doi: 103969/j. issn. 0490-6756. 2016. 01. 014

基于假分数阶激光混沌的数字图像加密研究

赵建峰[1], 王淑英[2], 李险峰[3], 张理涛[4]
(1. 河南职业技术学院信息工程系, 郑州 450046; 2. 黄河科技学院民族学院, 郑州 450053;
3. 香港城市大学土木建筑工程系, 香港 999077; 4. 郑州航空工业管理学院数理系, 郑州 450015)

摘 要: 为提高信息加密的安全性,设计了一种基于假分数阶激光混沌系统的加密算法,密钥空间由系统的初始状态变量、参数和分数阶次构成,且把所有明文像素值代入密钥,从而提高算法的抗破解能力. 数值模拟中对 Lena 灰度图和 Couple 彩色图等数字图像进行加密. 理论分析和数值仿真表明,该算法的加密空间大,可以有效抵抗密文攻击、差分攻击、选择明文攻击和统计攻击,在多媒体数据的安全通信中具有发展潜力.

关键词: 图像加密; 假分数阶; 激光混沌; 密钥
中图分类号: TP317.4 **文献标识码**: A **文章编号**: 0490-6756(2016)01-0079-08

Research on encryption of digital image based on improper fractional-order Laser chaos

ZHAO Jian-Feng[1], *WANG Shu-Ying*[2], *LI Xian-Feng*[3], *ZHANG Li-Tao*[4]
(1. Department of Information Engineering, Henan Polytechnic, Zhengzhou 450046, China;
2. Department of Nationalities, Huanghe Science and Technology College, Zhengzhou 450053, China;
3. Department of Civil and Architectural Engineering, City University of Hong Kong, Hong Kong 999077, China;
4. Department of Mathematics and physics, Zhengzhou Institute of Aeronautical Industry Management, Zhengzhou 450015, China)

Abstract: To improve the safety of information encryption, based on an improper fractional-order laser chaos, a digital image encryption algorithm is proposed. The key space is formed by initial state variables, parameters and orders of the system. Every pixel value is included in secret key, so as to improve anti-attack capability of the algorithm. Lena gray image and Couple color image are encrypted in numerical simulation. Theoretical analysis and simulation results show that this algorithm with a sufficiently large key space not only can perfectly resist the ciphertext attack and differential attack, but also is excellent against chosen plaintext attack and statistical attack, which can be used in secure communication of multimedia data.

Key words: Image encryption; Improper fractional-order; Laser chaos; Key

1 引 言

随着计算机技术的快速发展,网络成为通信和信息交换的重要途径,因此多媒体信息的安全通信问题亟待解决. 数字图像作为主要的信息载体,需要更加实用且安全的加密技术. 混沌系统对系统参数具有高度敏感性,并且所产生序列具有伪随机性等特点. 尽管在计算机的有效精度效应下,混沌序列在

收稿日期: 2015-02-04
基金项目: 国家自然科学基金(11161027,11262009,11501525); 国家自然基金数学天元基金(11226337); 中国航空科学基金(2013ZD55006)
作者简介: 赵建峰(1977—), 男, 河南淮阳人, 讲师, 研究方向为数字图像处理及应用. E-mail:zjfzwf@126.com

迭代中存在动态特征退化问题,但可采用提高计算精度、增加随机扰动、级联多个混沌和高维混沌等方法来缓解[1,2].因此使得其在密码学领域具有天然优势.20 世纪 80 年代末,英国数学家 Matthews 首次提出基于混沌序列的密码学[3].混沌映射的许多重要特征适用于数字图像加密[4-10].而分数阶混沌系统具有一切混沌系统和分数阶系统的特性,例如混沌系统的遍历性、初值敏感性和分数阶系统的历史记忆性等.同时分数阶混沌系统对于更加复杂的动力学系统和物理现象都可以有很好的描述.分数阶混沌系统已是广大专家学者的研究热点[11-14],胡建兵提出真分数阶系统和假分数阶系统的概念[15],假分数阶混沌系统(阶次大于 1)具有更大的密钥空间和复杂的随机序列,目前基于假分数阶的图像加密方面的研究很少,是一个很有研究价值的课题.

激光混沌不仅具有耗散系统的各种复杂现象,而且具有更多优良特性,如双稳、脉冲再现、接近理想模型、易于设计、固有的宽带混沌激光信号、类噪声和不可预测等特点,大大提高了光电侦察的困难,是光学信息安全的重要技术.Colet 于 1994 年提出了基于激光的数字通信技术[16],近年来有关激光混沌的研究越来越受欢迎[17-19],但鲜有关于假分数阶激光混沌的研究.

本文设计了一个假分数阶 Lorenz-Haken 激光混沌,随着阶数的变化,系统在很大范围内呈现出混沌特征,所产生的混沌序列具有良好的伪随机特性,基于此,提出一个数字图像加密算法,此算法优化了图像的加密效果且提高了抗破解能力.

2 Lorenz-Haken 激光混沌

洛伦兹—哈肯激光混沌系统[20]的分数阶形式的数学描述为:

$$\begin{cases} \dfrac{\mathrm{d}^{q_1}x}{\mathrm{d}t^{q_1}} = a(y-x) \\ \dfrac{\mathrm{d}^{q_2}y}{\mathrm{d}t^{q_2}} = bx - y - xz \\ \dfrac{\mathrm{d}^{q_3}z}{\mathrm{d}t^{q_3}} = xy - cz \end{cases} \tag{1}$$

其中,$X = (x,y,z)^T$ 是系统的状态变量;$(a,b,c)^T$ 表示参数向量;分数阶数为 q_1,q_2,q_3,如果 $\max(q_1,q_2,q_3) < 1$,称其为真分数阶系统,当 $q_1 = q_2 = q_3 = 1$ 时,称其为整数阶系统,当 $\max(q_1,q_2,q_3) > 1$,称其为假分数阶系统.根据分数阶稳定性理论和数值分析,当分数阶数 $q_1 = q_2 = q_3 = q \in [0.98,1.05]$,参数 $(a,b,c) = (1.4253,50,0.2775)$,初始状态 $(x_0,y_0,z_0) = (1,0,50)$,时间 $t \in [0,100s]$ 时,图 1(a)和(b)分别展示了分数阶激光混沌的相图和时间序列图.

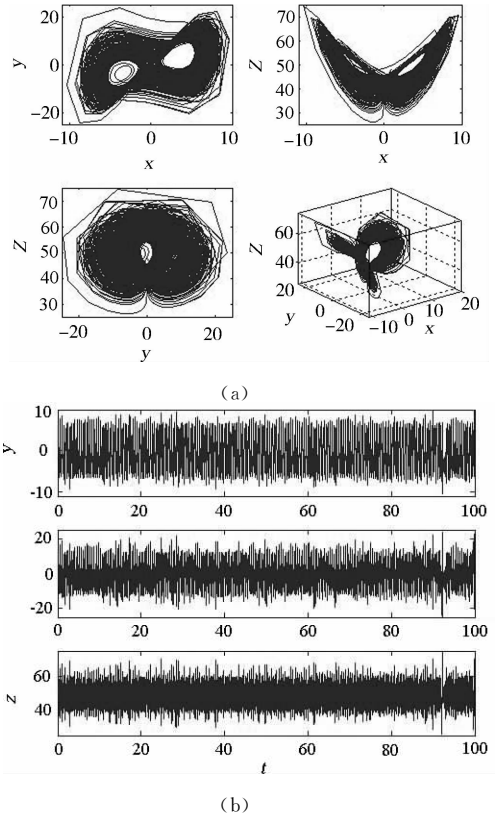


图 1 $q_1 = q_2 = q_3 = 1.013$ 时的假分数阶激光混沌系统
(a) 相平面图; (b) 混沌序列

Fig. 1 Improper fractional-order laser chaos when $q_1 = q_2 = q_3 = 1.013$
(a) Phase space; (b) Chaos sequences

3 算法描述

算法流程如图 2 所示.

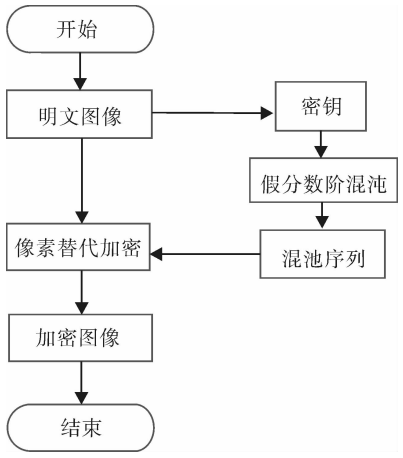


图 2 基于混沌的加密流程图

Fig. 2 Block diagram of the chaotic encryption algorithm

(1) 对大小为 $L = M \times N$ 的原始图像的像素值逐行排列为像素行矩阵 $P_{1\times L}$：

$$P = \begin{bmatrix} P(1) & P(2) & \cdots & P(N) \\ P(N+1) & P(N+2) & \cdots & P(2N) \\ \vdots & \vdots & \vdots & \vdots \\ P((M-1)N+1) & P((M-1)N+2) & \cdots & P(L) \end{bmatrix} \tag{2}$$

(2) 在明文图像像素值的干扰下生成混沌系统的初始变量和系统参数，而每次迭代都获得一组状态变量 $\{x,y,z\}$，接着组合状态变量，令 $m = \mathrm{mod}(\mathrm{abs}(x+y+z),3)$，首先定义空矩阵 B，接着按照表 1 扩充矩阵 B.

表 1　矩阵 B 的构成

Tab. 1　Component of matrix B

$m=0$	$m=1$	$m=2$
$B=\{B,x,y,z\}$	$B=\{B,z,x,y\}$	$B=\{B,y,z,x\}$

(3) 混沌序列中每个数据由整数和 15 位小数构成，由小数点后的第 $r,r+1,r+2$ 位的数字构成三位数的整数，接着按以下公式让其对数字 256 进行模运算，公式是 $K = \mathrm{mod}(\mathrm{fix}(B\times 10^r - \mathrm{fix}(B\times 10^r)\times 10^3),256)$　$(r \in Z^+, 1 \leqslant r \leqslant 15)$. 图 3 显示了序列 K 的自相关性接近 0，并且绝大多数数据集中在区间 $[-0.003, 0.003]$.

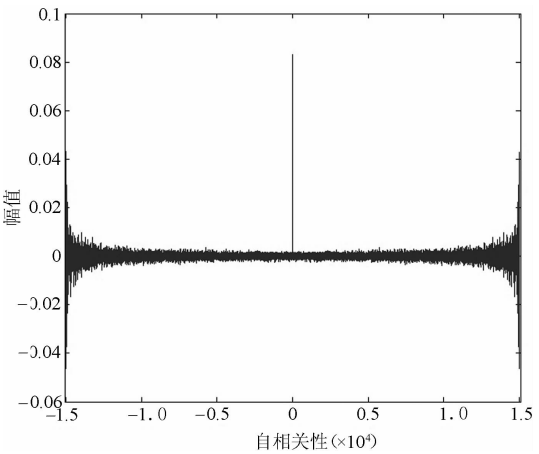


图 3　序列 K 的自相关性分析

Fig. 3　Self-correlation of sequence K

(4) 采用如下公式，逐像素对明文图像进行像素值替换加密：

$$\begin{cases} \mathrm{temp}(1) = \mathrm{mod}((P(L)+4) \oplus K(L+1),256) \\ \mathrm{temp}(i) = \mathrm{mod}(C(i-1) \oplus K(L+i),256), \ (i>1) \\ C(i) = \mathrm{mod}(P(i) \oplus K(i),256) \oplus \mathrm{temp}(i) \end{cases} \tag{3}$$

接着，把密文像素值序列 $\{C(i),\ i=1,2,\cdots,L\}$ 转换为 $M \times N$ 大小的矩阵，而后显示为密文图像 C.

而解密是加密的逆过程，公式如下：

$$\begin{cases} P(L) = \mathrm{mod}((\mathrm{temp}(1)+4) \oplus K(L+1),256) \\ \mathrm{temp}(i) = \mathrm{mod}(C(i-1) \oplus K(L+i),256), \quad (i>1) \\ P(i) = \mathrm{mod}(C(i) \oplus \mathrm{temp}(i) \oplus K(i),256) \end{cases} \tag{4}$$

4　统计分析

利用 Matlab 7.1 软件，对本文加密算法进行数值模拟. 原图采用大小为 256×256 的 8 位标准 Lena 灰度图、大小为 512×512 的 Boat 灰度图、大小为 256×256 的 Parrot 灰度图、大小为 199×199 的 Full-black 灰度图和大小为 256×256 的 Couple 彩色图，彩色图像的三基色为 RGB，每个基色都用 8 比特表示. 经过一轮像素值替代加密后，在图 4 (c)，(g))，(k)，(o)和图 5(e)～(h)所显示出的密图中已观察不到原图的主要特征.

4.1　灰度直方图分析

灰度直方图是体现图像像素的分布状况的最直观手段. 通过 Matlab 6.5 软件对原始图像和加密图像分别进行灰度直方图实验，可以得到各类灰度图及其密图的灰度直方图(如图 4)，而图 5 显示了 Couple 原始彩色图像及其加密图像，图 6 给出

Couple 原图和密图的灰度直方图,显然加密后图像的像素灰度分布发生了根本性改变,拥有很高的图像冗余性与伪随机性,灰度直方图呈平均分布,掩盖了加密前灰度分布规律,增加了破译的难度,从而可有效抵抗统计分析.

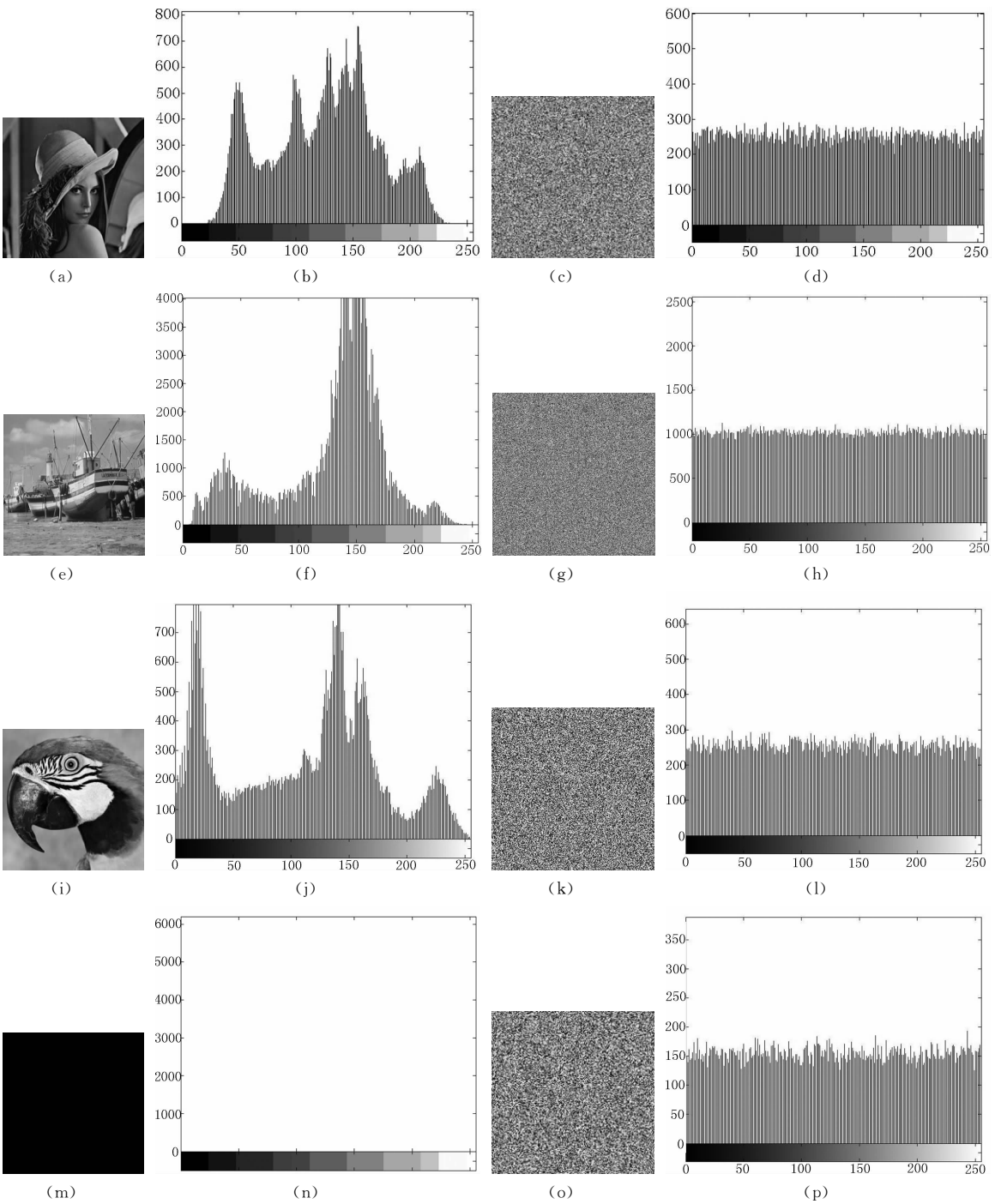
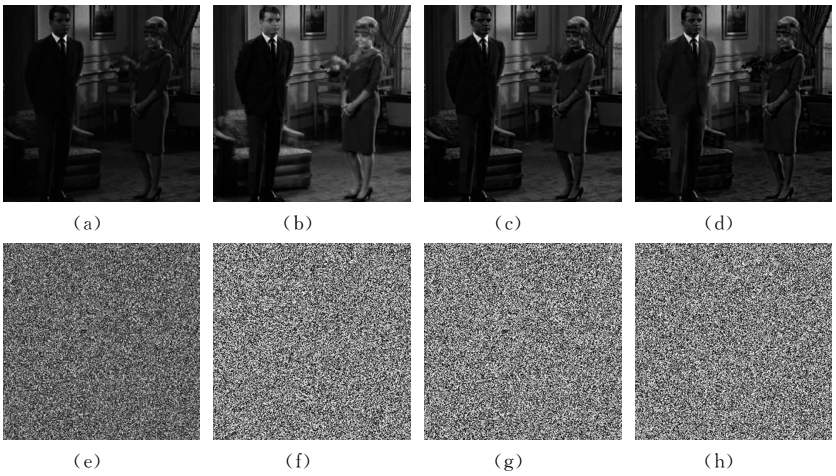


图 4 图像加密效果

(a), (e), (i)和(m)分别是 Lena, boat, parrot 和 full-black 原始图像; (b), (f), (j)和(n)是原图的直方图; (c), (g), (k) 和(o)是加密图像; (d), (h), (l) 和 (p)是密图的直方图

Fig. 4 Effect of image encryption

(a), (e), (i) and (m) depicts original images Lena, boat, parrot and full-black, respectively; (b), (f), (j) and (n) show histogram of the original images; (c), (g), (k) and (o) show the encrypted images; (d), (h), (l) and (p) show histogram of the encrypted images

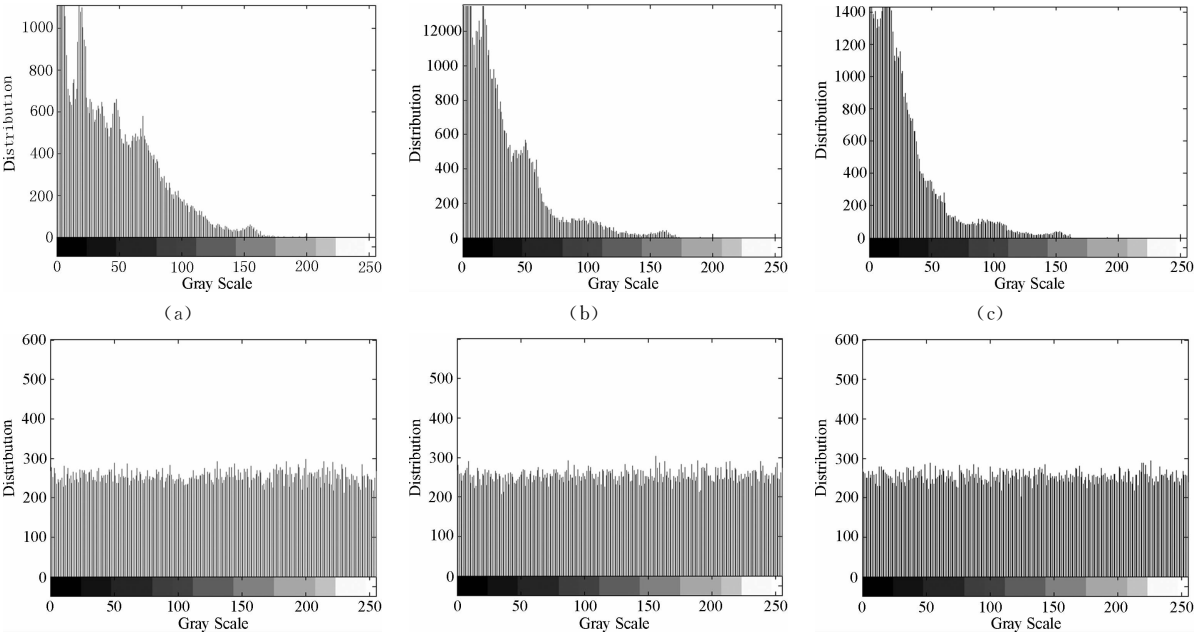


(a)　(b)　(c)　(d)

(e)　(f)　(g)　(h)

图 5　Couple 彩色原图及其 RGB 层分量(a~d)，彩色 Couple 密图及其 RGB 层分量(e~h)

Fig. 5　Effect of Couple image encryption for color couple in red, green and blue component



(a)　(b)　(c)

(d)　(e)　(f)

图 6　Couple 原图和密图的直方图

(a)原图 R 分量；(b)原图 G 分量；(c)原图 B 分量；(d)密图 R 分量；(e)密图 G 分量；(f)密图 B 分量

Fig. 6　Histograms corresponding of color Couple:

(a) red component of plain image; (b) green component of plain image; (c) blue component of plain image; (d) red component of encrypted image; (e) green component of encrypted image; (f) blue component of encrypted image

4.2　相邻像素相关性分析

相邻像素的相关性是衡量加密算法性能的一个重要指标. 首先，从原图和密图中随机选取 4×10^4 对相邻像素来考察其相关性，然后利用以下公式分别从水平方向、垂直方向和对角方向计算相关系数：

$$\begin{cases} E(x) = \dfrac{1}{N}\sum_{i=1}^{N} x_i \\ D(x) = \dfrac{1}{N}\sum_{i=1}^{N}[x_i - E(x)]^2, \\ \mathrm{Conv}(x,y) = \dfrac{1}{N}\sum_{i=1}^{N}[x_i - E(x)][y_i - E(y)], \\ R_{xy} = \dfrac{\mathrm{Conv}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}. \end{cases} \tag{5}$$

其中，x，y 表示图像中两相邻像素点的灰度值. 图 7 表示原图和密图在水平、垂直和对角方向相邻像素的相关性分布，从表 2 中可以看出，原图的相邻像素高度相关，相关系数接近于 1，而密图的相邻像素的相关系数接近于 0，也即加密后图像的相邻像素值较为均匀的分布到了整个像素值空间，相邻像素值不仅仅在低值空间均匀分布，在高值空间也同样均匀分布. 文中密钥考虑到了明文像素值的影响，针对经典 Lena 灰度图的相关系数，在表 2 中与其他算法[21−23]的结果进行比较，可见本文算法的加密效果较好，明文统计特性被随机扩散到密图中，并且加密后的图像灰度分层现象消失，因而图像的相邻像素相关性大大减弱.

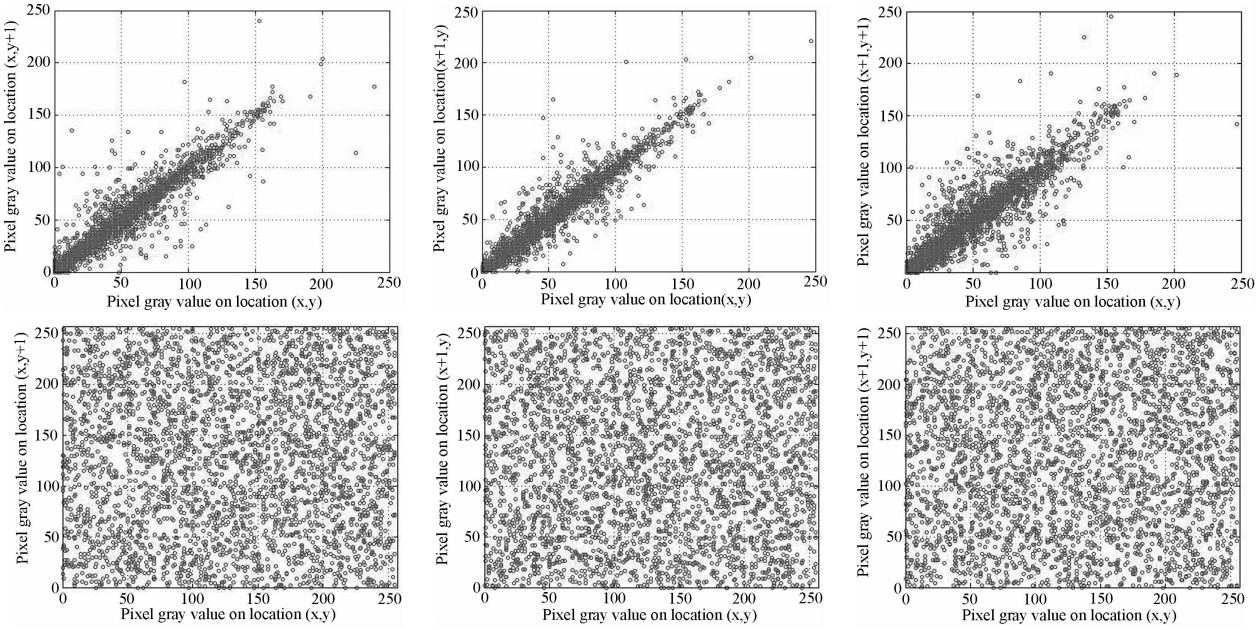


图 7 彩色 Couple 图及其密图的 R 层分量在水平方向、垂直方向及对角方向的相关性

Fig. 7 Distributions of horizontally, vertical and diagonal adjacent pixels of Red components in the plain Couple color image and its encrypted image

表 2 原图和密图中相邻像素的相关系数

Tab. 2 Correlation coefficient of two adjacent pixels in plain images and encrypted images

图像		水平方向	垂直方向	对角方向
彩色 Couple 原始图像	红色	0.9549035	0.964611	0.924501
	绿色	0.939104	0.958165	0.912766
	蓝色	0.935288	0.952165	0.90741
彩色 Couple 加密图像	红色	-1.542874×10^{-5}	3.116206×10^{-5}	-8.973568×10^{-5}
	绿色	-8.959178×10^{-5}	-6.721899×10^{-5}	-8.973533×10^{-5}
	蓝色	5.853481×10^{-5}	4.821585×10^{-5}	4.706159×10^{-5}
Lena 加密图像	本文	3.302087×10^{-5}	-2.139538×10^{-5}	6.420161×10^{-6}
	文献[21]	−0.7963925	0.01661560	0.00327795
	文献[22]	0.0008213	0.0008423	0.0005083
	文献[23]	−0.000072	0.002121	−0.000111
Boat 灰度图	原图	0.840268	0.943302	0.870957
	密图	6.869908×10^{-4}	-1.048962×10^{-5}	-9.487573×10^{-4}
Parrot 灰度图	原图	0.963618	0.941931	0.884591
	密图	-5.331198×10^{-4}	3.857585×10^{-4}	4.079463×10^{-5}
Full-black 灰度图	原图	1	1	1
	密图	8.296476×10^{-4}	4.559433×10^{-5}	2.372701×10^{-5}

4.3 信息熵

信息熵用于度量图像中灰度值的分布情况，图像信息熵越大，说明图像中灰度分布越均匀. 信息熵的计算表达式如下：

$$H(x) = -\sum_{i=1}^{n} p(x_i)\log_2 p(x_i) \tag{6}$$

其中，$p(x_i)$ 为图像像素值 x_i 出现的频率. 当所有灰度值出现的频率完全一样时，信息熵达到最大值 8. 表 3 显示出加密图像的信息熵都超过 7.98，虽 Lena 灰度图的信息熵与其它参考文献的相比略小，但是基本接近于 256 级灰度图像信息熵的最大值 8，可见，经本文加密算法后的各类加密图像的灰度分布非常均匀，攻击者要想通过像素值变化的统计分析来攻击加密方案极其困难，此加密算法的安全性较高.

表 3　原图和密图的信息熵

Tab. 3　The entropy of plain images and encrypted images

图像		原图信息熵	密图信息熵
Couple 彩色图	红色层分量	6.727885	7.9888430
	绿色层分量	6.257179	7.988776
	蓝色层分量	6.118510	7.989296
Lena 灰度图	本文	7.447144	7.989673
	文献[21]		7.9895792
	文献[22]		7.9979
	文献[23]		7.9976
Boat 灰度图		7.191316	7.991031
Parrot 灰度图		7.651075	7.989086
Full-black 灰度图		0	7.988011

4.4 抗差分能力分析

差分分析是一种选择明文攻击，其基本思想是：通过分析明文对的差值对密文对的差值的影响来恢复某些密钥比特. 度量差分攻击的两个常用性能指标是像素数变化率 NPCR (Number of Pixels Change Rate)和归一化像素值平均变化强度 UACI (Unified Average Changing Intensity)，具体计算公式如下：

$$\begin{cases} D(i,j) = \begin{cases} 0, & C_1(i,j) = C_2(i,j), \\ 1, & C_1(i,j) \neq C_2(i,j). \end{cases} \\ NPCR = \dfrac{1}{M \times N}\displaystyle\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j) \times 100\%, \\ UACI = \dfrac{1}{255 \times M \times N}\displaystyle\sum_{i=1}^{M}\sum_{j=1}^{N} |C_1(i,j) - C_2(i,j)| \times 100\% \end{cases} \tag{7}$$

其中，$C_1(i,j)$ 和 $C_2(i,j)$ 表示两幅大小均为 $M \times N$ 的加密图像在点 (i,j) 处的像素值，M 和 N 分别表示原始图像像素的行数和列数.

NPCR 和 UACI 的理想期望值可用以下公式计算：

$$\begin{cases} NPCR_E = (1 - 2^{-n}) \times 100\%, \\ UACI_E = \dfrac{1}{3}(1 + 2^{-n}) \times 100\%. \end{cases} \tag{8}$$

其中，n 是图像颜色位数. 由(8)可知 $NPCR_E + 3UACI_E = 2$，对于 $n = 8$ 的灰度图像，$NPCR_E = 99.6094\%$，$UACI_E = 33.4635\%$，所以 $NPCR_E$ 或者 $UACI_E$ 都可用来说明算法的抗明文攻击能力.

以 Lena 灰度图为例，当原始图像的某个像素值仅仅改变一个字节时，所生成两幅密图的 $NPCR = 99.6290\%$ 和 $UACI = 33.4507\%$，非常接近理想值，表明本文算法具有较强的抗差分攻击能力.

4.5 密钥空间分析

分数阶混沌的初始变量、参数和分数阶次构成了加密系统的密钥，由于计算机精度的问题，精确到小数点后的 15 位，密钥空间达到 $(10^{16})^9 \approx 2^{478}$，即密钥长度相当于 478 比特，已经基本满足密钥长度的要求.

5 结束语

本文首次给出分数阶形式的 Lorenz-Haken 激光混沌，并采用其假分数阶形式对彩色 Couple 图和经典灰度 Lena 图进行一轮像素值替代加密，明文的最后一个像素值影响第一个像素的加密，而后每一个像素的加密都受明文其他像素的影响，该算法在保证加密算法安全性的前提下，没有置乱操作，并且只有一次像素值替代加密，从而有效减少了加密时间，数值模拟结果表明，该算法的抗统计能力和抗差分攻击能力较强.

参考文献：

[1] 周红. 有限精度混沌系统的 m 序列扰动实现 [J]. 电子学报，1997，225(7)：95.

[2] 张雪峰，范九伦. 基于线性反馈移位寄存器和混沌系统的伪随机序列生成方法 [J]. 物理学报，2010，59(4)：2289.

[3] Matthews R. On the derivation of a chaotic encryption algorithm [J]. Crypto Logia，1989，13(1)：29.

[4] Chen G, R Mao Y B, Chui C K. A symmetric image encryption scheme based on 3D chaotic cat maps [J]. Chaos Soliton Fract, 2004, 21(3):749.

[5] Zhou Q, Wong K W, Liao X F, *et al*. Parallel Image Encryption Algorithm Based on Discretized Chaotic Map [J]. Chaos Soliton Fract, 2008, 38(4): 1081.

[6] Yang H Q, Wong K W, Liao X F, *et al*. A fast image encryption and authentication scheme based on chaotic maps [J]. Commun Nonlinear Sci Numer Simulat, 2010, 15(11): 3507.

[7] 朱从旭, 孙克辉. 对一类超混沌图像加密算法的密码分析与改进 [J]. 物理学报, 2012, 61(12): 120503.

[8] Wang X Y, Liu L T. Cryptanalysis and improvement of a digital image encryption method with chaotic map lattices [J]. Chin Phys B, 2013, 22(5): 50503.

[9] Ye G D. A block image encryption algorithm based on wave transmission and chaotic systems [J]. Nonlinear Dynam, 2014, 75(3): 417.

[10] 官国荣, 吴成茂, 贾倩. 一种改进的高性能 Lorenz 系统构造及其应用 [J]. 物理学报, 2015, 64(2): 020501.

[11] 刘晓君, 李险峰, 杨丽新, 等. 带有未知参数的改进半导体激光器的自适应同步与反同步 [J]. 四川大学学报: 自然科学版, 2012, 49(1): 168.

[12] 张凡弟. 不同维数分数阶混沌系统的 Q-S 同步 [J]. 四川大学学报: 自然科学版, 2014, 51(2): 381.

[13] 王雅庆, 周尚波. 基于分数阶陈氏混沌系统的图像加密算法 [J]. 计算机应用, 2013, 33(4): 1043.

[14] 赵建峰, 王淑英, 张理涛, 等. 基于分数阶超混沌的新图像加密算法 [J]. 四川大学学报: 自然科学版, 2014, 51(5): 958.

[15] 胡建兵, 肖建, 赵灵冬. 假分数阶 Chen 混沌系统同步 [J]. 上海大学学报: 自然科学版, 2011, 17(6): 734.

[16] Colet P, Roy R. Digital communication with synchronized chaotic lasers [J]. Opt Lett, 1994, 19(24): 2056.

[17] Wu L, Zhu S. Multi-channel communization using chaotic synchronization of multi-mode lasers [J]. Phys Rev A, 2003, 308(2-3): 157.

[18] Buldu J M, arcia-Ojjalvo J G, Torrent M C. Multimode synchronization and communication using unidirectionally coupled semiconductor lasers [J]. IEEE J Quantum, 2004, 40(6): 640.

[19] Chu Y D, Li X F, Zhang J G, *et al*. Nonlinear dynamics analysis of a modified optically injected semiconductor lasers model [J]. Chaos Soliton Fract, 2009, 41(1): 14.

[20] 罗晓曙. 混沌控制、同步的理论与方法及其应用 [M]. 1 版. 桂林: 广西师范大学出版社, 2007.

[21] Huang X L, Ye G D. An image encryption algorithm based on hyper-chaos and DNA sequence [J]. Multimed Tools Appl, 2014, 72(1): 57.

[22] Norouzi B, Seyedzadeh S M, Mirzakuchaki S, *et al*. A novel image encryption based on hash function with only two-round diffusion process [J]. Multimedia Syst, 2014, 20(1): 45.

[23] Zhu C X, Liao C L, Deng X H. Breaking and improving an image encryption scheme based on total shuffling scheme [J]. Nonlinear Dyn, 2013, 71(1-2): 25.