

引用格式: 魏慧, 李国东, 许向亮. 基于改进的复合混沌系统的图像加密算法[J]. 微电子学与计算机, 2020, 37(4): 19-25.
[WEI H, LI G D, XU X L, et al. Image encryption algorithm based on improved complex chaotic system [J]. Microelectronics & Computer, 2020, 37(4): 19-25.]

基于改进的复合混沌系统的图像加密算法

魏 慧, 李国东, 许向亮

(新疆财经大学 统计与数据科学学院, 新疆 乌鲁木齐 830012)

摘 要: 针对单一混沌系统加密不足的问题; 主要提出的算法是基于改进的 LCL 复合混沌系统和 DFT 变化的图像加密算法. 首先对图像 DFT 变换, 应用高维 Lorenz 系统产生的混沌序列进行随机组合排列, 将得到的一组索引序列结合改进的 Cat 系统对明文图像进行置乱; 其次, 采用超 Lorenz 混沌系统设计得到 Logistic 映射的伪随机序列, 将其进行异或处理得到密文图像; 为了达到加密效果更优良的目的, 重复以上步骤进行循环加密处理. 仿真结果表明本文设计算法具有优良的加密效果, 密钥空间大、明密文敏感性强、能有效抵抗统计攻击等.

关键词: 二维离散傅里叶变换; 混沌映射; 信息熵; 图像加密

中图分类号: TP309.7

文献标识码: A

文章编号: 1000-7180(2020)04-0019-07

Image encryption algorithm based on improved complex chaotic system

WEI Hui, LI Guo-dong, XU Xiang-liang

(School of Statistics and Data Science, Xinjiang University of Finance and Economics, Urumqi 830012, China)

Abstract: Aiming at the problem of insufficient encryption of a single chaotic system, the main proposed algorithm is an image encryption algorithm based on improved LCL composite chaotic system and DFT variation. Firstly, DFT transformation of images is carried out, chaotic sequences generated by high-dimensional Lorenz system are randomly combined and arranged, and a group of obtained index sequences are combined with an improved Cat system to scramble plaintext images; Secondly, the pseudo-random sequence of Logistic map is designed by using hyper-Lorenz chaotic system, and the encrypted image is obtained by XOR processing. In order to achieve better encryption effect, repeat the above steps for cyclic encryption. The simulation results show that the algorithm designed in this paper has excellent encryption effect, large key space, strong sensitivity to plaintext, and can effectively resist statistical attacks.

Key words: 2-D discrete Fourier transform; Chaotic mapping; Information entropy; Image encryption

1 引言

由于图像信息其本身的数据相关性强和数据冗余等特点, 传统的加密算法不再适用于数字图像加密体系. 国内外的诸多学者在数字图像加密的领域中提出了一系列不同类型、成果优良的加

密算法设计^[1-6], 汪乐乐等^[7]在 Henon 映射与 Logistic 混沌系统相结合的基础上对其改进升级, 并以游程性序列为基础, 将优化后的 H_L 算法应用于图像加密. 赵国敏等^[8]在广义的 Henon 映射与 CNN 神经网络相结合的基础上, 采用复合混沌生成的超混沌序列进行加密处理, 谢国波等^[9]针对

Arnold 变换存在周期性的弊端,设计出一种基于 Arnold 分层循环变换和混沌映射结合的数字图像加密算法. 基于以上分析,在保障混沌映射算法完备的基础上,本文提出了一种改进的 Lorenz-Cat 置乱系统与 Logistic 混沌扩散系统映射对 DFT 变换的图像加密算法.

2 混沌系统模型

傅里叶变化在线性系统分析中是一个有力分析工具,它能完成图像从空域到频域转化,从而使我们能更加定量地分析类似数字化系统、采样点、噪声、现实点等的效用.

(1)二维离散傅里叶变换的定义

对二维连续傅里叶变换在二维坐标上进行信息提取,对空域的取样间隔分别是 Δx 和 Δy ,对频域的取样间隔为 Δu 和 Δv ,它们的关系为:

$$\Delta u = \frac{1}{N\Delta x}, \Delta v = \frac{1}{N\Delta y} \tag{1}$$

式中, N 是在图像一个维上的总数. 则,二维离散傅里叶变换如下:

$$F(u,v) = \frac{1}{N^2} \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} f(x,y) \exp[-j2\pi(ux + vy)/N]$$

$$f(x,y) = \frac{1}{N^2} \sum_{u=0}^{N-1} \sum_{v=0}^{N-1} F(u,v) \exp[j2\pi(ux + vy)/N] \tag{2}$$

式中, $u,v = 0,1,\dots,N-1; n = 0,1,\dots,N-1$.

(2)Logistic 混沌系统

一类十分简单却被广泛应用的虫口模型: Logistic 映射,是剖析动力系统、混沌、分形等复杂系统的一种经典模型^[10]. 换言之虫口模型就是一个时间离散的动力系统.

Logistic 混沌映射定义:

$$x_{t+1} = \mu x_t(1 - x_t) \tag{3}$$

式中, $x_t \in (0,1)$, 当 $\mu = [3.5699456, 4]$ 时,系统处于混沌状态. 表明初始条件 x_0 在 Logistic 映射的作用下所生成的混沌序列是不收敛的、无周期律的且对初值十分敏感. Logistic 映射因 μ 值的不同而产生不同的混沌特性如图 1. 从图 1 可以明显观察到随着 μ 值的改变,不断呈现出倍周期分岔的现象,直到出现混沌状态. 该混沌系统具有正的李雅普诺夫指数,表明其处于混沌状态,如图 2 所示.

(3)超混沌 Lorenz 系统

Lorenz 混沌系统的定义方程如下:

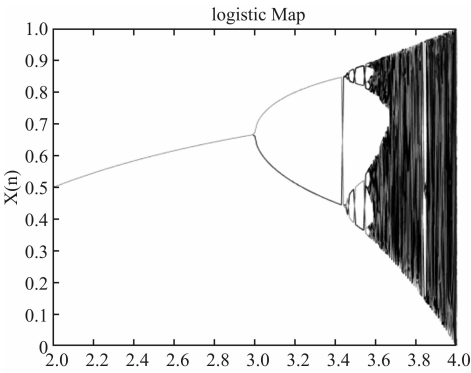


图 1 Logistic 分岔图

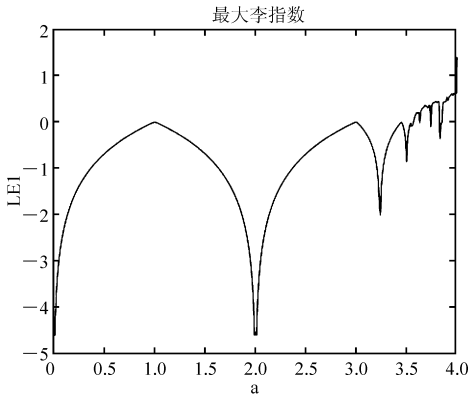


图 2 Logistic 李雅普诺夫指数图

$$\begin{cases} \dot{x} = a(y - x) + w \\ \dot{y} = cx - y - xz \\ \dot{z} = xy - bz \\ \dot{w} = -yz + rw \end{cases} \tag{4}$$

式中, $a = 10, b = \frac{8}{3}, c = 28, -1.52 \leq r \leq -0.06$ 时,式(4) 处于混沌状态. 当 $r = -1$,式(4) 的 4 个 Lyapunov 指数依次是 $\lambda_1 = 0.3381, \lambda_2 = 0.1586, \lambda_3 = 0, \lambda_4 = 15.1752$

(4)改进的 Cat 系统

经典的 Cat 变换^[11]是一个二维可逆映射,可表示为:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = A \begin{bmatrix} x \\ y \end{bmatrix} \bmod \begin{bmatrix} M \\ N \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \end{bmatrix}, A = \begin{bmatrix} 1a & \\ & bab + 1 \end{bmatrix} \tag{5}$$

上式中, $0 \leq x, y \leq 1, 0 \leq x', y' \leq 1$.

改进后的 Cat 映射:

$$\begin{bmatrix} x \\ y \end{bmatrix} = A' \begin{bmatrix} 1 \\ j \end{bmatrix} \bmod \begin{bmatrix} M \\ N \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \end{bmatrix}, A' = \begin{bmatrix} 1a & \\ & ba \end{bmatrix} \tag{6}$$

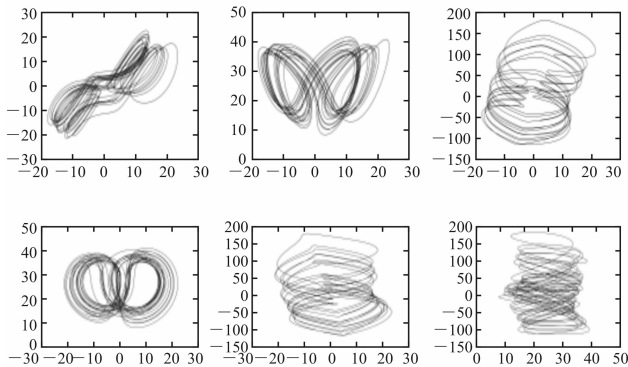


图3 超混沌 Lorenz 系统不同平面的相位图

3 算法设计

通常对图像进行加密的方法普遍只采用单一混沌系统进行图像的加密处理,这种方法仍存在被破译的危险,但将多种混沌映射的方法^[12-13]组合在一起进行图像加密处理,那么被破译的可能性大大降低,提高了加密信息的安全级别.基于此,本文提出的算法是一种改进的复合多重混沌算法.

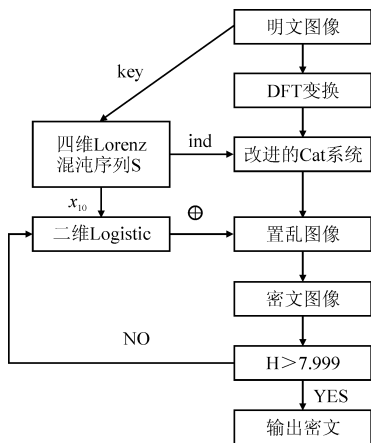


图4 算法流程图

本文提出的图像加密算法的主要步骤如下.一般,图像大小为 $M \times N$,设 P 表示大小为 $M \times N$ 的经典lenna彩色图像, $P(i, j)$ 表示明文图像第 i 行第 j 列处像素值大小.

3.1 像素置乱

Step1:将明文图像转换为 $M \times N$ 阶灰度图像,此时图像像素值属于 $[0, 255]$ 之间.

Step2:与明文图像相关的密钥生成:由式(7)可得到 P 的像素灰度值和为 sum ,式(8)、(9)可得超混沌 Lorenz 系统的初置值 x_0, y_0, z_0, w_0 .

$$sum = \sum_{i=1}^m \sum_{j=1}^n (P(i, j) + i + j) \quad (7)$$

$$\mu_1 = \text{mod}(sum, M * N) \quad (8)$$

$$\begin{cases} x_0 = \frac{\text{mod}(u_1 * 10^6, M)}{100} \\ y_0 = \frac{\text{mod}(u_1 * 10^7, M)}{100} \\ z_0 = \frac{\text{mod}(u_1 * 10^8, M)}{100} \\ w_0 = z_0 - y_0 \end{cases} \quad (9)$$

Step3:选定合适的参数和步骤1中的初始值,输入到超混沌 Lorenz 系统中,通过 Runge - Kutta 算法将混沌系统进行反复迭代,首先迭代次数为 N_0 次以消除暂态效果,然后迭代 N 次,可得到长度为 N 的四组混沌序列 x_k, y_k, z_k, w_k ,其中 $k = (1, 2, 3, \dots, N)$.

Step4:从步骤3得到的四组混沌序列 x_k, y_k, z_k, w_k 中,通过式(10)得到长度为 $2 * M * N$ 的序列,截取两组长 $M * N$ 的随机组合序列,记为 ind_s .并通过冒泡的方法将组合混沌序列从小到大排序.

以序列 w, x 为例,设 $w_{s1} = \{w_1, w_2, \dots, w_{M * N}\}$, $x_{s2} = \{x_{M * N + 1}, \dots, x_{2 * M * N}\}$,则 $ind = \{w_{s1}, x_{s2}\}$.即组合序列 ind 为式(6)中的伪随机向量 a, b .

$$S_i = \text{mod}(\text{floor}((s_i + 100) * 10^{10}), 10 * \max(M, N)) + 1 \quad (10)$$

式中, s_i 为四组混沌序列 x_k, y_k, z_k, w_k .

Step5:将明文图像 P 转化为一维行向量,记为 O ,大小为 $M * N$.对向量 O 的任意坐标位置 $(1, j)$ 进行 Cat 变换,达到新的坐标位置 (p, q) ,即由(6)式对明文图像置乱操作,得到置乱密文图像.

3.2 像素扩散

Step1:将 Lorenz 超混沌系统映射迭带过程中产生的 x_k, y_k, z_k, w_k 随机选取4位数值,并由式(11)进行量化,再由(12)式处理得到的参数作为 Logistic 映射的初始值.

$$x_l = \text{mod}((((\text{abs}(x_k + y_k + z_k + w_k) - \text{floor}(\text{abs}(x_k + y_k + z_k + w_k)))/4) * 10^{14}), M) \quad (11)$$

$$x_{l0} = \sin(x_l) \quad (12)$$

Step2:Logistic 映射先迭代 N_0 次防止过渡效应,再迭代 $2 * M * N$ 次产生混沌序列

$$S = \text{mod}(\text{floor}(s * 2^{16})), N).$$

Step3:将置乱后的图像像素值展开为一维向量序列 $O_i (i = 1, 2, \dots, M * N)$,设加密序列为 $C_i (i = 1, 2, 3, \dots, M * N)$.对置乱后的中间密文根据式(13),

(14) 进行正逆向扩散加密处理. 当加密第一个像素时,可以给定一个初始参数 $C_0 \in (0,256)$.

$$C_i = C_{i-1} \oplus S_i \oplus O_i \tag{13}$$

$$C_i = C_{i+1} \oplus S_i \oplus O_i \tag{14}$$

Step4: 为了实现明文图像经过置乱、基于异或运算的扩散处理,得到优良的加密效果,同时防止加密算法过多的循环,本文利用密文图像的信息熵作为评价加密效果的判断条件.

信息熵反应了图像的不确定性,通常认为,熵越大,不确定性越大(信息量越大),可视信息越少.

$$H = - \sum_{i=0}^L p(i) \log_2 p(i) \tag{15}$$

式中, $p(i)$ 为图像灰度 i 出现的概率.

Step5: 重复上述过程,循环加密 T 次,完成加密.

Step6: 图像解密是图像加密过程的逆运算. 对明文图像先进行正向和逆向扩散的逆运算处理,之后进行反置乱,即可恢复原图.

4 实验仿真及性能分析

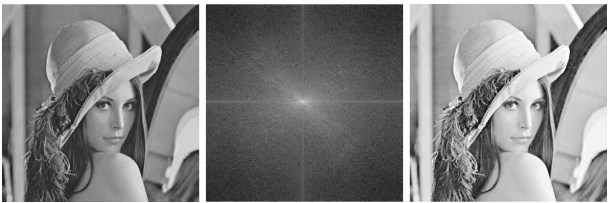
4.1 实验仿真

基于上述的加密算法,在仿真实验中选择大小为 512×512 的 Lenna 图像作为明文(加密中的原图像),其中超混沌 Lorenz 系统映射的初值 $x_0 = 2.195\ 981\ 145\ 3$, $y_0 = 1.479\ 814\ 453\ 1$, $z_0 = 4.558\ 144\ 531\ 2$, $w_0 = 3.078\ 330\ 078\ 1$ 设定内部参数为 $a = 10, b = 8/3, c = 28$, Logistic 混沌映射的初始参数为: $\mu = 4$, 初值取为 $x_{l\ 0} = 0.2, C_0 = 0, N_0 = 800$. $sum = 326\ 787\ 86, T = 1$. 依据上述加密算法,利用 MATLABR2017a 运行,得到如下结果如图 5、图 6,图 7 可以看到整幅加密图像是完全杂乱的,无法辨识. 其中图 5 中的(a)(b)为原始彩色图像变换为灰度图像(明文图像).



(a) 原始图像 (b) 明文图像

图 5 图像变换



(a) 明文图像 (b) 二维离散傅里叶变换 (c) 图像恢复

图 6 图像变换

4.2 性能分析

(1) 抗统计性能分析

图 7 给出了明密文图像灰度直方图,图 7 的[2, 1, 1]与[2, 1, 2]是明文图像的灰度像素直方图; [2, 2, 1]与[2, 2, 2]是加密图像的灰度像素直方图,可见加密后的图像的像素值整体分布平均,与原始图像中像素分布相比显著不同存在差异,说明加密后的图像能够很好的抵抗基于统计分析的攻击.

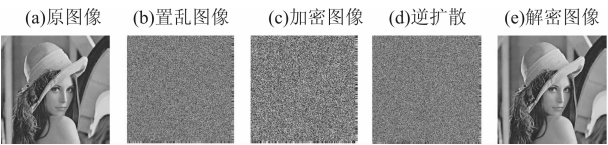


图 7 明密文灰度直方图

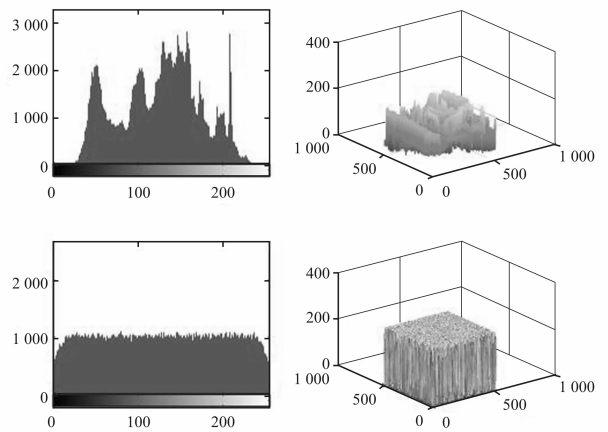


图 8 加密

(2) 明文图像和密文图像相关性分析

所谓相关性是两组随机变量之间在某个方向上的线性相关程度. 本文则分别随机选取 3000 对明文与密文中相邻的像素点通过式(16), 计算明文图像与密文图像上四个不同方向的相邻像相关系数进行对比分析, 其中对角线方向则以正反两个方向相邻像素进行分析, 并与文献[14]进行比较. 分析结果如下表 1、图 9、图 10 所示.

从图 9 中可知, 本文选取的明文图像相邻像素

间具有很强的线性关系,且由表 1 知,明文关系系数图中像素点之间的分布斜率趋近于 1. 而密文图像的相邻像素分布十分均匀、无序、分散,且像素值之间的分布斜率值极小,趋近于 0,并且与文献[14]相比较本文算法的相关系数值 ρ_{xy} 更小,说明达到更好的加密效果.

$$\rho_{xy} = \frac{\text{cov}(x,y)}{\sqrt{D(x) \cdot D(y)}}$$

(16)

表 1 相邻像素相关性系数

方向	明文	密文	密文 ^[4]
水平	0.983 2	0.006 2	0.008 9
垂直	0.974 1	−0.008 9	0.007 5
正对角	0.949 6	−0.007 4	0.001 6
反对角	0.961 7	−0.013 4	

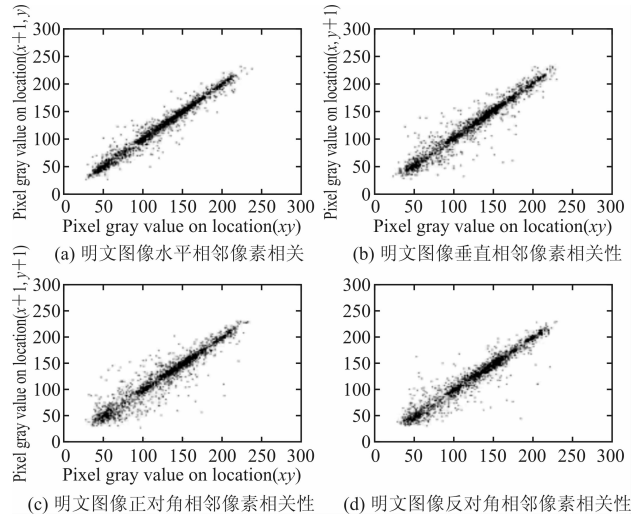


图 9 明文图像相邻像素分布图

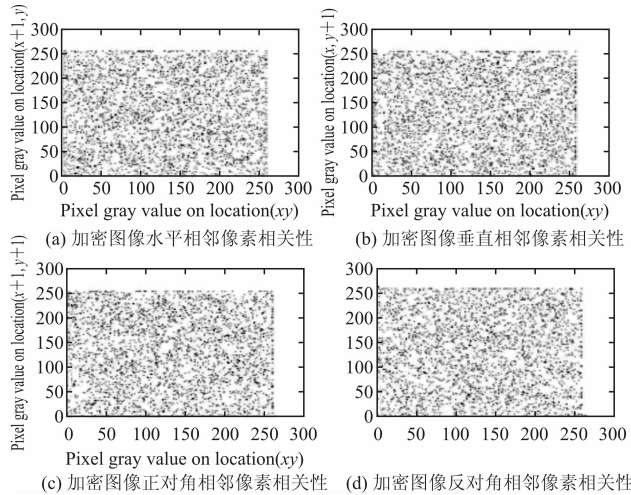


图 10 密文图像相邻像素分布图

4.3 密钥空间分析

本文加密算法采用基于 DFT 变换和改进的复合混沌循环加密算法对图形进行加密. 改进的超混沌 Lorenz—Cat 映射置乱算法的密钥采用双精度运算. 改进的超混沌 Lorenz—Cat 系统映射中的控制参数 x_0, y_0, z_0, w_0 密钥空间为 10^{40} . 中间密文像素扩散算法中 Logistic 映射的初始值 x_{10} , 密钥空间也为 10^{10} . 且式(3)与式(4)的控制参数 u, a, b, c, r , 也可作为密钥. 本文加密算法的密钥空间 $\gg 2^{200}$, 十分有效地抵抗了穷举攻击破解本文加密算法, 增强了算法的安全性, 确保图像的安全传输.

(1) 密钥敏感性分析

密钥敏感性分析指当密钥发生细微的变化时, 加密相同的明文图像得到的两个密文图像之间的差异情况. 如果两个密文图像具有显著的差别, 就称该图像密码系统的密钥敏感性强; 如果两个密文图像的差别较小, 则称密钥敏感性较差. 因本文算法密钥参数较多且与明文紧密相关, 故随机选择秘钥之一进行密钥的敏感性分析.

密钥选取为超 Lorenz 混沌系统映射的内部密钥 r 减少到 -2 , 解密时将会发生错误, 如图 11 所示.

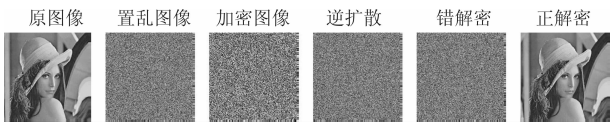


图 11 解密

(2) 明文敏感性分析

明文敏感性分析则表示当图像像素灰度值发生十分细微的变化时, 加密后的图像产生的截然不同的变化. 产生变化的分析指标一般用 NPCR(像素变化率)和 UACI(归一化像素平均值)来衡量.

$$NPCR(P_1, P_2) = \frac{1}{M \times N} \sum_{i=1}^M \sum_{j=1}^N | \text{Sign}(P_1(i, j) - P_2(i, j)) | \times 100\%$$

(17)

$$UACI(P_1, P_2) = \frac{1}{M \times N} \sum_{i=1}^M \sum_{j=1}^N (| P_1(i, j) - P_2(i, j) |) \div 255 \times 100\%$$

(18)

P_1 表示密文, P_2 表示明文图像像素值发生改变了的密文. 随机选取明文图像中的一点坐标, 将其进行微小变动, 如像素点(6,106)转化为(6,113), 由式(17)和(18)可知, 此时 $UACI = 33.535\%$ $NPCR = 99.633\%$. 综上, 本文的算法对明文具有很好的抗差分攻击能力.

表 2 NPCR 与 UACI

	本文算法	文献[14]算法
NPCR	0.996 5	0.996 1
UACI	0.336 2	0.334 6

(3)信息熵的分析

由信息熵定理知,它旨在描述信息的不确定性,反映的是图像中灰度分布情况.理论上,在理想状况下密文图像的信息熵值无限趋于 8. 为了分析本文加密算法抵御熵攻击性能,通过式(15)对本文加密算法的密文进行测试,并与相关文献对比分析,结果如下表所示.

表 3 信息熵

	明文	密文	密文[14]	密文[15]
H	7.431 0	7.999 3	7.967 6	7.889 2

由表 3 可知,本文算法相比较文献[14][15]信息熵值更接近于理想值,具有更强的能力抵御熵攻击.

(4)PSNR 分析

峰值信噪比 PSNR 用来评价处理后的图像与原始图像之间对应像素点间的误差指标.其值越大,表明图像失真就越小. 再此,也选择均方根误差 PMSE 这一指标对其进行分析.

$$PSNR = 10 \log_{10} \frac{M * N * 255^2}{\sum_{i=1}^M \sum_{j=1}^N (C(m,n) - C'(m,n))}$$

(19)

$$PMSE = (\frac{1}{M * N} (\sum_{i=1}^M \sum_{j=1}^N (C(m,n) - C'(m,n))^2))^{\frac{1}{2}}$$

(20)

式中, M,N 为明文图像的大小(长和宽), $C(m,n)$ 是明文图像; $C'(m,n)$ 是恢复后的图像. 通过式(19 — 20) 对本文图像测试结果如下表.

表 4 PSNR 和 PMSE 计算结果表

	PSNR	PMSE
明文与密文	1.134 9	169.289 7

由表 4 计算结果知明文图像与密文图像的 PMSE 值大于 160,对于变换后的图像来说,人们无法从肉眼识别图像失真. 也表明了本文算法的安全性.

5 结束语

本文提出的一种改进的 Lorenz-Cat 双混沌置乱系统与 Logistic 混沌扩散系统对 DFT 变换的图

像自适性加密算法. 该算法在置乱过程中增强置乱的随机性,达到了全局置乱,并有效的解决了 Cat 映射的周期性问题,利用明文像素与密文像素以及混沌序列间的相互作用,使得每个像素都扩散到整幅图像矩阵中. 仿真实验分析表明,该算法密钥空间大,能够有效的抵抗穷举攻击,明密文敏感度高,可以有效抵御选择明、密文攻击,密文相关性小且密文图像像素分布均匀,可有效抵御统计攻击. 因而,本文算法在图像加密中效果更加优良.

参考文献:

[1] WANG J, CHEN G. Design of a Chaos-Based Digital Image Encryption Algorithm in Time Domain [C]// IEEE International Conference on Computational Intelligence&Communication Technology. IEEE, 2015:26-29.

[2] SPROTT J C. A new class of chaotic circuit [J]. Physics Letters A, 2000, 266(1):19-23.

[3] ZHANG W, WONG K W, YU H, et al. An image encryption scheme using reverse 2-dimensional chaotic map and dependent diffusion [J]. Communications in Nonlinear Science and Numerical Simulation, 2013, 18 (8):2066-2080.

[4] ZHOU Y, BAO L, CHEN C. A new 1D chaotic system for image encryption [J]. Signal Processing, 2014, 97 (7): 172-182.

[5] 李巧君, 张亚楠. 基于混沌映射的图像快速加密改进算法 [J]. 计算机测量与控制, 2014, 22 (10): 3270-3273.

[6] 杨洋, 杨洁, 冯久超. 一种基于 Arnold 置乱和优化大素数选取方案的 RSA 数字图像加密算法 [J]. 计算机科学, 2013, 40(S2):178-180.

[7] 汪乐乐, 李国东. 基于游程性序列的双重混沌的图像加密算法 [J]. 计算机科学, 2018, 45(S2):361-366.

[8] 赵国敏, 李国东. 基于广义 Henon 映射以及 CNN 超混沌系统图像加密方案 [J]. 信阳师范学院学报(自然科学版), 2015, 28(01):141-145.

[9] 谢国波, 苏本卉. 基于 Arnold 分层循环变换的数字图像加密算法 [J]. 计算机工程与设计, 2017, 38(05): 1200-1204.

[10] 尹晓燕. 基于混沌技术的图像加密算法研究与实现 [D]. 大连, 大连海事大学, 2008.

[11] 谢国波, 陈志伟. 基于改进的 Cat 置乱与 Henon_Kent 混沌系统的彩色图像自适应加密算法 [J/OL]. 计算机应用研究, 2019 (11): 1-3 [2019-11-14] <http://kns.cnki.net/kcms/detail/51.1196.TP.20180811.1324.028.html>.

[12] 谢国波,朱润盈. 复合级联混沌的彩色图像加密算法 [J]. 计算机工程与应用,2018,54(08):189-194.

[13] 谢国波,姜先值. 二维离散分数阶 Fourier 变换的双混沌图像加密算法 [J]. 计算机工程与应用,2018, 54 (03):40-45.

[14] 猴新科,吴贻峰. 基于复合混沌的数字图像加密算法 [J]. 计算机与数字工程,2018,46(12):2574-2579.

[15] 汪乐乐,李国东. 最优解与二维离散分数阶 Fourier 的双混沌加密算法 [J]. 中国科技论文,2018,13(17):

2024-2031.

作者简介:
魏 慧 女,(1996-),硕士研究生. 研究方向为数字分析与图像处理.
李国东(通讯作者) 男,(1976-),博士,教授. 研究方向为数字分析与图像处理. E-mail:lgdzhy@126.com.