文章编号：2095-2163(2022)03-0173-07 中图分类号：TP309.7 文献标志码：A

Logistic-Sine 映射与比特重组的图像加密算法

唐传华，巫朝霞
（新疆财经大学 统计与数据科学学院，乌鲁木齐 830011）

摘 要：针对传统一维混沌映射结构方程简单的局限性，可以用少量的已知信息来加以预测混沌轨迹，以及参数值的安全性问题，本文介绍了一种由 Logistic 和 Sine 映射延伸推导得出的 Logistic-Sine 混沌映射，并结合比特重组的相关理论，提出了一种新的图像加密算法。该算法首先运用 Logistic-Sine 混沌映射迭代生成混沌序列，然后经过全局置乱、比特平面的交叉换位，以及异或扩散的加密算法得到加密图像。经仿真实验结果说明：该算法具有良好的加密效果，并且可以抵抗各种攻击，有较高的安全性和稳定性来保护图像。

关键词：Logistic-Sine 混沌映射；全局置乱；比特重组；比特平面

Based on Logistic-Sine chaotic mapping and bit reorganization image encryption method

TANG Chuanhua, WU Zhaoxia
(School of Statistics and Data Science, Xinjiang University of Finance and Economics, Urumqi 830011, China)

【Abstract】 Aiming at the traditional one-dimensional chaotic mapping structure equation is simple, and even a small amount of known information can be used to predict the chaotic trajectory and the security of parameter values, this article introduces a method derived from Logistic and Sine mapping. Logistic-Sine chaotic mapping, combined with the related theory of bit reorganization, proposes a new digital image encryption algorithm. The algorithm uses Logistic-Sine chaotic mapping to generate a chaotic sequence and then undergoes global scrambling, bit-plane exchange position scrambling, and horizontal XOR diffusion to obtain the final encrypted image. Relevant simulation experiment results and security analysis show that the algorithm can resist various attacks and can protect images with better encryption effect and higher security.

【Key words】 Logistic-Sine chaotic mapping; global scrambling; bit reorganization; Bit plane

0 引 言

数字图像是生物统计学、医学、军事、在线个人相册等领域最重要的信息载体之一。如一张自拍，可以描述人们的外貌，也可以反映其大致的年龄和健康状况。因此，如何保证图像信息具有安全的输入输出环境是一个很大的挑战。在各种图像安全技术中，最常用且有效的措施是图像加密技术。

混沌系统用于密码学是非常合理的，并且广泛应用在图像加密领域[1]。庹朝永等[2]提出一种新的彩色图像加密算法，该算法首先通过二维 Logistic 混沌映射产生伪随机序列进行像素置乱，然后联合比特异或与随机重组将各像素值转换为相应的二进制，最后对每个 24 位像素值进行 RGB 3 种颜色重新组合得到新的加密图像，然而该算法计算强度与空间需求偏高；廖春成等[3]利用明文像素值来计算混沌系统的参数和预迭代次数，有效提高了明文敏感性。该算法通过 Kent 混沌系统迭代产生混沌序列实现全局置乱，然后进行比特级置乱得到加密图像。Yueping Li 等[4]提出了一种基于高维混沌的图像加密算法，该算法通过 5 维多翼超混沌系统产生的密钥流与原始图像有关，然后分别运用像素级置乱和比特级置乱来混淆图像像素位置，最后使用扩散操作来改变像素值；伍朝阳等[5]提出一种结合像素置乱与比特置乱的超混沌 Chen 系统，对图像进行加密的算法；胡春杰等[6]提出了一种新的二维离散型混沌映射，并利用改进的 Logistic 映射，对图像进行置乱操作，然后进行异或运算和比特位的交叉换位得到最终密文图像。

本文设计了一种基于 Logistic-Sine 混沌映射与

基金项目：国家自然科学基金(61941205)。

作者简介：唐传华(1996-)，男，硕士研究生，主要研究方向：图像加密；巫朝霞(1975-)，女，博士，教授，硕士生导师，主要研究方向：信息安全研究。
通讯作者：巫朝霞 Email：wuzhaoxia828@163.com

收稿日期：2022-01-25

比特重组的图像加密方法,首先利用 Logistic-Sine 混沌映射对明文图像进行全局置乱,然后通过比特重组操作将经过全局置乱的图像转化为中间密文图像,最后经过水平方向扩散的比特异或得到最终的加密图像。最后的仿真实验分析说明:该算法可以抵御各种类型的攻击,有较高的安全性和稳定性来保护图像。

1 Logistic-Sine 映射与比特重组

1.1 Logistic-Sine 映射

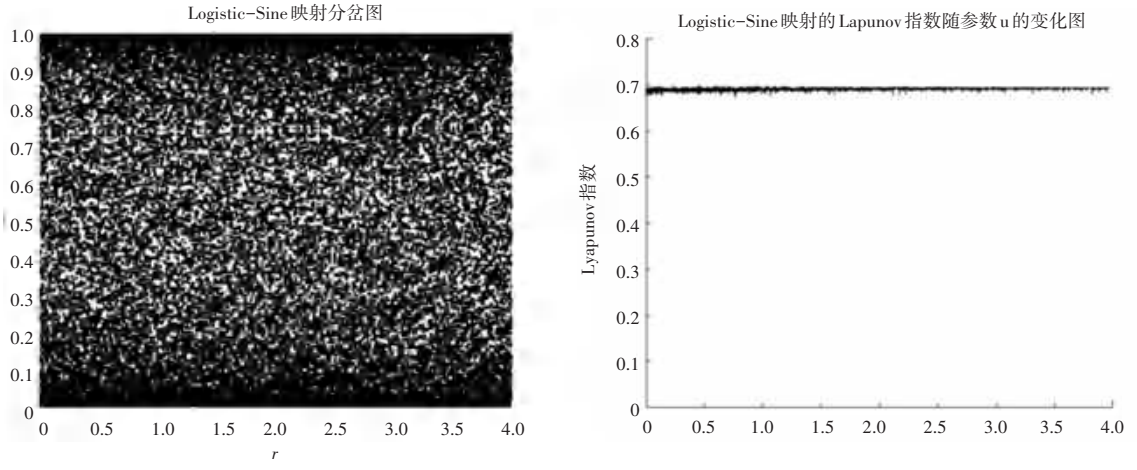
传统的一维 Logistic 和 Sine 映射虽然被广泛应用在图像加密中,但依然存在很大的局限性。如:其仅在相应的参数范围内处于混沌状态,但依然存在一些参数并不处于混沌状态。因此,本文设计了一种由 Logistic 和 Sine 映射延伸推导得出的 Logistic-Sine 混沌映射,其表达式如式(1):

$$x_{n+1} = mod((rx_n(1-x_n) + (4-r)\sin(\pi x_n)/4),1) \quad (1)$$

其中,模函数 $mod(\ )$ 表示取模,返回余数。

经过模运算后,循环迭代可以得到一个取值在 0~1 之间的混沌序列。虽然,模运算会加大运算量和加密时间,但是通过增加模运算,使得 Logistic-Sine 映射的参数 r 的范围不仅仅局限于(0,4]之间,并且扩大了系统的混沌区域,同时加密系统的密钥空间也会相应扩大,可以更好的抵抗穷举攻击。

图 1(a)~1(b)分别是 Logistic-Sine 映射的分岔图和 Lyapunov 指数变化图。从图中可以看出,Logistic-Sine 映射在整个参数范围内都处于混沌状态,且分布均匀。由此说明本文设计的 Logistic-Sine 映射,混沌性能比较优越,用于图像加密过程是可行的。



(a) 分岔图 (b) Lyapunov 指数图

图 1 Logistic-Sine 相关图

Fig. 1 Logistic-Sine correlation diagram

1.2 比特重组

现有的混沌系统图像加密思路可以从两方向入手:一是在像素的基础上对图像进行加密,将像素作为最小的元素加以研究,而数字图像就是所有像素的集合;二是在比特级的层次上对图像进行加密,将每个十进制像素值转换为二进制值,同时划分为若干个比特平面,并继续在这些比特平面上进行比特级操作。例如,256 级灰度图像中的每个像素值可以转化为对应的 8 位二进制数来表示,这时可以将一幅 256 级的灰度图像划分为 8 个比特平面,第 $i(i=1,2,\cdots,8)$ 个比特平面就是所有像素的第 i 个比特值的集合,而且比特平面位级越高,其中包含的原始图像的有用信息就会越多。

基于比特的图像加密算法是近些年才被提出来的,其可以在比特级层次上同时改变像素位置及其像素值。本文就是在比特级的层次上对图像进行加密,将 Logistic-Sine 混沌映射和比特重组相结合,该算法在安全性、稳定性等方面表现出了优越的特性。

2 加密算法过程

图像加密算法分为置乱、比特重组和扩散 3 个阶段。第一阶段的置乱过程是利用 Logistic-Sine 映射迭代,产生混沌伪随机序列,进行全局置乱。第二阶段的比特重组过程,是将全局置乱后的十进制矩阵经过比特重组操作,得到中间密文图像 $\boldsymbol{A}$。第三阶段的扩散过程是将中间密文图像 $\boldsymbol{A}$ 经过水平方向扩散的比特异或操作,得到最终的密文图像 C。本文加密算法流程如图 2 所示。

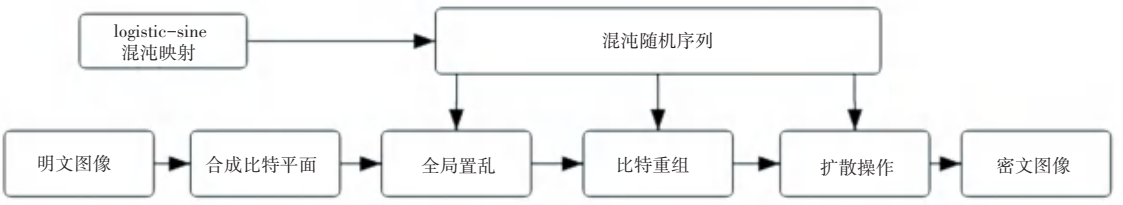


图 2　图像加密算法流程图

Fig. 2　Flowchart of image encryption algorithm

2.1　置乱

置乱过程的具体实现步骤如下：

(1)选取一幅大小为 $M \times N$ 的明文图像 P，利用式(2)和式(3)计算像素矩阵中所有像素值的总和 sum 和平均像素值 avg，然后利用式(4)、(5)分别计算出 Logistic-Sine 混沌系统的控制参数 r 和初始迭代的次数 Z。

$$\text{sum} = \sum_{m=0,n=0}^{m=M-1,n=N-1} f(m,n) \tag{2}$$

$$avg = \text{sum}/(M \times N) \tag{3}$$

$$r = mod(\text{sum} \times 100, M \times N)/M \times N \tag{4}$$

$$Z = M + N + mod(avg \times 10^8, M + N) \tag{5}$$

其中，Z 是与明文密切相关的量，可以有效抵抗选择对明文的攻击。

(2)将输入的初始密钥 (x_0, S) 带入到式(1)。

其中，S 是随机输入的控制参数。预迭代 Z 次后去掉前 Z 个迭代值，可以消除暂态效应的影响。

(3)全局置乱将分别进行行置乱和列置乱。

①行置乱：对 Logistic-Sine 混沌系统继续迭代 M 次，生成一个长度为 M，且数值在 0 ~ 1 之间的混沌序列 $E = \{e_1, e_2, e_3, \cdots, e_M\}$。将序列 E 的序列值按从小到大排序，继而得到一个对应排序的索引值序列 $p^E = \{p_1^E, p_2^E, p_3^E, \cdots, p_M^E\}$，利用 p^E 序列对像素矩阵进行行置乱。例如，对于序列{0.3,0.1,0.5,0.4}，对其进行从小到大排序后，得到序列{0.1,0.3,0.4,0.5}，则对应的索引值序列为{2,1,4,3}。运用索引值序列的行置乱示意如图 3 所示。

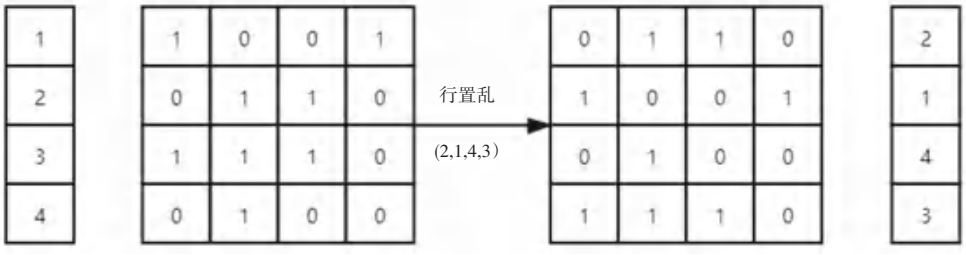


图 3　行置乱示意图

Fig. 3　Schematic diagram of row scrambling

②列置乱：对 Logistic-Sine 混沌系统继续迭代 $8 \times N$ 次，生成一个长度为 $8 \times N$ 的混沌序列 $F = \{f_1, f_2, f_3, \cdots, f_{8\times N}\}$，将 F 序列值按从小到大排序，得到一个对应的索引值序列 $p^F = \{p_1^F, p_2^F, p_3^F, \cdots, p_M^F\}$，利用 p^F 序列对像素矩阵进行列置乱，得到十进制矩阵 $\boldsymbol{P}_1$。

2.2　比特重组

将经过置乱阶段得到的十进制矩阵 $\boldsymbol{P}_1$ 进行比特重组操作，得到中间密文图像矩阵 $\boldsymbol{A}$。具体步骤如下：

(1)利用 Logistic-Sine 混沌系统继续迭代 $M \times N$ 次，生成一个长度 $M \times N$ 的混沌序列 $Q = \{q_1, q_2, q_3, \cdots, q_{M\times N}\}$。

(2)将十进制矩阵 $\boldsymbol{P}_1$ 依据行优先原则转化为一维混沌序列 $R = \{r_1, r_2, r_3, \cdots, r_{M\times N}\}$，同时将其像素值 r_i 转化为对应的二进制数。如，取出的像素值 $r_i = 145$，则对应的二进制数为 10 010 001。

(3) 通过比较序列 Q 中相邻像素的大小，对序列 R 的像素值 r_i 进行比特重组。操作过程如下：

若 $q_i < q_{i+1}$，则像素值 r_i 的第 1、2、3、4 比特位依次与第 8、7、6、5 比特位互换；若 $q_i > q_{i+1}$，则像素值 r_i 的第 1、3、5、7 比特位依次与第 2、4、6、8 比特位互换。例如：r_i = 145(10 010 001)，若 $q_i < q_{i+1}$ 则新的像素值 r_1' = 10 001 001(137)；若 $q_i > q_{i+1}$ 则新的像素值 r_1' = 01 100 010(98)。比特重组示意如图 4 所示。

(4)将比特重组后所有 r_i' 转成对应的十进制数，得到序列 $R' = \{r_1', r_2', r_3', \cdots, r_{M\times N}'\}$，再将其转化回 $M \times N$ 的矩阵，记为中间密文图像矩阵 $\boldsymbol{A}$。

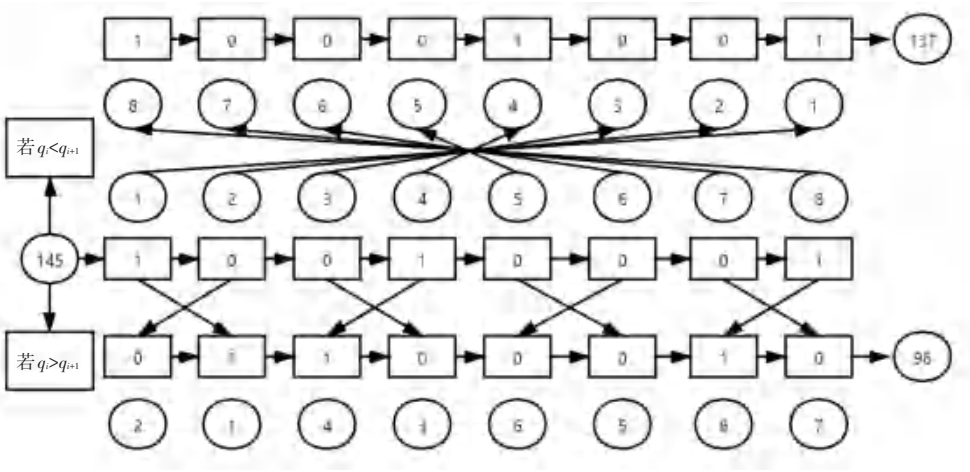


图 4 比特重组示意图

Fig. 4 Schematic diagram of bit reassembly

2.3 扩散

在本文的图像加密算法中,使用水平方向的扩散。将中间密文图像 $\boldsymbol{A}$ 作为输入端,从图像的第一个像素开始,依次逐行向前移动。在此过程中,依据行优先的原则,保留第一行第一个像素不变,对第一、二个像素进行比特异或得到新的第二个像素,将其与第三个像素进行比特异或得到新的第三个像素,以此类推,直到最后一行的倒数第二个像素与最后一个像素进行比特异或结束。经过水平方向的扩散操作,可以得到最终的密文图像 C。具体算法如下:

算法 1 水平方向扩散算法

输入:中间密文图像 $\boldsymbol{A}$

输出:最终密文图像 C

1:for $i = 1$ to M step 1

2:for $j = 1$ to $(N - 1)$ step 1

3: $A_{i,j+1} = A_{i,j+1} \oplus A_{i,j}$

4:end

5:If $1 < i \leqslant N$

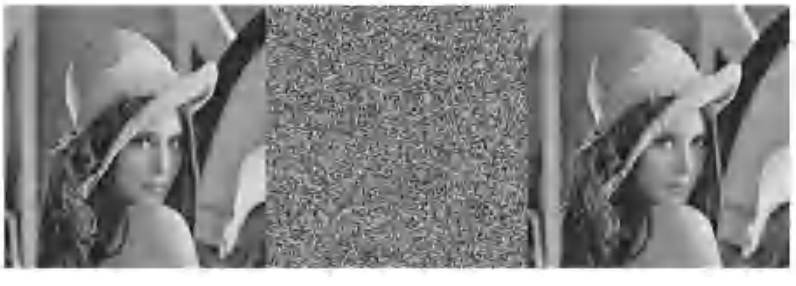
6: $A_{i+1,1} = A_{i+1,1} \oplus A_{i,N}$

7:end

以上是图像加密的算法过程。而解密算法其实就是加密算法的逆过程,在此不再赘述。

3 实验结果与分析

在本文的实验过程中,选取 256×256 的 Lena 灰度图,在 Win10 操作系统下,以 MATLAB R2017a 为软件工具模拟仿真实验过程。设定 Logistic-Sine 混沌系统的初始密钥 $(x_0, S) = (0.234, 0.128)$。对 Lena 图进行加密和解密后的图像如图 5 所示。



(a) 明文 (b) 密文 (c) 解密

图 5 加解密效果

Fig. 5 Encryption and decryption effect

由图中可见,该算法加密效果较好,既可以很好的隐藏原文信息,又可以很好地恢复原文图像。一个好的加密算法应该能够抵抗各种攻击,因此对该算法进行了密钥空间分析、统计分析和密钥敏感性分析等,验证了该算法的安全性和稳定性。

3.1 密钥空间分析

密钥空间是指在加解密过程中需要用到的密钥总数,密钥空间的大小影响着加密算法能否有效抵抗穷举攻击[9]。本文算法采用 Logistic-Sine 混沌系统的 2 个参数 (x_0, S) 作为初始密钥,计算机系统可

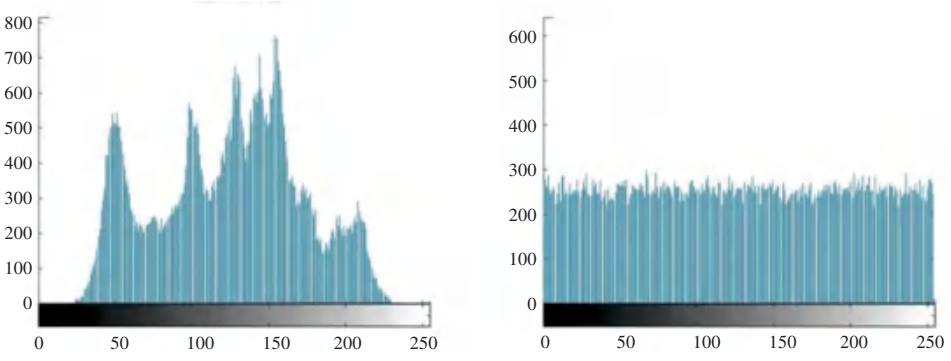
以处理 64 位数据，且数据设为双精度浮点类型，则密钥空间为2^{128}。一个理想的加密算法需要有足够大的密钥空间来抵御穷举攻击，其值不应该小于2^{100}。显然，本文加密算法具有足够大的密钥空间。

3.2　统计分析

良好的图像加密算法应该对任何形式的统计攻击都具有稳定性，因此可通过直方图、相邻像素间相关性和信息熵来分析加密算法的抗统计攻击能力。

3.2.1　直方图

图像直方图通过绘制图像的像素值来说明图像中的像素分布。理想的加密算法应该拥有均匀分布的密文直方图，因为其需要隐藏明文的有用信息[10]。本文加密算法生成的明文图像及密文图像的直方图分布如图 6 所示。密文图像的每个像素值近乎相等，呈现均匀分布，因此没有给攻击者提供任何使用统计攻击的有用信息，使其很难通过统计分析的方法来破解原始明文图像。



（a）明文图像直方图　　（b）密文图像直方图

图 6　明文与密文图像直方图

Fig. 6　Histogram of plaintext and ciphertext images

3.2.2　相邻像素间相关性

良好的加密算法应使密文图像相邻像素的相关系数足够低，用来抵御统计攻击。为了分析明文图像和密文图像中相邻像素的相关性，分别选取水平、垂直和对角方向上的相邻像素加以分析，相关性分布如图 7 所示。明文图像中相邻像素的分布比较集中，说明明文图像相邻像素相关性较高；密文图像中相邻像素比较离散，说明密文图像相邻像素相关性较低。相邻像素相关性计算公式如下：

$$\gamma_{xy} = cov(x,y)/\sqrt{D(x)D(y)} \tag{6}$$

$$E(x) = \sum_{i=1}^{T} x_i/T \tag{7}$$

$$D(x) = \sum_{i=1}^{T} (x_i - E(x))^2/T \tag{8}$$

$$cov(x,y) = \sum_{i=1}^{T} (x_i - E(x))(y_i - E(y))/T \tag{9}$$

其中，x、y 是图像中两个相邻像素的灰度值，T 为图像中选择的像素总数。

通过选取加密算法较好的 3 种算法与本文算法进行对比（对比结果见表 1）发现：本文提出的算法在水平、垂直、对角 3 个方向的相关系数都接近于 0，可以很好的消除相邻像素相关性；信息熵值更接近理想值 8；*NPCR* 值均超过 0.996、*UACI* 值均超过 0.334，能够有效抵抗差分攻击等攻击手段。因此，该加密算法可以很好的应用到图像加密过程中。

表 1　本文算法与文献[3,7,8]结果对比

Tab. 1　Comparison of the results of the algorithm in this paper and the literature [3, 7, 8]

	本文算法	文献[3]算法	文献[7]算法	文献[8]算法
相关性分析	水平-0.009 7	-0.000 4	0.003 1	0.000 8
	垂直-0.007 2	0.005 1	-0.000 9	-0.000 7
	对角-0.001 2	-0.000 4	0.003 1	0.000 2
信息熵	7.998 2	7.996 9	7.998 0	7.997 4
NPCR	0.996 0	0.996 0	0.996 3	0.998 7
UACI	0.334 2	0.336 3	0.334 7	0.333 8

从表 1 中可以看出，密文图像相邻像素的相关性较低，说明本文所提出的加密算法可以很好的抵抗统计攻击。

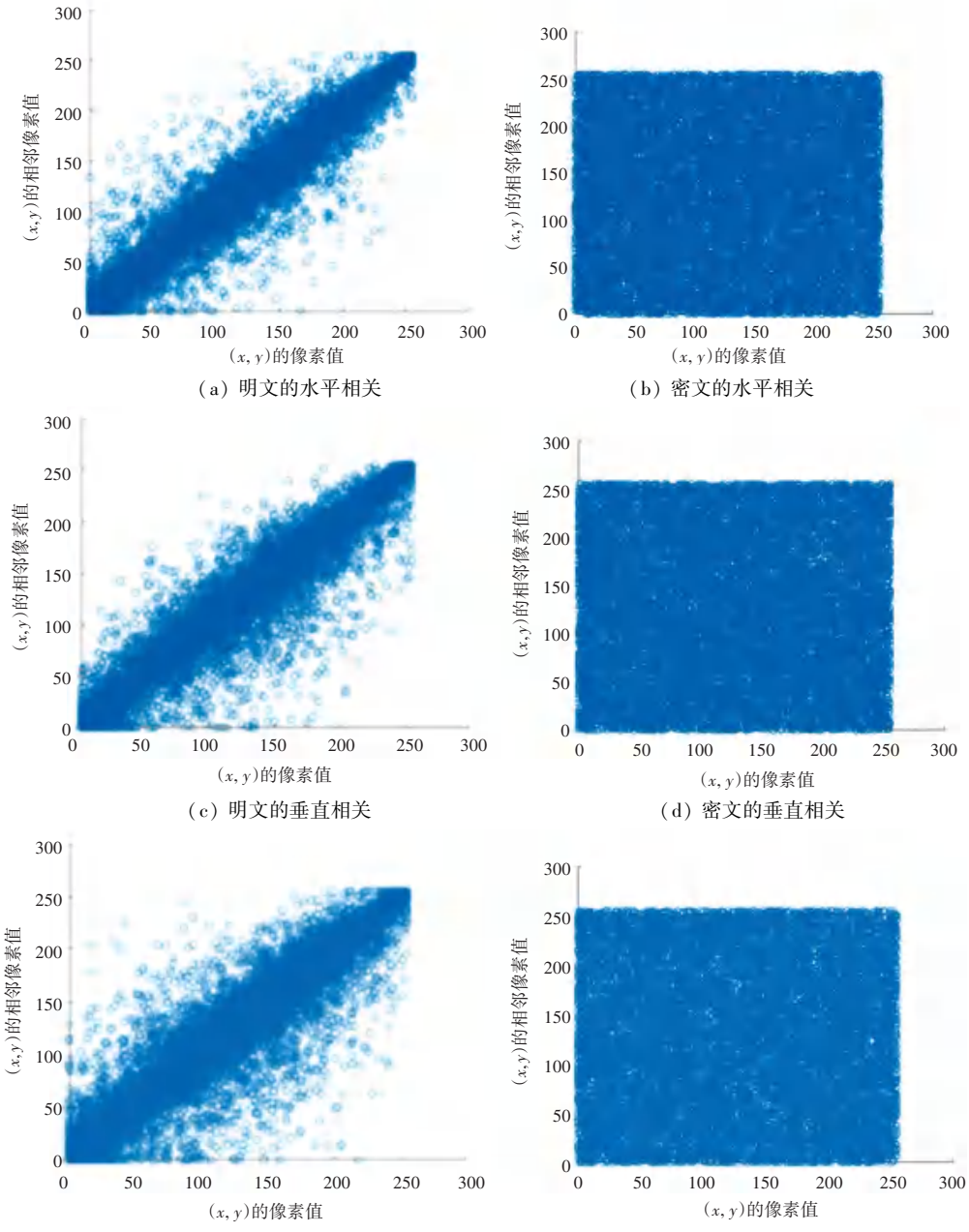
3.2.3　信息熵分析

信息熵是一种无序的、不可预测的不确定性度量。为了计算信息源 s 的信息熵 $H(s)$，则有：

$$H(s) = -\sum_{i=1}^{L} p(s_i)\log_2 p(s_i) \tag{10}$$

式中：$p(s_i)$ 为信号 s_i 的概率；L 是信号源的总数。

对于一个具有 256 个灰度级的加密图像，理想的信息熵应为 $H(s) = 8$。经过计算得到的密文图像的信息熵值见表 1，可以看出密文图像的熵非常接近理论值 8，说明本文加密算法可以很好地抵御信息熵攻击。



(a) 明文的水平相关 (b) 密文的水平相关

(c) 明文的垂直相关 (d) 密文的垂直相关

(e) 明文的对角相关 (f) 密文的对角相关

图 7 加密图像相关性

Fig. 7 Encrypted image correlation

3.3 敏感性分析

加密算法应能满足密钥的敏感性,这样才能在一定程度上保证加密系统可以有效抵抗差分攻击。

3.3.1 明文敏感性分析

良好的加密系统,应该确保对明文图像的任何微小改变都会导致加密图像的显著差异,即明文敏感性[11]。通过计算 *NPCR*(像素数变化率)和 *UACI*(归一平均变化强度)来衡量明文敏感性。

$$NPCR = \left(\sum_{i=1}^{M}\sum_{j=1}^{N} |D(C_1(i,j), C_2(i,j)|\right) \times 100\%/MN \tag{11}$$

$$UACI = \left(\sum_{i=1}^{M}\sum_{j=1}^{N} \left(|C_1(i,j) - C_2(i,j)|\right)\right) \times 100\%/255 \tag{12}$$

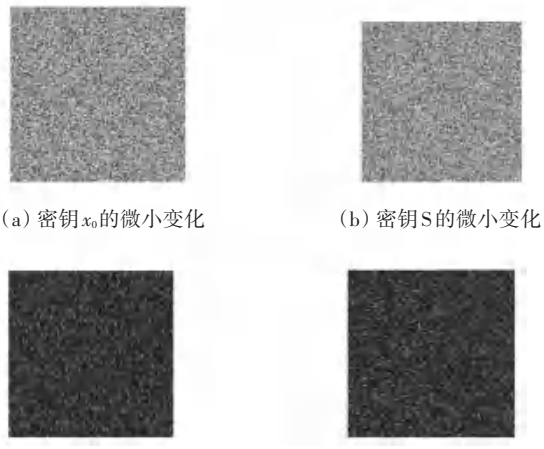
其中,M、N 分别为图像的行和列;C_1、C_2 分别表示密文图像和明文图像发生微小变化后的密文图像;函数 D 用来比较两个数值是否相同。

当 $C_1(i,j) = C_2(i,j)$ 时 $D(C_1(i,j), C_2(i,j)) = 0$,否则 $D(C_1(i,j), C_2(i,j)) = 1$。*NPCR* 越接近理想值 0.996 1,说明密文对明文的敏感性越好,而 *UACI* 越接近理想值 0.3446,说明加密算法抵抗差分攻击的能力越强。

3.3.2　密钥敏感性分析

密钥敏感性是指当密钥发生微小变化时，得到的密文图像也会引起很大变化。

以图 5(b)的加密图像为例，图 8 给出了密钥微小变化时的仿真实验结果。其中，图 8(a)和图 8(b)分别是密钥取 $(x_0,S)=(0.234+10^{-10},0.128)$ 和 $(x_0,S)=(0.234,0.128+10^{-10})$ 的密文图像。由此可见，即使密钥发生微小变化，也会生成完全不同的加密图像，证明该加密算法的密钥，即使存在微小的差异也不能正确解密图像。



(a) 密钥 x_0 的微小变化　(b) 密钥 S 的微小变化

(c) 密文与图(a)的差异　(d) 密文与图(b)的差异

图 8　密钥敏感性分析

Fig. 8　Key Sensitivity Analysis

4　结束语

本文设计了一种 Logistic 和 Sine 映射的非线性组合 Logistic-Sine 混沌映射，通过 Logistic-Sine 映射的分岔图、Lyapunov 指数变化图对其混沌性能进行了分析。结果表明，该算法具有良好的动态特性，适合应用于图像加密中。此外，比特重组方法也提高了加密效率。将 Logistic-Sine 映射与比特重组相结合，设计的图像加密方案，通过一系列安全性分析，表明该算法是安全可靠的图像加密算法。

目前，本文仅对标准 256×256 的 Lena 灰度图像进行了仿真实验和相关安全性分析，后续工作考虑进一步将加密方案推广到对彩色图像的研究上，同时考虑本文加解密算法能否进一步优化，以期获得更好的加密性能。

参考文献

[1] 鲜永菊，谢世杰，涂艳丽. 基于超混沌系统的多图加密算法[J]. 重庆邮电大学学报(自然科学版)，2020，32(6)：1065-1074.

[2] 庶朝永，秦拯，黎谦. 联合二维 logistic 混沌映射与比特重组的彩色图像加密算法[J]. 计算机科学，2013，40(8)：300-302，308.

[3] 廖春成，周小平，廖春龙，等. 像素位置与比特双重置乱的混沌图像加密算法[J]. 中国科技论文，2014，9(1)：112-116.

[4] LI Yueping，WANG Chunhua，CHEN Hua. A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation[J]. Optics and Lasers in Engineering，2017，90(3)238-246.

[5] 伍朝阳，孙树亮，刘庆. 基于像素层与比特层置乱的超混沌图像加密算法[J]. 中国科技论文，2018，13(14)：1609-1613.

[6] 胡春杰，阮聪，牛智星. 基于改进 Logistic 映射的图像加密算法[J]. 计算机系统应用，2019，28(6)：125-129.

[7] 韩雪娟，李国东. 动态猫变换和混沌映射的图像加密算法[J]. 计算机工程与设计，2020，41(8)：2381-2387.

[8] 郭媛，周艳艳，敬世伟. 基于图像重组和比特置乱的多图像加密[J]. 光子学报，2020，49(4)：174-186.

[9] 朱淑芹，王文宏，孙忠贵. 对一种基于比特置乱的超混沌图像加密算法的选择明文攻击[J]. 计算机科学，2017，44(11)：273-278.

[10] 董小雨，冯秀芳. 基于动态密钥的彩色图像扩散加密算法[J]. 计算机工程与设计，2021，42(5)：1383-1391.

[11] ZHU Zhiliang，ZHANG Wei，WONG Kwok-wo，et al. A chaos-based symmetric image encryption scheme using a bit-level permutation[J]. Information Sciences，2010，181(6)：1171-1186.

(上接第 172 页)

通过分析主要操作变量对辛烷值损失的影响，为企业汽油精制处理过程中的实际操作提供可靠参考，帮助企业实现经济效益最大化。

参考文献

[1] 包芳. 基于互信息的特征选择算法研究[D]. 长春：长春工业大学，2021.

[2] 侯旺超，梁华国，宋钦，等. 联合 mRMR 算法和 BP 神经网络的集成电路测试方法[J]. 微电子学，2021，51(5)：766-772.

[3] 王晓敏，刘希玉，戴芬. BP 神经网络预测算法的改进及应用[J]. 计算机技术与发展，2009，19(11)：64-67.

[4] 孙忠超，山红红，刘熠斌，等. 用于 FCC 汽油辛烷值预测的非线性数学模型[J]. 炼油技术与工程，2012，42(2)：60-64.

[5] 周欢，齐万松，李宏勋. S Zorb 装置辛烷值损失大原因的分析与措施[J]. 云南化工，2019，46(9)：90-91，95.

变更声明

因作者变更了文章中作者的顺序，而没有发给编辑部最终修改稿，导致《智能计算机与应用》2021 年第 11 卷第 7 期第 60 页文章《基于多特征优选的图像拼接算法及系统设计》的作者顺序出错，现作者顺序更正为：党良慧，张玉金，姜月武，路东生，杨永兆，施建新。

特此向读者致歉，并发此变更声明。

《智能计算机与应用》编辑部

2022 年 2 月 10 日