结合 Logistic 映射和直方图特征引导的非对称加密算法设计

李豪杰[1,2],李 梦[1,2],许晓曾[1]
1. 重庆工商大学 数学与统计学院,重庆 400067
2. 统计智能计算与监测重庆市重点实验室,重庆 400067

摘 要:目的 针对传统图像加密算法运算量大、速度慢且需要设计大量密钥的问题,提出结合 Logistic 映射和直方图特征引导的非对称加密方案。**方法** 在加密过程中提取直方图的峰值点和谷值点作为加密私钥,并利用 Logistic 映射生成两个混沌序列,分别指导图像像素的灰度加密和置乱加密。灰度加密的同时进行了像素的向后扩散;置乱加密时,先根据尺寸密钥对图像进行分块处理,然后将每个块的内部像素进行水平或垂直平移。**结果** 对多张灰度图像和彩色图像进行加密和解密测试,并从各种经典攻击角度验证方案的安全性,发现该方案对图像内容加密效果良好,并完整保留了图像的质量和视觉效果。此外,相比于其他对比算法,用该方案加密后的图像熵值更接近 8。**结论** 该方案通过引入非线性混沌运算,并利用图像自身信息作为密钥,在实现简易运算的同时,不仅增加了加密算法的复杂性,也使得私钥在加密过程就完成了自动设计,避免了人为设计私钥的过程,显著提高了加密效率。

关键词:图像加密;混沌序列;Logistic 映射;直方图特征
中图分类号:TP309.7 **文献标识码:**A doi:10.16055/j.issn.1672-058X.2026.0001.005

Design of Asymmetric Encryption Algorithm Combining Logistic Mapping and Histogram Feature Guidance

LI Haojie[1,2], LI Meng[1,2], XU Xiaozeng[1]
1. School of Mathematics and Statistics, Chongqing Technology and Business University, Chongqing 400067, China
2. Chongqing Key Laboratory of Statistical Intelligent Computing and Monitoring, Chongqing 400067, China

Abstract: Objective To address the issues of high computational complexity, slow speed, and the requirement for a large number of keys in traditional image encryption algorithms, an asymmetric encryption scheme guided by the combination of Logistic mapping and histogram features is proposed. **Methods** During the encryption process, peak and valley points from the image histogram were extracted to serve as private keys. Two chaotic sequences were generated using Logistic mapping to guide the grayscale encryption and scrambling encryption of image pixels, respectively. Pixel backward diffusion was performed concurrently with the grayscale encryption. During scrambling encryption, the image was first divided into blocks according to the size key, and then the internal pixels of each block were translated horizontally or vertically. **Results** Encryption and decryption tests were carried out on multiple grayscale and color images. The security of the scheme was verified from various classic attack perspectives. It was found that the scheme had a good encryption effect on image content and fully preserved the quality and visual effects of the images. Additionally, compared with other comparison algorithms, the entropy value of the images encrypted by this scheme was closer to 8. **Conclusion** By incorporating nonlinear chaotic operations and utilizing the image' s inherent information as keys, this scheme not only

收稿日期:2024-02-07 **修回日期:**2024-04-10 **文章编号:**1672-058X(2026)01-0039-08
基金项目:重庆市自然科学基金(CSTC2020JCYJ-MSXMX0162)项目资助.
作者简介:李豪杰(2001—),男,重庆长寿人,硕士研究生,从事信息安全研究.
通信作者:李梦(1973—),女,四川开江人,博士,教授,从事信息安全与大数据分析研究. Email:limeng7@ctbu.edu.cn.
引用格式:李豪杰,李梦,许晓曾. 结合 Logistic 映射和直方图特征引导的非对称加密算法设计[J]. 重庆工商大学学报(自然科学版),2026,43(1):39-46.
LI Haojie, LI Meng, XU Xiaozeng. Design of asymmetric encryption algorithm combining logistic mapping and histogram feature guidance[J]. Journal of Chongqing Technology and Business University (Natural Science Edition), 2026, 43(1): 39-46.

simplifies the computational process and increases the complexity of the encryption algorithm, but also automates the private key design during encryption, thereby eliminating the need for manual key design. This approach significantly enhances encryption efficiency.

Keywords: image encryption; chaotic sequence; Logistic mapping; histogram feature

随着互联网的高速发展和通信技术的广泛应用,每天都有成千上万的数字图像在网络上传输。如何安全有效加密保护这些图像数据已经成为信息时代的重要课题。图像加密在保护敏感信息、确保隐私、防止信息泄露等方面起着关键作用,但在提高加密算法的安全性、运算速度等方面还有待研究。

密码学中有对称加密与非对称加密两种机制。对于图像的对称加密,已有的经典加密方案包括RGB平移方案[1]、基于DES技术的加密方案[2]等,这些算法都是简单的线性操作,易被差分分析和线性分析破解[3]。因此有学者将混沌映射引入加密系统,增加了加密算法的随机性和非线性性[4-5]。在对称加密算法中,加密和解密采用的是某一固定密钥,无法实现安全认证,且密钥的管理是较大的负担。基于此,有许多学者提出非对称加密的概念和经典算法[6-7],使得不同图像具有不同的私钥,每个图像的加密都互不相干。但一般的非对称加密运算缓慢,计算量大,且每个图像都需要独立设置自己的私钥。随着信息量的成倍增加,这将造成较大的计算压力。近年来,有学者将深度学习用于图像变换[8],但是神经网络的构建和运行对计算机的运算能力有较高的要求。一种减少传输和计算成本的方法是将图像进行压缩加密[9],但是一般的压缩过程会造成像素的不可逆损失。因此本文依然从传统加密方法出发,提出一种运算简便,可以完成私钥自动设计的图像加密算法。

本文算法的创新之处在于从新的角度设置密钥,即利用图像自身的统计特征引导加密过程,并结合非线性混沌映射,在实现简易快速运算的同时达到安全加密的效果。在现实应用中,该方案可以让每张图像都有各自的私钥,从而加密方能将指定图像的私钥分发给任意的用户,完成对所有图像权限的控制和保护。

1 基本概念

1.1 Logistic 混沌序列

Logistic 映射定义为

$$f(x)=\mu x(1-x) \tag{1}$$

其中,μ 是常数。当 $x\in(0,1)$,$f(x)\in(0,1)$ 时,μ 满足 $0<\mu\leqslant 4$。

记 $\mu_\infty=3.569\,945\,67,\cdots$,当 $\mu_\infty\leqslant\mu\leqslant 4$ 时,利用式(1)构造混沌序列 $x_{n+1}=f(x_n)$,则 $\{x_n\}$ 具有如下3个特征:

(1) 对初始条件具有敏感依赖性;

(2) 非周期性;

(3) 存在着奇异吸引子。

称上述 $\{x_n\}$ 为 Logistic 混沌序列。

1.2 数字图像直方图

直方图(Histogram),是一种典型的统计图,用若干个高低不同的条纹代表数据的频数或频率,横轴代表所统计数据的取值类型。

对于一张 $M\times N$ 的灰度图像,其直方图是将图像中所有像素出现的频数(或频率),按照数值大小依次排列形成的条形图,若记像素的取值空间 $\{x_k,k=0,1,\cdots,L-1\}$,则直方图可以用 L 个频数表达:

$$h(x_k)=n_k,\ \sum_{k=0}^{L-1}n_k=MN \tag{2}$$

其中,n_k 表示像素值 x_k 在图像中出现的次数,将其除以总数可得直方图的频率表示:

$$F(x_k)=\frac{h(x_k)}{MN}=\frac{n_k}{MN} \tag{3}$$

对于彩色图像,可以对其进行RGB三色分解。然后和灰度图像一样,对各个颜色通道的像素值进行统计,可以得到相应通道的灰度直方图。

1.3 直方图的局部峰值点与谷值点

对于一张大小为 $M\times N$ 的灰度图像,记其直方图为 $h(x_k)$,$k=0,1,\cdots,L-1$。某一像素值 x_p 被称为局部峰值点,如果它满足

$$h(x_p)>h(x_{p+1}),h(x_p)>h(x_{p-1}) \tag{4}$$

x_v 被称为局部谷值点,如果它满足

$$h(x_v)<h(x_{v+1}),h(x_v)<h(x_{v-1}) \tag{5}$$

即直方图的局部峰值点和谷值点为局部范围内的最大值点或最小值点。

对于一张彩色图像,在每个颜色通道上同样可以定义和灰度图像一样的峰值点和谷值点。

2 加密与解密算法设计

2.1 加密算法

对于灰度图像而言,首先计算其直方图的局部峰值点集合 $\boldsymbol{P}_s$ 与局部谷值点集合 $\boldsymbol{V}_s$(若不存在局部峰值点或谷值点,则用全体奇、偶像素值集合分别代替 $\boldsymbol{P}_s$ 或

$\boldsymbol{V}_s$),并设置一个分块尺寸 P;然后利用 $\boldsymbol{V}_s$ 定义 $\boldsymbol{a}$ 的初始值,并进行多轮迭代得到序列 $\boldsymbol{a}$;再结合 $\boldsymbol{V}_s$ 和 $\boldsymbol{a}$ 对图像进行灰度加密和扩散;最后再将图像划分为 $P\times P$ 的小块,将 $\boldsymbol{P}_s$ 用于每一小块内部的置乱加密。置乱过程中,先利用 $\boldsymbol{P}_s$ 构造混沌序列 $\boldsymbol{b}$,对每个 $P\times P$ 小块的像素进行水平或者垂直平移操作。为了增强 Logistic 混沌序列 $\boldsymbol{a}$ 和 $\boldsymbol{b}$ 的混沌性,均设置混沌迭代系数 $\mu=3.6$。整个方案中,密钥为(P,$\boldsymbol{P}_s$,$\boldsymbol{V}_s$),其中($\boldsymbol{P}_s$,$\boldsymbol{V}_s$)是图像的私钥,分块密钥 P 是加密的公钥。本算法流程图如图 1 所示。

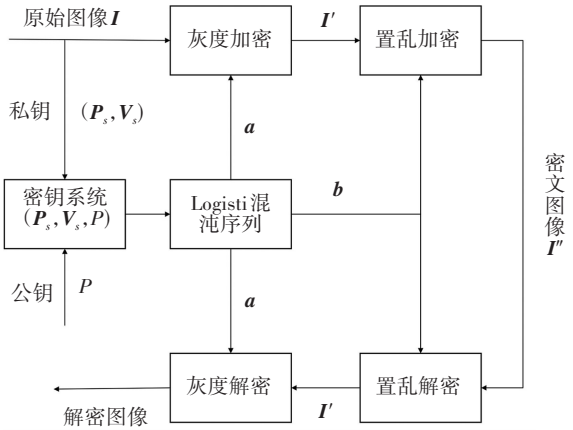


图 1　结合 Logistic 混沌映射和直方图特征引导的非对称加密算法设计流程图

Fig. 1　Flow chart of the asymmetric encryption algorithm design guided by combining Logistic chaotic mapping and histogram features

加密的具体步骤如下:

(1) 对图像 $\boldsymbol{I}$(大小为 $M\times N$)的像素进行统计,提取局部峰值点集合 $\boldsymbol{P}_s$ 与谷值点集合 $\boldsymbol{V}_s$,并记 $\boldsymbol{P}_s$ 与 $\boldsymbol{V}_s$ 的长度分别为 l_p 与 l_v。

(2) 灰度加密。将图像 $\boldsymbol{I}$ 从左至右、从上到下依次铺开为一个一维像素序列 $\boldsymbol{p}$,于是其长度为 $L=M\times N$。构造混沌序列 $\boldsymbol{a}$,设置混沌初始值 $\boldsymbol{a}[0]=\boldsymbol{V}_s[0]/255$,迭代系数 $\mu=3.6$。利用式(1)进行 $L-1$ 轮迭代,得到长度为 L 的 Logistic 混沌序列 $\boldsymbol{a}$。迭代式为

$$\boldsymbol{a}[i+1]=3.6\boldsymbol{a}[i](1-\boldsymbol{a}[i]),0\leqslant i\leqslant L-2 \tag{6}$$

利用得到的混沌序列 $\boldsymbol{a}$ 对像素进行灰度加密和扩散,设

$$K_0=\begin{cases}\boldsymbol{V}_s[0],\boldsymbol{a}[0]<0.5\\ \overline{\boldsymbol{V}_s[0]},\boldsymbol{a}[0]\geqslant 0.5\end{cases} \tag{7}$$

再令 $\boldsymbol{p}'[0]=\boldsymbol{p}[0]\oplus\boldsymbol{p}[L-1]\oplus K_0$,这里,$\overline{\boldsymbol{V}_s[0]}$ 表示对 $\boldsymbol{V}_s[0]$ 按位取反操作(下同),"⊕"表示二进制下的异或运算。然后进行 $L-1$ 轮循环运算:

$$\boldsymbol{p}'[i]=\boldsymbol{p}[i]\oplus\boldsymbol{p}'[i-1]\oplus K,1\leqslant i\leqslant L-1 \tag{8}$$

在每一轮迭代中,有

$$K=\begin{cases}\boldsymbol{V}_s[i \bmod l_v],\boldsymbol{a}[i]<0.5\\ \overline{\boldsymbol{V}_s[i \bmod l_v]},\boldsymbol{a}[i]\geqslant 0.5\end{cases} \tag{9}$$

这里,$i \bmod l_v$ 表示取模运算。为了获取更好的加密效果,将上述步骤重复 3 轮就得到灰度加密的像素序列 $\boldsymbol{p}''$,再将 $\boldsymbol{p}''$重新排成 $M\times N$ 的矩阵就得到灰度加密图像 $\boldsymbol{I}'$。

(3) 置乱加密。先构造混沌序列 $\boldsymbol{b}$,取初始值 $\boldsymbol{b}[0]=\boldsymbol{P}_s[0]/255$,迭代系数 $\mu=3.6$。利用式(1)进行 l_p-1 轮迭代,得到长度为 l_p 的 Logistic 混沌序列 $\boldsymbol{b}$。具体迭代式为

$$\boldsymbol{b}[i+1]=3.6\boldsymbol{b}[i](1-\boldsymbol{b}[i]),0\leqslant i\leqslant l_p-2 \tag{10}$$

设置分块密钥 P,将图像 $\boldsymbol{I}'$分成 $P\times P$ 的小块(并不一定恰好分完)。对于每一个 $P\times P$ 小块,遍历集合 $\boldsymbol{P}_s$:如果 $\boldsymbol{b}[i]<0.5$,则将该块的每一列水平向右平移 $\boldsymbol{P}_s[i]$ 个单位;如果 $\boldsymbol{b}[i]\geqslant 0.5$,则将该块的每一行垂直向下平移 $\boldsymbol{P}_s[i]$ 个单位。置乱以后就得到最终的加密图像 $\boldsymbol{I}''$。

(4) 输出加密图 $\boldsymbol{I}''$与($\boldsymbol{P}_s$,$\boldsymbol{V}_s$),并将($\boldsymbol{P}_s$,$\boldsymbol{V}_s$)作为私钥分发给授权用户。密文 $\boldsymbol{I}''$则通过安全信道传送给授权用户。

彩色图像中,对每一个颜色通道采用和灰度图像相同的方式进行加密,再将 3 个加密颜色通道合成即得到加密后的彩色图像。

2.2　解密算法

本方案的解密和加密是两个完全相反的过程,解密后的图像没有像素损失,即为无损加密。在该加密机制中,只有授权用户在获取私钥($\boldsymbol{P}_s$,$\boldsymbol{V}_s$)后才可以对密文图像 $\boldsymbol{I}''$进行解密。解密涉及的运算都是加密的逆运算,其具体过程如下:

首先令 $\boldsymbol{b}[0]=\boldsymbol{P}_s[0]/255$,并按照式(10)迭代 l_p-1 轮得到混沌序列 $\boldsymbol{b}$,结合 $\boldsymbol{P}_s$ 与 $\boldsymbol{b}$ 进行置乱解密,即对于每一个 $P\times P$ 小块,遍历集合 $\boldsymbol{P}_s$,得到置乱解密图像 $\boldsymbol{I}'$:如果 $\boldsymbol{b}[i]<0.5$,则将该块的每一列水平向左平移 $\boldsymbol{P}_s[i]$ 个单位;如果 $\boldsymbol{b}[i]\geqslant 0.5$,则将该块的每一行垂直向上平移 $\boldsymbol{P}_s[i]$ 个单位。接下来将 $\boldsymbol{I}'$从上到下、从左至右依次铺开为一维序列 $\boldsymbol{p}'$。然后令 $\boldsymbol{a}[0]=\boldsymbol{V}_s[0]/255$,并按照式(6)迭代 $M\times N-1$ 轮得到混沌序列 $\boldsymbol{a}$,再结合密钥 $\boldsymbol{V}_s$ 进行灰度解密,即遍历 $\boldsymbol{a}$:

$$\boldsymbol{p}[i]=\boldsymbol{p}'[i]\oplus\boldsymbol{p}'[i-1]\oplus K,1\leqslant i\leqslant L-1 \tag{11}$$

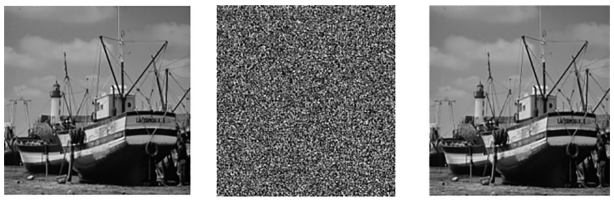
每一轮的 K 根据 $\boldsymbol{a}[i]$和 $\boldsymbol{V}_s[i]$按照式(9)生成,此过程重复 3 次。最后将序列 $\boldsymbol{p}$ 重新排成 $M\times N$ 的矩阵就得到解密后的图像 $\boldsymbol{I}$。

3　实验测试与分析

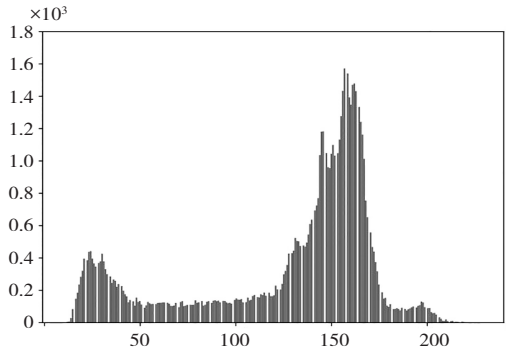
3.1　实验结果

为了测试加密方案,对尺寸为 512×512 的灰度 boat 图像以及 512×512×3 的彩色 Lena 图像进行加密和解

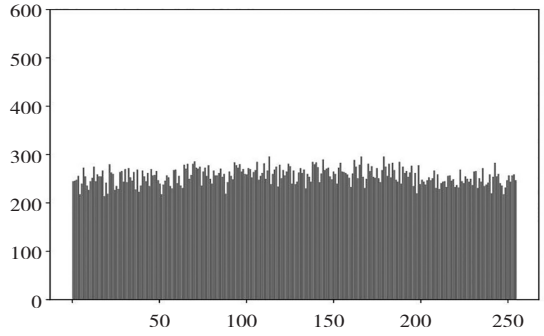
密,设置分块密钥 $P=32$。实验环境如下:处理器为 i7-8750H CPU @ 2.20GHz,操作系统为 Windows 11,采用 Python 3.11 配置下的 Pycharm 软件进行实验。加密结果如图 2、图 3 所示。实验结果表明:两幅图像的密文和明文完全不同,密文接近于随机噪声,且其直方图分布几乎均匀,这表明本算法在视觉上可以实现图像的良好加密。



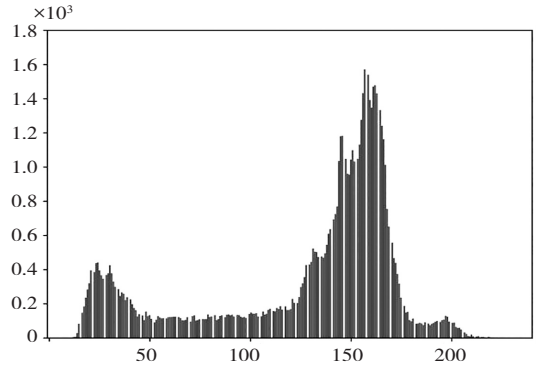
(a) boat 原图 (b) boat 加密图 (c) boat 解密图



(d) boat 原图直方图



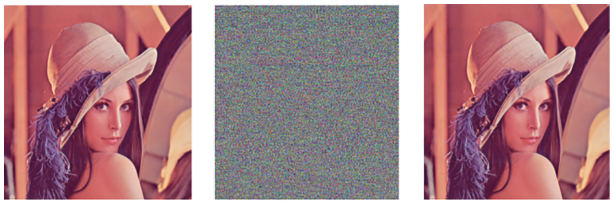
(e) boat 加密图直方图



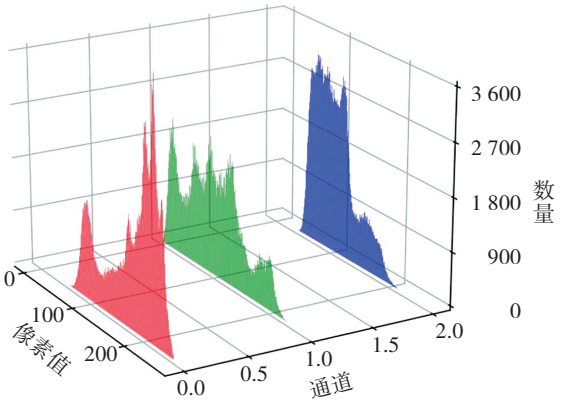
(f) boat 解密图直方图

图 2 boat 加密与解密图

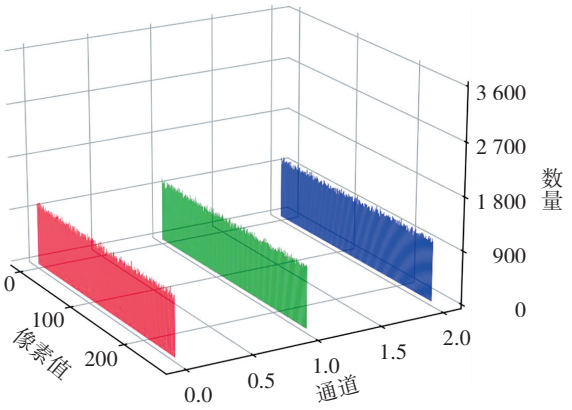
Fig. 2 Boat encryption and decryption histograms



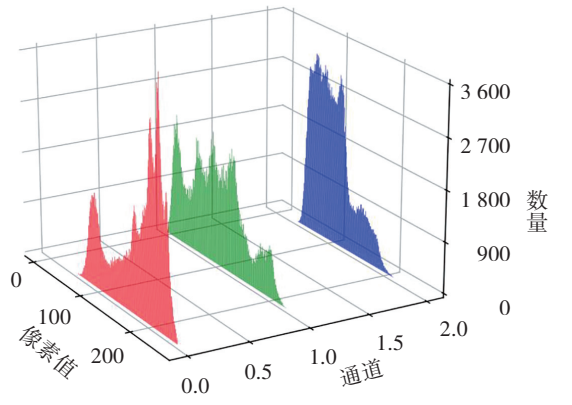
(a) Lena 原图 (b) Lena 加密图 (c) Lena 解密图



(d) Lena 原图直方图



(e) Lena 加密图直方图



(f) Lena 解密图直方图

图 3 Lena 加密图和解密图(0、1、2 分别代表 R、G、B 通道)

Fig. 3 Encrypted and decrypted histograms of Lena (0, 1, and 2 represent the R, G, and B channels, respectively)

3.2 密钥空间大小分析

本方案的密钥为 $(P, \boldsymbol{P}_s, \boldsymbol{V}_s)$,其中 P 为分块密钥(公钥),且 P 是公开的,$(\boldsymbol{P}_s, \boldsymbol{V}_s)$ 分别为置乱密钥和灰

度密钥(私钥)。$\boldsymbol{P}_s$ 与 $\boldsymbol{V}_s$ 是图像直方图的局部峰值点和局部谷值点集合。

下面考察 $\boldsymbol{P}_s$ 的密钥空间 S_p 的大小 L_{sp}。由于直接估计 L_{sp} 比较困难,将问题进行等价转换。根据式(4)关于局部峰值点的定义,一张 256 级灰度图像直方图的局部峰值点至多有 127 个。设 S_L 是长度为 254 的 0~1 序列集合,且对于 S_L 中任一序列 l,不存在连续的两个 1。显然可以得到 S_p 到 S_L 的一种双射:

$$\varphi: S_p \rightarrow S_L$$
$$\boldsymbol{P}_s \mapsto l$$

映射法则 φ:设 $\boldsymbol{P}_s=(x_1,x_2,\cdots,x_m)$,其中 $1\leqslant x_i\leqslant 254, 1\leqslant i\leqslant 127$,对应的 0-1 序列 $l\in S_L$ 的第 $x_1,x_2,\cdots,x_m$ 个位置为 1,其余位置全为 0。于是密钥空间 S_p 和 S_L 的大小相等,均为 L_{sp}。于是求 S_p 的大小等价于求 S_L 中全体 0-1 序列的数量。

设长度为 i 且不存在连续两个 1 的 0~1 序列一共有 $d(i)$ 个,满足这样条件序列的第 i 个位置可能为 0 或 1。若第 i 个位置为 0,则 0 可以跟在任何 $i-1$ 长度且不存在连续两个 1 的 0~1 序列后面,此时有 $d(i-1)$ 种方式;若第 i 个位置为 1,由于不能有连续的两个 1,所以第 $i-1$ 个位置必须是 0,这实际上是在长度为 $i-2$ 且不存在连续两个 1 的 0~1 序列后面加上 0、1,因此有 $d(i-2)$ 种方式。从而可建立如下递推关系:

$$d(i)=d(i-1)+d(i-2) \tag{12}$$

其中,$d(1)=2, d(2)=3$,显然 $\{d(i)\}$ 是斐波那契数列的子列。取 $i=254$,可得密钥空间 S_p 的大小 $L_{sp}\approx 2^{176.56}$,这只是 $\boldsymbol{P}_s$ 的空间大小,而整个私钥($\boldsymbol{P}_s$,$\boldsymbol{V}_s$)的空间更大。

一般当算法的密钥空间大于 2^{100} 时,可以认为加密方案可以抵抗暴力穷举攻击[10]。根据上面的分析结果可知,本方案可以抵抗穷举攻击。

3.3　信息熵分析

图像的信息熵是度量其像素分布均匀程度的指标。设 $\boldsymbol{x}$ 代表一种信息源(这里指数字图像),则 x 的信息熵 $H(x)$ 计算式为[10]

$$H(x)=-\sum_{i=0}^{255} p(i)\log_2 p(i) \tag{13}$$

其中,$p(i)$ 表示灰度值 i 出现的概率。

如果一种加密算法对图像加密以后,密文图像的每个像素出现的频率都相等,则其图像熵就为 8。一般来讲,密文的图像熵值越接近 8,则代表它在信息熵意义下抵抗统计分析攻击的能力越强。Lena 彩色图像加密以后各个通道的信息熵如表 1 所示。测试结果显示,本方案加密图各个通道的信息熵均比其他算法都更接近 8。

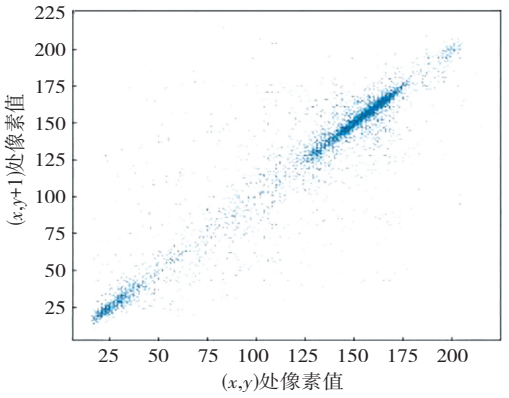
表 1　Lena 明文与密文的图像熵

Table 1　Image entropy of Lena's plaintexts and ciphertexts

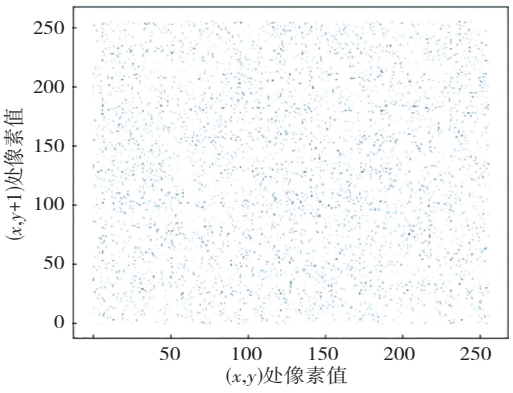
通道	明文	密文				
		文献[10]	文献[11]	文献[12]	文献[13]	本文算法
R	7.252 5	7.991 2	7.997 4	7.992 8	7.991 2	**7.999 2**
G	7.594 0	7.996 6	9.997 0	7.993 8	7.991 3	**7.999 3**
B	6.968 4	7.998 9	9.997 2	7.990 6	7.991 6	**7.999 1**

3.4　相关性分析

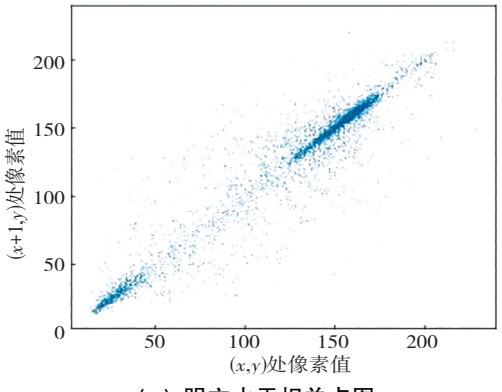
将灰度图像 boat 进行加密,随机抽取明文和密文的 5 000 像素点,并绘制出它们的垂直、水平、对角相邻点的相关点图,如图 4 所示。可以看到:明文图像中各个方向相邻点的像素值具有明显的关联性,大致分布在一条直线上;而密文图像的相邻点则随机分布在整个平面,没有相关性可言。



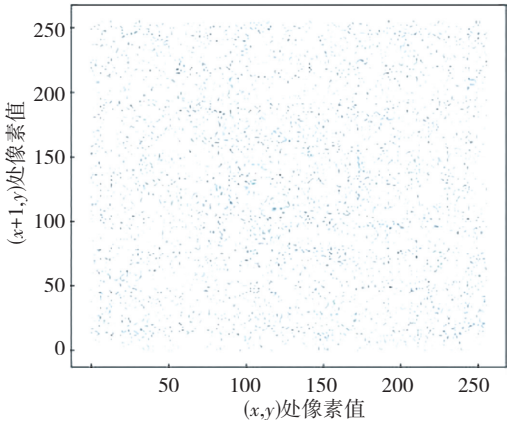
(a) 明文垂直相关点图



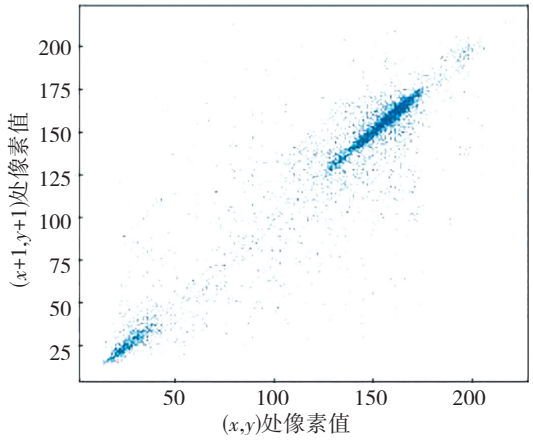
(b) 密文垂直相关点图



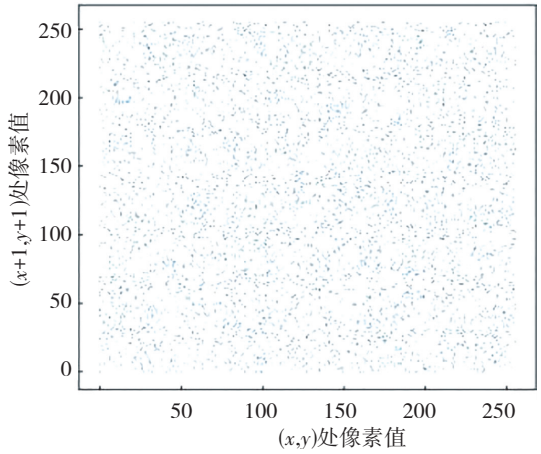
(c) 明文水平相关点图



(d) 密文水平相关点图



(e) 明文对角相关点图



(f) 密文对角相关点图

图 4 boat 图像的相关点图

Fig. 4 Correlation graph of image boat

此外,再分别对两张彩色和两张灰度标准测试图像 4.1.01、4.2.01 和 5.3.01 以及 cameraman 进行加密,并计算它们相邻点之间的相关系数,如表 2 所示。可以看到无论是彩色图像还是灰度图像,明文图像的垂直、水平和对角相邻点的相关系数都接近 1,而对应的密文图像则相反,相关系数明显降低且接近于 0。这说明本方案可以有效抵抗相关分析攻击。

表 2 不同图像的相关系数

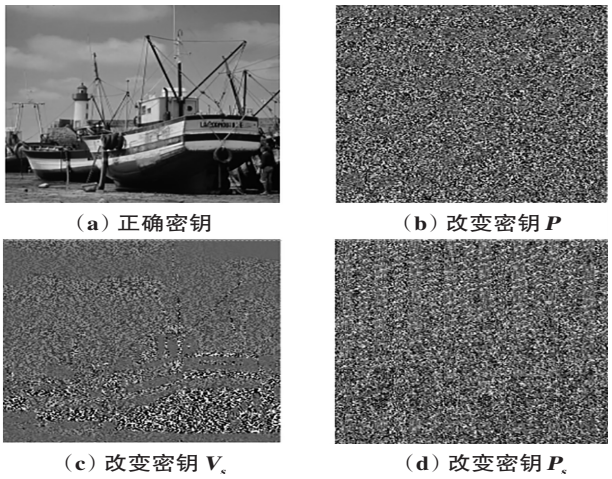
Table 2 Correlation coefficients of different images

图像		明文			密文		
		R	G	B	R	G	B
4.2.02	R	0.971 3	0.964 5	0.952 4	−0.006 2	0.015 4	−0.002 4
	G	0.969 5	0.961 9	0.949 6	0.020 5	−0.011 3	−0.006 1
	B	0.960 3	0.945 5	0.933 5	−0.002 1	−0.012	0.007 1
4.2.01	R	0.953 1	0.959 0	0.921 2	0.014 4	0.057 6	0.008 4
	G	0.930 9	0.950 2	0.897 2	−0.000 7	−0.010 6	0.010 1
	B	0.902 4	0.941 8	0.889 7	−0.005 2	0.025 9	−0.008 6
5.3.01	—	0.980 3	0.979 6	0.966 0	−0.012 5	0.000 2	−0.020 0
cameraman	—	0.936 6	0.958 6	0.913 0	−0.008 9	0.028	−0.007 2

3.5 密钥灵敏性分析

密钥敏感性是密码系统可靠性的重要指标。密钥灵敏性是指即使密钥受到微小扰动,解密出来的图像和明文的差别仍然很大[14]。

分别对密钥(P,$\boldsymbol{P}_s$,$\boldsymbol{V}_s$)的每个参数进行一个单位的扰动,而其他参数保持不变,其解密效果如图 5 所示。从图 5(b)—5(d)可知,即使密钥(P,$\boldsymbol{P}_s$,$\boldsymbol{V}_s$)只受到微小的扰动,原始图像还是无法完全恢复。



(a) 正确密钥 (b) 改变密钥 $\boldsymbol{P}$

(c) 改变密钥 $\boldsymbol{V}_s$ (d) 改变密钥 $\boldsymbol{P}_s$

图 5 密钥改变一个单位后的解密图

Fig. 5 Decryption images after keys changed by one unit

3.6 明文攻击与差分攻击分析

传统密码的 4 种经典攻击中,选择明文攻击是最具威胁性的[15]。如果一个加密系统有能力抵御选择明文攻击,则加密算法对其余 3 种攻击也是安全的。本方案的私钥由明文直方图的峰值点和谷值点决定,即私钥是根据明文特征自适应提取的。不同图像具有不同的私钥,密文图像的生成过程完全取决于明文的统计参数,故本算法对抗选择明文攻击是安全的[16]。

差分攻击是通过对明文进行细微扰动,观察密文变化情况的一种分析攻击。如果图像的明文受到轻微扰动,密文的像素改变率 R_{NPC} 接近 100%,像素一致改变强度 I_{UAC} 接近 33.33%,那么表明方案具有良好的抗差分攻击能力。R_{NPC} 与 I_{UAC} 的定义如下[11]:

$$R_{\mathrm{NPC}} = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N}\boldsymbol{D}(i,j) \times 100\% \qquad (14)$$

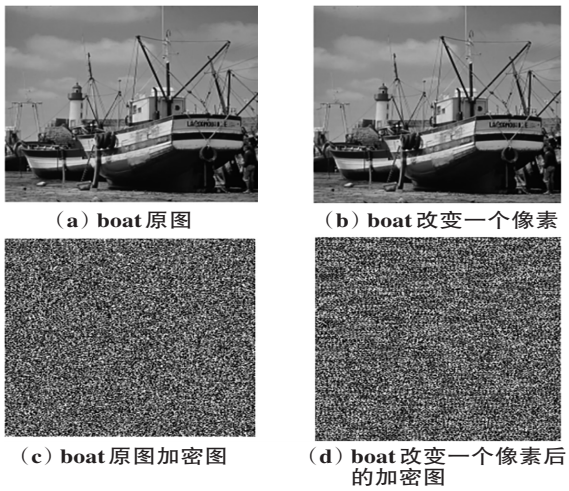
其中,

$$\boldsymbol{D}(i,j)=\begin{cases}1, \boldsymbol{C}(i,j)\neq \boldsymbol{C}'(i,j)\\ 0, \boldsymbol{C}(i,j)=\boldsymbol{C}'(i,j)\end{cases} \tag{15}$$

这里 $\boldsymbol{C}$、$\boldsymbol{C}'$表示改变像素前后密文图像的像素矩阵,$M\times N$ 表示图像的大小。

$$I_{\mathrm{UAC}}=\frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}\frac{|C(i,j)-C'(i,j)|}{255}\times 100\% \tag{16}$$

采用 boat 图像进行实验,改变(78,14)位置的像素,密文像素改变率 R_{NPC} 为 99.62%,像素一致改变强度 I_{UAC} 为 33.18%,都比较接近理想值,说明本方案可以有效对抗差分攻击。



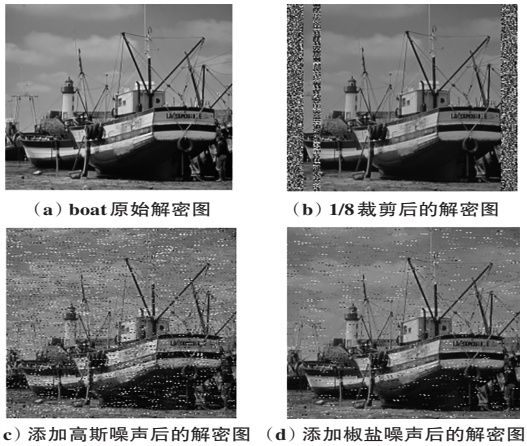
(a) boat 原图　(b) boat 改变一个像素　(c) boat 原图加密图　(d) boat 改变一个像素后的加密图

图 6　抵抗差分攻击测试

Fig. 6　Test for resistance against differential attacks

3.7　鲁棒性分析

加密后的图像需要在安全信道上进行传输,这时可能会受到各种图像攻击。良好的加密算法应该使得密文图像在受到攻击后,解密出来的图像仍然可以分辨。分别对 boat 密文图像进行 1/8 裁剪,添加均值为 1、方差为 0.005 的高斯噪声,添加密度为 0.1 的椒盐噪声,解密图如图 7 所示。可以发现经过各种攻击以后,解密图仍然可以辨认出来,表明本算法具有一定的鲁棒性。



(a) boat 原始解密图　(b) 1/8 裁剪后的解密图　(c) 添加高斯噪声后的解密图　(d) 添加椒盐噪声后的解密图

图 7　鲁棒性测试

Fig. 7　Robustness test

3.8　加密效率分析

以 256×256 的 Lena 灰度图像为对象,进行加密时间测试,并和标准 AES 算法以及其他几种文献的算法进行对比,运行时间如表 3 所示。可以看到:和其他几种算法相比,本文算法的加密时间更短,效率更高。

表 3　加密时间对比

Table 3　Comparison of encryption time

算　法	加密时间/s
标准 AES 算法	3.684 8
文献[17]	1.667 7
文献[18]	0.755 8
文献[19]	0.484 9
本文算法	0.356 8

4　结　论

本文构建了一种结合 Logistic 映射和直方图特征引导的图像加密方案。该方案不仅计算简单易行,而且在对图像进行加密的同时就完成了私钥的自动设计;并通过引入 Logistic 混沌映射这一非线性运算,完成对图像的置乱加密和灰度加密,有效提高了加密方案的复杂性和不可预测性。加密涉及的主要运算是置乱加密和灰度加密的几次循环计算,运算成本较低,加密速度较快。灰度加密的同时,多次向后扩散也提升了加密效果。对多张标准测试图像进行实验测试,并进行空间密钥分析、信息熵分析、相关性分析、密钥灵敏性分析、明文攻击与差分攻击分析、鲁棒性分析和加密时间分析,发现各项安全指标均表现优良,表明本文算法可以有效抵抗各种攻击。结合非线性运算操作,本算法以图像自身的信息来指导加密过程,不仅可以节省运算成本、提高运算效率,还可以完成图像的安全加密。

参考文献(References):

[1] MATHEWS R, GOEL A, SAXENA P, et al. Image encryption based on explosive inter-pixel displacement of the RGB attributes of a pixel[C]//Proceedings of the World Congress on Engineering and Computer Science. 2011, 1: 19-22.

[2] ELZOGHDY S F, NADA Y A, Abdo A A. How good is the DES algorithm in image ciphering [J]. International Journal of Advanced Networking and Applications, 2011, 2(5): 796-803.

[3] HEYS H M. A tutorial on linear and differential cryptanalysis[J]. Cryptologia, 2002, 26(3): 189-221.

[4] PRASAD, SUDHA K L. Chaos image encryption using pixel shuffling[J]. CCSEA, 2011, 1: 169-179.

[5] KHAN M, ALANAZI S A, KHAN S L, et al. An efficient image encryption scheme based on fractal tromino and chebyshev polynomial [J]. Complex Intelligent Systems, 2021, 7(5): 2751-2764.

[6] DIFFIE W, HELLMAN M. New directions in cryptography [J]. IEEE Transaction on Information Theory, 1976, 22(6): 644-654.

[7] IMAM R, ANWER F, NADEEM M. An Effective and enhanced RSA based public key encryption scheme (XRSA) [J]. International Journal of Information Technology, 2022, 14(5): 2645-2656.

[8] 栗风永, 魏璐, 曾祎姝. 融合神经网络变换和通道置乱的彩色图像加密[J]. 计算机工程与设计, 2023, 44(7): 2118-2124.
LI Feng-yong, WEI Lu, ZENG Yi-shu. Color image encryption based on neural network transformation and channel scrambling[J]. Computer engineering and design, 2023, 44(7): 2118-2124.

[9] 韦斌, 隋宇, 邓小玉, 等. 基于频域压缩和二维离散混沌的图像加密方案[J]. 计算技术与自动化, 2023, 42(4): 110-116.
WEI Bin. SUI Yu, DENG Xiao-yu, et al. Encryption scheme based on frequency domain compression and 2D discrete chaos[J]. Computing Technology and Automation, 2023, 42(4): 110-116.

[10] 张赛男, 李千目. 一种基于 Logistic-Sine-Cosine 映射的彩色图像加密算法[J]. 计算机科学, 2022, 49(1): 353-358.
ZHANG Sai-nan, LI Qian-mu. Color image encryption algorithm based on logistic-sine-cosine mapping[J]. Computer Science, 2022, 49(1): 353-358.

[11] 杨淑婷, 巫朝霞. 基于 DNA 与拉丁方的彩图加密算法研究[J]. 网络空间安全, 2022, 13(2): 37-42.
YANG Shu-ting, WU Zhao-xia. Research on color image encryption scheme based on DNA and Latin square[J]. Cyberspace Security, 2022, 13(2): 37-42.

[12] 袁立, 谢俐, 龙颖, 等. 基于哈希和 DNA 编码的彩色图像混沌加密算法[J]. 重庆大学学报, 2021, 44(7): 55-63.
YUAN LI, XIE LI, LONG Ying, et al. Hyper-chaotic color image encryption algorithm based on Hash and DNA coding[J]. Journal of Chongqing University, 2021, 44(7): 55-63.

[13] 任增凤, 巫朝霞. 基于二维复合混沌系统的彩图加密算法研究[J]. 网络空间安全, 2024, 15(1): 147-152.
REN Feng-xia, WU Zhao-xia. Research on color image encryption algorithm based on 2d composite chaos system[J]. Cyberspace Security, 2024, 15(1): 147-152.

[14] 温文媜, 洪宇坤, 方玉明, 等. 结合半张量积压缩感知的可验证图像加密[J]. 中国图象图形学报, 2022, 27(1): 215-225.
WEN Wen-ying, HONG Yu-kun, FANG Yu-ming, et al. Semi-tensor product compression sensing integrated to verifiable image encryption method[J]. Journal of Image and Graphic, 2022, 27(1): 215-225.

[15] GAO X, MOU J, BANERJEE S, ZHANG Y. Color-gray multi-Image hybrid compression-encryption scheme based on BP neural network and knight tour[J]. IEEE Transactions on Cybernetics, 2023, 53(8): 5037-5047.

[16] 罗玉玲, 欧阳雪, 曹绿晨, 等. 遗传模拟退火算法和混沌系统的图像加密方法[J]. 西安电子科技大学学报, 2019, 46(5): 171-179.
LUO Yu-ling, OUYANG Xue, CAO Lyu-chen, et al. Image encryption using the genetic simulated annealing algorithm and chaotic systems[J]. Journal of XiDian University, 2019, 46(5): 171-179.

[17] 王海珍, 廉佐政, 谷文成. 基于 L-P 混沌映射和 AES 的图像加密算法[J]. 计算机仿真, 2021, 38(10): 217-221.
WANG Hai-zhen, LIAN Zuo-zheng, GU Wen-cheng. Image encryption algorithm based on L-P chaotic map and AES[J]. Computer Simulation, 2021, 38(10): 217-221.

[18] 李蓝航, 丘森辉, 肖丁维, 等. 基于 DNA 序列和动态索引扩散的图像加密算法[J]. 广西师范大学学报(自然科学版), 2021, 39(3): 40-53.
LI Lan-hang, Qiu Sen-hui, XIAO Ding-wei, et al. Image encryption algorithm based on DNA sequence and dynamic index diffusion [J]. Journal of Guangxi Normal University: (Natural Science Edition), 2021, 39(3): 40-53.

[19] 费敏, 李国东. 基于 L-R 混沌系统和双重扩散的图像加密算法[J]. 新疆大学学报(自然科学版), 2021, 38(3): 290-299.
FEI Min, LI Guo-dong. Image encryption algorithm based on L-R chaotic system and double diffusion [J]. Journal of Xinjiang University(Natural Science Edition) (in Chinese and English), 2021, 38(3): 290-299, 333.

责任编辑:李翠薇