基于 L-K 双混沌系统的彩色位级图像加密算法

马 聪 李国东
(新疆财经大学应用数学学院 新疆 乌鲁木齐 830012)

摘 要 针对传统加密算法精度有限、安全性低等问题,提出一种新的彩色图像加密算法。利用 Liu 混沌系统产生的混沌序列对彩色图像 R、G、B 三层的低五位进行索引位置置乱,再对高三位进行 Arnold 置乱;采用自适应方式进行扩散,并将 R、G、B 三层的密文图像循环异或,得到初步密文图像;联合像素级加密进行 Hilbert 置乱,采用 Kawakami 超混沌结合图像信息进行分形扩散,得到最终密文图像。仿真实验表明,该算法 NPCR 和 UACI 达到 99.78% 和 33.37%,信息熵为 7.997 0,安全性很高。

关键词 位级 Liu 混沌 Kawakami 超混沌 Hilbert 置乱 彩色图像

中图分类号 TP309 **文献标志码** A DOI:10.3969/j.issn.1000-386x.2020.03.054

COLOR BIT-LEVEL IMAGE ENCRYPTION ALGORITHM BASED ON L-K DOUBLE CHAOTIC SYSTEM

Ma Cong Li Guodong
(*School of Mathematics, Xinjiang University of Finance and Economics, Urumqi 830012, Xingjiang, China*)

Abstract Aiming at the problems of limited precision and low security of traditional encryption algorithms, we propose a new color image encryption algorithm. The chaotic sequence generated by the Liu chaotic system was used to scramble the lower five bits of the three layers of the color image R, G, and B, and then Arnold was scrambled for the upper three bits. Then we adopted an adaptive method to perform diffusion, and cycled the R, G and B ciphertext images to obtain the preliminary ciphertext images. Finally, Hilbert scrambling was performed by combining pixel-level encryption, and the Kawakami hyperchaos was combined with the image information for fractal diffusion to obtain the final ciphertext image. Simulation experiments show that the NPCR and UACI of the algorithm reach 99.78% and 33.37%, and the information entropy is 7.997 0, and its security is very high.

Keywords Bit-level Liu chaotic Kawakami hyperchaos Hilbert scrambling Color image

0 引 言

密码学是研究信息安全、通信安全的重要工具,图像加密在互联网的传播安全中起到了重要作用。由于混沌是一种运动轨迹有界、无规律可循的非线性动力学系统,其具有很强的初值敏感性、遍历性、随机性以及难以预测等特点,近几年成为信息保密领域上的重点研究内容[1-3]。季诺然等[4]提出用 QR 码与混沌序列结合的方法加密图像,将密文图像嵌入到二级 Contourlet 变换的子带中,能够很好地保护数字图像信息。谢国波等[5]提出了一种基于像素置乱和比特替换的混沌图像加密算法,提高了算法的加密速度,但是算法简单安全性不高。柴秀丽等[6]提出了一种自适应在位级进行操作的加密算法,采用自适应方法加密,提高了算法的安全性。盛苏英等[7]利用耦合映象格子与位级图像相结合并进行逐位扩散,加密算法性能较强,但是不能抵御暴力穷举攻击。Zhang 等[8]使用比特级置换的基于混沌的对称图像加密方案,加密安全性高。Zhou 等[9]设计了一种利用量子交叉操作和 5D 超混沌系统

收稿日期:2019-05-16。国家自然科学基金项目(11461063);新疆维吾尔自治区自然科学基金项目(2017D01A24);新疆财经大学研究生科研创新项目(XJUFE2018K040)。**马聪**,硕士生,主研领域:数据挖掘,图像处理。**李国东**,教授。

的比特级量子彩色图像加密方案。

针对传统加密算法精度有限、安全性不高、加密空间小等不足，本文提出了通过双混沌系统，先对位级进行一次加密，再联合像素级进行二次加密。通过仿真实验表明该算法克服了精度有限、结构单一、加密空间小等问题，具有很高的安全性、抗统计攻击性等优点。

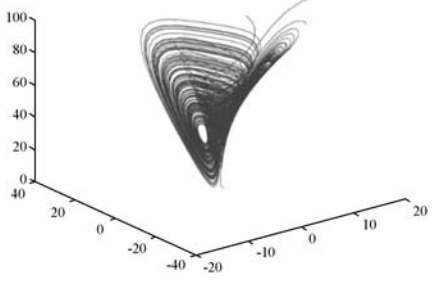
1 理论基础

1.1 Liu 混沌

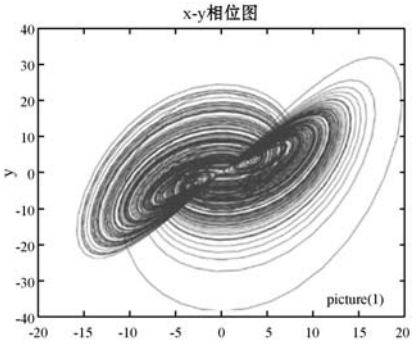
Liu 混沌系统是一类含有平方非线性项的混沌系统[10]，其动力学方程如下所示：

$$\begin{cases} \dot{x} = a(y-x) \\ \dot{y} = bx - kxz \\ \dot{z} = -cz + hx^2 \end{cases} \tag{1}$$

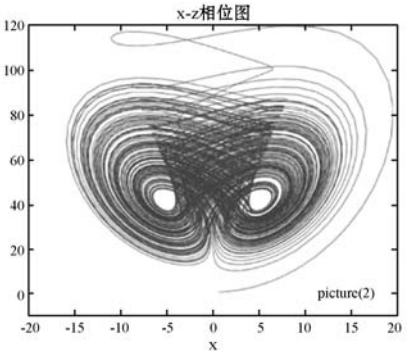
式中：a、b、c 为系统参数，h、k 为控制参数。当满足条件 $a=10$、$b=40$、$c=2.5$，$k=1$、$h=4$ 时系统表现出混沌行为。为了增加密钥空间的复杂性，消除混沌序列的随机性，Liu 混沌映射初值采用随机选取的方法，将一维 Logistic 映射迭代 1 000 次，在 1 000 次以内随机选取三个值作为 Liu 混沌映射的初值，选取结果为 $x_0=0.797\ 6$、$y_0=0.311\ 4$、$z_0=0.488\ 3$。一个混沌系统的奇异吸引子在相空间是整体有界的，Liu 混沌系统的奇异吸引子是一类具有无穷嵌套层次的自相似几何结构。经过 20 000 次迭代后的奇异吸引子和相位图如图 1 所示。



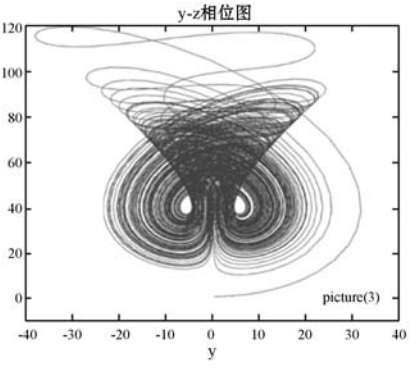
（a）奇异吸引子



（b）x-y 平面



（c）x-z 平面



（d）y-z 平面

图 1 Liu 混沌奇异吸引子及相位图

1.2 Kawakami 超混沌

超混沌系统的动力学具有更加随机、相空间更大等优势，将混沌运用在加密体统中能有效地提高加密性能。Kawakami 超混沌是 1979 年由 Kawakami 和 Kobayashi 提出的首个研究自同态的模型，Kawakami 映射的动力学表达式如下：

$$\begin{cases} x_{n+1} = -cx_n x_n + y_n \\ y_{n+1} = x_n^2 - d \end{cases} \tag{2}$$

式中：c、d 为控制参数。$c=0.1$、$d=1.6$ 时系统处于超混沌状态，Kawakami 超混沌的初值选取一维 Chebyshev 迭代 1 000 次以内的两个随机数，$x_1=0.401\ 3$，$y_1=0.100\ 7$，Kawakami 超混沌迭代 1 500 次的奇异吸引子如图 2 所示。

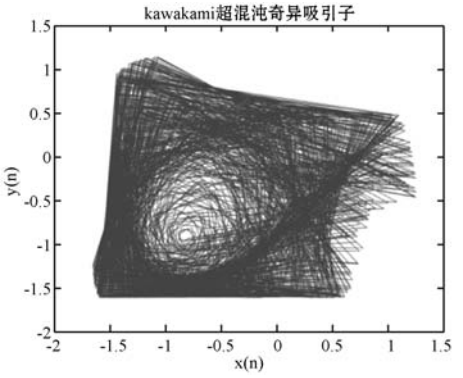


图 2 Kawakami 超混沌奇异吸引子

2　L-K 双混沌系统的彩色图像加密算法

加密算法流程如图 3 所示。

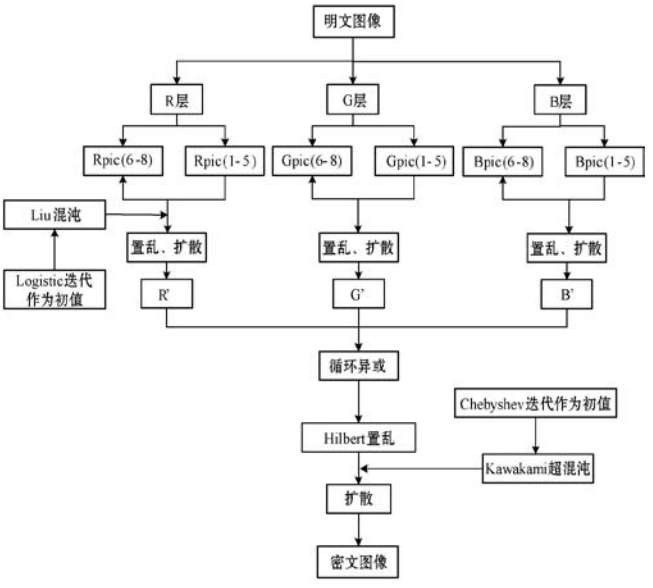


图 3　加密算法流程图

加密算法采用置乱-扩散-置乱-扩散的结构,首先将明文图像转换为 R、G、B 三个通道,将三通道中每个像素值分别进行二进制转换,这时每一个通道可以看作是由 8 个 $m \times n$ 的 0 和 1 序列组成的矩阵,即 $R_{(x,y)} = \{R_{1(x,y)}, R_{2(x,y)}, \cdots, R_{8(x,y)}\}$,不同位平面包含的信息量不同[11],如表 1 所示。

表 1　不同位平面信息量

位平面	信息量/%
P_{pic1}	0.39
P_{pic2}	0.78
P_{pic3}	1.57
P_{pic4}	3.14
P_{pic5}	6.28
P_{pic6}	12.55
P_{pic7}	25.10
P_{pic8}	50.20

由表 1 可以看出,高三位包含了主要的图像信息,位数越低,所包含的信息量越少,因此将高三位的每一位单独作为一个加密图像,将低五位的位平面向左移位异或构成一个加密图像,采用低五位和高三位分别置乱、交融扩散的方式进行第一轮加密。同时为了消除不同层之间的相关性,进行了第二轮置乱-扩散操作。

1)一次置乱-扩散算法。

按照浮点算法将 $3 \times m \times n$ 的彩色图像分为大小 $m \times n$ 的 R 层、G 层、B 层图像。

以 R 层的加密过程为例,将 R 层分解为 8 个位平面,鉴于高三位包含了主要的图像信息,因此将高三位分别单独作为一个平面,从高到低记为 *pic*1、*pic*2、*pic*3,将低五位如式(3)所示方式向左移位异或合成一个位平面,记为 *pic*4。

$$pic4(i,j) = P_5(i,j) \oplus P_4(i,j) \oplus P_3(i,j) \oplus P_2(i,j) \oplus P_1(i,j) \tag{3}$$

向左移位异或程序如下:

```
Bit4 = WW(:,:,4);
                % WW 是 Matlab 读取的图像信息
Bit5 = WW(:,:,5);
P1 = bitxor(Bit5,Bit4);
P2 = bitxor(P1,Bit3);
P3 = bitxor(P2,Bit2);
P4 = bitxor(P3,Bit1)。
```

步骤 1　将初值为 k_1 的 Logistic 模型迭代 k_2 次选取三个值作为 Liu 混沌系统的初值,并设置 Liu 混沌系统的参数。为了消除暂态效应,迭代 $S + 1\ 000$ ($S > m \times n$)次选取中间 S 个不重复的值,在 S 中截取三段 $m \times n$ 的混沌序列,得到序列 x_i、y_i、z_i。

步骤 2　采用 Arnold 置乱[12] k_3 次实现 *pic*1 – *pic*3 的像素值位置变换,Arnold 置乱思想是在矩阵中先做 x 轴方向的错切变换,再做 y 轴方向的错切变换,反复拉伸折叠;接着采用光栅扫描的方式将 *pic*4 变换成一维向量,对 *pic*4 位级采用索引位置置乱混淆的像素值位置,在 S 中任意截取 $m \times n$ 个的混沌序列构成一维向量,按降序排序,得到的序列为 $s_i = \{s_{m\times n}, s_{m\times n-1}, \cdots, s_1\}$,并记录原序列在 s_i 中的位置为 $Ts_i = \{Ts_1, Ts_2, \cdots, Ts_{m\times n}\}$,按此位置对原序列进行变换,此时得到一个新的一维向量,转换成 $m \times n$ 矩阵即完成位级置乱。

步骤 3　将已经加密的高三位 Pic_i ($i = 1,2,3$)分别进行像素值求和得到 $sumI_i$,采用低五位 *pic*4 加密高三位的混淆扩散方式,对混沌序列按照式(4)进行标准化处理,迭代 m 次,得到 m 个混沌序列。

$$\begin{aligned} x_i &= floor(\bmod(x_i \times 10^{14}), 256) \\ y_i &= floor(\bmod(y_i \times 10^{14}), 256) \\ z_i &= floor(\bmod(z_i \times 10^{14}), 256) \end{aligned} \tag{4}$$

按照式(5)进行自适应扩散操作,$Pic'(3)$、$Pic'(2)$、$Pic'(1)$分别是 x_i, y_i, z_i 的高三位。

$$h_i = sumI_i \bmod 256 = \begin{cases} \min \rightarrow Pic(i) \oplus Pic(4) \oplus Pic'(3) \\ middle \rightarrow Pic(i) \oplus Pic(4) \oplus Pic'(2) \\ \max \rightarrow Pic(i) \oplus Pic(4) \oplus Pic'(1) \end{cases} \tag{5}$$

然后,计算三个异或矩阵分别按位相加的结果,按照式(6)得到 R 层密文图像。

$$R' = (min + middle + max) \bmod 2 \tag{6}$$

步骤 4 G 层、B 层采用相同的方法分别加密,再按循环异或得到最终密文图像,循环异或的函数为 $BitCircShift(A,k,m)$。

$$C = R' \oplus G' \oplus B' \tag{7}$$

2) 二次置乱-扩散算法。

第一轮加密过程是基于位级层面进行像素值替代和扩散,为了消除层之间的相关性,增强加密算法的安全性,改进第一轮密文产生的像素值,在灰度图像上进行第二轮加密。

步骤 1 在初值为 k_4 的一维 Chebyshev 模型迭代 k_5 次随机选取两个数作为 Kawakami 超混沌的初值,设置 Kawakami 超混沌的参数,并迭代 $1\ 000 + m \times n$ 次,舍弃前 1 000 个迭代值,得到 x_i、y_i。结合 x_i、y_i 对密文图像像素值进行改进,改进方法如式(8)所示,取前 $\frac{m \times n}{2}$ 的 x_i 超混沌序列记为 x_{1i},取后 $\frac{m \times n}{2}$ 的 y_i 超混沌序列记为 y_{2i}。

$$C1 = \bmod(ceil(abs(x_{1i} + y_{2i}) \times 10^5) + C, 256) \tag{8}$$

步骤 2 对所生成的超混沌序列进行取余操作,新的混沌序列结合密文图像像素值信息,使超混沌序列更具有随机性,改进方法如式(9)所示,

$$x_i = \bmod(floor((sum(C1)/abs(x_i)) \times 10^6), 256)$$
$$y_i = \bmod(floor((sum(C1)/abs(y_i)) \times 10^6), 256) \tag{9}$$

步骤 3 采用 Hilbert 曲线对第一轮加密的密文图像进行置乱,Hilbert 曲线的思想是把一个方阵矩阵分成 4 个小方阵,依次从左下角的中心出发向上移动到左上角的中心,再向右扫描到右上角的中心,向下到右下角的中心,按此顺序不断迭代扫描,直到遍历整个方阵,置乱示意图如图 4 所示。

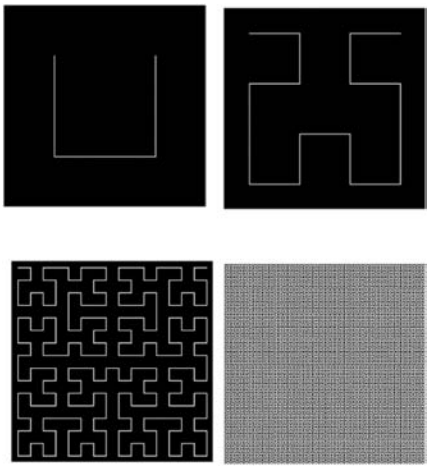


图 4 Hilbert 置乱示意图

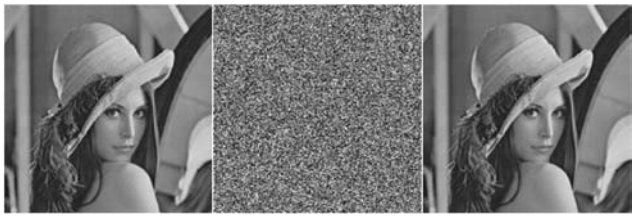
步骤 4 将 Hilbert 置乱后的图像记为 Q,在扩散加密操作中,将图像纵向分为两半 Q_1、Q_2,两半同时展开加密,最后合并得到完全扩散的密文图像。

$$\begin{cases} C_{1i} = Q_{1i} \oplus \bmod(C_{1i-1} + x'_i, 256) \\ C_{2i} = Q_{2i} \oplus \bmod(C_{2i-1} + y'_i, 256) \end{cases} \tag{10}$$

3) 为了达到加密图像充分混淆的目的,重复步骤 1) – 步骤 2) T 次,T 作为密钥保存,至此完成加密过程。

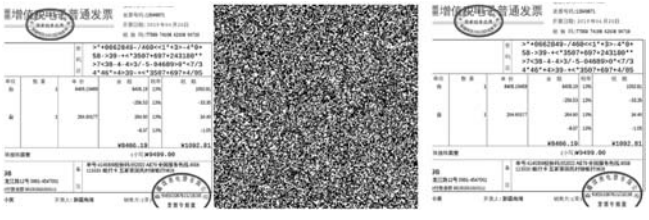
3 仿真实验

实验选用加密的经典图像 Lena 为对象,Lena 图像的分辨率为 256 × 256,大小为 192 KB。采用 Win10 系统在 MATLAB 2018b 的环境下对该算法进行仿真,其中,Liu 混沌的系统参数设置为 $a = 10$、$b = 40$、$c = 2.5$、$k = 1$、$h = 4$,Liu 混沌映射的初始值为 $x_0 = 0.797\ 6$、$y_0 = 0.311\ 4$、$z_0 = 0.488\ 3$,Kawakami 超混沌的系统参数设置为 $c = 0.1$、$d = 1.6$,初值为 $x_1 = 0.401\ 3$、$y_1 = 0.100\ 7$。除了上述密钥之外,本文算法的其余密钥为 $S = 92\ 463$、$k_1 = 0.3$、$k_2 = 1\ 000$、$k_3 = 99$、$k_4 = 0.75$、$k_5 = 999$、$T = 5$,仿真实验结果如图 5 所示。为了说明本文算法加密的实用性,使用分辨率为 512 × 512,大小为 1 MB 的电子发票为例,在同样的操作环境下,使用相同的系统参数和系统初值进行加密,结果如图 6 所示。



(a) 明文图像 (b) 密文图像 (c) 解密图像

图 5 仿真实验结果



(a) 明文图像 (b) 密文图像 (c) 解密图像

图 6 电子发票加密

4 安全性分析

4.1 置乱度分析

置乱度是衡量像素值位置变化杂乱程度的重要指标,置乱度越大,说明图像混淆的越乱,攻击者不能识别真实内容,因此图像更加不易被破解,置乱度的取值

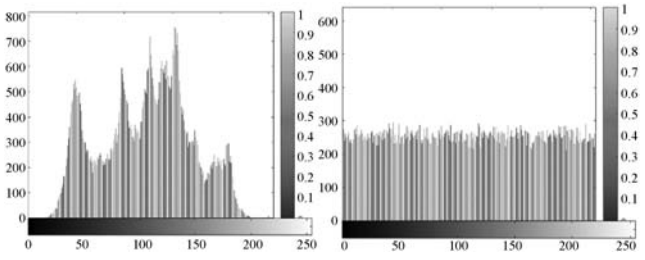
范围为 $SM \in (0,1)$,置乱度的数学表达如下:

$$SM(X,Y) = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n}(x_{ij}-y_{ij})^2}{\sum_{i=1}^{m}\sum_{j=1}^{n}(x_{ij}-r_{ij})^2} \tag{11}$$

$X=\{x_{ij}\}_{m\times n}$表示明文图像,$Y=\{y_{ij}\}_{m\times n}$表示密文图像,$R=\{r_{ij}\}_{m\times n}$表示与明文图像大小相同的随机分布图像,选取最终密文图像进行置乱度分析,用本文算法得到的置乱度为 0.992 8,接近 1,说明本文算法的置乱效果很好,图像信息的安全性更高。

4.2　直方图分析

直方图分析结果如图 7 所示,可以看出,明文图像像素值分布参差不齐,而密文图像像素值频率分布比较均匀,难以找出原始图像的规律,说明加密后的密文图像对穷举攻击有很好的抵抗作用。



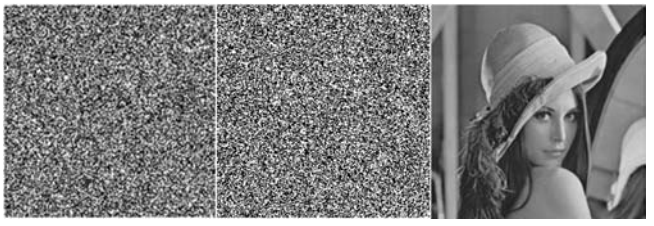
(a) 明文图像直方图　　(b) 密文图像直方图

图 7　明文和密文图像直方图

4.3　密钥空间及密钥敏感性分析

彩色图像信息包含的数据信息量大,若密钥选取的较少,则无法满足安全性,密钥空间越大,密钥长度就越长,密文图像更能有效地抵御穷举攻击,密钥是传递者和接受者的媒介,将加密算法中的密钥传送给信息接受者,接受者就能根据密钥还原出原始信息。本文算法的密钥空间为 $10^{16\times19}=10^{304}$,密钥长度为 $\log_2(10^{304})$,远大于 128 bit,可见密钥空间很大,足以抵御穷举攻击。

本文的加密算法对密钥的依赖性非常强,在解密过程中,密钥微小的变化都不能得到正确的解密图像,对 Liu 混沌系统和 Kawakami 超混沌系统的初值进行 2×10^{-14}的微小变动时,即 $x_0=0.797\ 6+2\times10^{-14}$,$x_1=0.401\ 3+2\times10^{-14}$,所得解密结果如图 8 所示。



(a) 错误解密　　(b) 错误解密　　(c) 正确解密

图 8　敏感性测试

4.4　明文敏感性分析

像素变化比率(简称:NPCR)显示的是不同像素点个数占全部像素点的比例,表明当明文中有一个像素值发生变化时密文图像中像素值变化的比率,NPCR 越接近 100%,说明明文像素值的微小变动都会大幅改变密文信息。D_1表示密文,D_2表示明文,公式如下:

$$NPCR = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}D(i,j)}{M\times N}\times100\% \tag{12}$$

归一化平均改变强度(简称:UACI)显示的是两幅图像全部相应位置像素点的差值和最大差值的比值的平均值。UACI 的理想值是接近 33.463 5%,这时对明文的细微改变敏感性强烈,计算公式如下:

$$UACI = \frac{1}{M\times N}\times\left[\sum_i\sum_j\frac{D_1(i,j)-D_2(i,j)}{256}\right]\times100\% \tag{13}$$

对明文图像中任意一点像素值(100,101)进行微小变动为(101,101),此时 NPCR 和 UACI 分别为 99.78%和 33.37%,均非常接近理想值,对比文献[13]和文献[14],结果如表 2 所示。

表 2　NPCR 和 UACI 值

评价指标	本文算法	文献[13]	文献[14]
NPCR	0.997 8	0.996 8	0.994 6
UACI	0.333 7	0.334 7	0.333 1

4.5　相邻像素相关性分析

在一幅图像中,其像素值之间存在一定的相关性,根据式(14),截取 1 000 对像素点(x,y)进行分析,计算结果如表 3 和图 9 所示。可以看出,明文图像相邻像素的相关性比较高,呈现出明显的线性相关性,相关系数接近 1,而密文图像各方向像素之间相关系数均在 0 左右,说明本文加密算法达到了理想效果。

$$r_{x,y}=\frac{\mathrm{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{14}$$

式中:

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

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

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

表 3 明文和密文图像相邻像素间相关系数

相邻像素方向	原始图像	密文图像
水平方向	0.951 3	-0.020 8
垂直方向	0.938 3	0.042 4
对角线方向	0.954 5	0.021 2

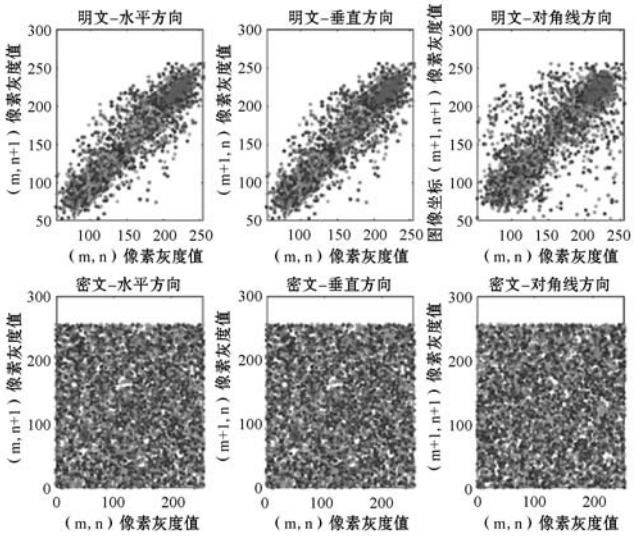


图 9 明文和密文图像相邻像素相关性

4.6 信息熵分析

根据 Shannon 定理[15-16]信息熵的理论,信息熵反应了一个序列的随机性,信息熵越大,随机性越强,灰度值分布越均匀。当图像中各灰度值出现的概率相等时,图像的信息熵最大,256 个灰度级的灰度图像信息熵的理想值为 8。为了体现本文算法的优越性,对 Lena 图像与电子发票的明文与密文信息熵进行对比,根据式(15)计算信息熵的结果见表 4。可以看出,经过本文算法加密的图像信息熵都非常接近理想值,表明本文算法能够有效地抵御穷举攻击,加密效果很好。

$$H(m) = -\sum_{i=1}^{255} p(m_i)\log_2 p(m_i) \qquad (15)$$

表 4 信息熵结果

图像	明文信息熵	密文信息熵
Lena	7.445 0	7.997 0
电子发票	2.220 8	7.993 4

5 结 语

本文将混沌理论用于图像加密领域,该算法主要特点是:先将 Liu 混沌系统用于位级图像,所得到的加密图像作为下一轮加密的载体,第二轮改进密文图像为像素级,并将 Kawakami 超混沌系统用于像素级加密,采用置乱-扩散-置乱-扩散的结构,分别在位级平面和像素级平面进行加密。实验结果表明,该算法能很好地抵御各种暴力攻击,密钥空间大,加密算法的安全性高,并且该算法解决了混沌加密的单一性,提高了加密的实时性,加密效果较好,在网络安全、信息传输、移动支付等方面具有广阔应用前景。

参 考 文 献

[1] Sahari M L, Boukemara I. A pseudo-random numbers generator based on a novel 3D chaotic map with an application to color image encryption[J]. Nonlinear Dynamics, 2018,94: 723-744.

[2] Li C, Luo G, Ke Q, et al. An image encryption scheme based on chaotic tent map[J]. Nonlinear Dynamics, 2017, 87(1):127-133.

[3] 程宁,王茜娟. 基于混沌 Gyrator 变换与矩阵分解的光学图像加密算法[J]. 电子测量与仪器学报,2019,33(1): 191-202.

[4] 季诺然,吕晓琪,谷宇,等. 基于 QR 码与混沌加密的 Contourlet 域彩色图像盲水印算法[J]. 包装工程 2017,38(15): 173-178.

[5] 谢国波,王添. 基于像素置乱和比特替换的混沌图像加密算法[J]. 微电子学与计算机,2016,33(3):80-85.

[6] 柴秀丽,甘志华. 一种基于时空混沌系统的彩色图像自适应位级加密算法[J]. 计算机科学, 2015, 42(7): 204-209.

[7] 盛苏英,吴新华. 基于耦合映象格子的混沌图像加密算法研究[J]. 微电子学与计算机,2014,31(1):43-46,51.

[8] Zhang Y Q, Wang X Y. Analysis and improvement of a chaos-based symmetric image encryption scheme using a bit-level permutation[J]. Nonlinear Dynamics, 2014, 77(3):687-698.

[9] Zhou N, Chen W, Yan X, et al. Bit-level quantum color image encryption scheme with quantum cross-exchange operation and hyper-chaotic system[J]. Quantum Information Processing, 2018, 17(6):137.

[10] Liu H, Wang X. Color image encryption using spatial bit-level permutation and high-dimension chaotic system[J]. Optics Communications, 2011, 284(16):3895-3903.

[11] 梁颖,张绍武. 位级同步置乱扩散和像素级环形扩散图像加密算法[J]. 中国图象图形学报,2018,23(6):814-826.

[12] Ye G, Wong K W. An efficient chaotic image encryption algorithm based on a generalized Arnold map[J]. Nonlinear Dynamics, 2012, 69(4):2079-2087.

[13] 程东升,谭旭,许志良,等. 结合四维超混沌系统和位分解的图像加密算法研究[J]. 电子科技大学学报,2018,47(6):906-912.

[14] Zhou Y C, Cao W J, Chen C L P. Image encryption using binary bitplane[J]. Signal Processing,2014,100(7):197-207.

[15] 柴秀丽,甘志华. 基于超混沌系统的位级自适应彩色图像加密新算法[J]. 计算机科学,2016,43(4):134-139.

[16] 刘西林,严广乐. 基于混沌映射与有限域 $GF(2^4)$ 域乘法运算的电子病历图像的加密[J]. 计算机应用与软件,2018,35(12):303-307.