一个对称的四维混沌系统及其图像隐藏应用

叶瑞松，兀松贤
（汕头大学 数学系，广东 汕头 515063）

摘 要：混沌动力系统具有对初值和系统参数敏感依赖性和拓扑转迁性以及混沌序列的伪随机性等优良性质，使得混沌动力系统在信息安全领域具有很好的应用价值。近年来，由于高维混沌动力系统具有比较大的密钥空间，使得高维混沌动力系统成为图像加密和隐藏的热门研究课题。文中构造了一个对称的四维混沌系统，基于该混沌系统，提出了一种数字图像隐藏方法。该方法将图像置乱技术、加密技术、分存技术、隐藏技术有机结合起来。该算法简单，安全性高，对剪切、噪声等攻击具有一定鲁棒性，也可以实现秘密图像和载体图像的无损复原。

关键词：混沌；图像置乱；图像加密；图像分存；图像隐藏
中图分类号：TP309；O415.5　　**文献标识码**：A　　**文章编号**：1673－629X(2010)01－0093－04

A 4D Symmetric Chaotic System and Its Application on Image Hiding

YE Rui-song, WU Song-xian
(Department of Mathematics, Shantou University, Shantou 515063, China)

Abstract: Chaotic dynamical systems play an important role in information security thanks to their good properties such as the sensitive dependence on initial conditions and system parameters, topological transitivity, pseudo－random property, etc. In particular, high dimensional chaotic dynamical systems have attracted more attentions in recent years thanks to their higher security. One four－dimensional symmetric chaotic system is constructed in this paper; an image hiding scheme is proposed, in which the technologies of image scrambling, encryption, sharing and hiding are applied together. The presented scheme is simple to manipulate and has high security. It is robust against some kinds of attacks and it can reconstruct the secret images and cover images in a lossless manner as well.

Key words: chaos; image scrambling; image encryption; image sharing; image hiding

0 引 言

1963年，气象学家 Lorenz 用一个三维自治常微分方程组来描述天气的演变情况，从而发现了系统的混沌特性。该经典 Lorenz 系统，成为混沌研究的典范。2006年～2007年，王兴元等更进一步讨论 Lorenz 系统通过怎样的路径通向混沌[1]。近几年来，四维混沌系统成为混沌研究领域的一个热点。四维混沌系统甚至四维超混沌系统相继出现[2～5]，而具有对称性的四维混沌系统研究较少。文中在 Lorenz 系统的基础上构造了一个四维对称动力系统，并通过计算及可视化揭示了该系统在一定的参数范围中具有混沌性质。

鉴于混沌系统在信息安全领域具有很好的应用价值[6]，文中将构造的混沌动力系统应用到图像信息的隐藏。在信息安全方面，目前人们的研究主要集中在数字图像隐藏、数字水印和数字图像分存。已有的图像分存隐藏算法，绝大多数是先对图像分解，再分别置乱，最后分存隐藏[7,8]。文中提出了一种图像分存隐藏的新方法，在实现置乱的同时将图像进行交叉分解，然后分存隐藏。算法首先通过矩阵运算，将秘密图像交叉分解为两幅同样大小的置乱图像，利用一个四维混沌系统对分解后的秘密图像进一步加密，提高安全性，然后分别把它们交叉分存隐藏在两幅经过放大的有意义的载体图像中。文中提供的算法有效地结合了图像置乱加密、图像隐藏、图像分存技术，使图像的安全传输有了更高的可靠性。算法实现简单，可以实现秘密图像和载体图像的无损复原，同时，该算法也具有一定的抗攻击性。

收稿日期：2009－04－24；**修回日期**：2009－07－17
基金项目：国家自然科学基金资助项目(A0324649)
作者简介：叶瑞松(1968－)，男，福建诏安县人，博士，教授，研究方向为分歧理论及其数值计算、分形混沌及其计算机应用、图像处理。

1 对称的四维混沌系统

Lorenz 系统为

$$\begin{cases}\dot{x}_1 = a(x_2 - x_1)\\ \dot{x}_2 = cx_1 - x_2 - x_1x_3\\ \dot{x}_3 = -bx_3 + x_1x_2\end{cases}$$

在此基础上，改变了它的一些非线性项，从而得到以下四维动力系统：

$$\begin{cases}\dot{x}_1 = a(x_2 - x_1) + x_2x_3x_4\\ \dot{x}_2 = cx_1 - x_2 - x_1x_3x_4\\ \dot{x}_3 = -bx_3 + x_1x_2x_4\\ \dot{x}_4 = dx_4 + x_1x_2x_3\end{cases}$$

该系统关于 $x_3 - x_4$ 平面，$x_1 - x_2$ 平面以及原点均是对称的，这使得其吸引子具有相关的对称性。这里取定参数 $a = 10, b = 8/3, c = 28$，初值 $x_1(0) = 1$，$x_2(0) = 1, x_3(0) = 1, x_4(0) = 1$，让参数 d 变化，绘图显示 $d - x_1$ 的分岔图，如图1所示。我们发现，系统在参数 d 很大的范围内会出现混沌状态。

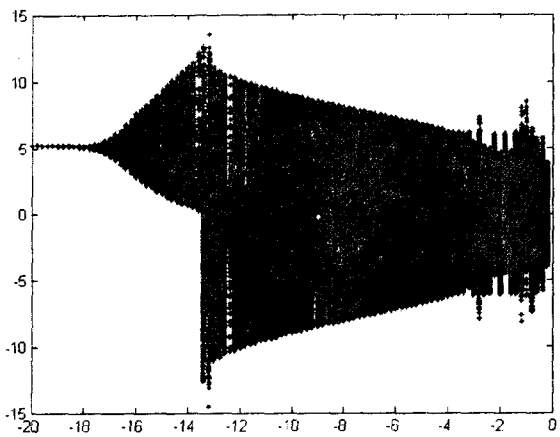


图1 $d - x_1$ 的分岔图

不妨取定 $d = -0.5$，计算其最大李雅普诺夫指数为4.8711，由此可知系统是混沌的。系统的部分二维相图和三维相图如图2所示。

2 基于对称的四维混沌系统图像信息隐藏

文中将构造一种新的图像隐藏算法。将基于位置的图像置乱和基于像素灰度值的置乱，以及利用第1节所提供的混沌系统产生的伪随机数进行秘密图像的加密；并利用图像的交叉分存和载体图像的放大技术结合进行秘密图像的隐藏。该算法可以无失真地恢复秘密图像和载体图像，并且对剪切、噪声等攻击具有较好的鲁棒性。

算法首先读取两幅同样大小的秘密图像 A, B。利用Arnold变换分别对这两幅图像进行基于位置的置乱，得到矩阵 $\boldsymbol{A}1, \boldsymbol{B}1$。可以进行多次置乱，以增强置乱效果。对秘密图像 $\boldsymbol{A}1, \boldsymbol{B}1$ 进一步作交叉分解。利用矩阵 $\boldsymbol{K} = \begin{pmatrix}1 & 2\\ 1 & 1\end{pmatrix}$，将 $\boldsymbol{K}$ 与 $\boldsymbol{A}1, \boldsymbol{B}1$ 组成的分块矩阵相乘，即 $\begin{pmatrix}\boldsymbol{A}2\\ \boldsymbol{B}2\end{pmatrix} = \boldsymbol{K} * \begin{pmatrix}\boldsymbol{A}1\\ \boldsymbol{B}1\end{pmatrix} \bmod 256$，从而实现 $\boldsymbol{A}1, \boldsymbol{B}1$ 的交叉分解，得到图像矩阵 $\boldsymbol{A}2, \boldsymbol{B}2$。

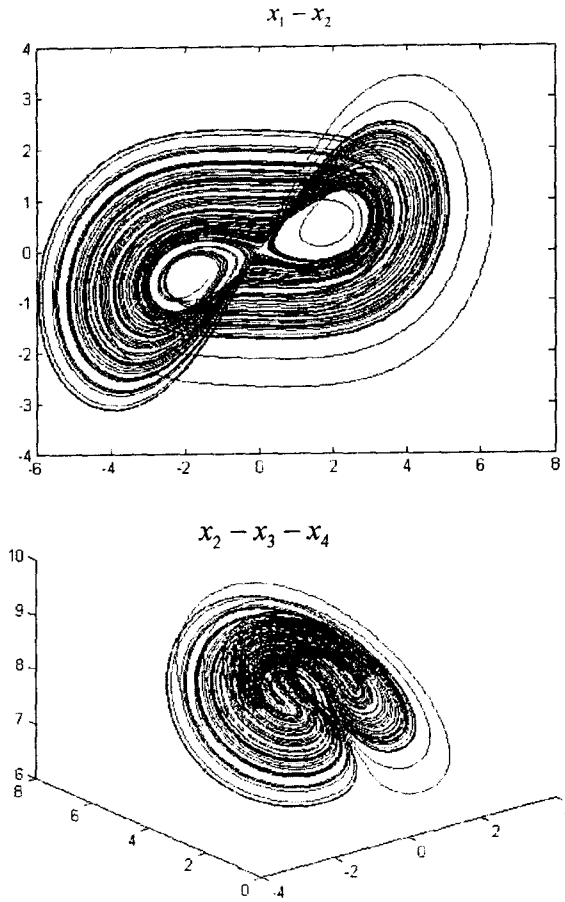


图2 $x_1 - x_2$ 二维相图和 $x_2 - x_3 - x_4$ 三维相图

为了提高交叉分解矩阵 $\boldsymbol{A}2, \boldsymbol{B}2$ 的安全性，采用上节所构造的四维对称混沌系统，设计了一种保密性更强、密钥空间更大、加密效率更高、适应现代密码体制要求的空域数字图像加密算法。在参数条件 $a = 10, b = 8/3, c = 28, d = -0.5$ 下，文中的四维混沌系统处于混沌状态，因此该系统的四个状态变量的初始条件和几个参数均可以作为密钥，从而使得密钥空间增大。利用该混沌系统生成一组伪随机数，将其量化排列为一个与 $\boldsymbol{A}2, \boldsymbol{B}2$ 大小相同的整数值矩阵 $\boldsymbol{P}$。利用 $\boldsymbol{P}$ 分别和图像 $\boldsymbol{A}2, \boldsymbol{B}2$ 做异或运算，生成加密图像 $\boldsymbol{A}3, \boldsymbol{B}3$。

为了进行加密图像的隐藏，并进行无失真的恢复加密图像和载体图像，可以采用载体图像放大的途径实现。这里采用最佳近邻像素插值的图像放大方法，对载体图像进行放大。读取两幅载体图像 C, D，要求与 A, B 同大小。将 C, D 采用线性放大4倍，分别记为 $C1, D1$。在原图像每个像素的右、下以及右下方增加了3个像素，这些增加的像素的灰度值取其原图像中被放大的像素点的灰度值。

为了表示方便,把放大前后的图像按区域对应起来,即原图像中每个像素点对应放大后的图像的一个 2×2 的区域。这个区域中左上角的像素点就是与它对应的原图像中的像素点(下面统称原点),而其它三个像素点是新增加的(依据其位置分别记为右点、下点、右下点)。

将加密后的秘密图像 $A3$,$B3$ 分别隐藏到放大了的载体图像 $C1$,$D1$ 中。将图像 $A3$,$B3$,$C1$,$D1$ 的灰度值用二进制表示,从低位到高位依次记为第 1 位,第 2 位,……,第 8 位。取 $A3$ 中像素点的灰度值二进制表示的第 1,2,8 位的值分别来替换 $C1$ 相应图像区域的右点灰度值二进制表示的低三位,即第 1,2,3 位的值;取 $A3$ 中像素点的灰度值二进制表示的第 3,4,7 位的值分别来分别替换 $C1$ 的下点灰度值二进制表示的低三位的值;取 $A3$ 中像素点的灰度值二进制表示的第 5,6 位的值来替换 $C1$ 的右下点灰度值二进制表示的低两位的值。这样,就实现了把 $A3$ 的像素值分散嵌入到 $C1$ 的右点、下点和右下点中去。这样做尽可能小的损坏载体图像,使载体图像不易被发现隐藏了秘密信息。同样可以将 $B3$ 隐藏到 $D1$。

由于上述过程的每一步都是可逆的。因此还原过程即是图像的分存隐藏和加密置乱的逆过程。可以很容易地将隐藏的秘密图像和载体图像无失真地恢复出来。

3　实验结果

取四幅大小均为 256×256 的图像。如图 3 所示,其中(a)、(b)是原始秘密图像,(c)、(d)是原始的载体图像;(a1)、(b1)是(a)、(b)经过 Arnold 变换后的置乱图像;在置乱图像(a1)、(b1)基础上经过基于两幅图像的灰度值的交叉分解并与混沌系统所产生的伪随机矩阵做异或运算后变得到加密图像(a2)、(b2);(c1)、(d1)是将(a2)、(b2)进行分存隐藏得到的伪装图像。对(c1)、(d1)可以无失真地还原出秘密图像。

从实验结果可以看出,文中算法有较好的置乱效果、加密效果、隐藏效果和还原效果。假设攻击者获取了其中一幅伪装图像,很难发现藏有秘密信息也没办法恢复得到秘密图像。

秘密图像隐藏到载体图像后,只需要传输、存储两幅伪装图像。伪装图像在传输过程中,很难避免一些必要的数据处理或人为攻击,如压缩、滤波、噪声污染及几何失真等,对一些比较常见的处理和攻击,文中也进行了实验测试。图 4 所示结果是图 3 中(c1)、(d1)经过 128×128 剪切破坏进行的还原测试。图 5 所示是图 3 中(c1)、(d1)受到强度为 5% 的椒盐噪声污染后进行的秘密图像还原结果。测试结果表明,该算法具有一定抗攻击的稳健性。

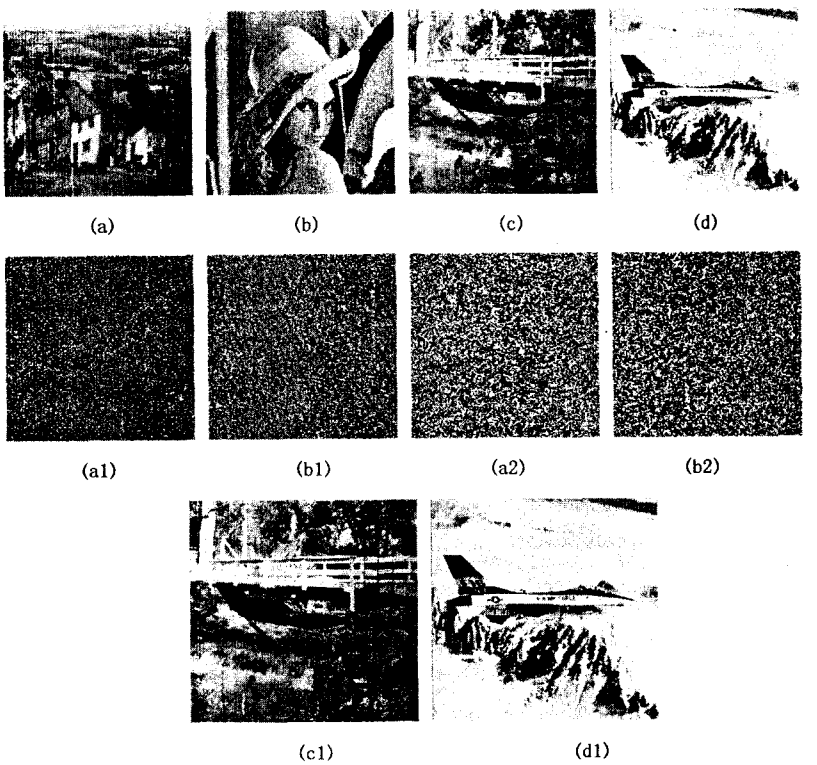
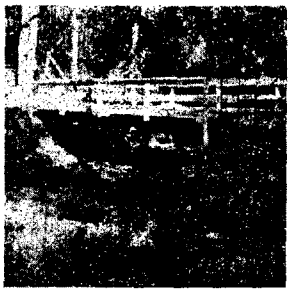


图 3　图像的隐藏效果

图 4　剪切攻击


(c1)椒盐攻击


(d1) 椒盐攻击


秘密图像(a)的还原图像


秘密图像(b)的还原图像

图 5 椒盐噪声攻击

4 结束语

讨论了一个具有对称性的四维动力系统的基本性质,并通过相图和最大李雅普诺夫指数判定该系统是否具有混沌性质。提出了一种新的数字图像隐藏算法。该算法利用 Arnold 变换做置乱,并用可逆矩阵做两幅图像的交叉分解,结合一个新的具有对称特性的四维混沌系统对秘密图像进一步加密,最后采用基于像素灰度值的位平面嵌入的隐藏方法做秘密图像的隐藏。该算法实现了秘密图像和载体的无损复原。实验结果表明,文中的算法具有很好的隐藏效果,具有较高的安全性和较好的抗攻击稳健性。

参考文献:

[1] 王兴元,骆 超. Lorenz 系统走向混沌的道路[J]. 大连理工大学学报,2006,46(4):582-587.

[2] Qi Guoyuan, Du Shengzhi, Chen Guanrong, et al. On a four-dimensional chaotic system[J]. Chaos, Solitions and Fractals, 2005,23:1671-1682.

[3] Nikolov S, Clodong S. Occurrence of regular, chaotic and hyperchaotic behavior in a family of modified Rossler hyperchaotic systems[J]. Chaos, Solitions and Fractals, 2004,22:407-431.

[4] Qi Guoyuan, Chen Guanrong. Analysis and circuit implementation of a new 4D chaotic system[J]. Physics letters A, 2006,352:386-397.

[5] 王兴元,王明军. 超混沌 Lorenz 系统[J]. 物理学报, 2007, 49(56):5136-5141.

[6] 郗坤洪,叶瑞松. 一种改进的基于混沌序列的图像加密算法[J]. 计算机技术与发展,2008,18:48-50.

[7] 眭新光,罗 慧. 基于矩阵分解的数字图像分存技术[J]. 计算机工程与应用, 2004,40(32):96-98.

[8] 王继军,张显全,张军洲,等,一种新的数字图像分存方法[J]. 计算机工程与应用, 2007,43(31):79-81.

(上接第 92 页)

4 结束语

移动实时数据库满足事务截止期的同时,还要考虑事务的紧迫度,这就要求实时事务在并发控制等处理技术方面有别于传统数据库的处理技术。

(1)给出了移动实时事务按关键性分类的方法;

(2)提出了区分事务关键性的优先级并发控制策略;

(3)对不同关键性的实时事务并发控制方法作了性能比较。

参考文献:

[1] 肖迎元,刘云生,廖国琼. 移动实时数据库系统综述[J]. 计算机工程与应用,2004(35):173-177.

[2] Lam K Y, Kuo T W, Tsang Wai Hung, et al. Concurrency control in mobile distributed real-time database systems[J]. Information Systems,2000(6):261-286.

[3] Liao Guo qiong, Liu Yun sheng, Yang Jin cai. A concurrency control mechanism for mobile real-time nested transactions [J]. Chinese Journal of Computers,2003(10):1326-1331.

[4] 刘云生. 现代数据库技术[M]. 北京:国防工业出版社, 2001.

[5] 韩 凯,王京春. 实时数据库调度策略综述[J]. 计算机工程与应用,2004(32):172-176.

[6] 魏志东,魏洪波. 面向混合实时数据库系统的调度与并发控制[J]. 计算机工程,2003,29(7):73-75.

[7] 何新贵,唐常杰,李 舜,等. 特种数据库技术[M]. 北京:科学出版社,2000.

[8] Xiao Qiao. 细化解析:不同类型数据库的死锁问题[DB/OL]. 2007. http://www.sudu.cn/info/html/edu/20070803/311782.html.

[9] Lam K Y, Kuo T W, Tsang Wai Hung. The Reduced Ceiling Protocol for Concurrency Control in Real-time Databases with Mixed Transactions[J]. The Computer Journal,2000,43(1):65-80.

[10] Lindstrom J. Distributed Optimistic Concurrency Control for Real-Time Database Systems[M]. Helsink: Helsinki Institute for Information Technology(HIIT), Advanced Research Unit (ARU),2000.

[11] 刘云生,王丽娜,廖国琼. 支持断接的移动实时事务调度[J]. 计算机科学,2005,32(4):155-158.