# 一种基于混沌系统部分序列参数辨识的混沌保密通信方法*

刘乐柱 张季谦† 许贵霞 梁立嗣 汪茂胜

(安徽师范大学物理与电子信息学院, 芜湖 241000)

(2013 年 9 月 4 日收到; 2013 年 9 月 25 日收到修改稿)

本文提出一种混沌保密通信方法, 即混沌系统的部分序列用于混沌系统参数辨识其他序列用于通信保密. 利用混沌蚁群优化算法对部分序列混沌系统进行参数辨识, 以达到了解混沌系统全部信息的目的. 在参数辨识过程中引入参数空间和蚁群空间, 通过空间变换函数使参数空间与蚁群空间之间相互变换. 文中使用 Lorenz 系统进行数值试验, 其结果验证混沌系统部分序列参数辨识及混沌保密通信的可行性.

**关键词**: 混沌蚁群优化, 参数辨识, 混沌保密通信, 数值模拟

**PACS:** 05.10.–a, 05.45.Gg, 02.60.Cb, 02.60.Pn **DOI:** 10.7498/aps.63.010501

## 1 引 言

混沌是非线性动力学系统中一个非常有意义的现象. 混沌现象表现出复杂性、类噪声性、不可预测性等行为. 基于这些行为, 混沌保密技术得到广泛关注和研究[1−3]. 文献 [2] 通过设计高阶自适应滑模控制器, 实现混沌系统参数辨识, 并用于混沌保密通信, 通过数值试验验证其可行性. 文献 [3] 把基于物理混沌的混合加密方法用于图像加密, 并比较分析了此混合加密方法的优越性. 混沌保密通信是在发射端将信息埋入发射系统的混沌信号中, 接收端接收含有信息的混沌信号并提取出信息. 混沌保密通信需要发射端 (驱动系统) 与接收端 (响应系统) 两混沌系统同步. 响应系统实现与驱动系统同步的最直接的方法是对驱动系统参数辨识.

近年来, 混沌系统参数辨识的研究引起了科研工作者的高度重视, 相应地提出多种富有成效的参数辨识方法. 文献 [4—6] 使用混沌蚁群优化算法对 Lorenz 系统进行参数辨识. 文献 [7] 提出的最小相对奇异值法虽然不是对混沌系统进行参数辨识, 但可以对混沌背景中的信号参数进行辨识如正弦信号的频率. 文献 [8] 使用自适应滤波方法实现混沌系统参数辨识, 对无噪声和有噪声环境均做了研究讨论. 文献 [9] 使用自适应滑模方法实现混沌系统同步. 文献 [10] 通过自适应控制器实现混沌系统参数辨识和同步. 文献 [11] 提出一种扩散草丛算法, 并对多个混沌系统分别进行参数辨识. 文献 [12] 采用梯度下降法实现混沌系统参数辨识和同步. 混沌系统参数辨识是在得到混沌系统数据序列的基础上, 计算出描述混沌系统的相应未知参数. 大部分已提出的混沌系统参数辨识方法需要混沌系统全部序列来实现参数辨识. 本文提出一种基于部分序列的参数辨识方法, 参数辨识使用混沌蚁群优化算法实现.

本文首先简要介绍混沌蚁群优化算法, 并对其简单改进引入蚁群空间和参数空间, 这样可以使混沌蚁群算法不受问题搜寻范围的约束. 引入蚁群空间和参数空间后, 算法可以求解任意有限实数空间的最优化问题. 接着介绍混沌系统部分序列参数辨识, 在混沌系统参数辨识的基础上提出一种混沌保密通信方法. 文章最后以 Lorenz 系统进行数值

* 国家自然科研基金 (批准号: 11047017, 21103002) 和安徽省教育厅高等学校省级优秀青年人才基金项目 (批准号: 2011SQRL023) 资助的课题.

† 通讯作者. E-mail: zhangcdc@mail.ahnu.edu.cn

 

试验, 主要包含Lorenz系统部分序列参数辨识和Lorenz系统保密通信.

## 2 混沌蚁群优化算法

混沌蚁群优化算法是一个基于蚁群单体混沌搜寻行为和群体自组织行为的群体智能算法. 本文在李丽香等提出并改进的混沌蚁群优化算法基础上, 引入蚁群空间和参数空间用以扩展算法的适用范围.

### 2.1 蚁群空间和参数空间

混沌蚁群优化算法蚁群空间定义为$\hat{\boldsymbol{x}} = (\hat{x}_1, \hat{x}_2, \cdots, \hat{x}_l), \hat{x}_d \in [-50, 50], d = 1, 2, \cdots, l$. 这样算法中的参数固定不再受求解问题参数空间的约束. 参数空间即实际问题的搜寻空间$\boldsymbol{x} = (x_1, x_2, \cdots, x_l), x_d \in [a_d, b_d], d = 1, 2, \cdots, l$. 蚁群空间和参数空间通过变换(1)及逆变换(2)相互转换.

$$x_d = a_d + (\hat{x}_d + 50)(b_d - a_d)/100, \tag{1}$$

$$\hat{x}_d = -50 + 100(x_d - a_d)/(b_d - a_d). \tag{2}$$

### 2.2 混沌蚁群优化算法

对于$z = \min f(\boldsymbol{x}), \boldsymbol{x} = (x_1, x_2, \cdots, x_l)$的$l$维最优化问题, 算法开始由

$$\hat{x}_{id}(0) = 100(1 - v_i)R, \quad d = 1, 2, \cdots, l. \tag{3}$$

为每只蚂蚁随机生成初始位置$\hat{\boldsymbol{x}}_i(0) = (\hat{x}_{i1}(0), \hat{x}_{i2}(0), \cdots, \hat{x}_{il}(0)), i = 1, 2, \cdots, N$. 其中$N$是蚁群中蚂蚁总数. 并作为初始可能最优位置$\hat{\boldsymbol{p}}_i$, 由$\hat{\boldsymbol{x}}_i(0)$经变换(1)得到$\boldsymbol{x}_i(0)$并作为$\boldsymbol{p}_i$, 计算目标函数$f(\boldsymbol{x}_i(0))$. 按迭代方程

$$y_i(k) = y_i(k-1)^{1+r_i}, \tag{4}$$

$$\begin{aligned}&\hat{x}_{i,d}(k)\\ &= (\hat{x}_{i,d}(k-1) + 100\nu_i)\\ &\quad \times \mathrm{e}^{(1-\mathrm{e}^{-ay_i(k)})\{3-\psi_d[\hat{x}_{i,d}(k-1)+100\nu_i]\}} - 100\nu_i\\ &\quad + [\hat{p}_{i,d}(k-1) - \hat{x}_{i,d}(k-1)]\mathrm{e}^{(-2ay_i(k)+b)},\end{aligned} \tag{5}$$

计算下一位置$\hat{\boldsymbol{x}}_i(1), \hat{\boldsymbol{x}}_i(1)$经变换(1)得到$\boldsymbol{x}_i(1)$, 计算目标函数$f(\boldsymbol{x}_i(1))$并判断是否更新最优位置$\hat{\boldsymbol{p}}_i$及$\boldsymbol{p}_i$. 依次进行迭代, 由初始值开始, 每经过一定迭代次数, 蚁群中全体蚂蚁进行交换信息. 在所有得到的可能最优位置中进行比较, 得到一个最优的可能最优位置, 所有蚂蚁都更新此最优信息. 接着继续搜寻可能最优解, 直至满足条件(8)迭代结束, 完成第一次搜寻, 把$\bar{\boldsymbol{p}}$记为$\bar{\boldsymbol{p}}(1)$. 在可能最优位置不变的基础上进行第二次混沌搜寻, 搜寻结束后得到$\bar{\boldsymbol{p}}(2)$, 依次进行下去, 当满足条件(9)时算法结束. 混沌蚁群优化算法中各参量取值如下$a = 200, b = 0.5, v_i$是0—1之间的随机数, $r_i = 0.1 + 0.02R$其中$R$是0—1之间的随机数[4−6,13−16].

$$\bar{p}_d = \frac{1}{N}\sum_{i=1}^{N} p_{i,d}, \tag{6}$$

$$s_d = \frac{1}{N}\sum_{i=1}^{N} |x_{i,d} - \bar{p}_d|, \tag{7}$$

$$s_d < 1 \times 10^{-7}; \quad d = 1, 2, \cdots, l, \tag{8}$$

$$|\bar{p}_d(n) - \bar{p}_d(n-1)| < 1 \times 10^{-6}; \quad d = 1, 2, \cdots, l. \tag{9}$$

## 3 混沌系统参数辨识及混沌保密通信

本文提出一种利用混沌系统部分序列进行参数辨识, 其余序列用于混沌加密的混沌保密通信方法. 由于混沌系统对初始条件具有极度敏感性, 用于参数辨识的可观察序列还将用于数据校正. 本文使用的混沌保密通信方法是将信号掩埋在混沌信号中, 这种方法是较简单的一种.

### 3.1 参数辨识

对于一个混沌系统有$m$个未知参数$x_1, x_2, \cdots, x_m$, 且此混沌系统包含$n$支序列, 但我们只能得到$n_1$支准确序列, 其余$n_2$支序列不可得到或者不能准确得到. 参数辨识的目的是由可观察的$n_1$支序列确定混沌系统的$m$个未知参数, 以达到了解混沌系统的全部信息.

现把上述参数辨识问题转化成最优化问题, 然后应用混沌蚁群优化算法解决最优化问题, 从而实现参数辨识. 从可观察的$n_1$支序列中的每一支序列都连续采样(以时间步长$\Delta t$)提取出$K$个数据, 得到

$$\boldsymbol{X} = \begin{bmatrix} X_1(0) & X_1(1) & X_1(2) & \cdots & X_1(K) \\ X_2(0) & X_2(1) & X_2(2) & \cdots & X_2(K) \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ X_{n_1}(0) & X_{n_1}(1) & X_{n_1}(2) & \cdots & X_{n_1}(K) \end{bmatrix}, \tag{10}$$

共$n_1$组数据. 未知参数$x_1, x_2, \cdots, x_m$与不可观察的$n_2$支序列的初值$x_{m+1}, x_{m+2}, \cdots, x_{m+n_2}$共同构成参数空间$\boldsymbol{x} = (x_1, x_2, \cdots, x_{m+n_2})$, 确定参数空间中每一个未知参数的搜寻区域. 参数空间中每个点确定的混沌系统都可计算得$n$支序列, 以相同时间步长得到

$$\boldsymbol{Y} = \begin{bmatrix} Y_1(0) & Y_1(1) & Y_1(2) & \cdots & Y_1(K) \\ Y_2(0) & Y_2(1) & Y_2(2) & \cdots & Y_2(K) \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ Y_n(0) & Y_n(1) & Y_n(2) & \cdots & Y_n(K) \end{bmatrix}, \tag{11}$$

共$n$组数据, 即混沌系统的全部序列. 利用$\boldsymbol{Y}$的前$n_1$组数据与$\boldsymbol{X}$定义目标函数

$$f(\boldsymbol{x}) = \sum_{i=1}^{n_1} \sum_{j=1}^{K} |Y_i(j) - X_i(j)|. \tag{12}$$

至此我们已经把参数辨识问题转化成最优化问题

$$z = \min f(\boldsymbol{x}). \tag{13}$$

数值试验表明混沌蚁群优化算法可以得到$10^{-6}$精度的数值解.

### 3.2 混沌保密通信

混沌保密通信过程如下, 首先在发射端把信息序列$\boldsymbol{s} = (s_1, s_2, \cdots, s_{n_2})$, 掩埋在混沌系统序列$\boldsymbol{X} = (X_1, X_2, \cdots, X_n)$中, 接收端接收到$\boldsymbol{S} = (X_1, X_2, \cdots, X_{n_1}, X_{n_1+1} + s_1, X_{n_1+2} + s_2, \cdots, X_n + s_{n_2})$, 其中$n_1$支是准确的混沌系统序列, $n_2$支是包含信息的混沌序列. 采用3.1中的参数辨识方法实现混沌系统部分序列参数辨识并完全了解混沌系统, 从而从混沌序列中提取出有用信息$\boldsymbol{s}$.

## 4 数值试验

数值试验主要包括Lorenz体系参数辨识和Lorenz系统混沌保密通信. 数值试验表明混沌蚁群优化算法可以得到精度较高的参数辨识结果. 由于混沌系统对初值极度敏感, 数值试验也表明混沌保密通信需要校正数据.

### 4.1 Lorenz系统参数辨识

我们使用混沌蚁群优化算法对Lorenz系统参数辨识, 数值试验中蚁群总数$N = 1000$. Lorenz系统方程为

$$\begin{aligned} \dot{x} &= -\sigma(x - y), \\ \dot{y} &= rx - y - xz, \\ \dot{z} &= -bz + xy. \end{aligned} \tag{14}$$

取参量$\sigma = 10$, $b = 8/3$, $r = 28$, 初值$x(0) = 2$, $y(0) = 1$, $z(0) = 1$, 时间步长$\Delta t = 0.001$, 得到Lorenz系统序列$x = (x(0), x(1), x(2), \cdots, x(K))$, $K = 600$. 我们由序列$x$对Lorenz系统进行参数辨识, 参数空间包含$(r, y(0), z(0))$, 搜寻范围分别为$r \in [0, 50]$, $y(0) \in [-10, 10]$, $z(0) \in [-10, 10]$. 混沌蚁群优化算法经过7次混沌搜寻2170次迭代运算得到精度$10^{-6}$的最优解$(27.99999969, 0.99999999, 0.99999958)$. 参数辨识搜寻演化过程如图1所示.

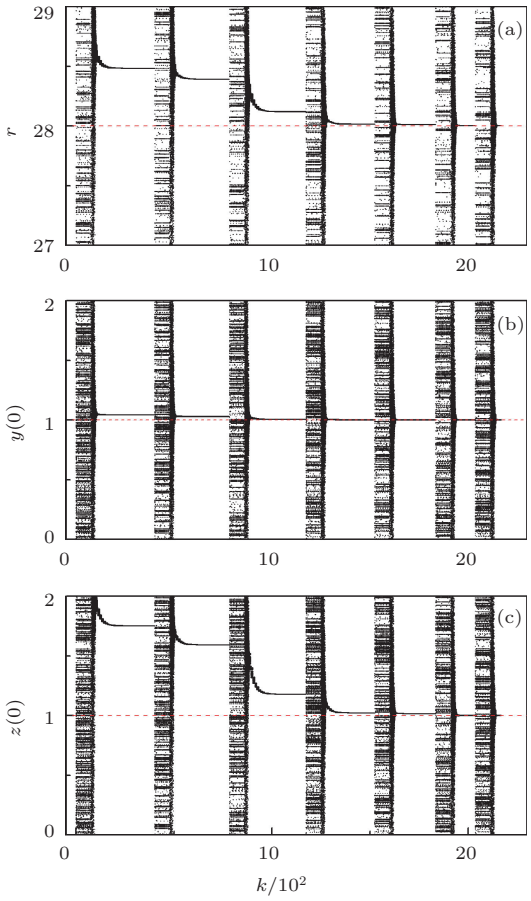


图1 混沌蚁群优化算法参数辨识演化图 (a) 参数$r$蚁群搜寻演化图; (b) 初值$y(0)$蚁群搜寻演化图; (c) 初值$z(0)$蚁群搜寻演化图

混沌系统对初值极度敏感, 我们得到了$10^{-6}$精度最优解, 但仍然不是精确解. 以数值解确定的Lorenz系统与原系统行为是否能完全一致, 这是混沌保密通信必须考虑的问题. 由$\sigma = 10$, $b = 8/3$, $r = 27.99999969$初值$x(0) = 2$, $y(0) = 0.99999999$,

$z(0) = 0.99999958$ 确定的Lorenz系统产生的序列 $x_N(t)$ 与由 $\sigma = 10$, $b = 8/3$, $r = 28$ 初值 $x(0) = 2$, $y(0) = 1$, $z(0) = 1$ 确定的原Lorenz系统产生的序列 $x(t)$ 的误差

$$e(t) = |x_N(t) - x(t)|, \tag{15}$$

如图2所示, $e(t)$ 随 $t$ 增加会突然变大, 当 $t = 17.588$ 时 $e(t) > 10^{-3}$, 当 $t = 23.131$ 时 $e(t) > 0.1$.

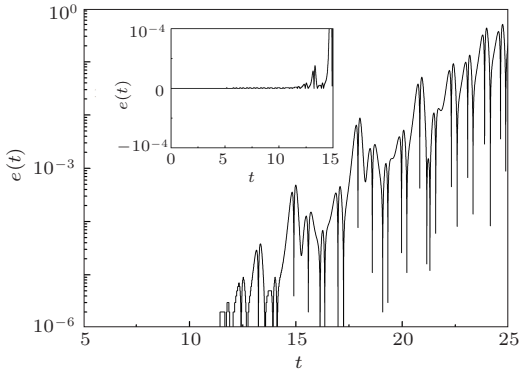


图2 参数辨识得到Lorenz系统与原系统 $x(t)$ 序列误差 $e(t)$

## 4.2 Lorenz系统保密通信

数值试验中我们采用图3(a)所示正弦信号 $s_1(t)$ 和方波信号 $s_2(t)$, 在发射端把信号 $s_1(t), s_2(t)$ 掩埋在 $\sigma = 10$, $b = 8/3$, $r = 28$ 初值 $x(0) = 2$, $y(0) = 1$, $z(0) = 1$ 的Lorenz系统混沌序列中. 接收端得到Lorenz系统序列 $x(t)$ 和带有信号的 $y(t) + s_1(t), z(t) + s_2(t)$ 混沌序列, 如图3(b)所示. 在接收端利用序列 $x(t)$ 采用混沌蚁群优化算法对 $r, y(0), z(0)$ 进行参数辨识, 如4.1所述, 从而得到与发射端同步的Lorenz系统. 这样接收端从序列 $y(t) + s_1(t), z(t) + s_2(t)$ 中滤去混沌序列, 便可提取出信号 $s_{N1}(t), s_{N2}(t)$, 如图3(c)所示. 从图3(c)可以发现由于混沌系统对初值具有极度敏感性, 接收端提取的信号经过一段时间会完全失真. 但是我们可以使用序列 $x(t)$ 进行校正, 当序列 $x(t)$ 的偏差 $e(t)$ 高于 $10^{-3}$ 时, 再次进行Lorenz系统部分序列参数辨识. 如4.1中所述, 当 $t = 17.588$ 时 $e(t) > 10^{-3}$. 利用序列 $x(t)$ 由 $t = 17.588$ 到 $t = 18.188$ 得到 $(x(17.588), x(17.589), \cdots, x(18.188))$, 由此序列我们对 $r, y(17.588), z(17.588)$ 进行辨识. 搜寻范围分别为 $r \in [0, 50], y(17.588) \in [y_N(17.588) - 10, y_N(17.588) + 10], z(17.588) \in [z_N(17.588) - 10, z_N(17.588) + 10]$, 其中 $y_N(t)$ 和 $z_N(t)$ 是参数辨识得到的Lorenz系统序列, 与原Lorenz系统序列的偏差也在 $10^{-3}$ 量级范围内, 因此这样确定的搜寻范围是可行的. 数值试验中分别在 $t = 17.588, 33.051, 38.588$ 进行了校正, 在偏差 $e(t) < 10^{-3}$ 条件下, 我们得到的信号与原信号完全一致, 如图3(d)所示.

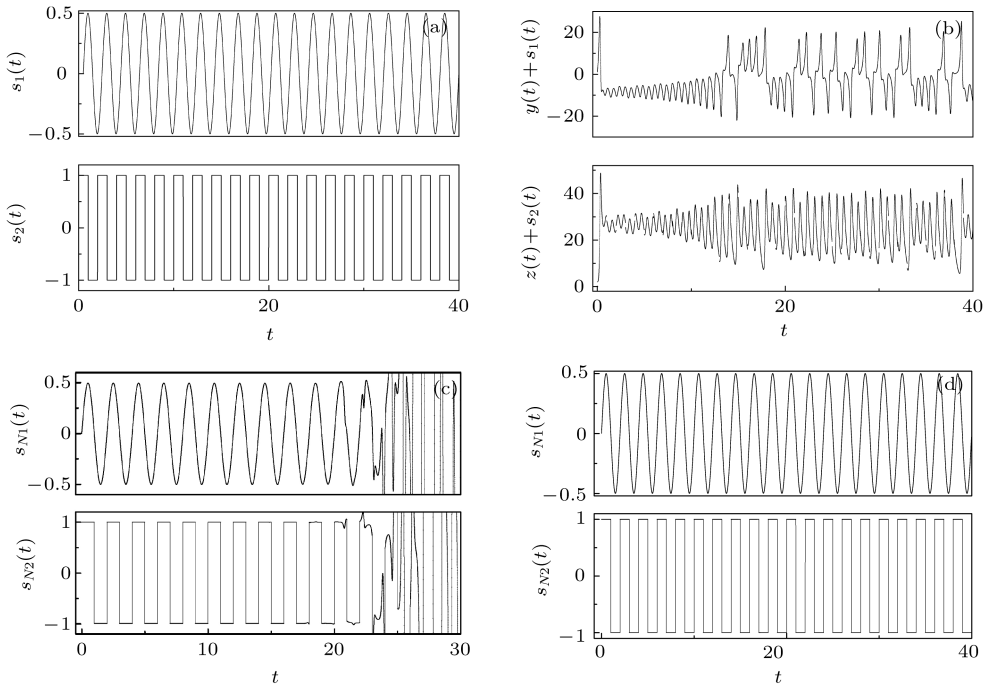


图3 Lorenz系统保密通信信号转换 (a) 原信号; (b) Lorenz系统加密信号; (c) 无校正, 接收端提取出的信号; (d) 有校正, 接收端提取出的信号

## 5 结 论

利用混沌蚁群优化算法对混沌系统部分序列参数辨识可以得到精度较高的结果, 但由于混沌系统自身具有极度初值敏感性, 经参数辨识得到的混沌系统经过一段时间演化后与原混沌系统会发生严重偏离. 因此, 在基于混沌系统部分序列参数辨识的混沌保密通信中, 混沌系统序列 $x(t)$ 不仅用于参数辨识, 还用于校正. 当序列 $x(t)$ 的偏差过大时, 需要再次进行参数辨识. 数值试验表明多次参数辨识的混沌保密通信接收端可以得到与发射端完全一致的有用信号.

## 参考文献


[1] Leandro d S C, Diego L d A B 2010 *Exp. Syst. Appl.* **37** 4198

[2] Juan L M M, Rafael M G, Ricardo A L, Carlos A I 2012 *Commun. Nonlinear Sci. Numer. Simulat.* **17** 1706

[3] Jin J X, Qiu S S 2010 *Acta Phys. Sin.* **59** 0792 (in Chinese) [晋建秀, 丘水生 2010 物理学报 **59** 0792]

[4] Li L X, Peng H P, Yang Y X, Wang X D 2007 *Acta Phys. Sin.* **56** 0051 (in Chinese) [李丽香, 彭海朋, 杨义先, 王向东 2007 物理学报 **56** 0051]

[5] Li L X, Peng H P, Yang Y X 2008 *Acta Phys. Sin.* **57** 0703 (in Chinese)[李丽香, 彭海朋, 杨义先 2008 物理学报 **57** 0703]

[6] Li L X, Yang Y X, Peng H P, Wang X D 2006 *Chaos, Soliton. Fract.* **28** 1204

[7] Chen Z, Zeng Y C, Fu Z J 2008 *Acta Phys. Sin.* **57** 0046 (in Chinese)[陈争, 曾以成, 付志坚 2008 物理学报 **57** 0046]

[8] Wang S Y, Feng J C 2012 *Acta Phys. Sin.* **61** 170508 (in Chinese)[王世元, 冯久超 2012 物理学报 **61** 170508]

[9] Huang L L, Qi X 2013 *Acta Phys. Sin.* **62** 080507 (in Chinese)[黄丽莲, 齐雪 2013 物理学报 **62** 080507]

[10] Zhu D W, Tu L L 2013 *Acta Phys. Sin.* **62** 050508 (in Chinese)[祝大伟, 涂俐兰 2013 物理学报 **62** 050508]

[11] Mohamadreza A, Hamed M 2012 *Chaos, Soliton. Fract.* **45** 1108

[12] Inés P M, Joaquín M 2006 *Phys. Lett. A* **351** 262

[13] Liu L Z, Zhang J Q, Xu G X, Liang L S, Huang S F 2013 *Acta Phys. Sin.* **62** 170501 (in Chinese)[刘乐柱, 张季谦, 许贵霞, 梁立嗣, 黄守芳 2013 物理学报 **62** 170501]

[14] Cai J J, Li Q, Li L X, Peng H P, Yang Y X 2012 *Int. J. Electr. Power Energy Syst.* **34** 154

[15] Li Y Y, Wen Q Y, Li L X, Peng H P 2009 *Chaos, Soliton. Fract.* **42** 880

[16] Wan M, Wang C, Li L X, Yang Y X 2012 *Appl. Soft Comput.* **12** 2387

# A chaotic secure communication method based on chaos systems partial series parameter estimation*

Liu Le-Zhu Zhang Ji-Qian† Xu Gui-Xia Liang Li-Si
Wang Mao-Sheng

(*College of Physics and Electronic Information, Anhui Normal University, Wuhu 241000, China*)

( Received 4 September 2013; revised manuscript received 25 September 2013 )

**Abstract**

We proposed a chaotic secure communication method, namely the partial series of the chaos system for parameter estimation and the other series for secure communications. Parameter estimation could be obtained from the partial series of chaos system with the chaotic ant swarm optimization algorithm, to understand all of the information of the chaos system. In the process of parameter estimation, the introduced parameter space and ant swarm space transformed into each other through space transformation function. Numerical simulation validated the feasibility of the chaos system partial series parameter estimation and the chaotic secure communication method.

**Keywords:** chaotic ant swarm optimization, parameter estimation, chaotic secure communications, numerical simulation

**PACS:** 05.10.–a, 05.45.Gg, 02.60.Cb, 02.60.Pn **DOI:** 10.7498/aps.63.010501

* Project supported by the National Natural Science Foundation of China(Grant Nos. 11047017, 21103002 ), and the Special Foundation of Education of Anhui Province for Excellent Young Scientists, China (Grant No. 2011SQRL023).

† Corresponding author. E-mail: zhangcdc@mail.ahnu.edu.cn