步控制器实现了混沌系统在另一混沌序列作为参数扰动下的同步控制问题. 由于混沌系统的特性, 不难得出, 利用混沌序列来进行参数扰动, 比利用周期信号来进行参数扰动更有利于系统产生复杂的动力学行为, 增加系统的内禀随机性. 同时, 扰动系统作为混沌系统, 本身也是对初值和参数敏感的, 再加上扰动强度σ的引入, 极大的增加了保密算法的密钥空间, 增强了算法的保密性, 具体将在下一节讨论. 设接收端的解密系统为

$$\begin{cases} \dot{y}_1 = (a_1 + \sigma z_1)(y_2 - y_1) - k(y_1 - s(t)), \\ \dot{y}_2 = (b_1 + \sigma z_2)y_1 - y_1 y_3 - y_2, \\ \dot{y}_3 = y_1 y_2 - (c_1 + \sigma z_3)y_3, \end{cases} \tag{14}$$

其中$s(t) = x_1 - \dfrac{\varepsilon}{k}m(t)$为加密系统发出的驱动信号, 由上节的讨论可知, 在正确的设定所有密钥以后, 只需$s(t)$一路信号即可驱使解密系统与加密系统实现同步. 在接收端与发送端达成同步后, 可利用下式恢复出信息信号:

$$\tilde{m}(t) = \frac{k}{\varepsilon}(y_1(t) - s(t)) \underset{y_1(t) \to x_1(t)}{\overset{t \to \infty}{\longrightarrow}} \frac{k}{\varepsilon}(x_1(t) - s(t)) = m(t). \tag{15}$$

为了提高通信信号的安全性, 本文不直接将驱动信号$s(t)$作为发送端与解密端之间的通信信号, 而是利用参数扰动系统(7)产生的混沌信号对$s(t)$进行如下非线性叠加:

$$\theta(t) = s(t) + \psi(z_1, z_2, z_3; \omega), \tag{16}$$

其中: $s(t)$为驱动信号, $\psi(\cdot)$为非线性函数, ω为调幅参数. 经过上述处理后的信号$\theta(t)$被用来作为发送端与接收端的通信信号, 该信号可有效对抗基于噪声削

减、回归映射和相空间重构等攻击方法.

下面进行数值模拟来说明该保密通信方案的有效性. 设信息信号$m(t)=\sin t$为一简单的正弦信号, 将$m(t)$代入加密系统(13), 取振幅控制因子$\varepsilon=0.1$, 系统(13)的参数为$a_1=16$, $b_1=45.92$, $c_1=4$, 扰动系统(7)的参数取值与上节相同, 扰动强度$\sigma=0.1$. 此时, 加密系统(13)的最大Lyapunov指数为1.127, 意味着系统处于混沌状态. 信息信号经过加密运算后产生的同步驱动信号$s(t)$如图6所示. 选取非线性函数$\psi(\cdot)$为

$$\psi(z_1,z_2,z_3;\omega)=\omega_1 z_1^2+\omega_2 z_2 z_3. \tag{17}$$

令调幅参数$\omega_1=-0.05$, $\omega_2=0.05$, 按式(16)对驱动信号$s(t)$进行叠加后得到通信信号$\theta(t)$, 其时间历程如图7(b)所示. 接收端接收到通信信号$\theta(t)$后, 先利用扰动系统(7)生成的信号从$\theta(t)$中提取出驱动信号$s(t)$、调幅参数ω以及系统(7)的参数和初值将作为密钥由通信双方事先约定. 由于系统(7)也是混沌系统, 对参数和初值具有敏感依赖性, 使得密钥的选取有很大的自由度以及便于更换等. 将提取出的驱动信号$s(t)$加入解密系统(14), 取耦合强度$k=250$即可实现解密与加密系统的同步, 然后利用式(15)得到恢复出的信息信号如图7(c)所示, 信号恢复误差$e_{\rm m}=\tilde{m}(t)-m(t)$如图7(d)所示. 当信息信号为方波信号如$m(t)=2\mathrm{square}(2t)$时, 在不更改其他参数的情况下, 利用上述方案进行方波信号的保密通信仿真, 仿真结果如图8所示. 可见, 无论是正弦信号还是方波信号, 都能被该保密通信方案进行加密和传输并且不失真的恢复出来, 表明了该方案的有效性. 该方案对信息信号没有严格要求, 只要选择合适的振幅控制因子ε使加密系统保持混沌, 则任何形式的时间序列都可以利用该方案来进行保密通信, 从而使得该方案有着较广的适用范围. 由于解密系统与加密系统的同步存在时间差, 所以对于需要从头至尾完整恢复的信号, 如图片、语音、文字等, 可在加密时适当选取时间延迟变量τ, 使信息信号从τ时刻起加入加密系统进行加密. 为了进一步说明该算法具有广泛的使用范围, 本文将对图片信号的保密通信过程进行仿真. 首先, 选取信息信号为一张灰度图片, 见图9(a). 众所周知, 在计算机系统中, 图像是以多维数组的形式存放的, 灰度图像通常是二维数组, 真彩图像通常是三维数组. 要利用本文算法来进行该图像的保密通信需先将图像调制成一个一维数组, 即一组一维离散数据. 然后将该组数据作为信息信号直接加入加密系统进行运算, 即可得到加密信号. 在信号恢复时, 由于需要完整的恢复出整个数组才能正确的还原图片, 因此通常会在加密与解密方之间约定一个延迟时间τ, 即在τ时刻以后才将信息信号加入加密系统. 解密时, 也只从τ时刻开始提取解密出的信息信号. 这样就可以避免加密与解密系统在同步过程中存在着的同步时间差对信号解密造成破坏性影响. 在不更改其他加密参数的情况下, 令延迟变量$\tau=20$并利用上述方案进行图像信号的保密通信仿真, 结果如图9所示. 对于音频或视频信号的传输, 则可先对音频或视频进行高频采样, 然后将采样结果调制成一维数组即可利用该方法进行保密通信, 在解密端先解密再解调, 即可有效恢复信号. 文字信号的传输也可类似处理, 先利用通用编码(如ACSII码等)或自定义编码将待传输的文字编译成数字, 然后即可利用本方法进行保密通信. 可见, 无论是连续信号还是离散信号, 该算法都可以进行有效的保密通信. 此外, 时间延迟变量的引入, 也有益于保持算法的密钥独立性, 具体将在第4节论述.

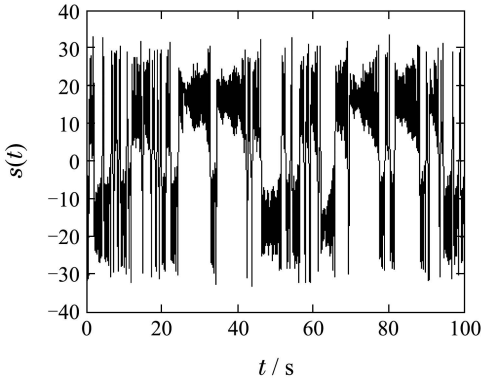
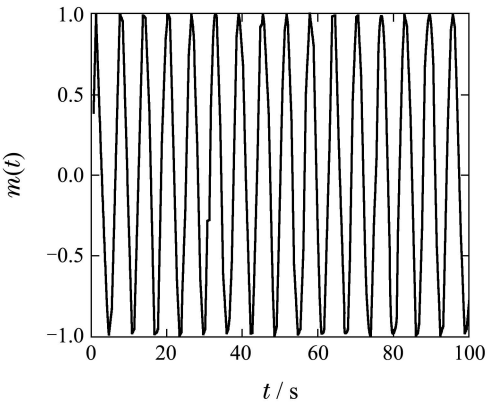
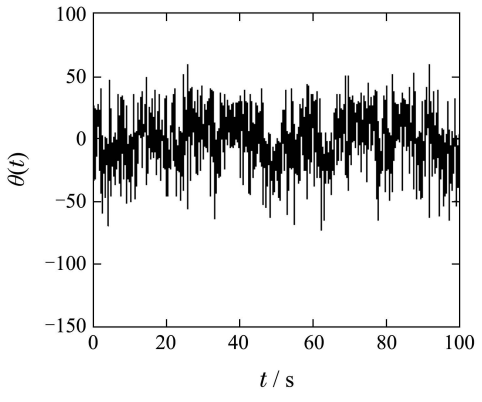


图 6　驱动信号$s(t)$的时间历程

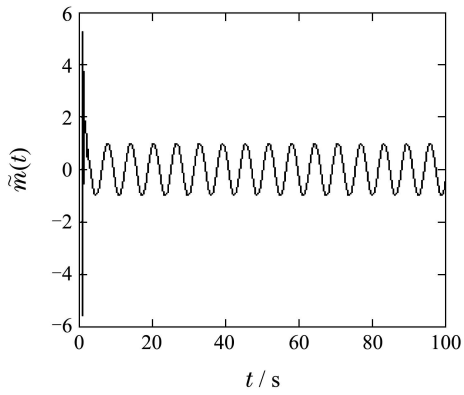
Fig. 6　Time evolution of the driven signal $s(t)$



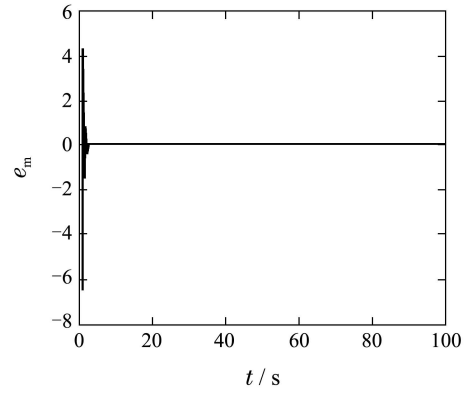
(a)　信息信号$m(t)$



(b)　通信信号$\theta(t)$的时间历程



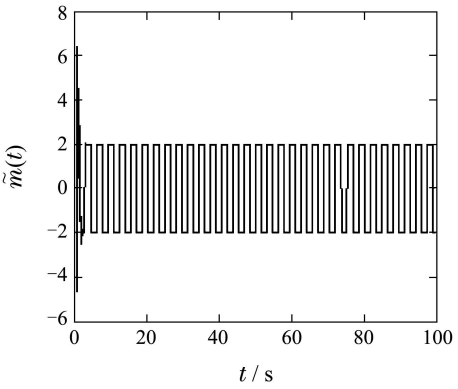
(c) 恢复后的信息信号$\tilde{m}(t)$



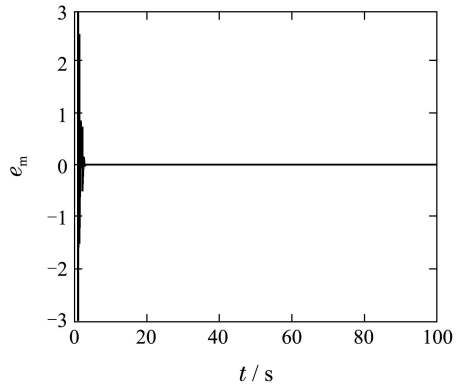
(d) 信息信号的恢复误差

图 7 正弦信号保密通信仿真结果

Fig. 7 Simulation result of the secure communication with sine signal



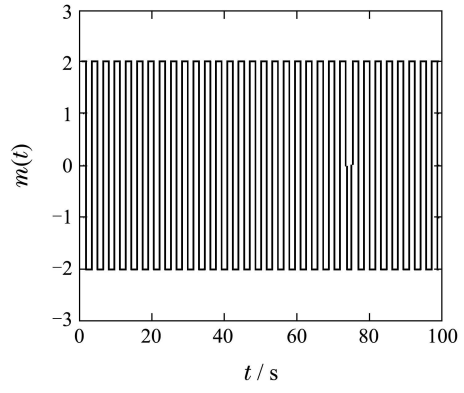
(c) 恢复后的信息信号$\tilde{m}(t)$



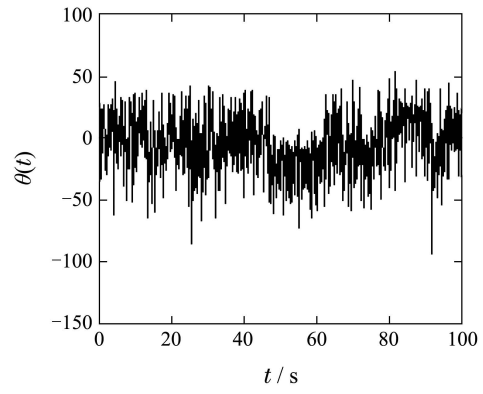
(d) 信息信号的恢复误差

图 8 方波信号保密通信仿真结果

Fig. 8 Simulation result of the secure communication with square signal

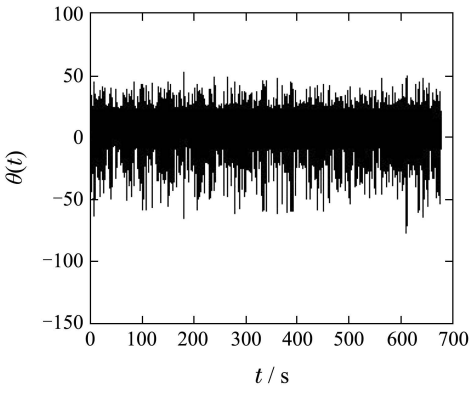


(a) 信息信号$m(t)$



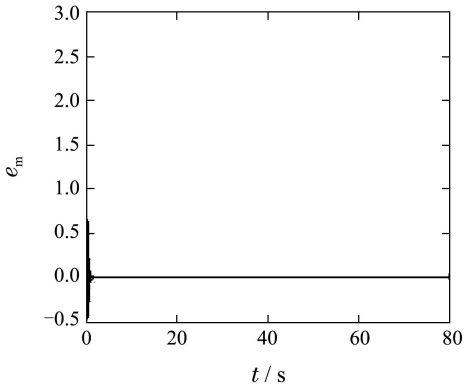
(b) 通信信号$\theta(t)$的时间历程

(a) 信息信号$m(t)$



(b) 通信信号$\theta(t)$的时间历程

(c) 恢复后的信息信号$\tilde{m}(t)$



(d) 信息信号的恢复误差

图 9 图像信号保密通信仿真结果

Fig. 9 Simulation result of the secure communication with image signal

4 讨论(Discussions)

对于保密通信算法来说, 保密性是至关重要的. 本文提出用混沌信号做参数扰动来构造变参数混沌系统的思想, 并基于该思想设计了相应的保密通信方案. 该方案有着较高的安全性和实用性, 原因如下:

1) 信息信号是直接加入系统的, 从而使得加密系统的输出信号与信息信号的构成有关. 信息信号不是“浮”在混沌信号之上, 而是参与了混沌信号的生成. 此外, 发送端与接收端之间的通信不是直接传输驱动信号, 而是利用扰动系统的混沌信号对驱动信号进行非线性叠加之后, 生成新的通信信号. 对于信道加密算法来说, 通信信号的安全性是整个通信算法安全性的核心, 在该算法中, 当通信信号被“敌方”截获时, 对方需要首先从通信信号中分离出驱动信号, 方可利用噪声削减、回归映射、相空间重构等方法尝试破解. 考虑到非线性叠加函数$\psi(\cdot)$之选取的多样性, 以及所叠加之信号仍为混沌信号, 使得从通信信号中分离出驱动信号这一步也变得异常艰难, 大大的增加的算法的保密性.

2) 加密系统是变参数系统, 且参数变化率也是混沌的. 混沌系统是参数敏感的, 变参数混沌系统无疑具有更复杂的动力学行为. 相对于周期扰动而言, 当参数变化率也是混沌时, 系统的保密性将大大提高, 使得该保密通信方案能有效对抗基于参数识别、非线性预期等攻击方法.

3) 密钥空间很大, 暴力破解时效性低. 文献[21]指出, 一个足够强的保密通信算法需要满足密钥空间$k > 2^{100}$. 由于混沌系统对参数的敏感度约为10^{-16}, 对初值的敏感度约为10^{-10}, 因而在本文的保密通信算法中, 由扰动强度σ构成的密钥子空间大小约为3.4×10^{15}. 若考虑扰动系统的初值仅在区间$(0, 10]$内变化, 则由扰动系统的初值构成的密钥子空间大小约为10^{33}. 显然, $3.4 \times 10^{15} \times 10^{33} > 2^{100}$. 事实上, 如果考虑到加密系统和扰动系统的参数也可在一定区间内变化该算法的密钥空间将更大, 从而使得暴力破解需付出极大的代价.

4) 发送端与接收端之间只需传送一路信号, 且同步控制器简单、同步效率高. 相对于参数调制等需传输多路信号的算法而言, 该方案在通信信号数上存在优势. 同时, 由于参数扰动系统的引进以及对驱动信号进行非线性叠加处理, 使得相对于一般混沌掩盖方法而言, 该方案的保密性大大提高. 此外, 该算法的控制器简单, 同步效率高, 解密系统与加密系统的状态误差在2 s左右即达到10^{-5}, 从而使得该方法具有较强的实用性.

5) 验证密钥的独立性. 虽然混沌系统对初值和参数是敏感依赖的, 但如果两个自结构系统的初值或参数误差很小, 如小于10^{-10}, 则两个系统的状态变量轨线在前10 s左右是十分接近的, 10 s以后才完全分离. 因此, 要保证密钥独立性的话, 信息信号不能在零时刻就加入加密系统, 而要引进一个时间延迟量τ, 即信息信号改写为

$$m(t) = \begin{cases} 0, & t < \tau, \\ \sin t, & t \geqslant \tau. \end{cases} \tag{18}$$

若按照上述讨论式(3)中提及的密钥精度来构造密钥空间, 则通过数值计算得时间延迟量$\tau \geqslant 15$ s即可保证密钥的独立性. 现用数值模拟来证明, 令所有加密参数的取值与第3节一致, 时间延迟量$\tau = 20$ s, 信息信号为式(18). 假设攻击方在所有参数均已获取而仅剩扰动强度σ未知时, 用$\hat{\sigma} = 0.1 + 10^{-16}$来估计$\sigma = 0.1$, 解密结果如图10所示. 可见20 s以后的恢复信号杂乱无章, 解密完全失败, 从而验证了密钥的独立性.

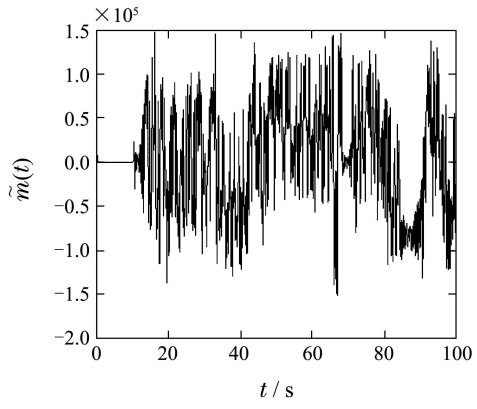


图 10 利用错误密钥解密出的信息信号

Fig. 10 The decrypted signal with using the wrong key

6) 虽然该保密通信算法具有上述讨论的各种优势. 然而, 若要将该方法投入实际应用仍有一些问题亟待解决. 首先, 该算法是利用计算机或微处理器来产生混沌信号, 属于数字通信范畴, 但是不同的混沌产生平台由于在处理器型号、构架类型以及数据精度等方面存在的差异会造成加密与解密系统之间的时钟精度和数值精度是否匹配的问题, 还有如何实现不同数字平台之间的快速同步等问题都有待进一步解决; 其次, 虽然数字通信相较于基于混沌电路的模拟通信能更好地解决因通信信道恶劣以及干扰严重等造成通信质量下降的问题, 但是在保密性和可靠性要求更高的场合, 需要采用更先进的数字式混沌通信算法, 并在其中融入更新的信道安全技术[15]; 此外, 在第3节中讨论了对于图像、音频和文字等离散信号的保密通信问题. 在本文的模拟中, 对原始数据进行调制时采用的是直接调制, 若在调制过程中能利用混沌密码学的相关算法将原始数据进行混沌加密调制, 则可更进一步地提高算法的保密通信, 也可将作为信源加密的混沌密码学和信道加密的混沌保密通信有机的结合起来, 这也将是接下来的研究重点.

5 结论(Conclusions)

本文提出了利用混沌系统状态变量来构造参数扰动项的思想, 研究了当混沌系统参数在另一组混沌序列持续扰动下的同步控制问题. 众所周知, 混沌系统对参数具有敏感依赖性, 当混沌系统的参数被另一组混沌序列持续扰动时, 系统将产生更加难以预测的动力学行为. 基于该特性, 设计了相应的保密通信方案. 首先, 在加密端将信息信号注入加密系统, 使得加密系统的输出与信息信号有关, 然后利用非线性叠加对驱动信号进行掩盖并生成通信信号, 使得该通信信号具有更复杂的形式从而有效对抗噪声削减、相空间重构、回归映射、参数识别和非线性预期等方法的攻击. 在解密端, 先利用扰动系统的输出将通信信号还原成驱动信号, 然后利用基于Lyapunov稳定性理论设计的单向耦合控制器, 使解密系统与加密系统实现完全同步从而不失真地恢复出信息信号. 该方案只需向接收系统发送一路信号, 且同步控制器简单、同步效率高、实用性较强. 第3节的数值模拟表明了该方案的有效性, 第4节的讨论和分析, 表明了该方案具有较高的保密性, 且同时具有参数调制方法保密性高和混沌掩盖方法易于实现的特性. 此外, 利用混沌系统状态变量来构造参数扰动项的思想还可以利用到高维超混沌系统中, 或者构造更多形式的参数扰动, 为混沌保密通信研究提供了新的思路.

参考文献(References):

[1] PECORA L M, CARROLL T L. Synchronization in chaotic system [J]. *Physical Review Letters*, 1990, 64(8): 821 – 824.

[2] CHEN G, DONG X. *From Chaos to Order* [M]. Singapore: Word Scientific, 1998.

[3] OTT E, GREBOGI C, YORKE JA. Controlling chaos [J]. *Physical Review Letters*, 1990, 64(11): 1196 – 1199.

[4] ZHANG L F, AN X L, ZHANG J G. A new chaos synchronization scheme and its application to secure communications [J]. *Nonlinear Dynamics*, 2013, 73(1/2): 705 – 722.

[5] MENGUE A D, ESSIMBI B Z. Secure communication using chaotic synchronization in mutually coupled semiconductor lasers [J]. *Nonlinear Dynamics*, 2012, 70(2): 1241 – 1253.

[6] SUN J W, SHEN Y, YIN Q, et al. Compound synchronization of four memristor chaotic oscillator systems and secure communication [J]. *Chaos*, 2013, 23(1): 013140.

[7] LUO R Z, WANG Y L. Finite-time stochastic combination synchronization of three different chaotic systems and its application in secure communication [J]. *Chaos*, 2012, 22(2): 023109.

[8] NGUIMDO RM, COLET P, LARGER L, et al. Digital key for chaos communication performing time delay concealment [J]. *Physical Review Letters*, 2011, 107(3): 034103.

[9] LEMOS G B, BENENTI G. Role of chaos in quantum communication through a dynamical dephasing channel [J]. *Physical Review A*, 2010, 81(6): 062331.

[10] REN H P, BAPTISTA S P, GREBOGI C. Wireless communication with chaos [J]. *Physical Review Letters*, 2013, 110(18): 184101.

[11] ZHOU J, XIANG L, LIU Z R. Global synchronization in general complex delayed dynamical networks and its applications [J]. *Physica A: Statistical Mechanics and its Applications*, 2007, 385(2): 728 – 742.

[12] ZHOU J, CHEN T, XIANG L. Chaotic lag synchronization of coupled delayed neural networks and its applications in secure communication [J]. *Circuits, Systems, and Signal Processing*, 2005, 24(5): 599 – 613.

[13] WU X J, WANG H, LU H T. Hyperchaotic secure communication via generalized function projective synchronization [J]. *Nonlinear Analysis: Real World Applications*, 2011, 12(2): 1288 – 1299.

[14] GRZYBOWSKI J M V, RAFIKOV M, BALTHAZAR J M. Synchronization of the unified chaotic system and application in secure communication [J]. *Communications in Nonlinear Science and Numerical Simulation*, 2009, 14(6): 2793 – 2806.

[15] 王兴元. 混沌系统的同步及在保密通信中的应用 [M]. 北京: 科学出版社, 2012.
(WANG Xingyuan. *Synchronization of Chaotic Systems and Its Applications in Secure Communication* [M]. Beijing: Science Press, 2012.)

[16] 李建芬, 李农. 一类混沌系统的修正函数投影同步 [J]. 物理学报, 2011, 60(8): 080507.
(LI Jianfang, LI Nong. Modified function projective synchronization of a class of chaotic systems [J]. *Acta Physica Sinica*, 2011, 60(8): 080507.)

[17] LORENZ E N. Deterministic nonperiodic flow [J]. *Journal of the Atmospheric Sciences*, 1963, 20(2): 130 – 141.

[18] CHEN G, UETA T. Yet another chaotic attractor [J]. *International Journal of Bifurcation and Chaos*, 1999, 9(7): 1465 – 1466.

[19] WOLF A, SWIFT J B, SWINNEY H L, et al. Determining Lyapunov exponents from a time series [J]. *Physica D: Nonlinear Phenomena*, 1985, 16(3): 285 – 317.

[20] BRIGGS K. An improved method for estimating Lyapunov exponents of chaotic time series [J]. *Physics Letters A*, 1990, 151(1/2): 27 – 32.

[21] ALVAREZ G, LI S J. Some basic cryptographic requirements for chaos-based cryptosystems [J]. *International Journal of Bifurcation and Chaos*, 2006, 16(8): 2129 – 2152.

作者简介:

李震波 (1986–), 男, 博士研究生, 目前研究方向为动力学与控制, E-mail: lizhenbo126@126.com;

唐驾时 (1948–), 男, 教授, 博士生导师, 目前研究方向为分岔与混动控制, E-mail: tangjiashi@hnu.edu.cn.