第 46 卷第 6 期
Vol. 46 No. 6 2025

青岛理工大学学报
Journal of Qingdao University of Technology

基于改进型 Zigzag 变换和 Logistic-Sine 映射的图像加密算法

徐新立，宋新广，王蒙蒙*
（青岛理工大学 信息与控制工程学院，青岛 266525）

摘　要：为了提高图像的安全性，介绍了一种基于改进型 Zigzag 变换和 Logistic-Sine 映射相结合的新型图像加密算法。利用 SHA-512 哈希算法生成与明文相关的密钥，将密钥输入混沌映射产生混沌序列；对混沌序列先进行行排序再进行列排序，获取的索引矩阵用于明文图像初步置乱；应用改进型 Zigzag 变换算法进一步置乱，重复以上置乱 3 轮；对置乱后的图像进行反向扩散处理来生成密文图像。实验结果表明，该算法密钥空间大，有较强的鲁棒性，能够抵御多种攻击。

关键词：图像加密；Zigzag 变换；混沌映射；哈希算法
中图分类号：TP391.9　　**文献标志码**：A　　**文章编号**：1673-4602(2025)06-0106-08

Image encryption algorithm based on improved Zigzag transformation and Logistic-Sine mapping

XU Xinli, SONG Xinguang, WANG Mengmeng*
(School of Information and Control Engineering, Qingdao University of Technology, Qingdao 266525, China)

Abstract: To enhance the security of images, a novel image encryption algorithm that combines improved Zigzag transformation with Logistic-Sine mapping is introduced. The SHA-512 Hash algorithm is employed to create a key linked to the plaintext, which is fed into the chaotic mapping to produce the chaotic sequence. The chaotic sequence is sorted first by rows and then by columns, and the obtained index matrix is used for the preliminary scrambling of the plaintext image. An improved Zigzag transformation algorithm is applied for further scrambling, and this scrambling process is repeated for three rounds. The scrambled image is processed through inverse diffusion to produce the encrypted image. Experimental results show that the algorithm has a large key space and strong robustness, and can withstand a variety of attacks.

Key words: image encryption; Zigzag transformation; chaotic mapping; Hash algorithm

伴随着通信技术的持续进步，信息交流变得日益频繁，图像因为能承载大量的信息被广泛使用。图像信息在传输和存储时可能会受到一些干扰导致信息丢失，从而导致接受信息的一方无法准确判断信息内容，因此，图像信息安全的需求使得图像加密技术成为研究领域的一个热门话题[1]。

收稿日期：2024-03-12
基金项目：国家自然科学基金青年科学基金(62202252)；青岛理工大学 2023 年本科教学改革与研究项目(F2023-193)；中国成人教育协会社会学习研究院 2023 年度科研课题(ZCXY2023004)
作者简介：徐新立(1982—　)，男，山东青岛人。博士，副教授，主要从事信号处理方面的研究。E-mail：xuxinli@qut.edu.cn。
*通信作者：王蒙蒙(1988—　)，男，山东济宁人。博士，副教授，主要从事信号和图像处理、图像加密等方面的研究。E-mail：wangmm26@163.com。

图像加密是通过算法来隐藏明文信息，降低传输过程中的干扰和攻击，保证图像信息的安全。近年来，图像加密研究方法主要有压缩感知[2]、混沌加密[3-4]、DNA 加密[5]等。混沌系统具有随机性和初始值高敏感性的特点，因此，基于混沌系统理论的图像加密算法被大量提出。传统的一维混沌映射结构简单，混沌行为容易被预测。高维混沌尽管混沌行为复杂，但是计算复杂，实现成本高。在此基础上，许多学者对传统的混沌映射进行了改进，文献[6]构造了新型余弦-指数映射的分块图像加密算法，该算法密钥空间大、安全性高。文献[7]对 Logistic-Tent 混沌映射进行了改进，得到参数范围更大、性能更好的混沌映射，用于后续的加密算法，提高了密钥的敏感性。基于混沌系统的图像加密算法不仅依赖性能优越的混沌系统，用于图像加密的算法结构也十分重要。文献[8]将六维混沌映射与 DNA 编码的图像加密算法相结合，实验证明算法能够应对各种攻击。

综合上述分析，针对传统一维混沌映射混沌行为简单，而高维混沌映射计算复杂等问题，本文使用 Logistic-Sine 混沌映射作为混沌系统，该映射能够产生复杂的混沌行为，具有良好的随机性。同时，在图像加密算法中，提出了一种改进型 Zigzag 变换，对明文图像执行行置乱—列置乱—扩散的操作，彻底打乱像素位置，并且将单个像素的改变扩散至整幅图像中。仿真实验证明，本文提出的加密算法能够很好地隐藏明文信息，具有很强的安全性。

1　Logistic-Sine 定义

Logistic 与 Sine 映射作为典型的一维混沌映射，在图像加密领域得到了广泛应用。其定义分别为

$$x_{i+1}=ax_i(1-x_i) \tag{1}$$

$$x_{i+1}=a\sin(\pi x_i) \tag{2}$$

式中：a 为控制参数，$a\in(0,\ 4]$；x_i 为混沌迭代公式的第 i 个值，初始值 $x_0\in(0,\ 1)$。

由于 Logistic 映射和 Sine 映射结构简单、参数范围小，因此，受到微小扰动就会影响混沌系统的性能。为了克服这些缺点，应用一维 Logistic-Sine 映射，其定义如下：

$$x_{i+1}=\left(\mu x_i(1-x_i)+\frac{\sin(\pi x_i)}{4}\right)\quad \mathrm{mod}1 \tag{3}$$

式中：μ 为控制参数，$\mu\in(0,\ +\infty)$。

2　图像加密算法

为了保障图像信息安全，提出一种基于改进型 Zigzag 变换和 Logistic-Sine 映射的图像加密算法，如图 1 所示。①利用 SHA-512 算法生成密钥，并以此密钥作为输入，通过 Logistic-Sine 产生混沌矩阵；②将混沌矩阵进行升序排序，并获取其索引矩阵，用以对明文图像行和列的置乱操作；③使用改进型 Zigzag 变换进一步置乱已被行列打乱的矩阵，重复 3 轮置乱过程；④通过反向扩散重复处理上述矩阵，以获得最终的密文图像。

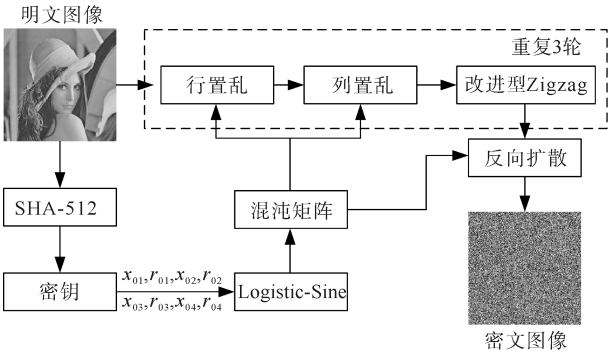


图 1　加密算法结构

2.1　密钥生成

为了提高加密算法的敏感度，增强明文相关性。结合 SHA-512 哈希算法生成密钥，具体步骤如下：

Step1：把大小为 $M\times N$ 的明文图像 P 的所有元素值输入到 SHA-512 哈希算法中，生成 512 位二进制的哈希值 K，即 $K=\{K_1,\ K_2,\ K_3,\cdots,K_{512}\}$。

Step2：将 512 位二进制的哈希值 K 首尾各去掉 56 位，剩下的二进制哈希值分为 8 组，每组各有 50 位，即 $G=\{G_1,\ G_2,\cdots,\ G_8\}$。

$$G_i=(50i-49:50i)\quad i=1,2,3,\cdots,8 \tag{4}$$

Step3：把每组二进制转化为十进制，得到初始值 x_{01}、x_{02}、x_{03}、x_{04}、r_{01}、r_{02}、r_{03}、r_{04}。

$$\begin{cases} x_{01}=\text{bin2dec}(G_1)\times 10^{-r} \\ x_{02}=\text{bin2dec}(G_2)\times 10^{-r} \\ x_{03}=\text{bin2dec}(G_3)\times 10^{-r} \\ x_{04}=\text{bin2dec}(G_4)\times 10^{-r} \\ r_{01}=\text{bin2dec}(G_5)\times 10^{-r} \\ r_{02}=\text{bin2dec}(G_6)\times 10^{-r} \\ r_{03}=\text{bin2dec}(G_7)\times 10^{-r} \\ r_{04}=\text{bin2dec}(G_8)\times 10^{-r} \end{cases} \tag{5}$$

式中：r 为控制参数，由实际初始值控制。

2.2 图像置乱

图像的置乱操作能够改变像素位置，提高抵御统计分析攻击的能力。

为了增强置乱效果，首先对明文图像的行和列进行置乱，然后对其使用改进型 Zigzag 变换，具体步骤如下：

Step1：选用初始参数 x_{01}、x_{02}、r_{01}、r_{02}，利用 Logistic-Sine 映射迭代 $M\times N\times 2+1000$ 次，为了消除瞬态效应，丢弃前 1000 次迭代结果，生成 2 个大小为 $M\times N$ 的混沌矩阵 $\boldsymbol{S}_1$ 和 $\boldsymbol{S}_2$。

Step2：将混沌矩阵 $\boldsymbol{S}_1$ 的每行进行升序排序，以获取行索引矩阵 $\boldsymbol{v}_1$；接着，对混沌矩阵 $\boldsymbol{S}_2$ 的每列进行升序排序，从而得到列索引矩阵 $\boldsymbol{v}_2$。

$$[\sim,\boldsymbol{v}_1]=\text{sort}(\boldsymbol{S}_1,2) \tag{6}$$

$$[\sim,\boldsymbol{v}_2]=\text{sort}(\boldsymbol{S}_2,1) \tag{7}$$

Step3：使用行索引矩阵 $\boldsymbol{v}_1$ 对明文图像矩阵 $\boldsymbol{P}$ 的每一行进行置乱，接着利用列索引矩阵 $\boldsymbol{v}_2$ 对其每一列进行置乱，最终得到置乱后大小为 $M\times N$ 的矩阵 $\boldsymbol{P}_1$。

Step4：为了重新排列像素分布位置，提高算法安全性，提出一种改进型 Zigzag 变换方法。该方法首先对主对角线进行遍历，接着对主对角线上方对角线遍历，然后再对主对角线下方的对角线遍历直到最后一个元素，如图 2 所示。对矩阵 $\boldsymbol{P}_1$ 应用改进型 Zigzag 变换，重复以上置乱过程 3 轮，最终获得大小为 $M\times N$ 的矩阵 $\boldsymbol{P}_2$。

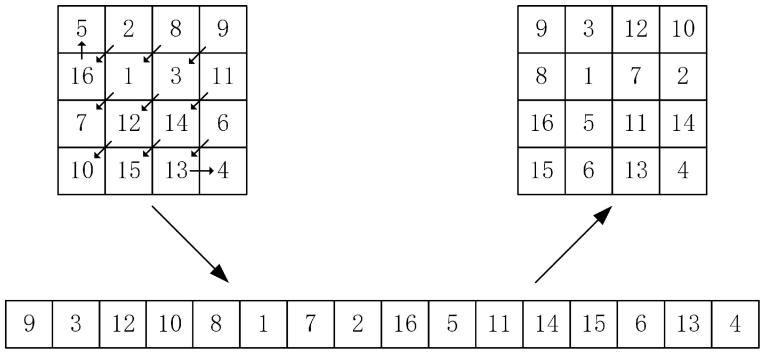


图 2 改进型 Zigzag 变换

2.3 图像扩散

为了提高加密算法抵抗选择明文攻击的能力，在将图像置乱后引入反向扩散，此方法能够使明文信息的统计特性和结构分散到密文中，提高安全性。具体步骤如下：

Step1：选用初始参数 x_{03}、x_{04}、r_{03}、r_{04}，通过 Logistic-Sine 映射迭代 $M\times N\times 2+1000$ 次，为了消除瞬态效应，丢弃前 1000 次迭代结果，产生 2 个大小为 $M\times N$ 的混沌矩阵 $\boldsymbol{S}_3$ 和 $\boldsymbol{S}_4$。

Step2：结合混沌矩阵 $\boldsymbol{S}_3$ 和 $\boldsymbol{S}_4$ 对矩阵 $\boldsymbol{P}_2$ 反向扩散，得到大小为 $M\times N$ 的密文图像矩阵 $\boldsymbol{P}_3$。

$$\begin{cases}\boldsymbol{P}_3(M,N)=(\boldsymbol{P}_2(M,N)+\boldsymbol{S}_3(M,N)+\boldsymbol{S}_4(M,N)) \mod 256\\ \boldsymbol{P}_3(M,j)=(\boldsymbol{P}_2(M,j)+\boldsymbol{S}_3(M,j)+\boldsymbol{S}_4(M,j)+\boldsymbol{P}_3(M,j+1)) \mod 256\\ \boldsymbol{P}_3(i,N)=(\boldsymbol{P}_2(i,N)+\boldsymbol{S}_3(i,N)+\boldsymbol{S}_4(i,N)+\boldsymbol{P}_3(i+1,N)) \mod 256\\ \boldsymbol{P}_3(i,j)=(\boldsymbol{P}_2(i,j)+\boldsymbol{S}_3(i,j)+\boldsymbol{S}_4(i,j)+\boldsymbol{P}_3(i+1,j)+\boldsymbol{P}_3(i,j+1)) \mod 256\end{cases} \tag{8}$$

2.4　解密流程

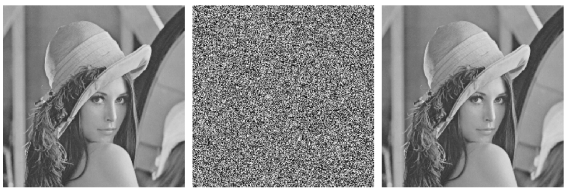
本文提出的图像加密算法是对称加密算法，因此需要在密钥正确的条件下，按照加密过程的反向顺序依次执行与加密密钥相同的操作，即可得到密文图像。将密文图像依次进行逆反向扩散、逆改进型 Zigzag 变换、逆列置乱和逆行置乱，重复逆置乱 3 轮得到解密图像。

3　仿真实验与结果分析

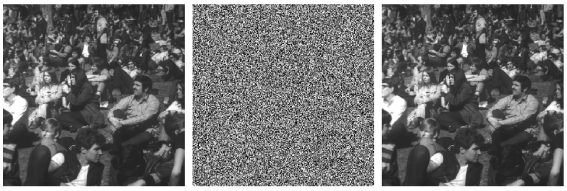
为了衡量图像加密算法的效果，对密钥空间、直方图分布、信息熵、差分攻击能力、相邻像素相关性及算法的鲁棒性等多个方面进行评价。所用实验软件为 Maltlab2016b，实验设备为 3.10 GHz 的 I5-12500H 的处理器，16 GB 内存的笔记本电脑。为了提高密钥与明文图像之间的敏感性，Logistic-Sine 映射的初始值由明文图像输入到 SHA-512 哈希算法中得出，其中生成密钥的参数 $r=24$。

3.1　加密结果

为了测试加密效果，测试图像选用 USC-SIPI 图像数据库中尺寸大小为 256×256 像素的灰度图——Lena 图像和 Crowd 图像进行加密。测试结果如图 3 所示，图像经加密算法加密后无法辨认，变成类似噪声的图片，经解密后成功恢复成明文图像。



(a) Lena加密和解密图像



(b) Crowd加密和解密图像

图 3　加密和解密效果

3.2　密钥空间分析

一个高效的图像加密算法应该具备足够大的密钥空间，以便有效抵御暴力破解攻击。通常认为，只有当密钥空间大于 2^{256} 才能够抵御现代计算机的破解攻击。本文提出图像加密方案，密钥敏感度均为 10^{-15}，密钥空间为 $10^{90}\approx 2^{298}$，远远大于 2^{100}。因此，该图像加密方案能够抵御暴力破解攻击，有足够的安全性。

3.3　直方图分布分析

直方图能够直观地展示出图像中像素分布的情况。图 4 展示了 Lena 和 Crowd 2 幅图像的明文图像和密文图像的直方图。在图中可以清楚地看到，2 幅明文图像的像素分布相对不均匀，而通过加密后，其密文图像像素分布变得十分均匀，能有效抵御统计分析攻击。

3.4　信息熵分析

信息熵是衡量图像像素分布随机性的重要指标。图像信息熵的理想值为 8，表示图像像素具有最高的随机性。信息熵接近 8 的密文图像表明其像素具有高度随机性和均匀分布，从而能有效防御统计分析攻击。其公式如下：

$$H=-\sum_{i=0}^{255}P(i)\log_2 P(i) \tag{9}$$

式中：H 为信息熵；$P(i)$为图像中像素值为 i 的概率。

表 1 展示了本文算法与其他算法的信息熵对比。与基于六维超混沌和 DNA 编码图像加密算法[8]、基于变参数的 logistic 混沌系统图像加密算法[9]、结合 DNA 编码的快速混沌图像加密算法[10]相比，本文提出的图像加密算法信息熵达到 7.9973，高于文献[9-10]，与文献[8]相同，十分靠近理想值。这表明该算法生成的密文具有高安全性。

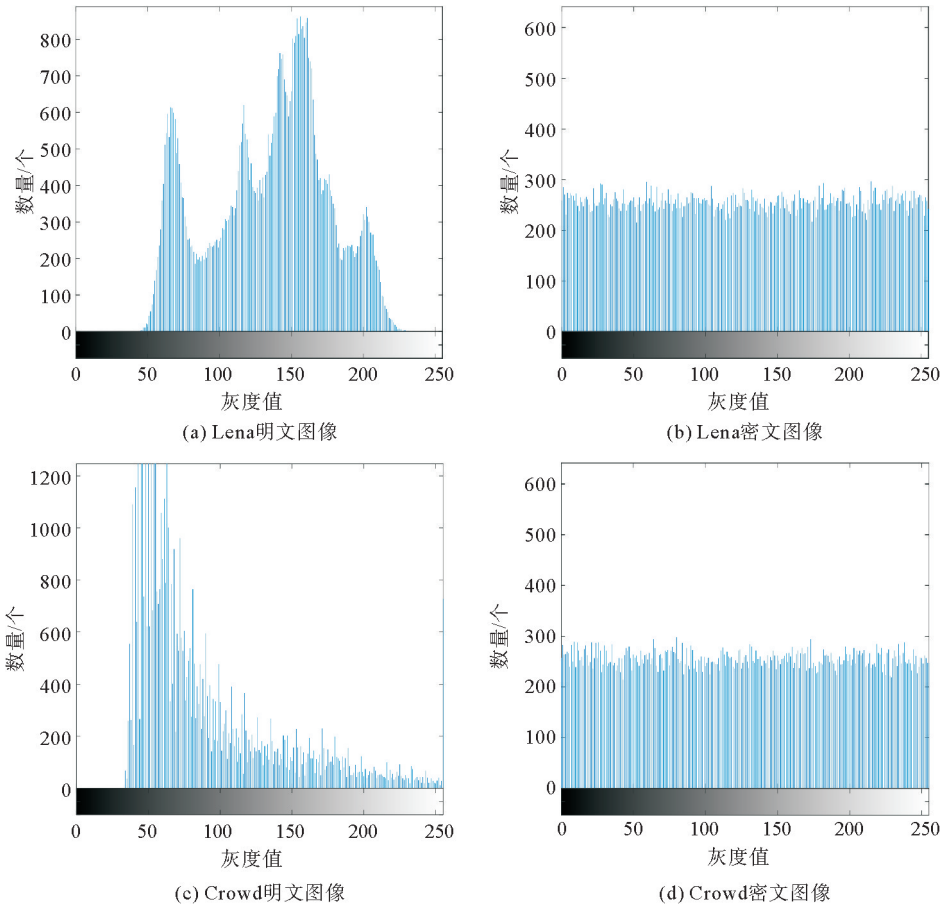


图4 直方图分析

3.5 差分攻击分析

差分攻击是一种通过分析明文图像在微小变化下对应密文图像的差异，从而推测加密算法内部结构或密钥信息的攻击方法。优秀的加密算法应该具有抵御差分攻击的能力。通常使用像素变化率(Number of Pixel Change Rate，NPCR)和统一平均变化强度(Unified Average Changing Intensity，UACI)来评估抵抗差分攻击的性能，其公式如下：

表1 不同算法信息熵对比

算法	本文算法	文献[8]	文献[9]	文献[10]
信息熵	7.9973	7.9973	7.9969	7.9655

$$N_{\mathrm{PCR}}=\frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}D(i,j)\times 100\ \% \tag{10}$$

$$D(i,j)=\begin{cases}0, & C_1(i,j)=C_2(i,j)\\ 1, & C_1(i,j)\neq C_2(i,j)\end{cases} \tag{11}$$

$$U_{\mathrm{ACI}}=\frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}\frac{|C_1(i,j)-C_2(i,j)|}{255}\times 100\ \% \tag{12}$$

式中：N_{PCR}为像素变化率；$D(i,j)$为像素差异矩阵$\boldsymbol{D}$中的元素；U_{ACI}为统一平均变化强度；$C_1(\cdot)$为原始图像经过加密算法处理后得到的密文图像；$C_2(\cdot)$为在原始图像中改变一个像素值后经过加密算法得到的密文图像。

NPCR和UACI的理想值分别是99.6094%和33.4635%，距离理想值越近，则抵抗差分攻击的性能越好。本文加密算法的NPCR和UACI值如表2所示。经过3轮置乱后，NPCR和UACI的值分别为99.6155%和33.4664%，都接近于理想值。尽管经过1轮置乱NPCR值比3轮置乱效果更好，但UACI值偏低。随着置乱次数增加，UACI的值显著提高，从33.3706%增加到33.4664%。因此，3轮置乱加密比1轮置乱加密抵御差分攻击能力更强。此外，与基于压缩感知和光学加密的多图像压缩加密算法[11]、基于Tent映射的图像加密算法[12]、基于超混沌序列和之型置乱的图像加密算法[13]相比，本文提出的算

法在抵御差分攻击方面有更加优越的性能。

3.6　相邻像素相关性分析

用相邻像素相关性来衡量相邻像素的相关程度。通常情况下，当相邻像素的相关系数趋近于 1 时，表明图像像素之间的相互关联性较强；当相关系数接近于 0 时，则意味着图像像素之间的相互关联性较弱。在本文中，通过测试水平、垂直和对角 3 个方向的像素相关性来评估图像加密算法的效果，公式如下：

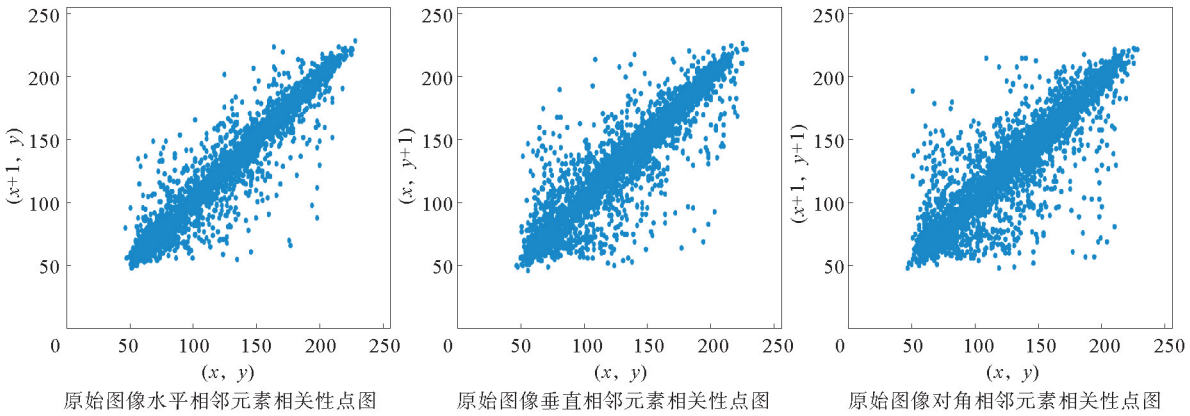
表 2　不同算法 NPCR 和 UACI 对比　　%

算法	本文算法			文献[11]	文献[12]	文献[13]
	1 轮置乱	2 轮置乱	3 轮置乱			
NPCR	99.6116	99.6124	99.6155	99.6087	99.3700	99.6170
UACI	33.3706	33.3772	33.4664	33.4924	31.8500	33.5582

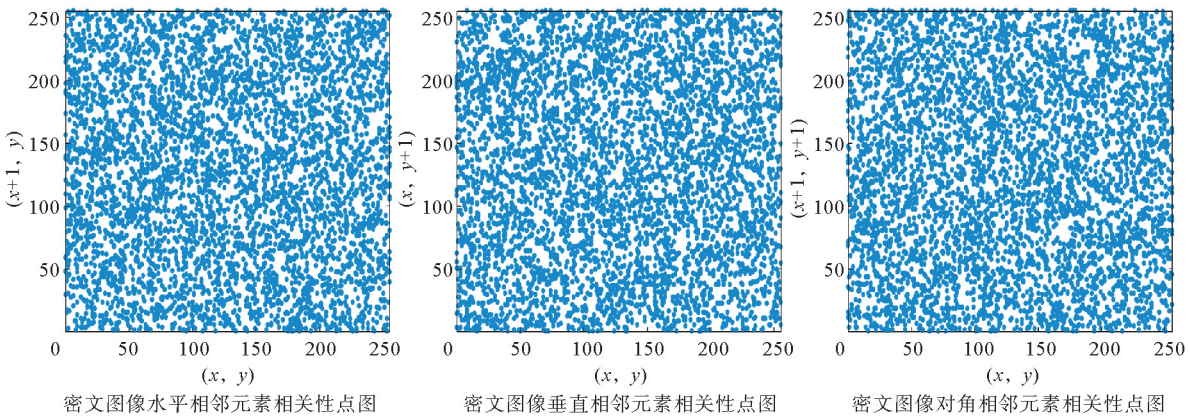
$$r=\frac{\sum(X-\bar{X})(Y-\bar{Y})}{\sqrt{(X-\bar{X})^2(Y-\bar{Y})^2}} \tag{13}$$

式中：r 为相邻像素相关系数；X 和 Y 分别为相邻像素值；$\bar{X}$ 和 $\bar{Y}$ 分别为 X、Y 的平均值。

图 5 展示了明文和密文的 Lena 图像在水平、垂直、对角方向上相邻像素的分布。对明文图像加密后，显著提升了像素值的均匀性并降低了相邻像素间的相关性。密文图像 Lena 的相邻像素相关系数见表 3，可以看出，与结合 DNA 编码的快速混沌图像加密算法[10]、基于分段线性混沌映射的医学图像加密算法[14]、融合二维压缩感知和同步混沌流密码的医学图像加密算法[15]相比，本文算法的相邻像素相关系数无论是在水平、垂直还是对角方向，都保持较低的相邻像素相关性，其数值都接近于 0。因此，本文提出的图像加密算法有效地降低了图像像素之间的相关性，增强了图像的安全性。



(a) 明文图像



(b) 密文图像

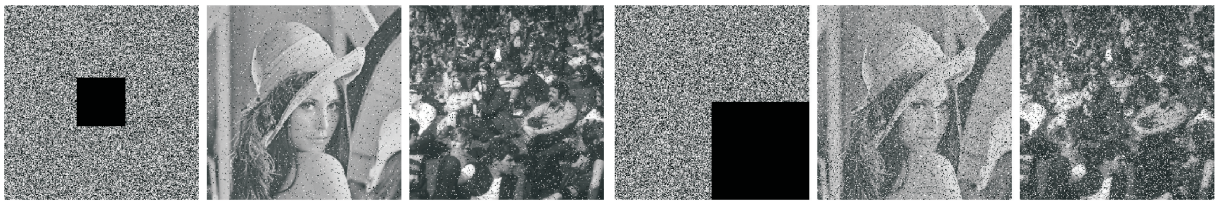
图 5　相邻像素相关性分布

3.7 鲁棒性分析

表3 不同算法像素相关系数对比

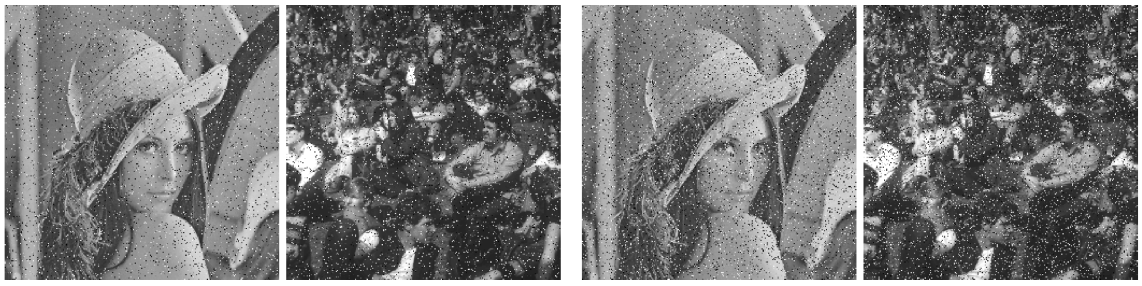
方向	本文算法	文献[10]	文献[14]	文献[15]
水平	−0.0020	−0.0013	−0.0060	0.0597
垂直	0.0017	−0.0041	0.0098	0.0220
对角	0.0017	−0.0208	−0.0053	0.0026

在传输和存储过程中，图像可能会受到噪声的影响，导致部分信息缺失。因此，图像加密算法必须能够抵御噪声攻击，并且在图像丢失信息后，能够解密剩余信息。对加密图像进行不同区域、不同大小的裁剪后，解密恢复的图像仍具有可识别性，如图6所示。即便在密文图像上加入不同程度的椒盐噪声和高斯噪声，解密后的图像依然保持了较高辨识度，如图7和图8所示。这3种情况均说明了加密算法对图像内容的保护效果以及其在面对局部损失或噪声干扰时的鲁棒性。



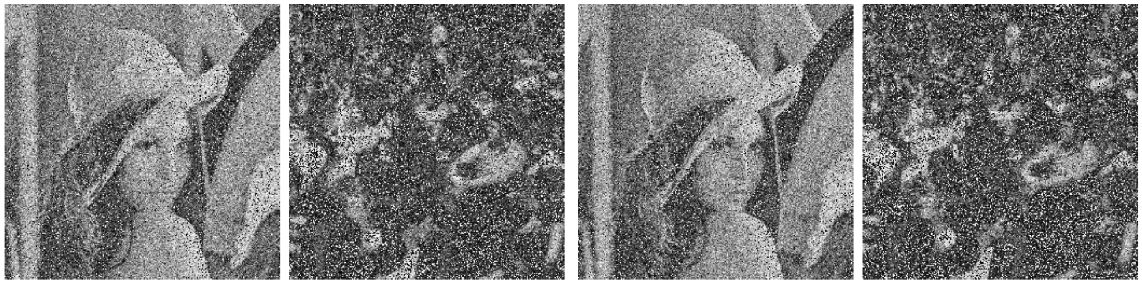
（a）1/8裁剪区域 （b）1/4裁剪区域

图6 裁剪密文图像不同区域大小的解密图



(a) 0.03椒盐噪声 (b) 0.05椒盐噪声

图7 不同强度椒盐噪声攻击的解密图



(a) 0.01高斯噪声 (b) 0.03高斯噪声

图8 不同强度高斯噪声攻击的解密图

4 结论

本文提出了一种基于改进型Zigzag变换和Logistic-Sine映射的图像加密算法。该算法主要包括密钥生成、混沌序列的生成、图像置乱以及图像扩散。密钥的初始值通过SHA-512哈希算法获得；置乱阶段运用Logistic-Sine映射产生混沌序列，并且对明文图像进行行置乱、列置乱和改进型Zigzag变换置乱，进一步提高了图像的置乱效果；在扩散阶段引入反向扩散算法，有效增强了密文图像对明文图像微小变化的敏感性。此外，该算法置乱部分采用3轮加密，有效地提高了算法的安全性。从仿真实验和安全性分析结

果可以看出，该算法的信息熵为 7.9973，密钥空间为 2^{298}，NPCR 和 UACI 值分别为 99.6155% 和 33.4664%。这证明本文提出的算法能够抵御多种攻击，具有较高的安全性。

参考文献(References)：

[1] 杨鑫. 数据加密技术在计算机网络通信安全中的应用分析[J]. 网络安全技术与应用，2023(8)：31-32.
YANG Xin. Analysis of the application of data encryption technology in computer network communication security[J]. Network Security Technology & Application，2023(8)：31-32.

[2] 叶柏君，吴小娜，叶斌辉，等. 基于一维压缩感知和混沌的医学图像加密研究[J]. 工业控制计算机，2023，36(10)：75-77.
YE Baijun，WU Xiaona，YE Binhui，et al. Research on medical image encryption based on one-dimensional compressive sensing and chaos[J]. Industrial Control Computer，2023，36(10)：75-77.

[3] MENG L Z，LIU L S，WANG X L，et al. Reversible data hiding in encrypted images based on IWT and chaotic system[J]. Multimedia Tools and Applications，2022，81(12)：16833-16861.

[4] 杨宇光，裴帅康. 基于双混沌系统和 DNA 编码的图像加密算法[J]. 安徽大学学报(自然科学版)，2022，46(5)：37-49.
YANG Yugang，PEI Shuaikang. Image encryption algorithm based on double chaotic systems and DNA encoding[J]. Journal of Anhui University (Natural Science Edition)，2022，46(5)：37-49.

[5] BAO W J，ZHU C X. A secure and robust image encryption algorithm based on compressive sensing and DNA coding[J]. Multimedia Tools and Applications，2022，81(11)：15977-15996.

[6] 周衍庆，葛斌，夏晨星，等. 基于余弦-指数混沌映射的分块图像加密算法[J]. 光电子·激光，2023，34(9)：984-996.
ZHOU Yanqing，GE Bin，XIA Chenxing，et al. A block image encryption algorithm based on cosine-exponential chaotic map[J]. Journal of Optoelectronics·Laser，2023，34(9)：984-996.

[7] 郭现峰，李浩华，魏金玉. 基于 Fibonacci 变换和改进 Logistic-Tent 混沌映射的图像加密方案[J]. 吉林大学学报(工学版)，2023，53(7)：2115-2120.
GUO Xianfeng，LI Haohua，WEI Jinyu. Image encryption scheme based on Fibonacci transformation and improved Logistic -Tent chaotic mapping[J]. Journal of Jilin University (Engineering and Technology Edition)，2023，53(7)：2115-2120.

[8] 武磊. 基于六维超混沌和 DNA 编码的图像加密算法设计[J]. 现代信息科技，2024，8(3)：149-153.
WU Lei. Design of image encryption algorithm based on six-dimensional hyperchaos and DNA encoding[J]. Modern Information Technology，2024，8(3)：149-153.

[9] 赵耿，李文健，马英杰. 基于变参数的 logistic 混沌系统图像加密算法[J]. 计算机应用与软件，2023，40(12)：325-331.
ZHAO Geng，LI Wenjian，MA Yingjie. Image encryption of logistic chaotic system based on variable parameter[J]. Computer Applications and Software，2023，40(12)：325-331.

[10] 周红亮，刘洪娟. 结合 DNA 编码的快速混沌图像加密算法[J]. 东北大学学报(自然科学版)，2021，42(10)：1391-1399.
ZHOU Hongliang，LIU Hongjuan. Fast chaotic image encryption algorithm combined with DNA encoding[J]. Journal of Northeastern University (Natural Science Edition)，2021，42(10)：1391-1399.

[11] WEI J J，ZHANG M，TONG X J. Multi-image compression-encryption algorithm based on compressed sensing and optical encryption[J]. Entropy，2022，24(6)：784.

[12] 李付鹏，刘敬彪，王康泰. 基于 Tent 映射的图像加密算法及其实验研究[J]. 杭州电子科技大学学报(自然科学版)，2020，40(3)：38-43.
LI Fupeng，LIU Jingbiao，WANG Kangtai. Tent-map based image encryption algorithm and its simulation[J]. Journal of Hangzhou Dianzi University (Natural Sciences)，2020，40(3)：38-43.

[13] 刘思洋，安新磊，施倩倩，等. 基于超混沌序列和之型置乱的图像加密算法[J]. 徐州工程学院学报(自然科学版)，2023，38(3)：49-60.
LIU Siyang，AN Xinlei，SHI Qianqian，et al. Image encryption algorithm based on hyperchaotic sequence and Zigzag scrambling algorithm[J]. Journal of Xuzhou Institute of Technology (Natural Science Edition)，2023，38(3)：49-60.

[14] 秦秋霞，梁仲月，徐毅. 一种基于分段线性混沌映射的医学图像加密算法[J]. 大连民族大学学报，2023，25(1)：57-63.
QIN Qiuxia，LIANG Zhongyue，XU Yi. A medical image encryption algorithm based on piecewise linear chaotic mapping[J]. Journal of Dalian Minzu University，2023，25(1)：57-63.

[15] 叶柏君，林卓胜，吴小娜，等. 融合二维压缩感知和同步混沌流密码的医学图像加密算法[J]. 机电工程技术，2023，52(11)：32-37.
YE Baijun，LIN Zhuosheng，WU Xiaona，et al. Medical image encryption combining two-dimensional compressive sensing and synchronous chaotic stream cipher[J]. Mechanical & Electrical Engineering Technology，2023，52(11)：32-37.

(责任编辑　赵金环；英文校审　程文华)