分数阶卡尔曼滤波在混沌保密通信中的应用

郭胜楠[1,2]，罗懋康[1,2]
（1.四川大学数学学院；2. 电子信息控制重点实验室，四川 成都 610065）

摘要：20 世纪 60 年代以来分数阶微积分开始受到人们的广泛关注，并被成功应用于物理、化学、生物学等学科领域。基于 G-L 分数阶微积分，给出了扩展分数阶卡尔曼滤波（EFKF）的定义，并将其应用到分数阶保密通信系统中，同时为了加密并准确解密传输的信息，引入了分数阶混沌 Chen 系统。仿真结果表明，EFKF 取得了非常好的滤波效果；有用信号通过基于分数阶 Chen 系统的保密通信系统，可以有效地在接收端恢复出来。

关键词：分数阶卡尔曼滤波；分数阶 chen 系统；混沌；保密通信
中图分类号：TN918 **文献标识码**：A **文章编号**：1673-1131（2013）01-0003-03

0 引言

自 1695 年分数阶微积分诞生，一直到 1982 年美籍法国数学家 Mandelbort 首次指出自然界和许多技术科学中存在大量分数维的事实，并在整体与部分之间存在自相似现象以后，分数阶微积分作为分形几何和分数维动力学的基础和有力工具才获得了飞跃的发展。近来，随着人们对分数阶混沌系统的深入研究，通过计算机数值仿真，已构造出了分数阶 Chua、Lorenz、Chen、Duffing、Sprott 以及 Rossler 混沌和超混沌系统等[1~2]。

混沌通信是利用混沌信号作为载波，代替传统的正弦波载波，将传输信号隐藏在混沌载波之中，在接收端利用混沌的属性或同步特性解调出所传输的信息。由于混沌信号的宽带类噪声特点，将信息信号隐藏或叠加到混沌信号上发送后，一般会以为是噪声信号，而窃听者也很难以从中窃取到信息信号，由此达到保密的效果。近十几年来，混沌保密通信技术有了很大的进展[3]。

2005 年 Sierociuk D. 将整数阶的卡尔曼滤波推广到分数阶，给出了分数阶卡尔曼滤波的递推公式及推导过程。本文在上述研究工作的基础上，将分数阶卡尔曼滤波应用到基于分数阶 Chen 系统的分数阶混沌保密通信系统中，并给出了仿真分析。

1 分数阶卡尔曼滤波[4]

考虑非线性离散随机分数阶系统：

$$\Delta^{\gamma}x_{k+1}=f(x_k,u_k)+\omega_k$$

$$x_{k+1}=\Delta^{\gamma}x_{k+1}-\sum_{j=0}^{k+1}(-1)^j\gamma_j x_{k+1-j}$$

$$y_k=h(x_k)+v_k$$

其中，γ为分数阶数 $x(k)\in R^n$，$u(k)\in R^p$，$y(k)\in R^m$，$\omega(k)\in R^n$，$v(k)\in R^m$ 分别为 k 时刻的状态向量，系统输入，系统输出，状态噪声和观测噪声。

$$\gamma_j=diag\left[\left(\begin{matrix}n_1\\j\end{matrix}\right)\cdots\left(\begin{matrix}n_N\\j\end{matrix}\right)\right],\quad \left(\begin{matrix}n\\j\end{matrix}\right)=\begin{cases}1, j=0\\ \dfrac{n(n-1)\cdots(n-j+1)}{j!}, j>0\end{cases},\quad \Delta^{\gamma}x_{k+1}=\begin{bmatrix}\Delta^{n_1}x_{1,k+1}\\ \vdots\\ \Delta^{n_N}x_{N,k+1}\end{bmatrix}$$

$n_1\cdots n_N$ 是状态方程的阶数，N 为方程的个数。

假定：ω(k) 和 v(k)是相互独立的零均值高斯白噪声：

$$E\omega(k)=0, Ev(k)=0$$

$$E\{\omega\omega^T\}=Q, E\{vv^T\}=V$$

$$E\{\omega v^T\}=0$$

定理 对于如上定义的非线性分数阶离散随机系统，扩展分数阶卡尔曼滤波（EFKF）为：

$$\Delta^{\gamma}\tilde{x}_{k+1}=f(\hat{x}_k,u_k)$$

$$\tilde{x}_{k+1}=\Delta^{\gamma}\tilde{x}_{k+1}-\sum_{j=0}^{k+1}(-1)^j\gamma_j\hat{x}_{k+1-j}$$

$$\tilde{P}_k=(F_{k-1}+\gamma_1)P_{k-1}(F_{k-1}+\gamma_1)^T+Q_{k-1}+\sum_{j=2}^{k}\gamma_j P_{k-j}\gamma_j^T$$

$$\hat{x}_k=\tilde{x}_k+K_k[y_k-h(\tilde{x}_k)]$$

$$P_k=(I-K_kH_k)\tilde{P}_k$$

$$K_k=\tilde{P}_kH_k^T(H_k\tilde{P}_kH_k^T+R_k)^{-1}$$

其中，$F_{k-1}=\left[\dfrac{\partial f(x,u_{k-1})}{\partial x}\right]_{x=\hat{x}_{k-1}}$，$H_k=\left[\dfrac{\partial h(x)}{\partial x}\right]_{x=\tilde{x}_k}$。

初始值为 $x(0)=x_0\in R^N$ $P_0=E[(\hat{x}_0-x_0)(\hat{x}_0-x_0)^T]$。

2 分数阶混沌保密通信系统

1993 年，Cuomo 和 Oppenheim 基于 Lorenz 系统，构造了混沌掩盖保密通信系统的模拟电路试验。全过程如下：在发送端，将有用信号 s(t) 与混沌信号 x(t) 相加，使通过公共信道传送的只是形似噪声的信号 c(t)，达到保密传送的目的。在接收端，响应系统能复制混沌信号 x(t)，只需从 c(t) 中减去响应系统产生的混沌信号 x'(t)，就可获得还原的有用信号 $\hat{s}(t)$[5]。

上述系统在实际应用过程中，由于系统中存在信道失真和测量噪声，所以相关器的输出值是一个随机变量。要想获得较好的误码性能，就要利用带有噪声的观测数据进行随机信号本身取值的估计，所采用的方法是线性最小均方误差估计，实现这一估计的典型滤波器是卡尔曼滤波器[3]。

如果我们将系统改进为分数阶系统，则改进的分数阶混沌保密通信系统可以描述为：

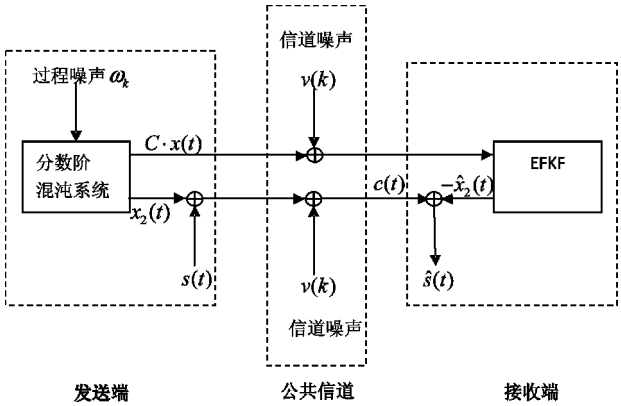

图 1 分数阶混沌保密通信系统

我们假定混沌信号由分数阶 Chen 系统产生，分数阶 Chen 模型由如下方程组描述：

$$\begin{cases} {}_0D_t^{q_1}x_1(t)=a(x_2(t)-x_1(t)) \\ {}_0D_t^{q_2}x_2(t)=(c-a)x_1(t)-x_1(t)x_3(t)+cx_2(t) \\ {}_0D_t^{q_3}x_3(t)=x_1(t)x_2(t)-bx_3(t) \end{cases}$$

当$(a,b,c)=(35,3,28)$，且q_1,q_2,q_3均大于 0.8244 时，上述系统为一个混沌系统[1]。

保密通信过程可描述为：由分数阶 Chen 系统产生混沌信号，其中分量 $x_1(t)$经过信道 1 作为同步信号经过 EFKF 系统输出分量 $x_2(t)$的估计值 $\hat{x}_2(t)$。在信道 2 中，有用信号 s(t)与混沌信号的分量 $x_2(t)$进行叠加，达到被掩蔽的目的。经过信道 2 的传输，最终减去 $x_2(t)$的估计值 $\hat{x}_2(t)$，输出 s(t) 的估计值 $\hat{s}(t)$，从而恢复出有用信号。

上述混沌信号还可以描述为：

$$\begin{bmatrix} x_1^{(q_1)}(t) \\ x_2^{(q_2)}(t) \\ x_3^{(q_3)}(t) \end{bmatrix}=\begin{bmatrix} -a & a & 0 \\ c-a & c & -x_1(t) \\ 0 & x_1(t) & -b \end{bmatrix}\begin{bmatrix} x_1(t) \\ x_2(t) \\ x_3(t) \end{bmatrix}=A(x(t))x(t)，\ 其$$

中，$(a,b,c)=(35,3,28)$，q_1,q_2,q_3，均取为 0.9。$C=[1\ \ 0\ \ 0]$，混沌系统的初始值和 EFKF 的初始值分别设为 $x(0)=[-9\ \ -5\ \ 14]^T$，$\hat{x}(0)=[40\ \ 17\ \ 17]^T$。过程噪声和信道噪声分别设定为$\omega$=0.0016，$v$=0.0024；输入的有用的信号为$s(t)=\sin(2\pi ft)$，$f=2Hz$。

$$F_{k-1}=\left[\frac{\partial f(x,u_{k-1})}{\partial x}\right]_{x=\hat{x}_{k-1}}=\begin{bmatrix} -a & a & 0 \\ c-a & c & -\tilde{x}_1(t-1) \\ 0 & \tilde{x}_1(t-1) & -b \end{bmatrix}$$

$$H_k=[0\ \ 1\ \ 0],\quad R=E[vv^T]=0.0024,$$

$$P(0)=\begin{bmatrix} 0.1 & 0 & 0 \\ 0 & 0.1 & 0 \\ 0 & 0 & 0.1 \end{bmatrix},\quad Q=E[ww^T]=\begin{bmatrix} 0.0016 & 0 & 0 \\ 0 & 0.0016 & 0 \\ 0 & 0 & 0.0016 \end{bmatrix},$$

3 仿真分析

分数阶 Chen 系统的吸引子如图 2 所示：

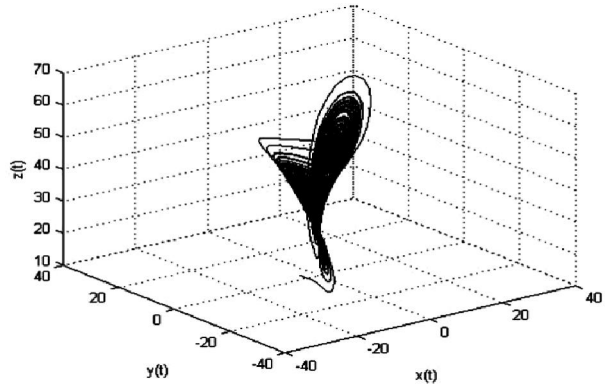

图 2 分数阶 Chen 系统的吸引子

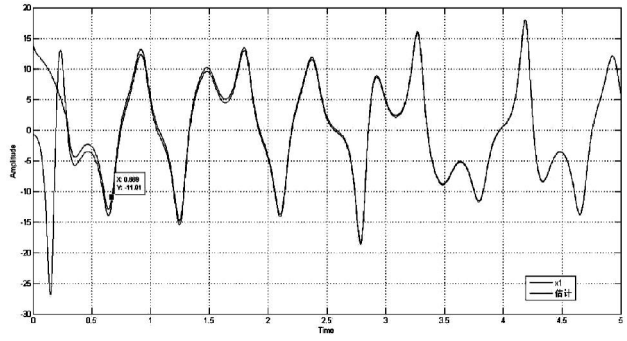

图 3 分数阶 Chen 系统的第一个分量 $x_1(t)$与其估计值

图 3 和图 4 分别表示区间[0，5]上分数阶 Chen 系统 $x_1(t)$和 $x_2(t)$两个分量以及他们各自的估计值。从图中可以看出，经过 EFKF 的估计值收敛速度还是非常快的。

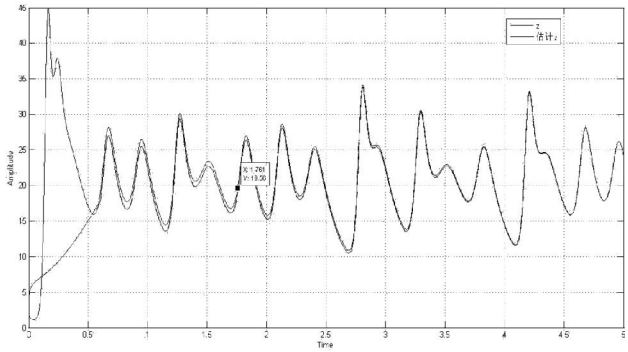

图 4 分数阶 Chen 系统的第 3 个分量 $x_3(t)$与其估计值

被分数阶 Chen 系统掩盖之后的有用信号如图 5 所示，与图 6 对照之后可以看出，被掩盖后的有用信号与原信号显示出了极大的不同，从而表明有用信号被很好地掩盖了。图 6 表示原信号与由改进的分数阶混沌保密通信系统中恢复出来的信号。从图中可以看出。1.761s 之后恢复出来的信号收敛到原信号，也就是说，通过我们所改进的分数阶混沌保密通信系统，原有用信号可以被精确地恢复。

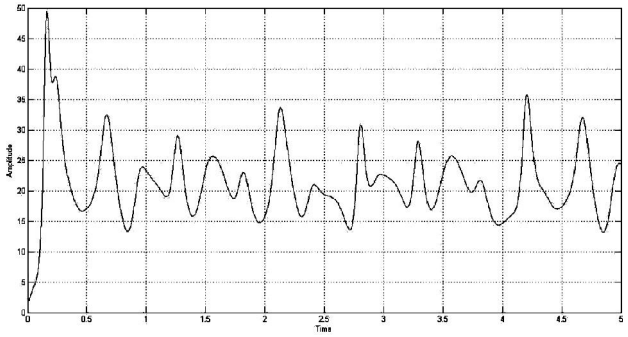

图 5 被分数阶 Chen 系统掩盖之后的信号

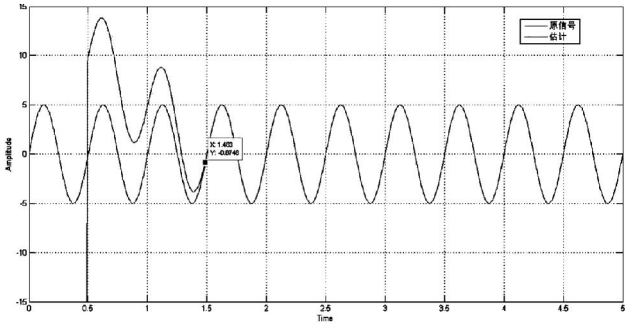

图 6 原信号与还原信号

4 结语

本文主要研究了分数阶卡尔曼滤波在混沌保密通信中的应用。不加证明地给出了分数阶卡尔曼滤波的递推公式，进而给出了基于分数阶 Chen 系统的分数阶混沌保密通信系统的构成及实现过程。仿真分析发现，我们给出的改进系统可以很好地掩盖有用信号，达到保密通信的效果。这一研究工作将会引导我们继续研究基于其他分数阶系统的分数阶混沌保密通信系统。

变种群规模遗传算法的研究

张 俞
（贵州职业技术学院，贵州 贵阳 550023）

摘要：结合人类进化过程中的人口数量变化规律，提出了一种种群规模随进化代数规律性变化的改进型遗传算法(VPGA)，该算法只是使种群规模在收敛之前做梯形周期性变化，并不影响其他操作算子。实验与经典遗传算法比较，证明本文改进遗传算法更节省时间、降低能耗，能够以极小的代价得到更优的结果。

关键词：遗传算法；变种群；计算代价
中图分类号：TN919.81 **文献标识码**：A **文章编号**：1673-1131(2013)01-0005-02

Genetic Algorithm with Variable Population Size

Zhang Yu

Abstract: By simulating the population increasement in the human evolution, a variable population size genetic algorithm (VPGA) is proposed that its population size changes with population generations like trapezia. Without effecting the other operators, the experiment compares with standard GA, the results show that the VPGA can obtain better solutions with less computation time and waste sources than the others.

Key Words: genetic algorithm variable population size computational cost

遗传算法是由美国 Michigan 大学的 John Holland 教授提出的一种模拟生物体进化过程的随机搜索算法，采用几种简单的编码方式来表示生物界各种复杂结构，对进化对象执行选择、交叉、变异一系列遗传操作，从而产生更优秀的下一代。那么，算法面临的第一个问题就是进化对象的数目，即是群体规模的大小。根据模式定理及算法的隐并行性，群体规模越大，多样性就越好，算法陷入早熟的危险越小，但同时算法的计算量随之增加，这使得在解决应用问题时功耗过大，不利实际。若群体规模较小，将使算法搜索空间受限，容易导致欺骗问题和早熟现象的产生。近年出现了许多关于群体方面的研究，文献[1]对群体规模和遗传算法的收敛速度之间的关系进行了初步的研究。文献[2]研究了在变化的环境中群体规模对遗传群体多样性的关系。文献[3]在解决不同类型问题的时候，合适 N 值的计算方法需要自适应变化。

1 种群规模

在经典遗传算法中，群体规模在整个进化过程中是个恒值，这与遗传算法的最初思想不太符合，生物界动态的发展，其个体数量当然也随之变动。并且，固定的种群规模值不能根据总体适应度的变化去调节群体多样性和选择压力间的联系，凸显了欺骗问题和早熟现象的出现。图 1 就是种群规模变化示意图，示意图中的 T 表示的是进化过程中种群规模变化的周期，D 是种群规模振荡的振幅。

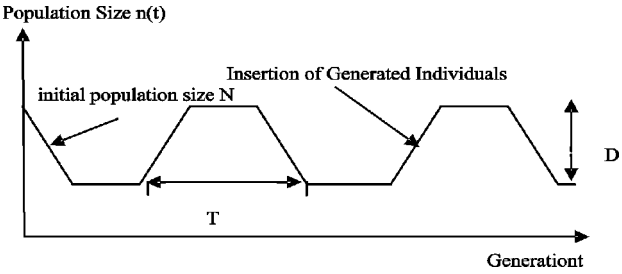

图 1 种群规模变化图

2 函数试验

这里对两个典型的求最小值函数进行优化，将本文提出的梯形算法与经典遗传算法作比较。本文用于检验算法收敛性能标准有：(1)收敛时间及收敛代数，分别表示算法收敛到最优值所用时间及遗传代数的平均值，体现算法收敛的快慢；(2)收敛率，表示算法成功找到最优值的效率；(3)资源占用，表示算法运行整个过程所占的总的字节数。

2.1 测试函数

$$F1: f(x_1,x_2)=\sum_{i=1}^{5} i*\cos[(i+1)*x_1+i]*\sum_{i=1}^{5} i*\cos[(i+1)*x_2+i],\ -10\le x_1,x_2\le 10$$

该函数是一个无穷多密集尖峰的多模态函数，有 760 个局部极小值点，其中有 18 个点是全局最小值点，其全局最小值为-186.7309088。

参考文献：

[1] Ivo Petrās. Fractional-Order Nonlinear Systems. Springer, 2010.
[2] 于茜，罗永健，史德阳，吴刚.超 Lorenz 混沌系统的同步及其在保密通信中的应用[J].兵工自动化,2011(3)
[3] 许娟.混沌保密通信系统的调制与解调技术研究.
[4] Dominik S,Andrzej D.Fractional kalman filter algorithm for the states,parameters and orders of fractional system estimation.Int.J.Appl.Math.Comput.Sci.,2006,Vol.16,No.1,129-140
[5] 关新平等.混沌控制及其在保密通信中的应用[M].北京：国防工业出版社，2002,10

基金项目：国家自然科学基金“分数阶非线性动力系统的不确定性数学理论及应用研究”，项目编号 11171238
作者简介：郭胜楠(1987-)，女，河北沧州人，在读硕士研究生，研究方向为不确定性处理的数学、雷达信号处理；罗懋康(1956-)，男，重庆市人，教授，博士生导师，教育部“长江学者奖励计划”特聘教授，国家“杰出青年科学基金”获得者，目前主要研究方向为不确定性处理，为该领域国家自然科学基金重点项目，教育部创新团队负责人。