Journal of Computer Applications
计算机应用,2012,32(8):2262 - 2264
ISSN 1001-9081
CODEN JYIIDU
2012-08-01
http://www.joca.cn

文章编号:1001 - 9081(2012)08 - 2262 - 03
doi:10.3724/SP.J.1087.2012.02262

基于高维超混沌系统和矩阵张量积的图像分组加密新算法

唐　宋*,徐桂兰,李清都
(重庆邮电大学 非线性电路与系统研究所,重庆 400065)
(*通信作者电子邮箱 kao_123@163.com)

摘　要:目前混沌加密算法主要存在三方面的不足:1)采用低维混沌序列造成混沌退化;2)采用的混沌系统结构过于简单;3)算法只依赖于混沌系统的结构和密钥。针对这些不足,提出一种新的图像分组加密算法。为了克服混沌退化,算法借助矩阵张量积将高维超混沌系统所产生混沌序列和一维混沌序列充分耦合,产生像素扩散矩阵。在此过程中,用明文信息控制扩散矩阵生成,使算法与明文相关,提高了算法的安全强度。

关键词:混沌系统;图像加密;矩阵张量积;像素扩散矩阵
中图分类号:TP309.7　　**文献标志码**:A

New image group encryption algorithm based on high dimensional hyperchaos system and matrix tensor product

TANG Song*, XU Gui-lan, LI Qing-du
(*Institute for Nonlinear Circuit and Systems, Chongqing University of Posts and Telecommunications, Chongqing* 400065, *China*)

Abstract: Shortcomings of image encryption schemes based on chaos currently can be mainly classified into three types as follows: firstly, low dimensional chaotic sequences cause degradation of chaos; secondly, the structure of chaotic system adopted is too simple; thirdly, the algorithm is merely related to the structure of chaotic system and key. Concerning the shortcomings above, this paper presented a new image group encryption algorithm. In order to overcome the degradation of chaos, the algorithm generated pixel diffusion matrix by coupling chaotic sequences of high dimensional hyperchaos system with chaotic sequences of one dimensional chaotic mapping by means of matrix tensor product. In the process, the generation of pixel diffusion matrix was controlled by plaintext, thus the algorithm was related to plaintext, which enhanced the security of the algorithm.

Key words: chaos system; image encryption; matrix tensor product; pixel diffusion matrix

0　引言

目前,图像正日益成为信息交流和人机交互的主要手段,而且大量的信息都是以图像的形式存在于科学研究、军事活动、商业活动等诸多领域中。随着针对图像信息的攻击日益增多,其保密和安全问题显得越来越重要。

混沌行为以初值敏感性、类似随机性和连续宽带功率谱为特点,这些特点使混沌在与信息安全结合方面具有天然的优势。混沌轨道的混合特性与传统加密系统的扩散特性相对应,其类随机特性和初值敏感性与传统加密系统的混乱特性相对应,这正好符合 Shannon 提出的关于密码设计的两个基本原则:扩散和混乱[1]。

自从 Chaos 概念[2]提出以来,广大学者和研究人员对混沌行为进行了深入和广泛的研究。其中,Pecora 等[3]对混沌振荡同步的研究进一步推动了混沌理论在密码学中的应用。近年来,如何有效地将信息安全和混沌理论结合已经成为一个研究热点[4-7],但是很多提出的混沌加密算法存在诸多不足,低维系统尤为突出。文献[8]指出,低维混沌序列具有密码周期短、精度低等问题,造成混沌特性退化,而且密钥空间偏小,容易产生碰撞;另外,所选择混沌模型结构简单,如果用非线性研究领域中诸如相空间重构等方法进行攻击,存在被破解的危险。文献[9-10]则提出,如果算法与明文无关,其安全性仅仅只依赖于混沌系统的结构和密钥,将无法抵御已知明文攻击和选择明文攻击。

针对以上问题,本文提出了一种基于超混沌系统和矩阵张量积的图像分组加密算法,用前一分组明文信息控制置乱混沌序列和像素扩散矩阵的产生,实现"一次一密"。该算法极大地扩展了密钥空间,具有密钥敏感性强、安全性高、统计特性好等优点。

1　超混沌动力系统和矩阵张量积

1.1　Newton-Leipnik 超混沌系统

超混沌系统是指正李雅普诺夫指数(Lyapunov Exponents, LE)个数大于等于2的系统。相对于低维系统,超混沌系统处于拉伸状态的维数更多,系统结构更复杂,具有更强的随机性,更难被破译,因此更适合用于加密。基于力矩作用下刚体姿态运动的研究,文献[11]提出了被称为 Newton-Leipnik 的混沌系统。Ghosh 等[12]提出了一个新的4维超混沌 Newton-Leipnik 系统。该系统可以用微分方程组(1)描述:

$$\begin{cases} \dot{x}_1 = -ax_1 + x_2 + 10x_2x_3 + x_4 \\ \dot{x}_2 = -x_1 - 0.4x_2 + 5x_1x_3 \\ \dot{x}_3 = bx_3 - 5x_1x_2 \\ \dot{x}_4 = -cx_1x_3 + dx_4 \end{cases} \tag{1}$$

当系统参数取:$a = 0.4$,$b = 0.175$,$c = 0.8$ 和 $d = 0.01$

收稿日期:2012-02-24;**修回日期**:2012-04-06。　**基金项目**:国家自然科学基金资助项目(61104150,10972082)。
作者简介:唐宋(1982 -),男,四川达州人,硕士研究生,主要研究方向:动力系统、数值计算;　徐桂兰(1985 -),女,四川遂宁人,硕士研究生,主要研究方向:动力系统、数值计算;　李清都(1980 -),男,重庆人,教授,博士,主要研究方向:混沌动力系统、流形计算。

时,系统处于超混沌状态。系统 LE 近似为: $\lambda_1 = 0.05124$, $\lambda_2 = 0.00334$, $\lambda_3 = -0.11725$, $\lambda_4 = -0.11725$。超混沌吸引子在各个方向的投影如图 1 所示。

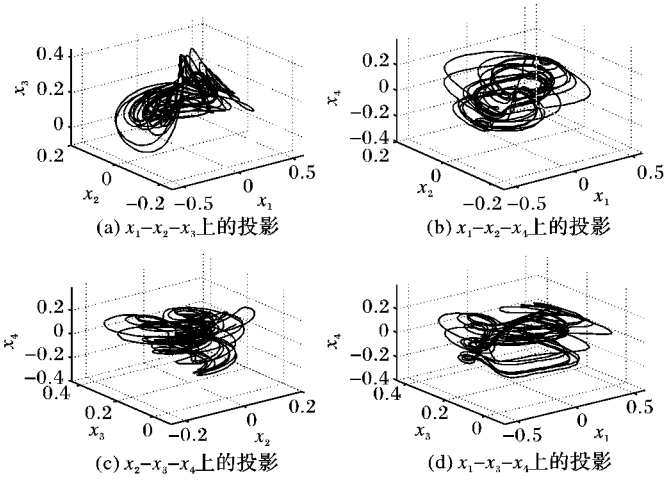


图 1　超混沌吸引子在各个方向的投影

1.2　矩阵张量积

矩阵张量积定义如下:

$$\boldsymbol{A} \otimes \boldsymbol{B} = \begin{bmatrix} a_{11}\boldsymbol{B} & a_{12}\boldsymbol{B} & \cdots & a_{1n}\boldsymbol{B} \\ a_{21}\boldsymbol{B} & a_{22}\boldsymbol{B} & \cdots & a_{2n}\boldsymbol{B} \\ \vdots & \vdots & & \vdots \\ a_{m1}\boldsymbol{B} & a_{m2}\boldsymbol{B} & \cdots & a_{mn}\boldsymbol{B} \end{bmatrix} \tag{2}$$

其中: $\boldsymbol{A} = (a_{ij})_{m\times n}$, $\boldsymbol{B} = (b_{ij})_{k\times l}$。本文加密算法中,分别用两个混沌序列填充矩阵 $\boldsymbol{A}$ 和 $\boldsymbol{B}$,然后按照式(2)计算其矩阵张量积,使混沌序列充分耦合,有效抵御混沌特性退化;同时生成高维矩阵,与图像分组矩阵异或运算,完成像素值的扩散。

1.3　Logistic 映射

Logistic 映射,又称虫口模型,其动力学方程如下:

$$x_{n+1} = \mu x_n(1 - x_n) \tag{3}$$

当 $3.5699456\cdots \leqslant \mu \leqslant 4$, $x \in (0,1)$ 时,系统处于混沌状态,动力学行为十分复杂。

2　本文算法设计

加密算法主要分为分组、置乱和扩散三个部分。具体步骤如下。

步骤 1　产生超混沌序列。采用四阶 Runge-Kutta 法对 4 维超混沌 Newton-Leipnik 系统进行求解,得到 4 维混沌实数序列 $\{\{x_i\},\{y_i\},\{z_i\},\{u_i\} \mid i = 1,2,\cdots\}$。为了确保序列进入混沌状态,将前 N 项截去。

步骤 2　对混沌序列进行变换。按照式(4),对序列 $\{x_i\},\{y_i\},\{z_i\},\{u_i\}$ 作处理,将其变换成整数序列 $\{x_i'\},\{y_i'\},\{z_i'\},\{u_i'\} \in (0,255)$。

$$d_i = \mathrm{mod}(((\mathrm{abs}(d_i) - \mathrm{floor}(\mathrm{abs}(d_i)))10^5),256) \tag{4}$$

其中:abs(x) 表示取 x 的绝对值,floor(x) 表示不超过 x 的最大整数,mod(x,256) 表示对 x 进行模 256 运算。

步骤 3　图像矩阵分块。将明文图像矩阵划分成一系列长度为 n^2 的向量 $\boldsymbol{I}_i$,然后将 $\boldsymbol{I}_i$ 整形为分组矩阵 $\boldsymbol{P}_i$,满足 $\boldsymbol{P}_i = \mathrm{reshape}(\boldsymbol{I}_i,n,n)$。在本文中 $n = 16$。

步骤 4　分组矩阵行置乱。首先,取出 $\boldsymbol{P}_i$ 中第 j 行,记为 r_j,同时按顺序选取混沌序列 $\{x_i'\}$ 中从 $(j+\delta+1)\times n+1$ 到 $(j+\delta)\times n$ 的 n 个数值,记为 s_j;然后,将 r_j 与 s_j 中的元素按序号一一对应以后,按升序对 s_j 排序,得到序列 s_j';接着,按照 s_j' 新的序号重新排列 r_j,完成该行的置乱;最后,对 $\boldsymbol{P}_i$ 各行进行如上变换,将行置乱后的分组矩阵记为 $\boldsymbol{Pr}_j$。其中,$\delta \in (0,255)$ 与前一分组明文矩阵相关,具体计算方法见步骤 7。需要特别指出,对第 1 个分组矩阵进行加密时,令 $\delta = 0$。

步骤 5　分组矩阵列置乱。列置乱过程等价于首先对 $\boldsymbol{Pr}_j$ 转置,然后按照步骤 4 进行行置乱,再将结果转置。列置乱后的分组矩阵记为 $\boldsymbol{Pc}_j$。本步骤选用 $\{y_i'\}$ 为列置乱混沌序列。

步骤 6　分组矩阵像素值扩散。首先将两个一维 Logistic 映射分别迭代 $500+\delta$ 次所产生的混沌实数序列 $\{v_i\},\{w_i\}$,按照式(4)变换生成整数序列 $\{v_i'\},\{w_i'\}$,分别选取其最后 n^2 个数整形生成两个低维矩阵 $\boldsymbol{V}_{n\times n}$ 和 $\boldsymbol{W}_{n\times n}$;对 $\{z_i'\},\{u_i'\}$,分别按顺序选取从 $\delta\times(n^2)+1$ 到 $(\delta+1)\times(n^2)$ 的 n^2 个数值整形生成两个低维方阵,记为 $\boldsymbol{Z}_{n\times n}$ 和 $\boldsymbol{U}_{n\times n}$。然后,按照 2.3 节中式(3),得 5 个备选扩散矩阵:

$$\boldsymbol{D}_0 = \boldsymbol{Z}_{n\times n} \otimes \boldsymbol{U}_{n\times n},\quad \boldsymbol{D}_1 = \boldsymbol{V}_{n\times n} \otimes \boldsymbol{Z}_{n\times n},$$
$$\boldsymbol{D}_2 = \boldsymbol{V}_{n\times n} \otimes \boldsymbol{U}_{n\times n},\quad \boldsymbol{D}_3 = \boldsymbol{W}_{n\times n} \otimes \boldsymbol{Z}_{n\times n},$$
$$\boldsymbol{D}_4 = \boldsymbol{W}_{n\times n} \otimes \boldsymbol{U}_{n\times n}$$

如果 mod(δ,5) = k,那么选择 $\boldsymbol{D}_k$ 作为扩散矩阵与 $\boldsymbol{Pc}_j$ 异或计算,得到最后的分组密文矩阵。

步骤 7　更新 δ。选取当前分组明文矩阵中一系列位置上的数值求和之后进行模运算得到 δ。具体的计算方法为:

$$index = [2,5,12,25,30,42,51,59,63],$$
$$ver = \boldsymbol{P}_i(index),\quad \delta = \mathrm{mod}(\mathrm{sum}(ver),256)$$

步骤 8　如果分组明文矩阵全部加密完毕,则结束;否则转到步骤 3。

由对称性可知,将加密过程逆向即为解密过程。

3　实验结果与分析

3.1　仿真结果

采用 Lena.bmp 作为测试图像,明文和密文图像分别如图 2(a)、(c)所示,对应直方图如图 2(b)、(d)所示。

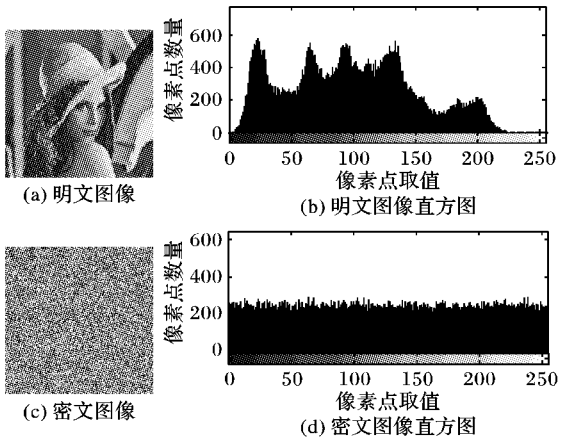


图 2　测试图像

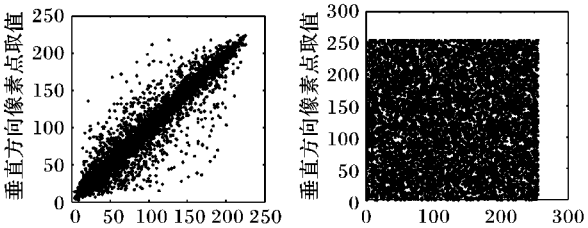
3.2　相邻像素相关性分析

相邻像素相关性能衡量图像的置乱效果,因此可以通过计算相关系数来进行量化比较,其计算公式如下所示:

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i,\quad D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2,$$
$$\mathrm{cov}(x,y) = \frac{1}{N}\left(\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y))\right),$$
$$r_{xy} = \frac{\mathrm{cov}(x,y)}{\sqrt{D(x)D(y)}}$$

其中:x,y 分别表示图像中相邻两个像素的灰度;r_{xy} 为相邻两个像素的相关系数。

在水平、垂直和对角方向，分别从明文和密文图像中随机选取5000对相邻像素作为计算样本。在垂直方向上，明文和密文图像相邻像素的相关分布如图3所示。加密前后水平、垂直和对角方向上的相关系数如表1所示。实验结果表明，相对于文献[13－16]的算法，本文算法在垂直和对角方向的相关性有显著的改进，结果如表2所示。



(a) 明文图像 (a) 密文图像

图3 明文和密文图像相邻像素的相关分布

表1 原始图像和密文图像相邻像素的相关性

方向	原始图像	加密图像
水平	0.9342	0.007500
垂直	0.9679	－0.000808
对角	0.9401	－0.000410

表2 不同算法的密文图像相邻像素的相关系数比较

算法	水平	垂直	对角
本文算法	0.007500	－0.000808	－0.000410
文献[13]算法	0.002637	－0.009177	0.003429
文献[14]算法	－0.014200	－0.007400	－0.018300
文献[15]算法	0.002300	－0.012900	－0.001600
文献[16]算法	0.000707	0.002165	0.014886

3.3 密钥空间分析

密钥由NL超混沌系统初值 x_0, y_0, z_0, u_0 以及两个一维Logistic映射的系统参数和初值 μ_1, μ_2, v_0, w_0 构成。假设计算精度为 10^{-15}，密钥空间结构如表3所示，总的密钥空间为 3.44×10^{120}，表明算法具有足够大的密钥空间，能够有效抵御穷举密钥攻击。

表3 密钥空间估算

密钥组成	含义	取值范围	空间大小
μ_1, μ_2	Logistic映射系统参数	(3.57,4)	1.72×10^{30}
v_0, w_0	Logistic映射初值	(0,1)	2×10^{30}
x_0, y_0, z_0, u_0	NL超混沌系统初值	任意取值	1×10^{60}

3.4 信息熵分析

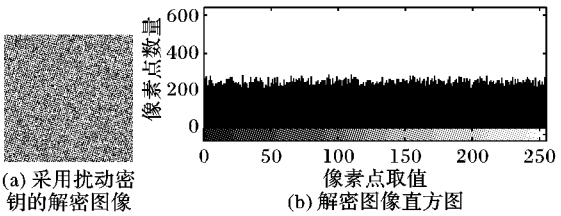
信息熵是用来表征信息量的一个概念，其大小与系统的混乱程度成反比，当图像中像素值出现的频率相同时，熵值达到最大理论值8。按如下公式可计算信息熵的值：

$$H(m) = \sum_{i=0}^{M-1} p(m_i) \mathrm{lb} \frac{1}{p(m_i)}$$

其中：$m_i \in m$ 为像素值，M 为 m_i 取值总个数，$p(m_i)$ 表示 m_i 出现的概率。采用本文提出的算法加密所得密文图像的信息熵为7.997≈8，数据表明加密过程中几乎没有丢失信息，从而能够有效抵抗熵攻击。

3.5 密钥敏感性分析

假设密钥有微小的扰动，$y_0 = 0.2 + 10^{-15}$。采用扰动密钥加密所得图像灰度差异率为96.5%；另一方面，采用扰动密钥解密，解密图像和对应直方图如图4所示。实验表明，密钥的微小扰动，产生几乎完全不同的加解密效果，密钥敏感性高，能有效抵御差分攻击。



(a) 采用扰动密钥的解密图像 (b) 解密图像直方图

图4 扰动密钥解密结果

4 结语

基于超混沌系统和矩阵张量积，本文提出了一种新的图像分组加密算法。像素扩散矩阵通过混沌序列作矩阵张量积的方式产生，使混沌序列充分耦合；而且，通过明文信息控制置乱混沌序列和像素扩散矩阵的生成，使算法的安全性在依靠混沌系统结构复杂性和密钥强度的同时，还与明文有关，进一步提高了安全性。最后对算法的安全性能作了分析，证明了加密算法的有效性；而且与其他算法比较，本文算法在密钥空间和相邻像素相关性方面有了显著的提高。

参考文献：

[1] SHANNON C E. Communication theory of secrecy systems [J]. Bell System Technical Journal, 1949, 28(4): 656－715.

[2] LI T-Y, YORKE J A. Period three implies chaos [J]. The American Mathematical Monthly, 1975, 82(10): 985－992.

[3] PECORA L M, CARROLL T L. Synchronization in chaotic systems [J]. Physical Review Letters, 1990, 64(8): 821－824.

[4] ARMOSKI G, KOCAREV L. Chaos and cryptography: block encryption ciphers based on chaotic maps [J]. IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, 2001, 48(2): 163－169.

[5] BEHNIA S, AKHSHANI A, MAHMODI H, *et al*. A novel algorithm for image encryption based on mixture of chaotic maps [J]. Chaos, Solitons & Fractals, 2008, 35(2): 408－419.

[6] LANG JUN, TAO RAN, WANG YUE. Image encryption based on the multiple-parameter discrete fractional Fourier transform and chaos function [J]. Optics Communications, 2010, 283(10): 2092－2096.

[7] YE GUODONG. Image scrambling encryption algorithm of pixel bit based on chaos map [J]. Pattern Recognition Letters, 2010, 31(5): 347－354.

[8] 佟晓筠, 崔明根. 基于扰动的复合混沌序列密码的图像反馈加密算法[J]. 中国科学 F 辑: 信息科学, 2009, 29(6): 588－597.

[9] RHOUMA R, BELGHITH S. Cryptanalysis of a new image encryption algorithm based on hyper-chaos [J]. Physics Letters A, 2008, 372(38): 5973－5978.

[10] 刘金梅, 丘水生. 基于超混沌系统的图像加密算法的安全性分析 [J]. 计算机应用研究, 2010, 27(3): 1042－1044.

[11] LEIPNIK R B, NEWTON T A. Double strange attractors in rigid body motion with linear feedback control [J]. Physics Letters A, 1981, 86(2): 63－67.

[12] GHOSH D, BHATTACHARYA S. Projective synchronization of new hyperchaotic system with fully unknown parameters[J]. Nonlinear Dynamics, 2010, 61(1/2): 11－21.

[13] WONG K-W, KWOK B S-H, LAW W-S. A fast image encryption scheme based on chaotic standard map [J]. Physics Letters A, 2008; 372(15): 2645－2652.

[14] GAO TIEGANG, CHEN ZENGQIANG. A new image encryption algorithm based on hyper-chaos [J]. Physics Letters A, 2008, 372(4): 394－400.

[15] 杨雪松, 于万波, 魏小鹏. 基于复合超混沌系统且与明文相关联的图像加密[J]. 计算机应用研究, 2011, 28(10): 3807－3810.

[16] WANG YONG, WONG K-W, LIAO XIAO-FENG, *et al*. A new chaos-based fast image encryption algorithm [J]. Applied Soft Computing, 2011, 11(1): 514－522.