

文章编号:1000-5013(2015)06-0655-04

doi:10.11830/ISSN.1000-5013.2015.06.0655

新三维混沌映射及其在数字图像 信息加密中的应用

刘冰, 潘大兵

(达州职业技术学院 公共事务管理系, 四川 达州 635001)

摘要: 引入新的三维混沌映射, 结合有限域运算处理, 构建一种数字图像加密方法. 首先, Lu 映射将原始图像信息映射为 2 个混沌矩阵; 其次, 将原始图像矩阵和生成的 2 个混沌矩阵, 在有限域上执行 4 个轮次的运算处理. 实验结果表明: 提出的加密方法可以获得均匀细腻的置乱效果, 在直方图评价、三向相关性评价等方面都表现出良好的加密性能, 整个算法的加密速度也比较快.

关键词: 数字图像; 图像加密; 三维混沌映射; 三向相关性; Lu 映射

中图分类号: TP 311

文献标志码: A

数字图像信息, 作为数字信息中最重要的一类, 如何保障其安全可靠地传输, 成为数字技术中的关键问题^[1]. 数字图像加密技术^[2]利用各种加密模型和加密算法, 对原始图像信息进行置乱处理, 加密后的图像必须通过特定的密钥及解密算法才能恢复成原始图像, 从而确保图像传输和使用过程的安全性^[3]. 然而, 早期的数字图像加密技术的加密思路和置乱规律被逐步破译, 其安全性和可靠性大大降低^[4-6]. 因此, 更为复杂的加密模型和置乱算法开始逐步进入图像加密领域. 近年来, 基于混沌理论和混沌系统的加密方法在数字图像信息加密过程中获得广泛地应用, 大大增强了加密安全性和可靠性^[7-8]. 基于混沌映射的数字图像加密方法, 已具有许多成功的案例^[9-12]. 鉴于混沌理论在数字图像加密领域中的成功应用, 本文采用一种新的三维混沌映射, 构建一种基于此映射的数字图像加密算法.

1 新的三维混沌映射

在数字图像加密领域, Logistic 混沌映射、Lorenz 混沌映射都有比较成功的应用. 为了进一步增强后续图像加密算法的抗攻击能力, 引入一个新的三维混沌映射^[13], 称为 Lu 映射, 其动力学方程为

$$\left. \begin{aligned} \dot{x} &= a(z - y), \\ \dot{y} &= bx - dx^2, \\ \dot{z} &= kxy - cy - gz. \end{aligned} \right\} \quad (1)$$

式(1)中: a, b, c, d, k, g 等 6 个参数的取值分别为 8.0, 40.0, 10/3, 3.0, 1.0, 4.0.

Lu 映射是一个典型的三维混沌系统, 内含 2 个非线性项. Lu 混沌系统含有 2 个平衡点 (0, 0, 0), (40/3, 0, 0), 且都是不稳定的鞍焦点, 这说明 Lu 映射是一个耗散系统.

2 基于 Lu 映射的数字图像加密算法

2.1 加密算法的总体流程

在 Lu 映射的基础上, 结合有限域上的相关运算构建图像加密算法, 有利于提升加密过程的安全性

收稿日期: 2015-10-08

通信作者: 刘冰(1970-), 男, 副教授, 主要从事计算机信息技术及其应用的研究. E-mail: newbing@126.com.

基金项目: 四川省教育厅重点科技计划项目(14ZA0330); 四川省达州市 2014 年科技计划项目(2014-8220)

与抗攻击能力. 此外, 由于有限域运算在速度上的优势, 不会导致整个加密算法的执行时间明显增加. 构建的数字图像加密算法整体流程, 如图 1 所示. 由图 1 可知: Lu 映射在前几个环节用于混沌置乱处理, 而有限域运算则用于进一步增加加密过程的复杂性.

2.2 Lu 混沌映射置乱处理

将要执行加密处理的原始图像信息作为 x 代入式(1), 通过 Lu 映射计算出 y, z , 进而对 y, z 执行标度变换, 使其数值范围正好映射在 $(0, 255)$ 这个区间, 恰好符合数字图像的灰度值范围要求. 其数学模型为

$$\left. \begin{aligned} A &= (y \times 1\,000) \bmod 256, \\ B &= (z \times 1\,000) \bmod 256. \end{aligned} \right\} \quad (2)$$

式(2)中: A, B 为 y, z 标度变换后的映射序列; mod 为取模的运算.

由式(2)获得 2 个一维数据变量 A, B , 且这 2 个变量的数据长度和原始图像的数据长度一致. 为了满足后续执行有限域矩阵运算的处理, 将这 2 个一维数据变量, 进一步映射成图像像素矩阵的形式, 即

$$A_{M \times N} = A_n, \quad B_{M \times N} = B_n. \quad (3)$$

式(3)中: M, N 为原始图像的宽度和高度.

2.3 有限域加密处理

为了提升整个加密过程的复杂性, 进一步执行有限域矩阵运算处理. 首先, 选取原始图像数据矩阵 $I^1_{M \times N}$ 和混沌映射矩阵 $A_{M \times N}$, 分别在有限域上执行一次加法处理和一次乘法处理, 即

$$I^2_{M \times N} = I^1_{M \times N} \oplus A_{M \times N}, \quad (4)$$

$$I^3_{M \times N} = I^2_{M \times N} \otimes A_{M \times N}. \quad (5)$$

式(4), (5)中: $I^2_{M \times N}$ 为原始图像矩阵 $I^1_{M \times N}$ 执行有限域上加法处理的结果; $I^3_{M \times N}$ 为 $I^2_{M \times N}$ 执行有限域上乘法处理的结果.

其次, 针对图像矩阵 $I^3_{M \times N}$, 利用 $B_{M \times N}$ 再执行两次有限域上的加法处理和乘法处理, 即

$$I^4_{M \times N} = I^3_{M \times N} \oplus B_{M \times N}, \quad (6)$$

$$I^5_{M \times N} = I^4_{M \times N} \otimes B_{M \times N}. \quad (7)$$

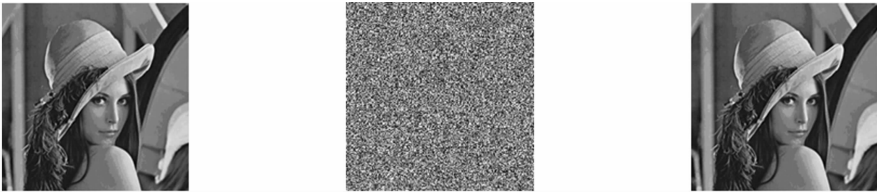
式(6), (7)中: $I^4_{M \times N}$ 为 $I^3_{M \times N}$ 执行有限域上加法处理的结果; $I^5_{M \times N}$ 为 $I^4_{M \times N}$ 执行有限域上乘法处理的结果.

2.4 加密算法的解密流程设计

为了确保加密图像能够被正确解密, 需要根据加密过程设计相应的解密过程. 对于设计的基于 Lu 映射的图像加密算法, 在解密过程中, 仍然要采用 Lu 映射, 并设置同加密端一样的初始状态, 再在有限域上执行加密过程的各种逆运算. 加密算法的解密流程为: 1) 根据 Lu 混沌映射设置初始状态; 2) 根据 Lu 混沌映射和加密图像矩阵 $I^5_{M \times N}$ 生成混沌序列 A, B ; 3) 将混沌序列 A, B 转换为图像形式; 4) 将 $I^5_{M \times N}$ 和 B 在有限域上执行乘法处理的逆运算, 恢复出图像矩阵 $I^4_{M \times N}$; 5) 将 $I^4_{M \times N}$ 和 B 在有限域上执行加法处理的逆运算, 恢复出图像矩阵 $I^3_{M \times N}$; 6) 将 $I^3_{M \times N}$ 和 A 在有限域上执行乘法处理的逆运算, 恢复出图像矩阵 $I^2_{M \times N}$; 7) 将 $I^2_{M \times N}$ 和 A 在有限域上执行加法处理的逆运算, 恢复出原始图像 $I^1_{M \times N}$.

3 结果与分析

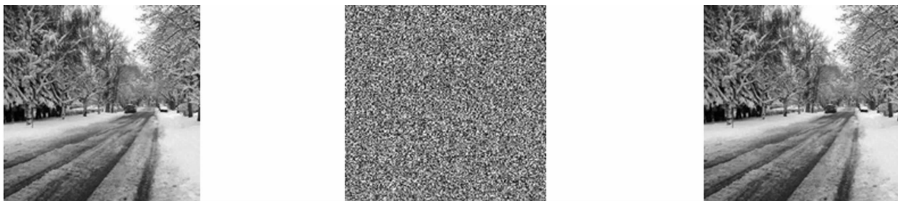
实验的计算机硬件配置: 酷睿双核; 主频 2.0 GHz 的 CPU; 4 GB 大小的内存. 计算机软件配置: Windows 7.0 操作系统; Matlab 编译环境. 选取 2 幅灰度图像作为实验对象, 结果如图 2 所示.



(a) 原始图像(Lena) (b) 加密图像(Lena) (c) 解密图像(Lena)



图 1 加密原理及流程图
Fig. 1 Encryption principle and flow chart



(d) 原始图像(风景) (e) 加密图像(风景) (f) 解密图像(风景)

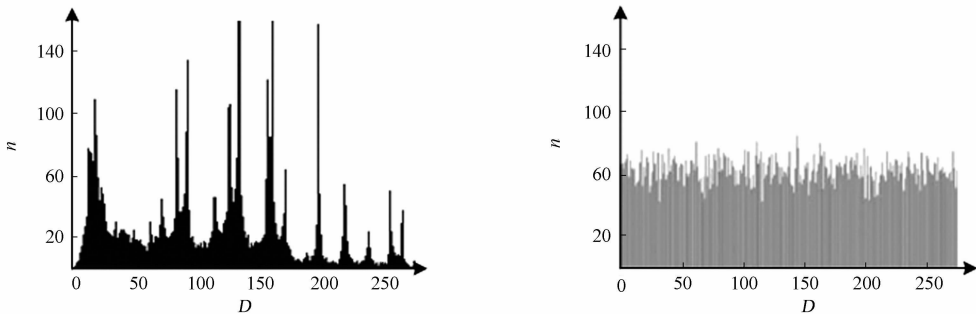
图 2 图像的加密效果

Fig. 2 Effect of image encryption

由图 2 可知:Lena 图像经加密处理后,原始图像信息被均匀置乱,无法看到和原始图像有关的细节信息.进一步对加密结果实施解密算法,解密结果准确地恢复出原始图像信息.风景图像与 Lena 有同样的表现,这充分证实了加密方法的鲁棒性.

3.1 灰度直方图评价

一般而言,一幅纹理特征明显的图像,其灰度(D)分布会比较集中.经图像加密算法处理后,灰度直方图的分布比较均匀,均匀性越好,证明加密效果越好.风景数字图像加密前后的直方图效果,如图 3 所示.由图 3 可知:经加密后,图像的灰度直方图分布变得非常均匀,证明文中方法的加密安全性较高.



(a) 图像加密前 (b) 图像加密后

图 3 灰度直方图评价

Fig. 3 Evaluation of gray histogram

3.2 三向相关性评价

三向相关性,指的是图像像素在水平方向、垂直方向和对角线方向之间的相关性.无论哪个方向上的相关性高,都会使图像数据容易破译.因此,衡量一个加密算法性能的好坏,最直接的思路就是评价这 3 个方向上的相关性.相关性计算公式为

$$E(x) = \frac{1}{N} \sum_{i=1}^N x_i, \tag{8}$$

$$D(x) = \frac{1}{N} \sum_{i=1}^N (x_i - E(x))^2, \tag{9}$$

$$\text{cov}(x,y) = \frac{1}{N} \sum_{i=1}^N (x_i - E(x))(y_i - E(y)), \tag{10}$$

$$r_{x,y} = \frac{\text{cov}(x,y)}{\sqrt{D(x)} \times \sqrt{D(y)}}. \tag{11}$$

利用上述公式可得,风景图像加密前 3 个方向的相关系数为 0.904 6,0.924 0,0.917 0,加密后 3 个方向的相关系数为 0.001 8,0.002 1,0.002 3.由此可知:文中加密方法具有较高的安全性能.

3.3 执行时间分析

对加密方法的执行时间进行测试. Lena 图像加密和解密的时间分别为 0.078,0.080;风景图像加密和解密的时间分别为 0.081,0.083.由此可知:加密过程和解密过程的时间较短,执行速度较快.

4 结束语

引入一种新的三维混沌映射,结合有限域上的运算处理构建图像加密算法.原始图像信息在 Lu 映

射下被置乱为 2 个混沌矩阵,进而将原始图像和这 2 个混沌矩阵执行 4 个轮次的有限域运算处理. 选择 2 组实验图像,分别进行加密效果测试、加密效果评价、执行时间测试等验证性实验. 结果表明:对于 Lena 图像和风景图像,基于新的三维混沌映射的图像加密方法表现出加密效果良好、抗攻击性能强、执行时间快的特点.

参考文献:

[1] ROHITH S,BHAK K N,SHARMA A N. Image encryption and decryption using chaotic key sequence generate by sequence of logistic map and sequence of states of linear feedback shift register[C]// International Conference on Advances in Electronic, Computers and Communications. New Jersey:IEEE Press,2014:1124-1130.

[2] 王玉惠,陈哨东. 基于五维超混沌的全球信息栅格图像加密算法[J]. 吉林大学学报(信息科学版),2011,29(1):51-56.

[3] PATIDAR V. A robust and secure chaotic standard map based pseudorandom permutation-substitution scheme for image encryption[J]. Optics Communications,2010,284(19):4331-4339.

[4] BARRERA J F. Experimental opto-digital synthesis of encrypted sub-samples of an image to improve its decoded quality[J]. Optics Communications,2009,51(11):1822-1827.

[5] CHANG W L,HUANG S C,LIN K W,et al. Fast parallel DNA-based algorithms for molecular computation: Discrete logarithm[J]. J Supercomputing,2011,5(6):129-133.

[6] 赵文博,田小平,吴成茂. 基于低密度奇偶校验编码和混沌系统的图像加密[J]. 计算机应用,2012,32(7):2018-2021.

[7] SHIU H J,NG K L,FANG J F,et al. Data hiding methods based upon DNA sequences[J]. Information Sciences,2010,180(11):2196-2208.

[8] 孙劲光,汪洁,孟祥福. 改进的 Fibonacci 双置乱图像加密算法[J]. 计算机科学,2012,39(11):249-253.

[9] BANERJEE S. Synchronization of spatiotemporal semiconductor lasers and its application in color image encryption[J]. Optics Communications,2009,284(9):2278-2291.

[10] ELABADY N F,ABDALDADER H M,MOUSSA M I,et al. Image encryption based on new one-dimensional chaotic map[C]// International Conference on Engineering and Technology. Berlin:Springer,2015:851-892.

[11] FU Chong,ZHU Zhiliang. A chaotic image encryption scheme based on circular bit shift method[C]// The 9th International Conference for Young Computer Scientists. New Jersey:IEEE Press,2013:3057-3061.

[12] SINGH H,YADAV A K,VASHISTH S,et al. Double phase-image encryption using gyrator transforms, and structured phase mask in the frequency plane[J]. Optics and Lasers in Engineering,2015,67(4):145-156.

[13] 陆安山,周小珠. 一个新三维混沌系统及其同步[J]. 河南师范大学学报(自然科学版),2008,36(1):66-68.

New 3D Chaotic Mapping and Its Application
in Digital Image Encryption

LIU Bing, PAN Dabing

(Department of Public Affairs Management, Dazhou Vocational and Technical College, Dazhou 635001, China)

Abstract: Based on the new 3D chaotic mapping and finite field operations, a new method of digital image encryption is constructed. Firstly, Lu mapping is used to map the original image information into two chaotic matrices. Secondly, the original image matrices and two generated chaotic matrices, are executing four rounds operations in the finite field. Experimental results show that the proposed encryption method can obtain uniform and fine scrambling effect. The evaluation of the histogram and three-direction correlation evaluation also has good encryption performance, and the encryption speed of the whole algorithm is also relatively fast.

Keywords: data image; image encryption; 3D chaotic mapping; three correlation; Lu mapping