

# 一种基于 Logistic-Sine-Cosine 映射的彩色图像加密算法



张赛男 李千目

南京理工大学计算机科学与工程学院 南京 210094

(18805156909@163.com)

**摘要** 科技的飞速发展为拍摄和分享图像带来了便利,但随着图像数据的急剧增多,泄露和篡改等安全问题也频频发生,图像加密技术的应用迫在眉睫,尤其是彩色图像的加密急需改进与发展。传统的加密技术主要是针对数据流加密,其效率低、计算量大,存在一定的局限性。基于变换域加密将图像从空域变换到频域进行加密再变换到空域,属于一种有损加密。基于混沌的加密,密钥空间大,实现简单,加密速度快,一般需要采用多个混沌系统来增强加密的安全性。为此,文中设计了一种针对彩色图像 RGB 三通道的简单安全的空域加密算法,先由 Logistic-Sine-Cosine 映射生成较为安全的混沌序列,接着利用混沌序列设计 4 轮置乱和扩散像素,最后,在一系列安全性分析实验中验证了基于 Logistic-Sine-Cosine 映射的彩色图像加密算法的安全性和有效性。

**关键词:**RGB 彩色图像;Logistic-Sine-Cosine 映射;行列通道置乱;三通道像素;图像加密

**中图法分类号** TP309.7

## Color Image Encryption Algorithm Based on Logistic-Sine-Cosine Mapping

ZHANG Sai-nan and LI Qian-mu

School of Computer Science and Engineering, Nanjing University of Science and Technology, Nanjing 210094, China

**Abstract** The rapid development of technology has brought convenience for shooting and sharing images. However, with the rapid increase of image data, security problems such as leakage and tampering have frequently occurred. The application of image encryption technology is imminent. Especially the encryption of color images is in urgent need of improvement and development. The traditional encryption technology is mainly for data stream encryption, which is low in efficiency and large in calculation, having certain limitations. Based on the transformation domain encryption, the image is transformed from the spatial domain to the frequency domain for encryption, and then transformed to the spatial domain, which is a lossy encryption. Encryption based on chaos has a large key space, simple implementation, and fast encryption speed. However, multiple chaotic systems are generally required to enhance the security of encryption. For this reason, a simple and secure spatial encryption algorithm for the RGB three-channel color image is designed in this paper. The Logistic-Sine-Cosine mapping generates safer chaotic sequences. These chaotic sequences are used for four rounds of scrambling and spreading pixels. After a series of security analysis experiments, the security and effectiveness of the color image encryption algorithm based on Logistic-Sine-Cosine mapping have been verified.

**Keywords** RGB color image, Logistic-Sine-Cosine mapping, Row column channel scrambling, Three-channel pixel, Image encryption

## 1 引言

社交网站分享平台的快速发展导致图像数据量不断增长,海量的图像数据中彩色图像居多,大都是以明文形式存储的,以节省存储与计算资源的开销。这样存在着泄露隐私的巨大风险,亟需安全、快速的彩色图像加密手段来保护数据安全和用户隐私安全。

传统的加密技术如 DES, 3-DES, IDEA, AES<sup>[1]</sup> 主要是针

对数据流进行加密,效率低、计算量大<sup>[2]</sup>,尤其是在处理彩色图像时,计算量将大大增加。根据文献[3],目前的图像加密可大致分为:基于空间域的像素置乱、基于混沌的加密、基于变换域的加密、基于秘密分割与秘密分享的加密、基于神经网络和元胞自动机的加密等。

基于空间域的像素置乱是打乱图像像素位置但不改变像素值的图像加密方法,常用的置乱方法有 Arnold 变换、Baker 映射、SCAN 模式、骑士巡游等。一般来说,这种加密算法的

到稿日期:2020-10-09 返修日期:2021-01-21 本文已加入开放科学计划(OSID),请扫描上方二维码获取补充信息。

基金项目:国家重点研发计划(2020YFB1804604);2020 年工信部工业互联网创新工程;江苏省重点研发计划(BE2016904)

This work was supported by the National Key Research and Development Program(2020YFB1804604), 2020 Industrial Internet Innovation Project of the Ministry of Industry and Information Technology and Jiangsu Province Key Research and Development Program(BE2016904).

通信作者:李千目(lqianmu@126.com)

安全性较低,计算复杂度小。

基于混沌<sup>[4-5]</sup>的加密方法,顾名思义汲取混沌理论的良好特性来构建加密系统,基于混沌的加密系统的优点有密钥空间大、实现简单、加密速度快,但也存在缺点:1)单一的混沌系统生成的混沌序列周期短、随机性不好,存在平凡或拟平凡密钥<sup>[6]</sup>,平凡密钥或拟平凡密钥作为初始值生成的混沌序列是固定不变的,无法用于图像加密;一维或者二维的混沌系统容易破解,高维混沌系统或超混沌系统等复杂的混沌系统可能生成随机性能更好的混沌序列,但是这种随机性是以牺牲速度来换取的。

基于变换域的加密是一种有损加密算法,原因是计算机精度有限,将图像从空域变换到频域进行加密处理,然后再变换到空域,会丢失一部分的数据精度。一般常与压缩结合,以最大限度地利用变换与反变换耗费的计算量。与压缩结合之后的频域加密算法,需要在考虑压缩效果和图像质量的基础上进行局部置乱、代换和扩散,从而缩减加密数据、加快效率,实现加密、压缩。

基于秘密分割与秘密分享的加密是将图像加密成  $m$  个密文图像,并且设置一个  $n(n \leq m)$  值,只有收集到任意  $j(j \geq n)$  个密文图像,将它们结合才可重构原图。基于秘密分割与秘密共享的优点在于密文图像分存,且有冗余,丢失少量密文图像不影响图像的解密和信息泄露。缺点也显而易见,即密文数据量过于冗余。基于神经网络和元胞自动机的图像加密算法都是结合自身非线性或者自组织性等适宜特性生成图像加密所需的伪随机序列。这类方法的一大优点就是为图像并行加密开拓了思路。

此外,还有基于 DNA<sup>[7]</sup> 的加密算法、选择加密算法<sup>[8]</sup>、光学加密<sup>[9]</sup> 算法、随机格<sup>[10-11]</sup> 可视化加密等。本文设计的加密算法属于空域上的加密算法,是一种无损的图像加密算法,计算量较小,基于混沌序列设计混淆和扩散,安全性较高,并且针对彩色图像,适合应用于当前大部分图像数据。

## 2 相关工作

目前已经有许多学者对彩色图像的加密进行了研究。文献[12]基于 4 种混沌映射复合混沌和有限整数域上的仿射变换,结合 JPEG 压缩编码进行加密。文献[13]利用超混沌系统结合 DNA 序列,针对彩色图像的 RGB 3 个矩阵进行混淆和扩散。文献[14]组合 Logistic, Sine 和 Tent 映射提出新的混沌系统,并基于此设计循环移位和分块等操作加密图像。文献[15]提出了基于余弦变换的混沌系统,并基于其中的 Logistic-Sine-Cosine 映射生成混沌序列设计位置置乱和像素扩散加密灰度图像,没有针对彩色图像进行另外设计,彩色图像的三通道是分开处理的,其中位置置乱针对的是图像中最大的正方形区域,之后旋转 90° 进行像素扩散,如此重复 4 轮。

本文采用的 Logistic-Sine-Cosine 映射是由文献[15]提出的,基于 Logistic-Sine-Cosine 映射良好的混沌特性,设计新的高效的行、列、通道位置置乱方法和循环扩散像素方法,如此重复 4 轮以保障图像数据的安全,图 1 所示为加密流程图。

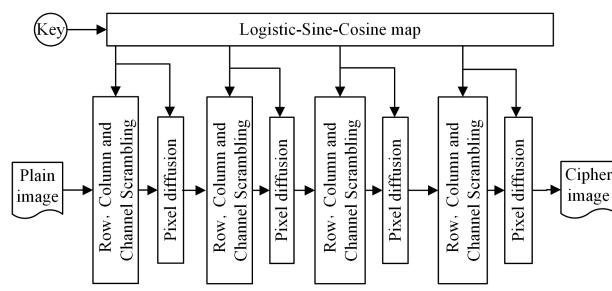


图 1 图像加密流程图

Fig. 1 Image encryption flowchart

## 3 基于 Logistic-Sine-Cosine 映射的彩色图像加密算法

### 3.1 Logistic-Sine-Cosine 映射

将两个一维混沌映射(Logistic 映射和 Sine 映射)作为种子映射,与余弦映射级联,构成 Logistic-Sine-Cosine 映射<sup>[15]</sup>:

$$x_{i+1} = \cos(\pi(F(a, x_i) + G(b, x_i) + \beta)) \quad (1)$$

其中,  $F(a, x_i) = \mathcal{L}(r, x_i)$ ,  $G(b, x_i) = \mathcal{H}(1-r, x_i)$ 。

Logistic 映射为:  $x_{i+1} = \mathcal{L}(r, x_i) = 4rx_i(1-x_i)$ , Sine 映射为:  $x_{i+1} = \mathcal{H}(r, x_i) = r \sin(\pi x_i)$ 。最终, Logistic-Sine-Cosine 映射为:  $x_{i+1} = \cos(\pi(4rx_i(1-x_i) + (1-r)\sin(\pi x_i) - 0.5))$ 。其中,  $r \in [0, 1]$ ,  $x \in (0, 1)$ 。可以通过设置初始状态  $x_0$  和控制参数  $r$  作为密钥,来决定生成的确定的混沌序列。

Logistic-Sine-Cosine 映射的混沌性能已在文献[15]中通过分叉图、Lyapunov 指数、样本熵这 3 方面得到充分验证,这里不再赘述。简单地说,Logistic-Sine-Cosine 映射中无论参数怎样变化,即  $r \in [0, 1]$ ,  $x \in (0, 1)$ , 都能呈现出复杂的行为,输出状态是随机分布的,如图 2 所示。如图 3 所示,  $r \in [0, 1]$ , Logistic-Sine-Cosine 映射的 Lyapunov 指数都大于 0, 且在 1.374~1.386 范围内,即  $r \in [0, 1]$ , Logistic-Sine-Cosine 映射都能呈现复杂的混沌行为。

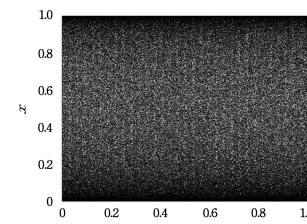


图 2 Logistic-Sine-Cosine 映射的分叉图

Fig. 2 Bifurcation graph of Logistic-Sine-Cosine mapping

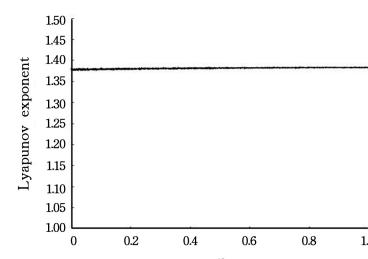


图 3 Logistic-Sine-Cosine 映射的 Lyapunov 指数

Fig. 3 Lyapunov exponent of Logistic-Sine-Cosine mapping

### 3.2 密钥分布和加密算法结构

密钥是随机生成的 256 位二进制数,密钥组成为:4 个 32

位的初始状态  $x_0$ 、4 个 32 位的控制参数  $r$ 。32 位二进制数由式(2)转换成 0~1 之间的小数。

$$\begin{cases} x_{0\text{float}} = \sum_{i=1}^{32} x_{0\text{bin}_i} * 2^{-i} \\ r_{\text{float}} = \sum_{i=1}^{32} r_{\text{bin}_i} * 2^{-i} \end{cases} \quad (2)$$

密钥空间为  $2^{256} > 2^{100}$ , 足够抵抗各种攻击<sup>[16]</sup>。由这 4 组初始状态  $x_0$  和控制参数  $r$  生成 4 组混沌序列, 分别用于每轮明文图像的行列通道置换、像素扩散。如图 1 所示, 经过 4 轮的行列通道置换、像素扩散生成密文图像。

### 3.3 行、列、通道置乱

假设明文彩色图像  $P$  高为  $H$ 、宽为  $W$ , 由初始状态  $x_0$  和控制参数  $r$  生成  $H * W * 3$  长度的混沌序列  $S$ 。利用生成的混沌序列对图像的行、列、通道进行置乱的流程如下:

Step 1 抽取混沌序列组成 4 个序列  $J, c, l, U$ 。 $J$  长为  $H * W$ ,  $c$  长为  $H$ ,  $l$  长为  $W$ ,  $U$  即  $S$ , 长为  $H * W * 3$ 。

Step 2 排序  $c, l$ , 得到相应的索引向量  $\mathbf{I}_c, \mathbf{I}_l$ 。将  $J$  序列转换成  $(H, W)$  大小的矩阵, 每行按列排序得到  $(H, W)$  大小的索引矩阵  $Q$ , 每列按行排序得到  $(W, H)$  大小的索引矩阵  $\mathbf{I}$ 。将  $U$  序列转换成  $(H, W, 3)$  大小的矩阵, 将每  $(i, j, :)$  中的 3 个数排序, 生成  $(H, W, 3)$  大小的索引矩阵  $\mathbf{L}$ 。将  $U$  序列转换成  $(W, H, 3)$  大小的矩阵, 将每  $(i, j, :)$  中的 3 个数排序, 生成  $(W, H, 3)$  大小的索引矩阵  $\mathbf{V}$ 。

Step 3 先按照行、列、通道的顺序置乱, 假设置乱后是大小为  $(H, W, 3)$  的矩阵  $D$ , 其中  $D(i, j, u) = P(c(i), Q(c(i), j), L(c(i), Q(c(i), j), u))$ 。其中,  $i \in [1, H], j \in [1, W], u \in [1, 3]$ , 若无特殊说明, 本文中  $i, j, u$  都属于这一范围。

Step 4 再按照列、行、通道的顺序进行置乱, 假设密文图像大小为  $(H, W, 3)$  的矩阵  $C$ , 其中  $C(i, j, u) = D(I(l(j), i), l(j), V(l(j), I(l(j), i), u))$ 。

为了更生动形象地说明上述步骤, 假设  $H=2, W=3$ , 如图 4 所示, 每个框内 3 个数字分别表示行、列、通道索引(黑色底框表示红色通道, 灰色底框表示绿色通道, 白色底框表示蓝色通道)。

111	112	113	121	122	123	131	132	133
211	212	213	221	222	223	231	232	233

图 4 置乱前的行、列、通道顺序示意图

Fig. 4 Schematic diagram of the sequence of rows, columns and channels before scrambling

$$\text{假设 } \mathbf{I}_c = (2, 1), \mathbf{I}_l = (2, 1, 3), \mathbf{Q} = \begin{pmatrix} 1, 3, 2 \\ 3, 1, 2 \end{pmatrix}, \mathbf{I} = \begin{pmatrix} 1, 2 \\ 2, 1 \\ 1, 2 \end{pmatrix},$$

$$\mathbf{L} = \begin{pmatrix} \langle (1, 3, 2) | (2, 1, 3) | (1, 2, 3) \rangle \\ \langle (2, 3, 1) | (3, 2, 1) | (3, 1, 2) \rangle \end{pmatrix},$$

$$\mathbf{V} = \begin{pmatrix} \langle (3, 2, 1) | (1, 3, 2) \rangle \\ \langle (2, 3, 1) | (1, 2, 3) \rangle \\ \langle (2, 1, 3) | (3, 1, 2) \rangle \end{pmatrix}.$$

根据 Step3, 以置乱后位置为  $(1, 1, :)$  的像素为例:

(1) 置乱后位置  $(1, 1, 1)$  的像素, 是第  $\mathbf{I}_c(1) = 2$  行、第  $\mathbf{Q}(2, 1) = 3$  列、第  $\mathbf{L}(2, 3, 1) = 3$  通道的像素。

(2) 置乱后位置  $(1, 1, 2)$  的像素, 是第  $\mathbf{I}_c(1) = 2$  行、第  $\mathbf{Q}(2, 1) = 3$  列、第  $\mathbf{L}(2, 3, 2) = 1$  通道的像素。

(3) 置乱后位置  $(1, 1, 3)$  的像素, 是第  $\mathbf{I}_c(1) = 2$  行、第  $\mathbf{Q}(2, 1) = 3$  列、第  $\mathbf{L}(2, 3, 3) = 2$  通道的像素。图 4 所示的像素按行、列、通道顺序置乱后的结果如图 5 所示。

233	231	232	212	213	211	223	222	221
111	113	112	131	132	133	122	121	123

图 5 按行、列、通道顺序置乱后的示意图

Fig. 5 Schematic diagram after scrambling in the order of row, column and channel

根据 Step4, 以置乱后位置为  $(1, 2, :)$  的像素为例, 在 Step3 置乱的基础上再按照列、行、通道顺序置乱。

(4) 置乱后位置  $(1, 2, 1)$  的像素, 是第  $\mathbf{I}_l(2) = 1$  列、第  $\mathbf{I}(1, 1) = 1$  行、第  $\mathbf{V}(1, 1, 1) = 3$  通道的像素。即图 5 中第 1 行第 1 列第 3 通道的像素, 为框内数字 232 代表的像素。

(5) 置乱后位置  $(1, 2, 2)$  的像素, 是第  $\mathbf{I}_l(2) = 1$  列、第  $\mathbf{I}(1, 1) = 1$  行、第  $\mathbf{V}(1, 1, 2) = 2$  通道的像素, 即 231 代表的像素。

(6) 置乱后位置  $(1, 2, 3)$  的像素, 是第  $\mathbf{I}_l(2) = 1$  列、第  $\mathbf{I}(1, 1) = 1$  行、第  $\mathbf{V}(1, 1, 3) = 1$  通道的像素, 即 233 代表像素。

图 5 所示像素按列、行、通道顺序置乱后的结果如图 6 所示。

131	132	133	232	231	233	222	223	221
213	211	212	111	112	113	123	122	121

图 6 按列、行、通道顺序置乱后的示意图

Fig. 6 Schematic diagram after scrambling in the order of column, row and channel

由上述说明及图 4—图 6 可以看出, 按行、列、通道顺序置乱, 是先确定置乱的行数, 之后在该行中打散像素的列位置, 在该行该列的像素中打散像素通道的位置。按列、行、通道顺序置乱, 就是先确定置乱的列数, 然后在这一列打散像素的行位置, 之后在该列该行像素中打散通道位置。最终实现图像像素行、列、通道上的位置置乱。

解密时, Step1—Step2 与加密时相同, 区别是 Step3—Step4。

Step 3 先按照列、行、通道的顺序还原, 还原为  $(H, W, 3)$  的矩阵  $D$ , 其中  $D(I(l(j), i), l(j), V(l(j), I(l(j), i), u)) = C(i, j, u)$ 。

Step 4 再按照行、列、通道的顺序进行置乱, 还原为  $(H, W, 3)$  的矩阵  $P$ , 其中  $P(c(i), Q(c(i), j), L(c(i), Q(c(i), j), u)) = D(i, j, u)$ 。

这样就实现了彩色图像行、列、通道的置乱与还原。

### 3.4 像素扩散

由初始状态 $x_0$ 和控制参数 $r$ 生成 $H * W * 3$ 长度的混沌序列 $S$ ,将 $S$ 转换成 $(H, W, 3)$ 的矩阵,整体乘以 $2^{32}$ 并向右取整得到新的 $S$ 矩阵,大小为 $(H, W, 3)$ 。

设置乱后扩散前的矩阵为 $P$ ,扩散后的矩阵为 $C$ ,依据如下规则进行像素扩散, $i, j, u$ 由1分别递增至 $H, W, 3$ :

$$(1) i=1, j=1, u=1: C(i, j, u) = \text{mod}(P(i, j, u) + P(H, W, 3) + S(i, j, u), 256)$$

$$(2) i=1, j=1, u>1: C(i, j, u) = \text{mod}(P(i, j, u) + C(i, j-1, u) + S(i, j, u), 256)$$

$$(3) i=1, j\neq 1, u=1: C(i, j, u) = \text{mod}(P(i, j, u) + C(i, j-1, u) + S(i, j, u), 256)$$

$$(4) i=1, j\neq 1, u>1: C(i, j, u) = \text{mod}(P(i, j, u) + C(i, j-1, u) + C(i, j-1, u-1) + S(i, j, u), 256)$$

$$(5) i\neq 1, j=1, u=1: C(i, j, u) = \text{mod}(P(i, j, u) + C(i-1, j, u) + S(i, j, u), 256)$$

$$(6) i\neq 1, j=1, u>1: C(i, j, u) = \text{mod}(P(i, j, u) + C(i-1, j, u-1) + C(i-1, j, u) + C(i, j, u-1) + S(i, j, u), 256)$$

$$(7) i\neq 1, j\neq 1, u=1: C(i, j, u) = \text{mod}(P(i, j, u) + C(i-1, j, u) + C(i, j-1, u) + S(i, j, u), 256)$$

$$(8) i\neq 1, j\neq 1, u>1: C(i, j, u) = \text{mod}(P(i, j, u) + C(i-1, j, u-1) + C(i-1, j, u) + C(i, j, u-1) + C(i-1, j-1, u-1) + C(i-1, j-1, u) + C(i, j-1, u-1) + S(i, j, u), 256)$$

总体来说,扩散过程就是当前行列通道的像素加上行数-1或列数-1或通道数-1的已经扩散到的像素值,再加上 $S$ 当前行列通道的数值,最终取模256。若 $i=1$ 且 $j=1, u=1$ ,即该点像素是扩散操作的起始点,该点加上扩散末尾点即 $i=H, j=W, u=3$ 的像素值,再加上 $S(1, 1, 1)$ ,最后模256,得到扩散后的值。选择加上末尾的像素值,是考虑到若不在起始点加上末尾点的像素值,这样一轮扩散下来,末尾的像素无法扩散到除自身之外的像素值。因此,将末尾点像素加在扩散起始点,将大大提升本文加密算法的扩散性。

解密时, $i, j, u$ 分别由 $H, W, 3$ 递减至1。遵循的规则与加密时一致,不同之处仅仅在于加密时是加,解密时是减。受篇幅限制,仅列出与加密相对应的第一和最后一条规则的解密操作,其余规则的解密操作类似:

$$(1) i=1, j=1, u=1: P(i, j, u) = \text{mod}(C(i, j, u) - P(H, W, 3) - S(i, j, u), 256)$$

$$(2) i\neq 1, j\neq 1, u>1: P(i, j, u) = \text{mod}(C(i, j, u) - C(i, j-1, u) - C(i-1, j, u-1) - C(i-1, j, u) - C(i, j, u-1) - C(i-1, j-1, u-1) - C(i-1, j-1, u) - C(i, j-1, u-1) - S(i, j, u), 256)$$

## 4 实验及安全性分析

从密钥空间、密钥灵敏度、直方图分析、相关性分析、信息熵、像素改变率和一致改变强度等方面来进一步验证本文彩色图像加密算法的安全性和有效性。

### 4.1 密钥安全分析

首先从密钥空间分析密钥的安全性,密钥是随机生成的256位二进制数,密钥组成由4个32位的初始状态 $x_0$ 、4个32位的控制参数 $r$ 组成,密钥空间为 $2^{256} > 2^{100}$ ,足够抵抗各种攻击<sup>[16]</sup>。

接着利用改变密钥一个比特导致加密图像改变的比特数占图像所有比特数的比重(Number of Bit Change Rate, NBCR)<sup>[17]</sup>来测量密钥的灵敏度,一定程度上证实了密钥的实际空间不会小于理论值,即不能用与正确密钥差别很小的错误密钥解开加密图像。

假设两张彩色图像为 $P_1$ 和 $P_2$ ,NBCR为:

$$\text{NBCR}(P_1, P_2) = \frac{\text{Ham}(P_1, P_2)}{3 * H * W * 8} \quad (3)$$

$\text{Ham}(P_1, P_2)$ 是 $P_1$ 和 $P_2$ 所有像素的汉明距离, $3 * H * W * 8$ 是图像的总比特数。

给定密钥 Key,依次改变 Key 中的 256 位比特,每改变一位比特,用改变后的密钥与原密钥 Key 加密相同图像 $P$ ,得到密文图像 $C_1$ 和 $C_2$ ,并计算相应的  $\text{NBCR}(C_1, C_2)$ ,解密 $C_1$ 时利用改变后的密钥和 Key 解密得 $D_1$ 和 $D_2$ ,并计算相应的  $\text{NBCR}(D_1, D_2)$ ,结果如图 7、图 8 所示,  $\text{NBCR}(C_1, C_2)$ 和  $\text{NBCR}(D_1, D_2)$ 都在 0.5 左右以很小的幅度振荡,说明本文加密算法的密钥很灵敏,当密钥的一个比特改变时,所获得的加密图像、解密图像大相径庭。

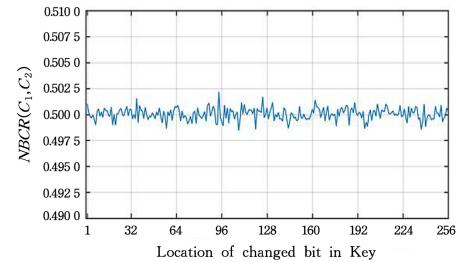


图 7  $\text{NBCR}(C_1, C_2)$

Fig. 7  $\text{NBCR}(C_1, C_2)$

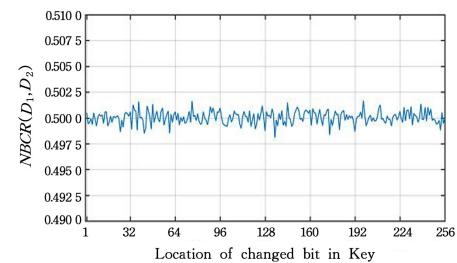


图 8  $\text{NBCR}(D_1, D_2)$

Fig. 8  $\text{NBCR}(D_1, D_2)$

### 4.2 统计分析

接着对加密算法进行统计分析,通过分析加密图像的直方图、相邻像素的相关性、信息熵,来测试算法的混乱和扩散性能以及抵抗统计攻击的能力。

如图 9 所示,加密后图像的三通道直方图都接近一致分布,与原图的三通道直方图完全不一样。

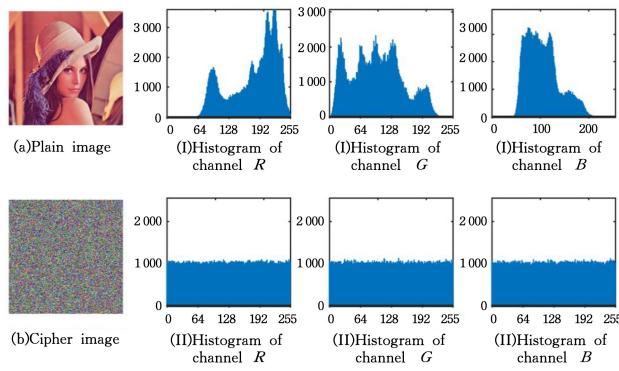


图 9 Lena 图及 Lena 加密图的 RGB 直方图

Fig. 9 RGB histogram of Lena and Lena encrypted image

在 Lena 原图( $512 \times 512$ )三通道和加密图的三通道上分别随机选取 2000 对水平、垂直、对角方向上的相邻像素,计算水平、垂直、对角线方向的相关性。如表 1 所列,加密前所有方向上的相邻像素的相关性都接近 1,加密后所有方向上的相邻像素的相关性都接近 0,说明本文加密算法具有良好的混淆和扩散性能。

表 1 Lena 原图与加密图的三通道相关性对比

Table 1 Comparison of three-channel correlation between Lena original image and encrypted image

	R	G	B
Plain image	7.2525	7.5940	6.9684
Cipher image	7.9912	7.9917	7.9912

当图像中各灰度值出现概率相等时,图像信息熵最大。信息熵也是分析图像加密算法的一个度量,有效的加密算法应该生成一个理想的随机加密图像,信息熵等于 8。如表 2 所列,加密图像的信息熵都为 7.99+,十分接近 8。

表 2 Lena 原图与加密图的三通道信息熵对比

Table 2 Comparison of three-channel information entropy between Lena original image and encrypted image

	Horizontal	Vertical	Diagonal
Channel R	Plain	0.9810	0.9902
	Cipher	0.0091	0.0007
Channel G	Plain	0.9704	0.9821
	Cipher	-0.0195	0.0153
Channel B	Plain	0.9339	0.9591
	Cipher	0.0196	0.0297

#### 4.3 扩散性分析

最后,针对本文提出的加密算法进行扩散性测试,使用像素改变率(Number of Pixels Change Rate, NPCR)和一致平均改变强度(Unified Average Changing Intensity, UACI)来测量稍微改变原图中一个像素时对加密图的影响。

本文选择了 USC-SIPI “Aerials”中的彩色图<sup>1)</sup>进行 NPCR 和 UACI 测试,其中图 4.1.01, 4.1.02, 4.1.03, 4.1.04, 4.1.05, 4.1.06, 4.1.07, 4.1.08 是  $256 \times 256$  大小的,图 4.2.01, 4.2.03, 4.2.05, 4.2.06, 4.2.07, house 是  $512 \times 512$  大小的。每次都是随机生成密钥,随机选择行、列、通道索引,将选择的像素值加一,计算改变前后加密图的平均像素改变

率和平均一致改变强度。测试结果是随机测试 10 次的平均值,如表 3 所列,当图像为  $256 \times 256$  大小时,只有加密算法的  $NPCR > 99.5693\%$ ,  $UACI \in (33.2824\%, 33.6447\%)$  才算通过了测试;图像为  $512 \times 512$  大小时,只有加密算法的  $NPCR > 99.5893\%$ ,  $UACI \in (33.3730\%, 33.5541\%)$ ,才算通过了测试<sup>[15]</sup>。表 3 中,所有图片都通过了测试,表明本文算法的扩散性良好。

表 3 14 张彩色图的 NPCR 和 UACI 测试结果

Table 3 NPCR and UACI test results of 14 color pictures

Image	NPCR			UACI			test
	R	G	B	R	G	B	
4.1.01	99.62	99.60	99.61	33.45	33.47	33.45	✓
4.1.02	99.62	99.60	99.61	33.47	33.47	33.46	✓
4.1.03	99.60	99.61	99.61	33.50	33.45	33.44	✓
4.1.04	99.61	99.60	99.61	33.42	33.46	33.50	✓
4.1.05	99.62	99.61	99.60	33.48	33.47	33.50	✓
4.1.06	99.62	99.61	99.61	33.47	33.53	33.49	✓
4.1.07	99.61	99.61	99.61	33.47	33.51	33.48	✓
4.1.08	99.61	99.60	99.59	33.45	33.41	33.46	✓
4.2.01	99.61	99.61	99.61	33.48	33.49	33.46	✓
4.2.03	99.61	99.61	99.61	33.48	33.49	33.46	✓
4.2.05	99.61	99.61	99.60	33.46	33.46	33.44	✓
4.2.06	99.61	99.61	99.61	33.48	33.44	33.46	✓
4.2.07	99.60	99.60	99.61	33.46	33.47	33.46	✓
house	99.60	99.62	99.61	33.46	33.49	33.48	✓

随机加密 Lena( $256 \times 256$ )图 100 次,每次都是随机生成密钥,随机选择行、列、通道索引,将选择的像素值加一,计算改变前后加密图的平均像素改变率和平均一致改变强度,如表 4 所列。与文献[18-21]相比,本文算法的平均像素改变率和平均一致改变强度总体来说略高一些。可以说,本文所用的加密算法具有良好的扩散性,当稍微改变某一个像素时,将导致加密图像中平均 99.61% 以上像素的变化,变化幅度平均在 33.46% 以上,达到了不错的像素改变率和一致平均改变强度。

表 4 不同加密算法加密 Lena 图的 NPCR 和 UACI 对比

Table 4 Comparison of NPCR and UACI for the Lena by different encryption algorithms

	R	G	B
NPCR/%	99.6093	99.6117	99.6130
Ref. [18]	99.60	99.61	99.61
Ref. [19]	99.6078	99.6088	99.6081
Ref. [20]	99.63	99.60	99.60
Ref. [21]	99.6097	99.5994	99.5975
UACI/%	33.4638	33.4603	33.4630
Ref. [18]	33.56	33.45	33.49
Ref. [19]	33.0291	33.4252	33.4219
Ref. [20]	33.60	33.30	33.40
Ref. [21]	33.4477	33.4655	33.4769

综上所述,各种评估和检测证明,本文提出的加密算法安全可靠,具有足够安全的密钥空间,能够抵抗统计攻击、差分攻击等。

**结束语** 结合已有研究的图像加密算法的优缺点,本文提出了一种计算量较小、安全可靠的图像加密算法,主要是利用 Logistic-Sine-Cosine 映射生成混沌序列,基于这种较为

<sup>1)</sup> <http://sipi.usc.edu/database/database.php?volume=misc>

安全的混沌序列,设计了4轮行列通道置乱和循环像素扩散,简单、快速而有效地增强了算法的混淆性和扩散性,保障了本文加密算法的安全性和可靠性。

在实际应用中,在一些情况下,如图像隐私保护,不需要对所有图像信息进行加密,以免过于浪费计算资源。在之后的研究中,将考虑对图像部分信息加密,这样既可保护图像隐私信息,又可节省计算资源和时间。

## 参 考 文 献

- [1] ZHANG Q,DING Q. Digital Image Encryption Based on Advanced Encryption Standard (AES)[C]// Proceedings of Fifth International Conference on Instrumentation and Measurement, Computer, Communication and Control (IMCCC). Qinhuangdao:IEEE Press,2015:1218-1221.
- [2] WEN C C,WANG Q,CHEN Q,et al. A new JPEG color image encryption algorithm[J]. System Engineering and Electronic Technology,2012,34(6):1283-1287.
- [3] WEN C C,WANG Q,MIAO X N,et al. Overview of Digital Image Encryption[J]. Computer Science,2012,39(12):6-9.
- [4] TIAN J F,PENG J J,ZUO X Y,et al. Image Encryption Algorithm Based on Cyclic Shift and Multiple Chaotic Maps[J]. Computer Science,2020,47(10):327-331.
- [5] BAN D H,LV X,WANG X Y. Efficient Image Encryption Algorithm Based on 1D Chaotic Map[J]. Computer Science,2020,47(4):278-284.
- [6] FAN Y J,SUN X H,YAN X D,et al. An image scrambling encryption algorithm based on mixed chaotic sequence[J]. Journal of Image and Graphics,2006(3):93-99.
- [7] CHAI X,FU X,GAN Z,et al. A color image cryptosystem based on dynamic DNA encryption and chaos[J]. Signal Processing, 2019,155:44-62.
- [8] HONG K,JUNG K. Partial Encryption of Digital Contents Using Face Detection Algorithm[C]// Proceedings of the 9th Pacific Rim International Conference on Artificial Intelligence. Berlin:Springer-Verlag,2006:632-640.
- [9] JUAN M V O,JIMENEZ C J,CESAR O T M. Optical Image Encryption System Using Several Tilted Planes[J]. Photonics, 2019,6(4):116.
- [10] SHYU S J. Image encryption by random grids [J]. Pattern Recognition,2007,40(3):1014-1031.
- [11] SHYU S J. Image encryption by multiple random grids[J]. Pattern Recognition,2009,42(7):1582-1596.
- [12] WEN C C,WANG Q,HUANG F M,et al. Adaptive encryption algorithm for JPEG color images[J]. Journal of Computer Aided Design and Graphics,2012,24(4):500-505.
- [13] WEI X,GUO L,ZHANG Q,et al. A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system[J]. Journal of Systems & Software, 2014, 85 (2): 290-299.
- [14] PARVAZ R,ZAREBNIA M. A combination chaotic system and application in color image encryption[J]. Optics & Laser Technology,2018,101:30-41.
- [15] HUA Z,ZHOU Y,HUANG H. Cosine-transform-based chaotic system for image encryption[J]. Information Sciences, 2019, 480:403-419.
- [16] ALVAREZ G,LI S. Some basic cryptographic requirements for chaos-based cryptosystems[J]. International Journal of Bifurcation and Chaos,2006,16(8):2129-2151.
- [17] CASTRO J C H,SIERRA J M,SEZNOC A,et al. The strict avalanche criterion randomness test[J]. Mathematics and Computers in Simulation,2005,68(1):1-7.
- [18] CHAI X,FU X,GAN Z,et al. A color image cryptosystem based on dynamic DNA encryption and chaos[J]. Signal Processing, 2019,155:44-62.
- [19] REHMAN A U,LIAO X,ASHRAF R,et al. A color image encryption technique using exclusive-OR with DNA complementary rules based on chaos theory and SHA-2[J]. Optik,2018,159: 348-367.
- [20] WANG X,ZHANG H,BAO X. Color image encryption scheme using CML and DNA sequence operations[J]. Biosystems,2016, 144:18-26.
- [21] KADIR A,AILI M,SATTAR M. Color image encryption scheme using coupled hyper chaotic system with multiple impulse injections[J]. Optik,2017,129:231-238.



**ZHANG Sai-nan**, born in 1997, post-graduate. Her main research interests include image encryption and privacy protection.



**LI Qian-mu**, born in 1979, Ph.D, professor, Ph.D supervisor. His main research interests include information security, computing system management, and data mining.

(责任编辑:喻藜)