第 19 卷 第 6 期　　控 制 与 决 策　　2004 年 6 月
Vol. 19 No. 6　　*Control and Decision*　　June 2004

文章编号: 1001-0920(2004)06-0714-04

Baker 映射的三维扩展及其在多媒体加密中的应用

廉士国, 茅耀斌, 王执铨
(南京理工大学 自动化系, 江苏 南京 210094)

摘　要: 对 Baker 映射进行三维扩展,提出一种基于三维混沌映射的混沌加密方案. 与二维映射相比,扩展后的三维 Baker 映射具有更大的密钥空间、更快的混迭速度和更广的应用范围. 这种三维 Baker 映射与扩散函数相结合,增加了密码强度,起到良好的加密作用. 实验结果表明,与传统基于数论的 DES 加密算法相比,该算法具有更快的速度,更适合于多媒体数据的加密.

关键词: Baker 映射; 混沌加密; 图像加密; 多媒体信息加密
中图分类号: TP13　　**文献标识码**: A

3D extension of Baker map and its application to multimedia information encryption

LIAN Shi-guo, MAO Yao-bin, WANG Zhi-quan
(Department of Automation, Nanjing University of Science and Technology, Nanjing 210094, China. Correspondent: LIAN Shi-guo, E-mail: sg_lian@hotmail.com)

Abstract: Baker map is proposed to 3D space and an Baker map based encryption scheme is proposed. Compared to 2D Baker map, the extended 3D Baker map has much larger key space, much faster mixing speed and much wider applications such as the encryption of images, videos or multi-spectral image sequences. The encryption scheme combining the extended Baker map with spreading functions is of high security. And experiments show that the algorithmis much faster than DES, which makes it more suitable for multimedia encryption.

Key words: Baker map; chaotic encryption; image encryption; multimedia information encryption

1 引　　言

随着多媒体技术和网络技术的发展,多媒体数据的应用越来越广泛,其安全性便成为值得关注的问题. 对于图像、音频、视频等大数据量的多媒体信息,传统的基于数论的加密算法很难满足实时性要求. 与其相比,混沌加密则能满足实时性要求且具有较高的安全性. 由于混沌具有初值敏感性、参数敏感性、各态历经性、混乱性以及类随机性等特点,它在加密中的应用已得到了广泛研究.

文献[1]使用斜帐篷映射构造了分块密码;[2]使用修改的二维 Baker 映射构造了分组密码;[3]则分析了用混沌映射构造密码的通用方法. 但这些方法由于同时用到整型和浮点型数据的运算,对计算精度要求较高,且降低了计算速度. 文献[4]对斜帐篷映射离散化,构造了新的密码;[5]通过离散化二维 Baker 映射,建立了基于混沌置乱的密码;[6]分析了离散化后的混沌映射和原始映射的关系;[7]研究了二维 Baker 映射和 Cat 映射用于加密的方法,并分析了这两种映射的密钥空间和密钥可靠性,但其中的三维扩展只针对灰度,并不适于三维空间的

收稿日期: 2003-05-01; **修回日期**: 2003-07-21.
基金项目: 国家自然科学基金资助项目(60174005); 教育部博士点基金资助项目(20020288025).
作者简介: 廉士国(1978—),男,江苏徐州人,博士生,从事混沌加密、多媒体信息加密等研究; 王执铨(1939—),男,湖北武汉人,教授,博士生导师,从事动态大系统控制、混沌控制等研究.

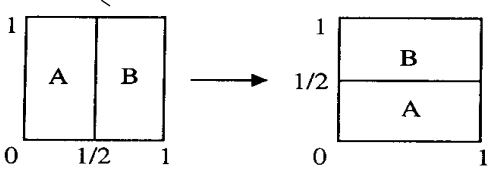
位置置乱,如视频流、多频段图列等.

本文利用 Baker 映射在平面上的切割伸缩原理,将其扩展到三维空间,并对其离散化,推广到任意尺寸的长方体和任意分割的情况,从而扩大了它的适用范围. 与二维映射相比,三维 Baker 映射具有更大的密钥空间和更快的置乱速度,将其用于多媒体数据加密具有较高的安全性.

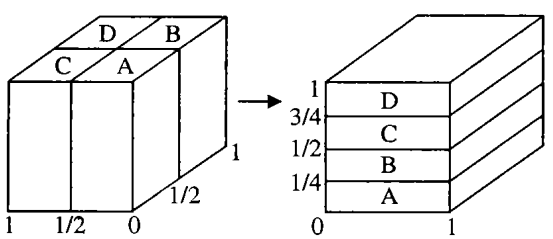
2　二维 Baker 映射扩展到三维

连续二维 Baker 映射是在平面内沿 x 轴切分竖条,并将每个竖条沿 x 轴扩展,再沿 y 轴压缩,保持面积不变,这样层层垒起. 这是一个混沌映射,其过程如图 1(a) 所示,变换公式为

$$B(x,y)=\begin{cases}\left(2x,\dfrac{y}{2}\right), 0\le x<\dfrac{1}{2};\\ \left(2x-1,\dfrac{y}{2}+\dfrac{1}{2}\right), \dfrac{1}{2}\le x\le 1.\end{cases}\tag{1}$$



(a)　连续二维 Baker 映射



(b)　连续三维 Baker 映射

图 1　连续二维和三维 Baker 映射的映射过程

将 Baker 映射过程用于三维空间,即将立方体分别沿 x 轴和 y 轴切块,得到 4 个立方条,再将每个立方条在保持体积不变的情况下压扁,层层堆叠成新的立方体. 此过程延续了二维 Baker 映射的混沌特性,如图 1(b) 所示. 这种扩展的映射过程也可先按 xz 平面作一次二维 Baker 映射,再按 yz 平面作一次二维 Baker 映射而得到. 具体过程如下:

1) 设原立方块中一点 P 的坐标为 (x,y,z);

2) 按 xz 平面作一次二维 Baker 映射,此时 P 点映射到新的位置 P′,即

$$B(x,y,z)=\begin{cases}\left(2x,y,\dfrac{z}{2}\right), 0\le x<\dfrac{1}{2};\\ \left(2x-1,y,\dfrac{z}{2}+\dfrac{1}{2}\right), \dfrac{1}{2}\le x\le 1.\end{cases}\tag{2}$$

3) 按 yz 平面作一次二维 Baker 映射,此时 P′点映射到新的位置 P″,即

$$B(x,y,z)=\begin{cases}\left(2x,2y,\dfrac{z}{4}\right),\\ \quad 0\le x<\dfrac{1}{2}, 0\le y<\dfrac{1}{2};\\ \left(2x,2y-1,\dfrac{z}{4}+\dfrac{1}{2}\right),\\ \quad 0\le x<\dfrac{1}{2}, \dfrac{1}{2}\le y\le 1;\\ \left(2x-1,2y,\dfrac{z}{4}+\dfrac{1}{4}\right),\\ \quad \dfrac{1}{2}\le x\le 1, 0\le y<\dfrac{1}{2};\\ \left(2x-1,2y-1,\dfrac{z}{4}+\dfrac{3}{4}\right),\\ \quad \dfrac{1}{2}\le x\le 1, \dfrac{1}{2}\le y\le 1.\end{cases}\tag{3}$$

按文献[7]的方法,将三维 Baker 映射一般化和离散化,并推广到任意分割和任意尺寸长方体的情况. 具体算法如下:

设长方体尺寸为 $N\times M\times H$,沿 x 轴方向分割成 L_x 块,有 $\{n_i \mid i=1,2,\cdots,L_x, n_1+n_2+\cdots+n_{L_x}=N\}$;沿 y 轴方向分割成 L_y 块,有 $\{m_j \mid j=1,2,\cdots,L_y, m_1+m_2+\cdots+m_{L_y}=M\}$. 分割后块 $n_i\times m_j\times H$ 中的一点 (x,y,z),经三维 Baker 映射为

$$B_3(x,y,z)=\left(\mathrm{mod}(\mathrm{mod}(\mathrm{num},MN),N),\left[\frac{\mathrm{mod}(\mathrm{num},MN)}{N}\right],\left[\frac{\mathrm{num}}{MN}\right]\right).\tag{4}$$

其中

$$\mathrm{num}=\mathrm{pre\_num}+(z-1)m_jn_i+(y-1)n_i+x,$$

$$\mathrm{pre\_num}=(NG_j+m_jF_i)H,$$

$$F_i=\sum_{k=1}^{i-1}n_k,\ F_1=0,\ G_j=\sum_{t=1}^{j-1}m_t,\ G_1=0.\tag{5}$$

3　三维和二维 Baker 映射的比较

3.1　参数空间

Fridrich[7] 对二维 Baker 映射的参数空间作了分析,得出长度为 N 的映射矩形,其参数空间为 2^{N-1}. 在三维情况下,分别沿 x 和 y 两个方向分块,比二维情况下获得的参数空间更大,密钥空间也更大. 对于三维 Baker 映射,如果沿 x 轴和 y 轴的长度分别为 N_x 和 N_y,则其参数空间为

$$D_3 = 2^{N_x+N_y-2}. \quad (6)$$

3.2 混乱速度

分别用二维和三维 Baker 映射来置乱相同的图像(将图像像素排列成长方体,便可利用三维 Baker 映射来置乱),并用分形维数[8]来比较二维和三维 Baker 映射的置乱速度. 对 256 ×256 的 lena 和 couple 进行测试,得到分形维数和置乱次数的关系如图 2 所示. 映射的分割方式随机选定,计算图像分形维数的距离序列为{4,6,8,10,12,13,15}.

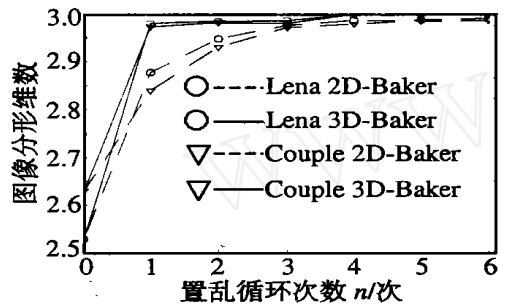


图 2 同一幅图像的置乱次数与分形维数的关系

由图 2 可见,lena 图像的分形维数为 2.529 2,经过一次三维置乱后为 2.979 1,经过一次二维置乱后为 2.876 4,且随着置乱次数的增加,分形维数越接近于 3;对于 couple 图像也有类似的结果. 选择不同的分割方式,结论类似. 对于相同的图像,三维 Baker 映射只需较少的置乱次数,便可获得较高的分形维数,可见三维 Baker 映射比二维 Baker 映射具有更快的混乱速度.

3.3 应用范围

扩展后的三维 Baker 映射可实现三维空间的位置置乱. 除了用于图像的置乱外,还可用于立体图像、视频图像序列和多频谱图像序列的加密,以及其他三维数据的加密等.

4 一种基于三维 Baker 映射的加密方案

混沌映射实现的是混乱功能,如果只用它进行加密,对于已知明文攻击是不安全的. 将其与扩散函数相结合,同时增加混乱和扩散的次数,能够增强密码强度. 由此构建如图 3 所示的对称加密方案.

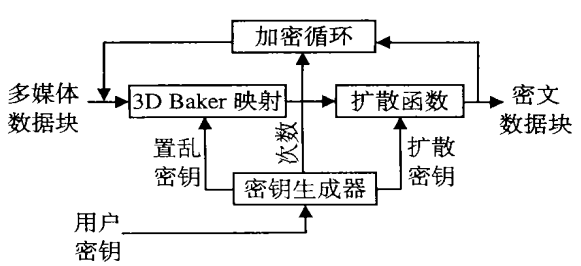


图 3 三维 Baker 映射加密方案

在图 3 中,扩散函数按光栅扫描方式,采用当前像素灰度值与前一个相邻的像素之间的扩散,这种方式的扩散速度更快. 这里按此方法设计一种扩散函数,令 P_i 为扩散前的像素值,C_i 为扩散后的像素值,L 为像素灰度级数,则扩散过程为

$$C_i = (P_i + C_{i-1}^2) \bmod L, \quad (7)$$

C_0 由用户密钥提供. 解密时,反扩散过程为

$$P_i = (C_i - C_{i-1}^2) \bmod L. \quad (8)$$

5 密码分析及实验结果

5.1 密文图像直方图均匀分布

图 4 为图像加密前后的直方图比较. 显然,加密后 couple 图像的直方图比加密前更均匀. 通过对多幅图像测试都得到了类似结果. 由 Shannon[9]对高强度理想密码和唯一性距离的定义可知,对于已知密文攻击,用该方法加密后,密文图像像素间的相关性较小,密文信息对推测密钥的贡献很小,这就增加了破译的工作难度. 可见,此密码能够抵抗统计和已知密文攻击.

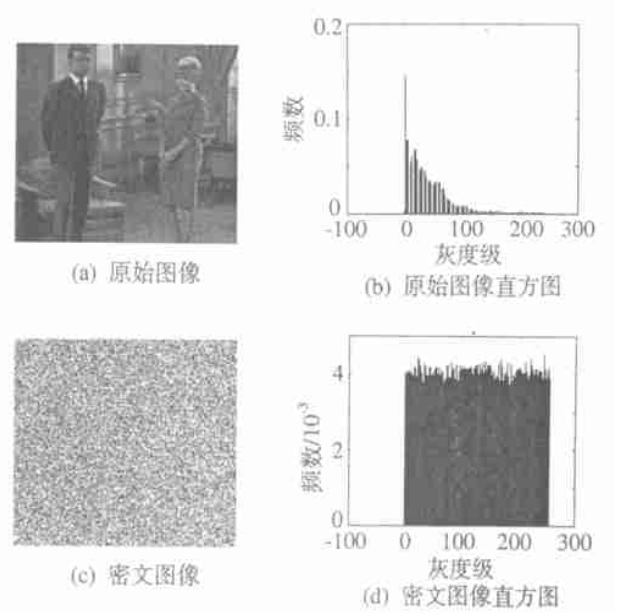


图 4 图像加密前后的直方图比较

5.2 图像序列加密

用以上算法加密 Bus 图像序列,图像尺寸为 240 ×352. 以 240 ×352 ×32 的图像块加密,原图像序列和加密后图像序列分别如图 5 所示(仅列出 3 幅). 可见,加密后图像内容完全不可理解.

5.3 算法速度测试

对以上算法与 DES 加密算法的加密速度进行比较. 运行计算机为 1.4 GHz CPU/256M RAM/

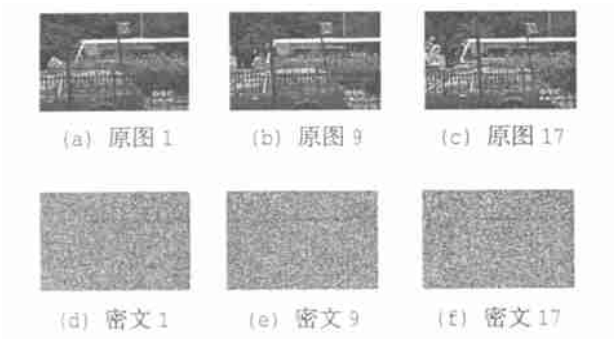


图 5　视频图像序列加密结果

Microsoft Windows 98 操作系统,Baker 映射的循环次数为 4 次. 实验结果如表 1 所示. 可见,基于三维 Baker 映射加密方法的加解密速度很快,达到 1.2 MB/ s 以上,因此更适于大数据量、实时性要求高的多媒体数据的加密.

表 1　两种加密算法加解密速度比较

测试图像 长 ×宽	基于 3D Baker 的密码		DES 算法	
	加密/ s	解密/ s	加密/ s	解密/ s
aerial 128 ×128	0.05	0.03	0.50	0.44
boats 256 ×256	0.06	0.05	1.92	1.87
cougar 640 ×480	0.22	0.22	8.93	8.90
girl 1 024 ×768	0.60	0.60	22.52	23.13
city 2 048 ×2 048	3.24	3.19	122.05	120.45

6　结　　语

本文将 Baker 映射扩展到三维,并保持了原映射的混沌特性. 扩展后的三维映射具有更大的密钥空间和更快的混乱速度,能够实现三维空间的位置置乱,适合于视频或多频谱图像序列的加密及其他三维数据的保密应用. 本文提出将三维混沌映射用于加密的方案,对图像序列的加密结果表明,该方案具有较高的安全性. 针对视频数据量大的特点,将三维混沌映射用于视频流的部分加密,将是进一步研究的课题.

参考文献(References):

[1] Habutsu T, Nishio Y, Sasase I, et al. A secret key cryptosystem by iterating chaotic map[J]. *Lect Notes Comput Sci*, 1991, 547: 127-140.

[2] Tsueike M, Ueta T, Nishio Y. An application of two dimensional chaos cryptosystem [R]. Japanses: IEICE, 1996.

[3] Kotulski Z, Szczepanski J. Discrete chaotic cryptography [J]. *Ann Physik*, 1997, 6(5): 381-394.

[4] Naoki Masuda, Kazuyuki Aihara. Cryptosystems with discretized chaotic maps[J]. *IEEE Trans on Circuits and Systems — I: Fundamental Theory and Applications*, 2002, 49(1): 28-40.

[5] Pichler F, Scharinger J. Finite dimensional generalized Baker dynamical systems for cryptographic applications[J]. *Lect Notes in Comput Sci*, 1996, 1030: 465-476.

[6] Kocarev L, Jakimoski G, Stojanovski T, et al. From chaotic maps to encryption schemes[A]. *Proc IEEE Int Symp ISCAS '98*[C]. Monterey: IEEE, 1998. 514-517.

[7] Fridrich J. Symmetric ciphers based on two-dimensional chaotic maps[J]. *Int J Bifurcation and Chaos*, 1998, 8(6): 1259-1284.

[8] Chen C C, Daponte J S, Fox M D. Fractal feature analysis and classification in medical imaging[J]. *IEEE Trans on Medical Imaging*, 1989, 8(2): 133-142.

[9] Shannon C. Communication theory of secrecy systems[J]. *Bell System Technical J*, 1949, 28(4): 656-715.

(上接第 713 页)

[3] Byrnes C I, Isidori A. Output regulation for nonlinear systems: An overviews[J]. *Int J Robust Nonlinear Control*, 2000, 33(10): 323-337.

[4] 王强德,陈卫田,魏春玲,等. 一类不确定非线性系统的鲁棒自适应控制[J]. 控制理论与应用,2000,17(2):244-248.
(Wang Qiangde, Chen Weitian, Wei Chunling, et al. Robust adaptive control of a class of a uncertain nonlinear systems[J]. *Control Theory and Applications*, 2000, 17(2): 244-248.)

[5] Jiang Zhongping, Laurent Praly. Design of robust adaptive controller for nonlinear systems with dynamic uncertainties [J]. *Automatica*, 1998, 34(7): 825-840.

[6] 王强德,魏春玲,王华建. 一类非线性参数系统的鲁棒自适应控制[J]. 控制理论与应用,2002,19(2):197-202.
(Wang Qiangde, Wei Chunling, Wang Huajian. Robust adaptive controller of a class of nonlinear parameterization systems[J]. *Control Theory and Applications*, 2002, 19(2): 197-202.)

[7] Qian Chunjiang, Lin Wei. Practical output tracking of nonlinear systems with uncontrollable unstable linearization [J]. *IEEE Trans on Automatic Control*, 2002, 47(1): 21-36.