Computer Science and Application 计算机科学与应用, 2025, 15(7), 164-181
Published Online July 2025 in Hans. https://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2025.157190

Hans汉斯

基于HLSE混沌映射和改进Zigzag变换的图像加密算法

金晓瑞，陈初侠*，陈冠宇，郑　忍，杨敬雪

巢湖学院电子工程学院，安徽　巢湖

收稿日期：2025年6月20日；录用日期：2025年7月21日；发布日期：2025年7月28日

摘　要

针对现有图像加密算法中一维混沌映射存在的混沌范围有限、易出现周期窗口以及标准Zigzag变换置乱效果不佳等问题，本文提出了一种基于HLSE (Hybrid Logistic-Sine-Exponential)混沌映射和改进Zigzag变换的图像加密算法。首先，设计了一种新的一维HLSE混沌映射，该映射通过结合Logistic映射、Sine映射和指数函数，相比于传统的Logistic映射和Sine映射，展现出更大的混沌范围、更复杂的动态行为和对初始值的强敏感性。其次，对标准Zigzag变换进行了改进，通过引入分两次扫描并将结果交叉排列的方式，有效克服了原变换置乱不充分、部分像素位置可能不变的缺陷，增强了置乱的均匀性和彻底性。加密算法利用SHA-256算法根据明文图像生成HLSE混沌映射的初始值和控制参数，确保了密钥的敏感性和与明文的关联性。加密过程包括改进Zigzag置乱、基于混沌序列的索引置乱以及异或扩散操作。实验结果和安全性分析表明，该算法具有足够大的密钥空间、高度的密钥敏感性，能够有效抵抗统计攻击和差分攻击，同时对数据裁剪和噪声污染也表现出较好的鲁棒性，且具有较高的加密效率。

关键词

图像加密，HLSE混沌，改进Zigzag变换，混沌映射

Image Encryption Algorithm Based on HLSE Chaotic Map and Improved Zigzag Transform

Xiaorui Jin, Chuxia Chen*, Guanyu Chen, Ren Zheng, Jingxue Yang

School of Electronic Engineering, Chaohu University, Chaohu Anhui

Received: Jun. 20th, 2025; accepted: Jul. 21st, 2025; published: Jul. 28th, 2025

*通讯作者。

文章引用: 金晓瑞, 陈初侠, 陈冠宇, 郑忍, 杨敬雪. 基于 HLSE 混沌映射和改进 Zigzag 变换的图像加密算法[J]. 计算机科学与应用, 2025, 15(7): 164-181. DOI: 10.12677/csa.2025.157190

Abstract

To address the issues that existing one-dimensional (1D) chaotic maps in image encryption algorithms suffer from limited chaotic range, proneness to periodic windows, and the unsatisfactory scrambling effect of the standard Zigzag transform, this paper proposes an image encryption algorithm based on an HLSE (Hybrid Logistic-Sine-Exponential) chaotic map and an improved Zigzag transform. Firstly, a novel 1D HLSE chaotic map is designed. By combining the Logistic map, Sine map, and exponential function, this map exhibits a larger chaotic range, more complex dynamical behavior, and strong sensitivity to initial values compared to traditional Logistic and Sine maps. Secondly, the standard Zigzag transform is improved. By introducing a two-pass scanning method and cross-arranging the results, it effectively overcomes the deficiencies of the original transform, such as insufficient scrambling and the possibility of some pixel positions remaining unchanged, thereby enhancing the uniformity and thoroughness of the scrambling. The encryption algorithm utilizes the SHA-256 algorithm to generate the initial values and control parameters for the HLSE chaotic map based on the plaintext image, ensuring the sensitivity of the key and its correlation with the plaintext. The encryption process includes improved Zigzag scrambling, chaotic sequence-based index scrambling, and XOR diffusion operations. Experimental results and security analysis demonstrate that the proposed algorithm possesses a sufficiently large key space and high key sensitivity, can effectively resist statistical attacks and differential attacks, and also exhibits good robustness against data cropping and noise pollution, while maintaining high encryption efficiency.

Keywords

Image Encryption, HLSE Chaos, Improved Zigzag Transform, Chaotic Map

1. 引言

随着信息技术的飞速发展，多媒体在我们的日常生活中变得越来越普遍。作为多媒体数据的一部分，数字图像因其直观、抽象层次低且易于阅读的特点，深受人们喜爱。在广泛使用图像的同时，如何确保图像在传输和存储过程中的安全性，近年来受到了越来越多的关注。目前，学者们已经提出了许多方法来解决这个问题[1]-[3]。在这些方法中，图像加密是最常用的技术。

混沌系统由于其独特的特性，经常被用于密码系统中。与多维混沌系统相比，一维混沌系统因其结构简单、易于实现和计算复杂度低而更受欢迎[4]。Belazi 等人利用正切函数和正弦函数设计了一种改进的正弦－正切映射。然后，通过各种分析方法对正弦映射、正弦－指数映射、正弦－正切映射以及改进的正弦－正切映射的混沌性能进行了分析[5]。Xiao 等人利用 Logistic 映射和 Sine 映射设计了一种新颖的一维混沌，它包含两个控制参数。这种新颖的混沌具有较大的混沌范围，但在混沌区间内仍存在许多周期窗口[6]。Liu 等人采用分段线性混沌映射设计了一种比特级置乱方案，其中原始图像中像素的位置和值可以同时改变[7]。然而，这些一维混沌映射存在一些缺点，例如混沌范围有限、存在周期窗口。

标准的 Zigzag 变换常用于置乱图像，但它有许多缺点。例如，像素矩阵中某些元素的位置在多次变换后不会改变。此外，标准的 Zigzag 变换只能应用于方阵并且具有周期性。因此，人们提出了一些改进的 Zigzag 变换来克服这些缺点。Wang 等人设计了一种扩展的 Zigzag 变换，它适用于任意大小的像素矩

阵，而不仅限于方阵[8]。Vidhya 等人提出了四种不同的 Zigzag 变换扫描方法，可以从像素矩阵的四个角点中的任意一个开始扫描[9]。Yang 等人提出了一种新颖的 Zigzag 变换，它可以从任意位置开始扫描，而不局限于像素矩阵的四个角点[10]。Wang 等人使用 3D Zigzag 变换来置换原始图像，并比较了 Arnold 变换、循环移位、标准 Zigzag 变换和 3D Zigzag 变换的置换效果。从比较结果可以看出，3D Zigzag 变换比其他变换具有更好的置换效果[11]。

为确保图像安全的同时，提高加密效率，本文提出了一种新颖的图像加密算法。主要贡献如下：1) 设计了一种新的基于 Logistic 映射、Sine 映射和指数函数的一维混合混沌映射。2) 提出了一种改进的 Zigzag 变换，以克服标准 Zigzag 变换的缺点。3) 提出了一种使用新的一维混合混沌映射、改进的 Zigzag 变换的图像加密算法，该算法可以实现高安全性和高加密效率。

本文其余部分的组织如下：第 2 节介绍了所提出的一维混合混沌映射及其性能分析。第 3 节提出了一种改进的 Zigzag 变换并给出加密和解密算法。第 4 节给出实验结果并进行安全性分析。第 5 节为结束语。

2. 混沌映射

2.1. Logistic 映射

Logistic 映射[6]的数学表达式如式(1)所示：

$$x_{n+1} = \mu x_n \left(1 - x_n\right) \tag{1}$$

式中，μ 代表控制参数，其取值范围为(0, 4]。其中，x_0 为初始值，x_{n+1} 为生成的混沌序列，其取值范围为(0, 1)。注意 Logistic 映射只有在 $\mu > 3.57$ 时才处于混沌状态。

2.2. Sine 映射

Sine 映射[5]的数学表达式如式(2)所示：

$$x_{n+1} = \lambda \sin\left(\pi x_n\right) \tag{2}$$

其中，λ 代表控制参数，其取值范围是(0, 1]。x_0 为初始值，x_{n+1} 为生成的混沌序列，其取值范围是(0, 1)。注意，Sine 映射仅在 $\lambda > 0.87$ 时处于混沌状态。

2.3. HLSE 映射

对于 Sine 映射，将控制参数设为 $\lambda = 1$，因此我们可以将公式(2)改写为：

$$x_{n+1} = \sin\left(\pi x_n\right) \tag{3}$$

然后，将公式(3)和指数函数结合起来得到公式(4)：

$$x_{n+1} = \sin\left(\pi \mathrm{e}^{x_n}\right) \tag{4}$$

最后，将公式(1)和(4)结合起来得到 HLSE (Hybrid chaotic map using the Logistic map, Sine map and the Exponential function，结合逻辑斯蒂映射、正弦映射和指数函数的混合混沌映射)映射的数学表达式：

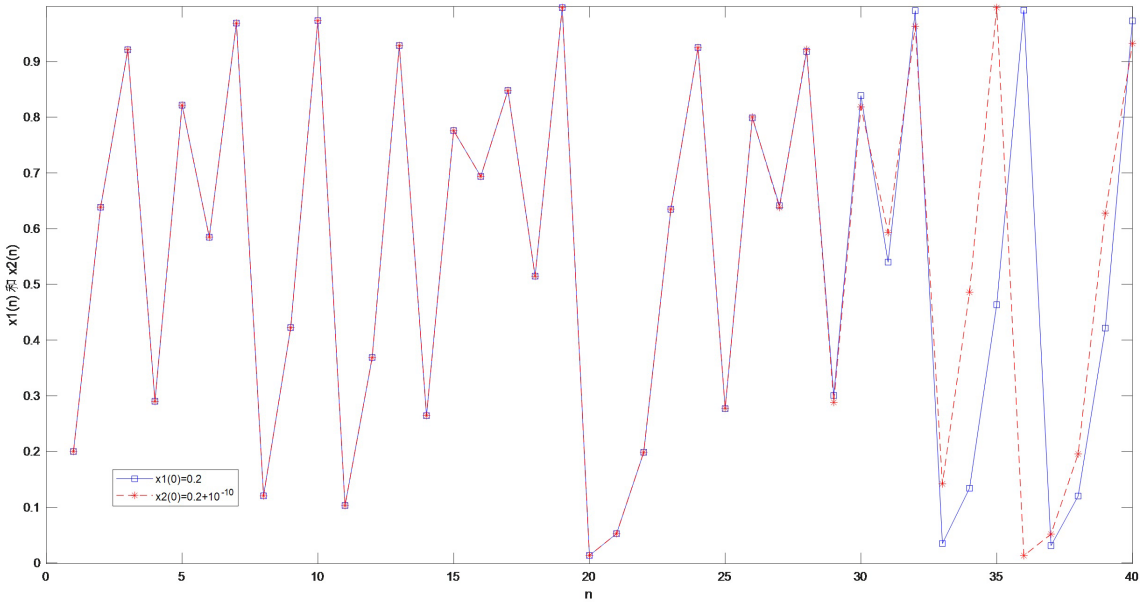
$$x_{n+1} = \gamma \sin\left(\pi \mathrm{e}^{x_n}\right)\left[1 - \sin\left(\pi \mathrm{e}^{x_n}\right)\right] \bmod 1 \tag{5}$$

其中，mod(·)代表模运算符，γ 代表控制参数，其取值范围是$(0, \infty)$。x_0 代表初始值，x_{n+1} 代表生成的混沌序列，其取值范围是(0, 1)。注意，HLSE 映射仅在 $\gamma > 3.5$ 时处于混沌状态。

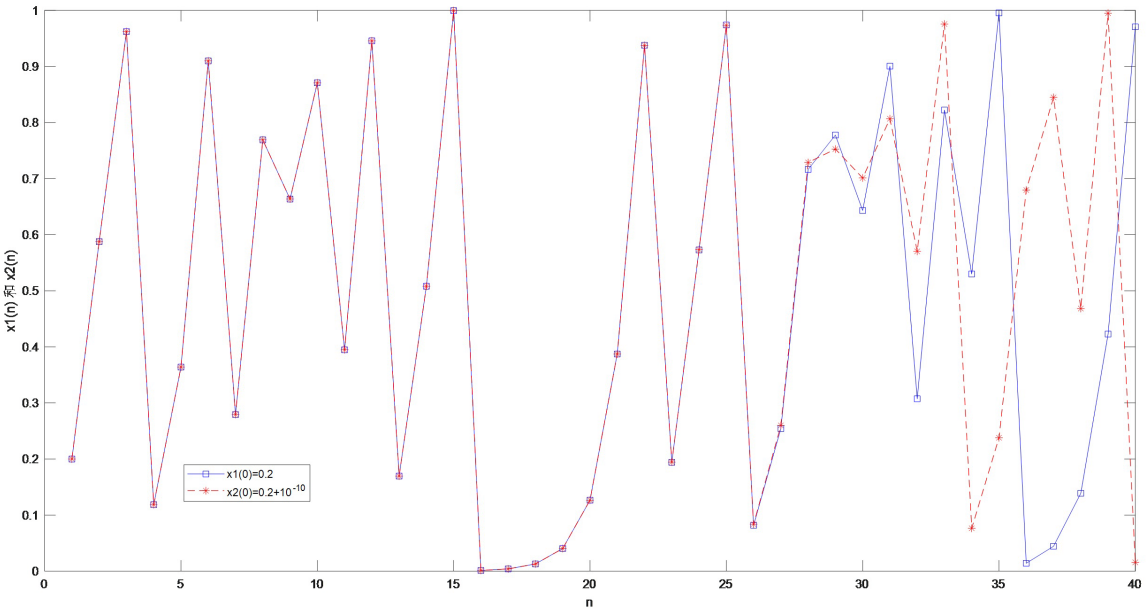
2.4. 混沌性能分析

2.4.1. 敏感性分析

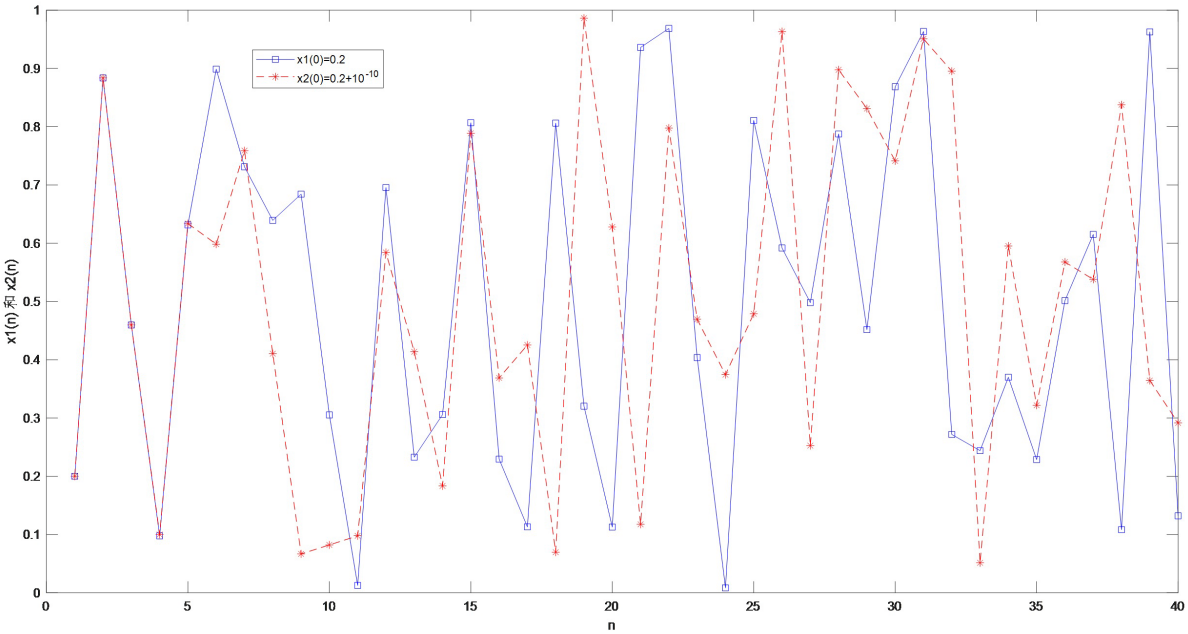
混沌敏感性分析是理解和应用混沌系统的基石。本文仿真了上述三种混沌映射的轨迹图，以验证其对初始值的敏感性，如图 1 所示。注意，蓝色和红色线条分别代表初始值为 $x_1(0) = 0.2$ 和 $x_2(0) = x_1(0) + 10 - 10$ 时生成的混沌序列的轨迹。对于图 1(a)、图 1(b)中的 Logistic 映射和 Sine 映射，蓝色和红色线条迭代 30 次左右时才分开。换句话说，Logistic 映射和 Sine 映射在最初的 28 次迭代中对初始值没有强敏感性。对于图 1(c)中的 HLSE 映射，蓝色和红色线条在迭代 5 次后就分开。因此，我们设计的 HLSE 映射比 Logistic 映射和 Sine 映射对初始值具有更强的敏感性。



(a) $\mu = 4$ 时的 Logistic 映射轨迹图



(b) $\lambda = 1$ 时的 Sine 映射轨迹图

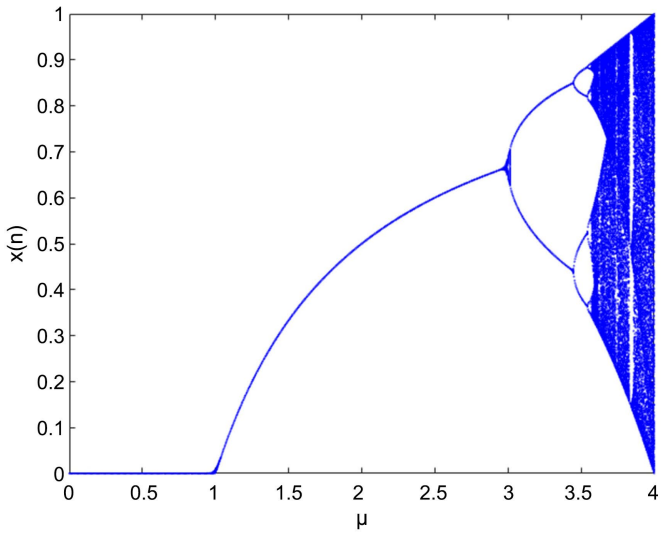


(c) $\gamma = 10$ 时的 HLSE 映射轨迹图

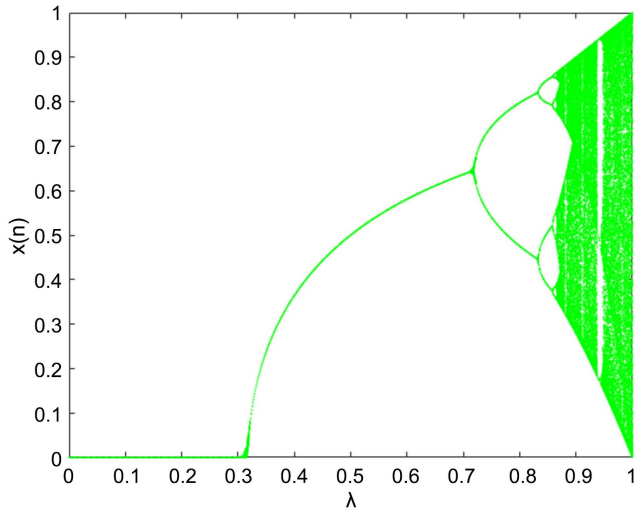
Figure 1. Sensitivity analyses
图 1. 敏感性分析

2.4.2. 分岔图

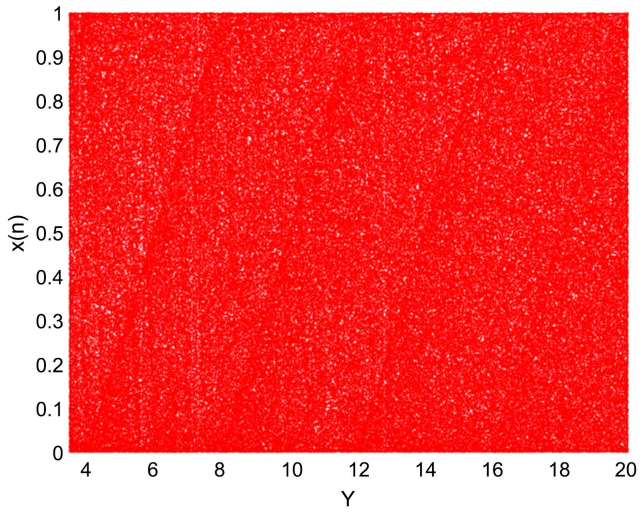
分岔图可以反映随着控制参数的变化，系统的稳定性、周期性和混沌特性的演变过程。从图 2(a)中我们可以看到，Logistic 映射在 $\mu > 3.57$ 时表现出混沌行为。图 2(b)中的 Sine 映射在 $\lambda > 0.87$ 时处于混沌状态。对于 Logistic 映射和 Sine 映射，在给定的控制参数范围内都会出现周期窗口。对于我们设计的 HLSE 映射，如图 2(c)所示，当 $\gamma > 3.5$ 时出现全映射，并且没有周期窗口出现。换句话说，我们设计的 HLSE 映射几乎在整个控制参数范围内都表现出混沌行为。因此，我们设计的 HLSE 映射比 Logistic 映射和 Sine 映射具有更大的混沌区间和更复杂的动态行为。



(a) Logistic 映射分岔图



(b) Sine 映射分岔图



(c) HLSE 映射分岔图

Figure 2. Bifurcation diagrams
图 2. 分岔图

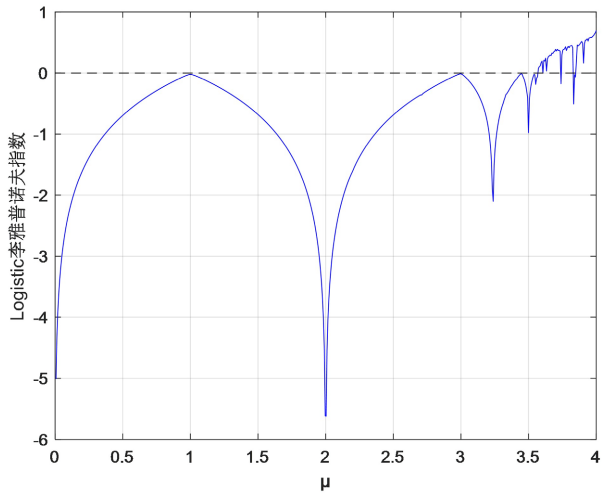
2.4.3. 李雅普诺夫指数

李雅普诺夫指数(LE, Lyapunov Exponent)常被用来描述一个混沌系统的动态特性。只有当系统中李雅普诺夫指数值大于 0 时，该系统才处于混沌状态。对于一个一维混沌映射，其李雅普诺夫指数值[5]可以通过以下公式计算：

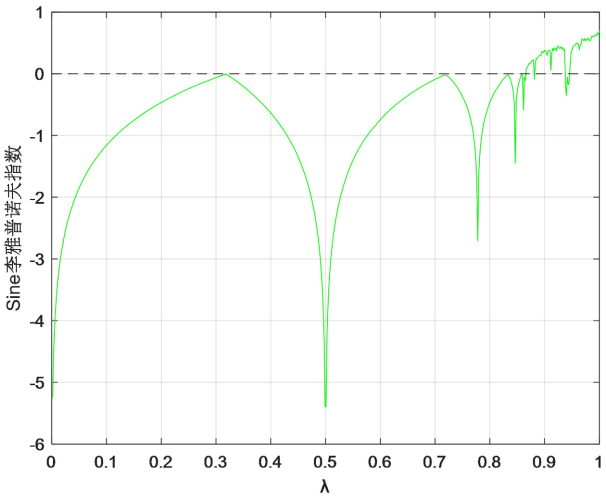
$$\lambda = \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln\left|f'\left(x_i\right)\right| \tag{6}$$

式中，$f'\left(x_i\right)$是$f\left(x_i\right)$的一阶导数，并且$f\left(x_i\right) = x_{i+1}$。

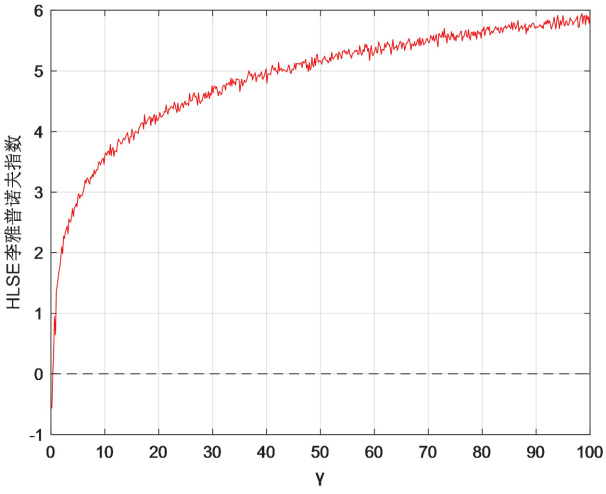
从图 3(a)、图 3(b)中可以看出，对于 Logistic 映射和 Sine 映射，它们的 LE 值仅在一个相对较小的控制参数范围内大于 0，即 Logistic 映射是在参数$\mu \in (3.57, 4]$时，Sine 映射是在参数$\lambda \in (0.87, 1]$时，它们的 LE 大于 0。而对于图 3(c)中我们设计的 HLSE 映射，当控制参数$\gamma > 3.5$时，其 LE 值就大于 0。此外，HLSE 映射的 LE 值随着控制参数的增加而持续增大，这意味着其混沌行为变得更加复杂。



(a) Logistic 映射李雅普诺夫指数



(b) Sine 映射李雅普诺夫指数



(c) HLSE 映射李雅普诺夫指数

Figure 3. Lyapunov exponents
图 3. 李雅普诺夫指数

显而易见，与 Logistic 映射和 Sine 映射相比，HLSE 映射拥有更大的参数范围和更大的 LE 值。这表明我们设计的 HLSE 映射具有复杂的动态特性，使其非常适合用于图像加密。

3. 图像的加密和解密

3.1. Zigzag 变换

3.1.1. 标准 Zigzag 变换

标准的 Zigzag 变换[12]经过多次变换后，矩阵中某些元素的位置并不会改变，而且有些像素还扎堆出现在一起，这意味着标准 Zigzag 变换的置乱效果有待改进。图 4 展示了一个 4 × 5 方阵的标准 Zigzag 扫描过程。

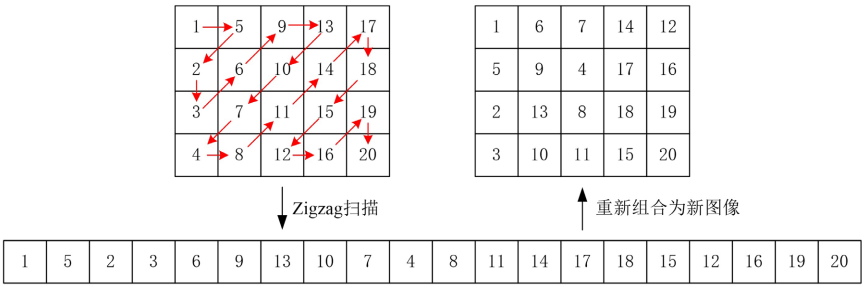


Figure 4. Scanning process of the standard Zigzag transformation
图 4. 标准 Zigzag 变换的扫描过程

3.1.2. 改进 Zigzag 变换

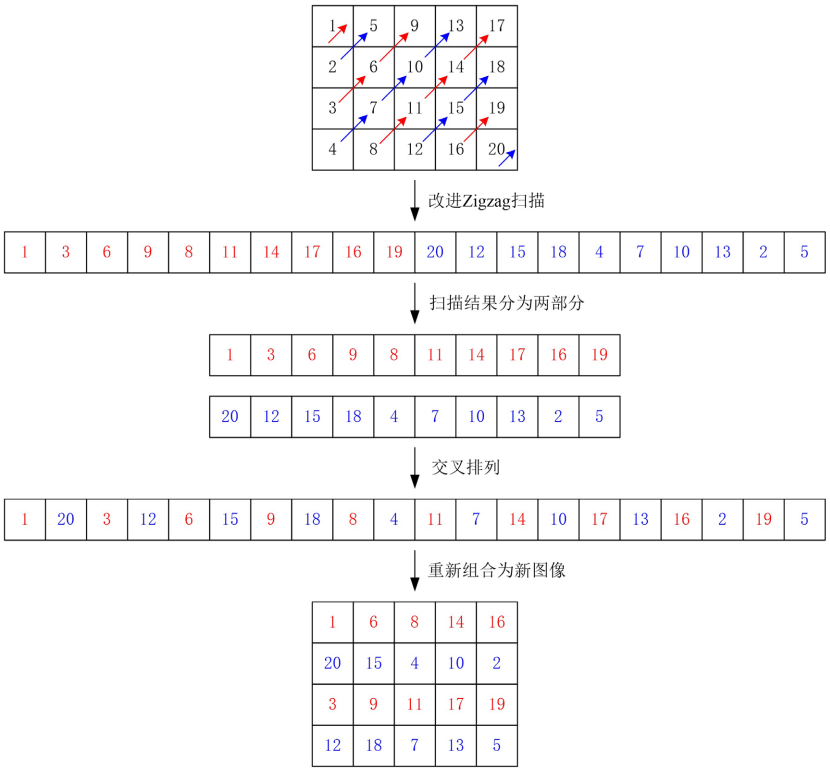


Figure 5. Scanning process of the improved Zigzag transformation
图 5. 改进 Zigzag 变换的扫描过程

为了克服标准 Zigzag 变换的缺点，本文提出一种分两次扫描的改进 Zigzag 变换，图 5 展示了一个 4 × 5 方阵的改进 Zigzag 扫描过程。

图 5 改进 Zigzag 变换算法详细描述如下：

1) 首先以左上角为起始点开始第一次扫描，扫描方式为 45 度斜向上。每一行扫描完成后，隔一行以类似的方式进行扫描，直至全部扫描完成为止。如图 5 中红色箭头所示。

2) 接下来从右下角开始往回进行第二次扫描，扫描方式依然为 45 度斜向上。每一行扫描完成后，隔一行以类似的方式往回进行扫描，直至全部扫描完成为止。如图 5 中蓝色箭头所示。

3) 把两次扫描的结果分为两部分。

4) 对两次扫描的结果进行交叉排列。

5) 把排列结果重新组合为新的图像。

从扫描结果可以看出，相比于标准 Zigzag 变换，改进 Zigzag 变换把原始数据打乱得更彻底，像素进行了更均匀的分散，没有出现扎堆的情况。这说明改进的 Zigzag 变换具有较好的效果。

3.2. 图像加密算法

3.2.1. 密钥生成

首先，采用 SHA-256 算法对明文图像进行处理，得到 64 个十六进制数的哈希值。然后，将这 64 个十六进制数转换为一个 256 位的二进制数。之后，把这个 256 位的二进制数分成 16 组，每组 16 位，用 $k_i\left(i=1,2,\cdots,16\right)$ 表示。最后，利用公式(7)和(8)来获取我们设计的 HLSE 混沌映射所需的两个初始值和两个控制参数。

$$\begin{cases} x_{01}=\dfrac{k_1\oplus k_2\oplus k_3\oplus k_4}{2^{16}} \\ x_{02}=\dfrac{k_5\oplus k_6\oplus k_7\oplus k_8}{2^{16}} \end{cases} \tag{7}$$

$$\begin{cases} \gamma_1=10+\dfrac{k_9\oplus k_{10}\oplus k_{11}\oplus k_{12}}{2^{16}} \\ \gamma_2=15+\dfrac{k_{13}\oplus k_{14}\oplus k_{15}\oplus k_{16}}{2^{16}} \end{cases} \tag{8}$$

式中，$\oplus$ 代表异或运算，x_{01}、x_{02} 为混沌 HLSE 映射的两个初值，γ_1、γ_2 为混沌 HLSE 映射的两个参数。

3.2.2. 加密算法

加密过程主要包括密钥生成、Zigzag 置乱、混沌索引置乱和异或扩散，加密流程如图 6 所示。加密算法详细描述如下：

步骤 1：生成密钥。明文图像通过哈希函数得到哈希值，对哈希值进行处理得到混沌的 2 个初值和 2 个控制参数，哈希值处理方法参考 3.2.1。

步骤 2：生成两个混沌序列 X1 和 X2。把步骤 1 得到的初值和参数代入 HLSE 映射，得到两个混沌序列 X1 和 X2。对于 X2 用公式(9)把它们转变为数值为 0~255 之间的整数数据。

$$\mathrm{X2}=\mathrm{mod}\left(\mathrm{X2}\times 10^{10},256\right) \tag{9}$$

式中，mod 为取模运算。

步骤 3：Zigzag 置乱。对明文图像用改进的 Zigzag 进行 Zigzag 置乱，改进的 Zigzag 变换参考 3.1.2。

步骤 4：混沌索引置乱。求取混沌序列 X1 的索引值，对 Zigzag 置乱后的结果进行混沌索引置乱。

步骤 5：异或扩散。用步骤 2 求出的混沌序列 X2 与步骤 4 混沌索引置乱后的图像进行异或扩散，得

到加密图像。

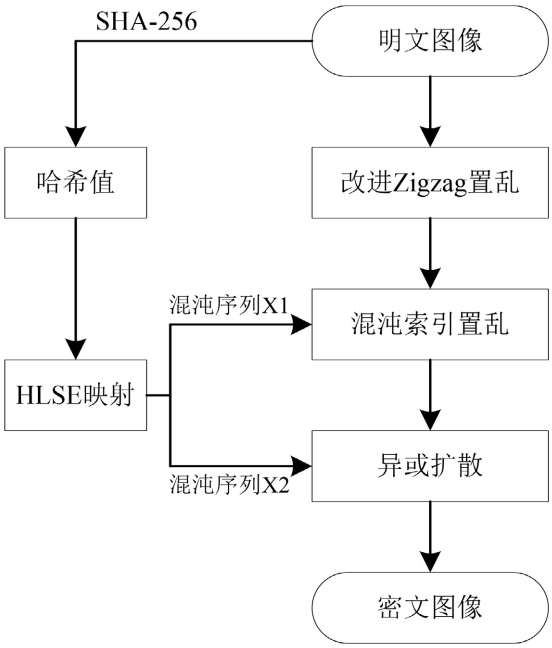


Figure 6. Flowchart of the encryption algorithm
图 6. 加密算法流程图

3.3. 图像解密算法

解密是加密的逆过程，其流程图如图 7 所示。

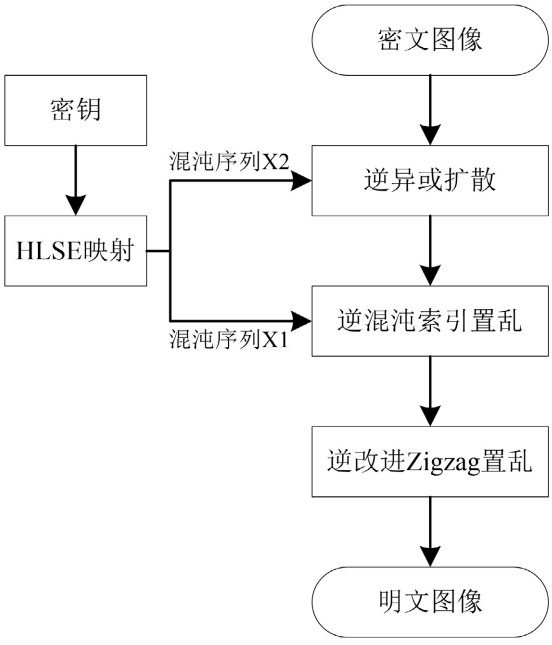


Figure 7. Flowchart of the decryption algorithm
图 7. 解密算法流程图

解密算法描述如下：

步骤 1：生成两个混沌序列 X1 和 X2。把给定的密钥代入 HLSE 映射，得到两个混沌序列 X1 和 X2。对于 X2 用公式(9)把它们转变为数值为 0~255 之间的整数数据。

步骤 2：逆异或扩散。用步骤 1 得到的序列 X2 与密文进行异或运算。

步骤 3：逆混沌索引置乱。求取混沌序列 X1 的索引值，对步骤 2 异或运算后结果进行逆混沌索引置乱。

步骤 4：逆 Zigzag 置乱。对步骤 3 结果进行逆 Zigzag 置乱，得到明文图像。

4. 实验结果与安全性分析

4.1. 实验结果

我们实验中所用计算机的软件平台和硬件配置如下：Matlab R2024b 以及一台配备 Intel(R) Core(TM) i5-1035G1 CPU @ 1.00 GHz 1.19 GHz 和 8 GB 内存的笔记本电脑。此外，实验中所用的所有灰度图像均来自南加州大学图像处理与图像分析数据库(https://sipi.usc.edu/database/)。图 8 展示了 Clock (256 × 256)、Boat (512 × 512)和 Male (1024 × 1024)灰度图像的实验结果，可以看出原始图像与解密后的图像完全一致，而加密后的图像则无法辨认。因此，所提出的加密算法能够实现理想的加密效果。

(a) Clock 明文　(b) Boat 明文　(c) Male 明文

(d) Clock 密文　(e) Boat 密文　(f) Male 密文

(g) Clock 密文解密图　(h) Boat 密文解密图　(i) Male 密文解密图

Figure 8. Experimental results
图 8. 实验结果

4.2. 安全性分析

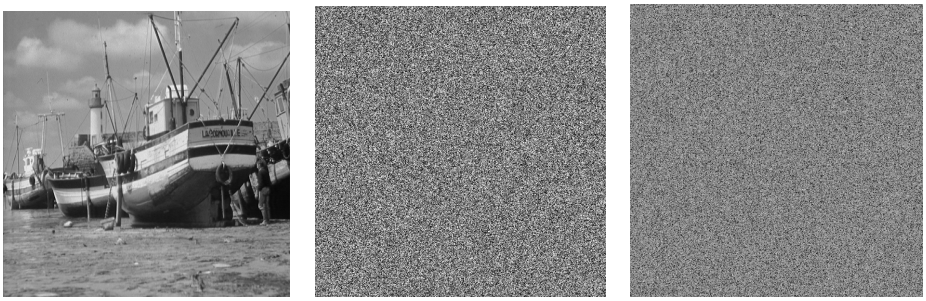
4.2.1. 密钥空间分析

密钥空间是指在密码学中，所有可能的密钥组成的集合。密钥空间的大小决定了密码系统的安全性。一般来说，密钥空间越大，暴力破解难度越高，反之，如果密钥空间过小，攻击者可以很容易地尝试所有可能的密钥，从而破解密码。

在我们的算法中，密钥的生成用的是 SHA-256 函数，另外在生成控制参数 γ_1 和 γ_2 时还有用到两个固定的值。假设计算精度为 10^{-14}，则每个密钥参数可视为拥有 10^{14} 种可能取值。该算法的密钥空间为 $2^{256} \times (10^{14})^2$，约等于 2^{349}，远大于 2^{100}，说明该算法具有较大的密钥空间，能够抵御暴力破解攻击。

4.2.2. 密钥敏感性分析

在密码学领域，密钥敏感性是用于评估加密算法安全性的关键指标之一，指的是密钥的微小变化对加密结果的影响程度。如果用于解密图像的密钥和加密原始图像的密钥存在些许偏差，就不能成功地将原始图像恢复出来。如图 9 所示，(a)为明文图像，(b)为正确密钥加密的图像，(c)为对密文用错误密钥解密的图像。本文只对解密的密钥参数 γ_1 由原值加上 10^{-14}，微小的变化导致了不能正确解密，说明该加密算法对密钥敏感。

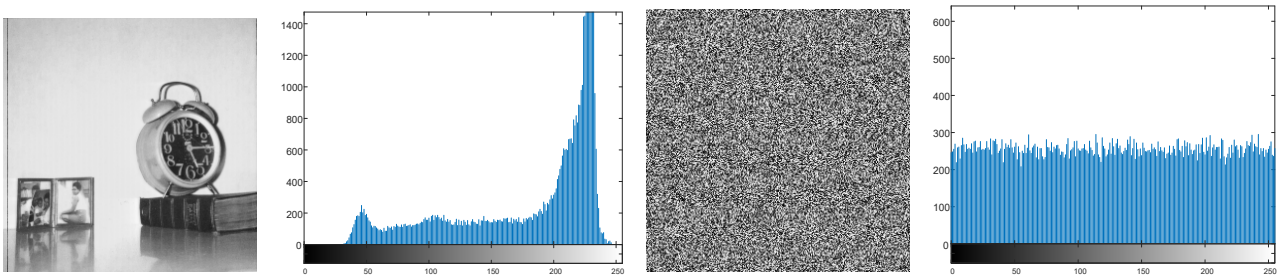


(a) Boat 明文　(b) Boat 密文　(c) 错误密钥解密图像

Figure 9. Key sensitivity analysis
图 9. 密钥敏感性分析

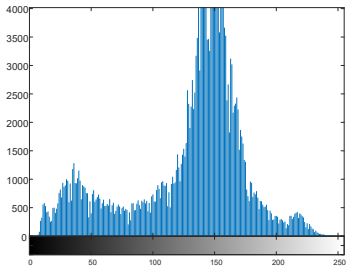
4.2.3. 直方图分析

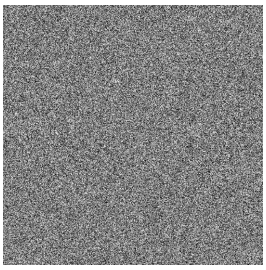
图像的直方图能够统计图像中每个灰度级出现的像素点数量。在原始图像中，灰度值通常具有一定的分布规律，其直方图可能呈现出特定的形状。当图像被加密后，在理想的情形下，其灰度值应尽可能地呈现出均匀分布的状态，即直方图应接近均匀分布。这意味着每个灰度级出现的像素数量大致相等。图 10 为加密前和加密后的图像直方图，可以看出加密后图像的直方图分布均匀。

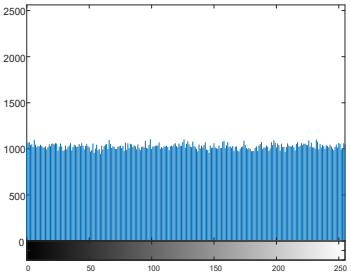


(a) Clock 明文　(b) Clock 明文直方图　(c) Clock 密文　(d) Clock 密文直方图

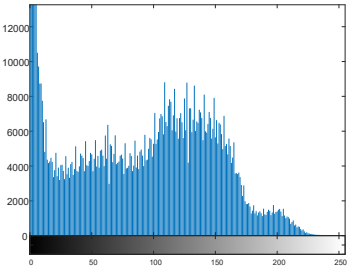

(e) Boat 明文

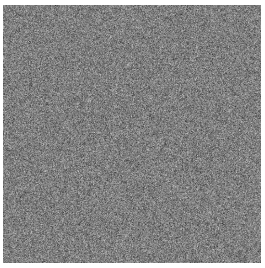

(f) Boat 明文直方图


(g) Boat 密文


(h) Boat 密文直方图


(i) Male 明文


(j) Male 明文直方图


(k) Male 密文

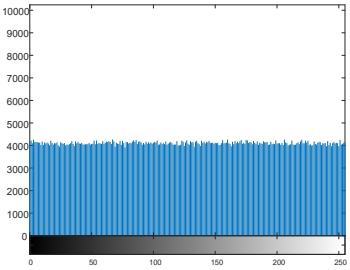

(l) Male 密文直方图

Figure 10. Histograms
图 10. 直方图

4.2.4. 相关性分析

正常图像相邻像素间存在显著空间关联性，易被攻击者利用以获取明文信息，威胁图像安全。为抵御攻击，需通过加密操作削弱像素在水平、垂直和对角线三个方向的相关性。

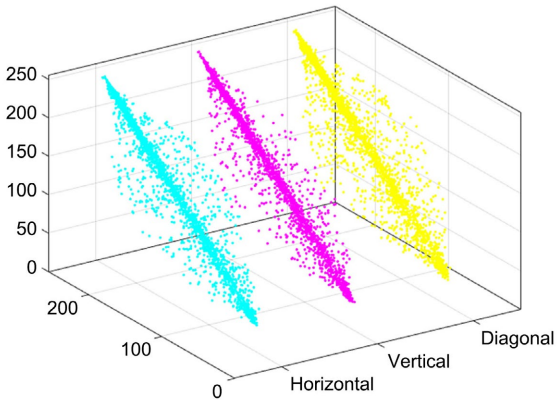
相关性计算公式如下：

$$r_{x,y}=\frac{E\left(x-E\left(x\right)\right)\left(y-E\left(y\right)\right)}{\sqrt{D\left(x\right)D\left(y\right)}} \tag{10}$$

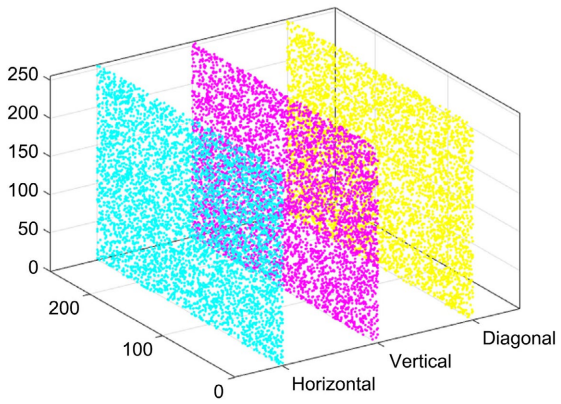
$$E\left(x\right)=\frac{1}{K}\sum_{i=1}^{K}x_i \tag{11}$$

$$D\left(x\right)=\frac{1}{K}\sum_{i=1}^{K}\left(x_i-E\left(x\right)\right)^2 \tag{12}$$

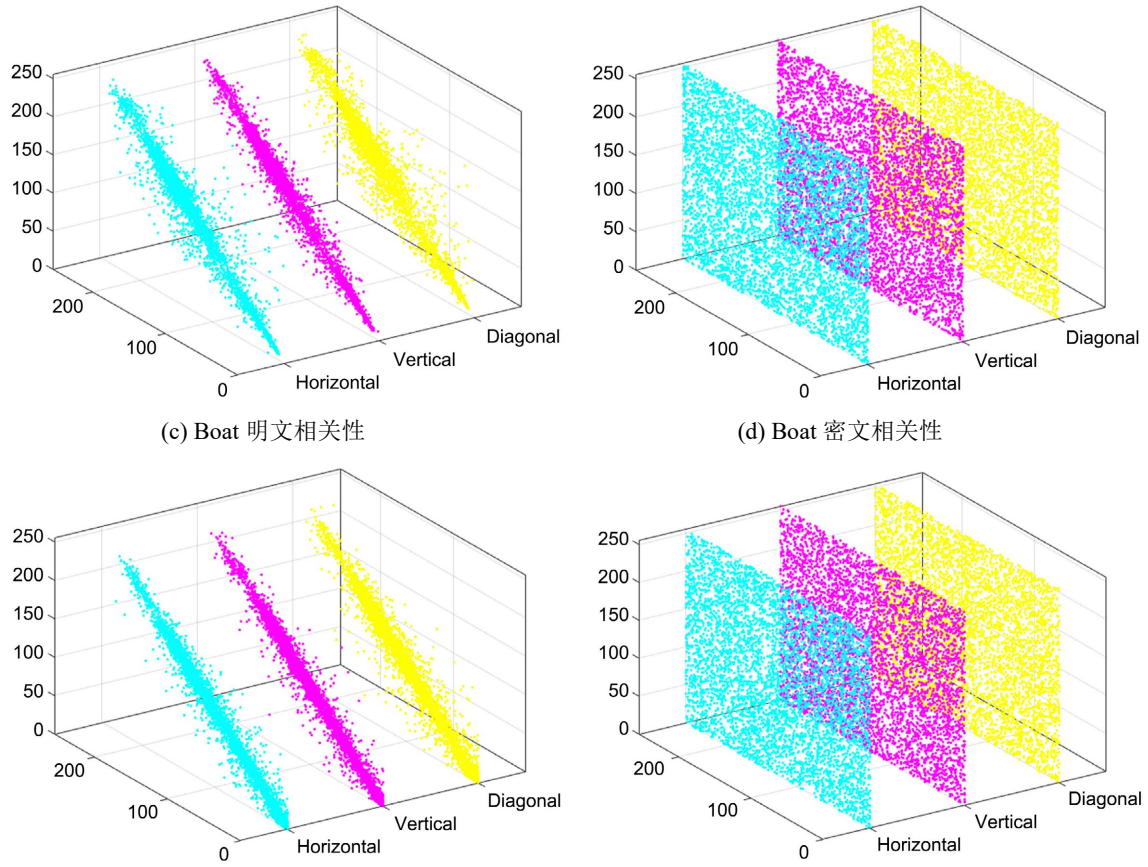
其中，x 是 y 的相邻像素，K 代表图像中像素的总数。$D(x)$是方差，$E(x)$是均值。



(a) Clock 明文相关性



(b) Clock 密文相关性



(c) Boat 明文相关性　(d) Boat 密文相关性

(e) Male 明文相关性　(f) Male 密文相关性

Figure 11. Correlation analysis between adjacent pixels
图 11. 相邻像素间的相关性分析

像素相关性图能直观反映此变化，从图 11 中可以看出，原始图像点分布密集，表明相关性高；加密后图像点分布均匀，表明相关性低，证明加密有效降低了相关性。

表 1 为相邻像素相关系数的对比结果，相关系数的值越接近 1，表示相关性越强；越接近 0，表示相关性越弱。可以看出，对比文献[13]-[15]，本加密算法的相关系数更接近 0，表明加密效果更好。

Table 1. Comparison of correlation coefficients of adjacent pixels
表 1. 相邻像素相关系数对比

算法	图像	水平	垂直	对角
本文算法	Clock 明文	0.9528	0.9712	0.9332
	Clock 密文	0.0045	−0.0232	−0.0012
	Boat 明文	0.9430	0.9727	0.9287
	Boat 密文	−0.0088	−0.0026	−0.0030
	Male 明文	0.9785	0.9802	0.9679
	Male 密文	−0.0008	−0.0040	−0.0067
文献[13]	Boat 密文	0.0050	0.0164	0.0033
文献[14]	Boat 密文	−0.0035	−0.0010	−0.0126
文献[15]	Boat 密文	0.0089	−0.0037	−0.0042

4.2.5. 信息熵分析

在图像加密领域，信息熵用于衡量加密图像中信息的不确定性或随机性。加密的目的之一是让加密后的图像尽可能随机，使攻击者很难从中提取出原始信息内容。信息熵越高，表明加密图像的像素分布越随机，保密效果越好。信息熵计算公式如下：

$$H(x)=-\sum_{i=1}^{n}P(x_i)\log_2 P(x_i) \tag{13}$$

其中，n 代表图像灰度值的种类数，x 表示像素值，$P(x_i)$表示像素值 x_i 出现的概率。对于 8 位灰度图像，理想加密状态下，图像各灰度值出现概率应近似相等，此时信息熵接近最大值 8。表 2 中展示了本加密算法的信息熵，并与其他文献进行了对比。从结果可知，本算法的信息熵近乎达到 8，说明本加密算法复杂度很高，攻击者难以对其进行破解。

Table 2. Comparison of information entropy
表 2. 信息熵对比

算法	图像	明文	密文
本文算法	Clock	6.7057	7.9971
	Boat	7.1914	7.9994
	Male	7.5237	7.9998
文献[13]	Boat	7.1914	7.9984
文献[14]	Boat	7.1914	7.9993
文献[15]	Boat	7.1914	7.9992

4.2.6. 差分攻击分析

图像加密的差分攻击是专门用于攻击图像加密算法的一种手段，为了防止受到差分攻击的威胁，就要确保明文图像的微小变动能够带来密文图像的显著变化。NPCR 和 UACI 是用于评估图像加密算法抗差分攻击强度的两项关键标准，其计算公式如下：

$$D(i,j)=\begin{cases}0, C_1(i,j)=C_2(i,j)\\ 1, C_1(i,j)\neq C_2(i,j)\end{cases} \tag{14}$$

$$\mathrm{NPCR}=\frac{1}{M\times N}\sum_{i=0}^{M}\sum_{i=0}^{N}D(i,j)\times 100\% \tag{15}$$

$$\mathrm{UACI}=\frac{1}{M\times N}\times\sum_{i=0}^{M}\sum_{i=0}^{N}\frac{\left|C_1(i,j)-C_2(i,j)\right|}{255}\times 100\% \tag{16}$$

其中，C_1 和 C_2 分别代表这样两个密文图像，它们所对应的明文图像中，只有一个像素灰度值发生了改变，M 和 N 分别表示图像的行数和列数。

当加密算法的输入有轻微变化时，输出就会有显著差异，这样的加密方式通常是安全可靠的，我们对 NPCR 和 UACI 进行了评估。理想状态下 NPCR 的值为 99.6094%，UACI 的值为 33.4635%。表 3 为 NPCR 和 UACI 的比较结果，可以看出，与文献[13]-[15]相比，本文算法更接近理想值。

4.2.7. 鲁棒性分析

鲁棒性分析是评估图像加密算法性能的关键，主要衡量加密图像遭受噪声、裁剪等攻击时的安全性

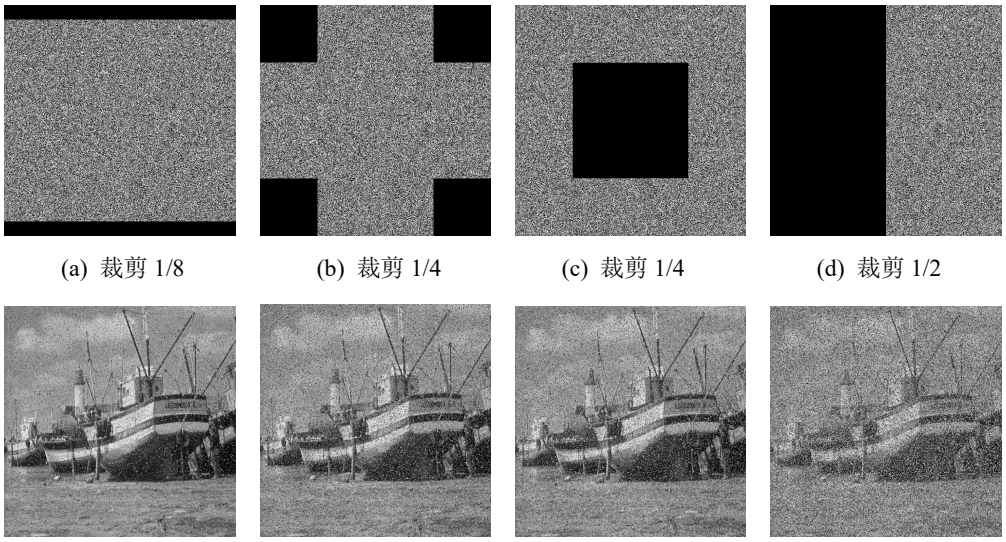
与完整性。优秀的加密算法需具备抗噪声和抗裁剪能力，确保受攻击后仍能准确解密，保证图像信息的完整性和准确性。

Table 3. Comparison of NPCR and UACI values
表 3. NPCR 和 UACI 的比较

算法	图像	NPCR (%)	UACI (%)
本文算法	Clock	99.6002	33.4586
	Boat	99.6048	33.4412
	Male	99.6095	33.4186
文献[13]	Boat	99.6153	33.4398
文献[14]	Boat	99.6035	33.4332
文献[15]	Boat	99.6024	33.4088

1) 裁剪攻击分析

为了验证图像在传输过程中遭到裁剪攻击后仍旧能保留图像的基础信息这一特性，进行了实验，结果如图 12 所示。其中图(a)~(d)分别为密文被裁剪 1/8 (顶部/底部)、1/4 (四角)、1/4 (中心)、1/2 (左半)，(e)~(h)分别为它们的解密图像。由图可知，解密后的图像能在最大程度上还原了原始图像的可视部分，证明了该加密算法具有较好的抗裁剪攻击能力。



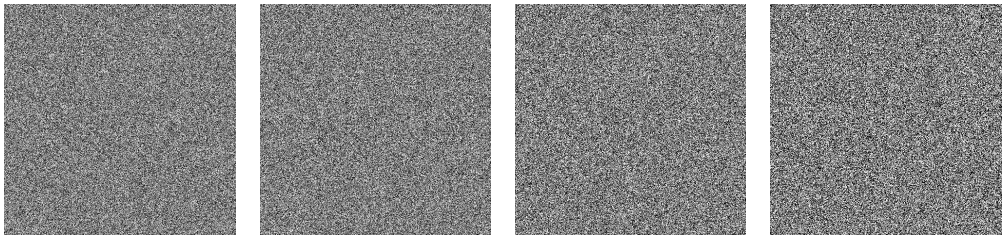
(a) 裁剪 1/8　(b) 裁剪 1/4　(c) 裁剪 1/4　(d) 裁剪 1/2

(e) 裁剪 1/8 解密结果　(f) 裁剪 1/4 解密结果　(g) 裁剪 1/4 解密结果　(h) 裁剪 1/2 解密结果

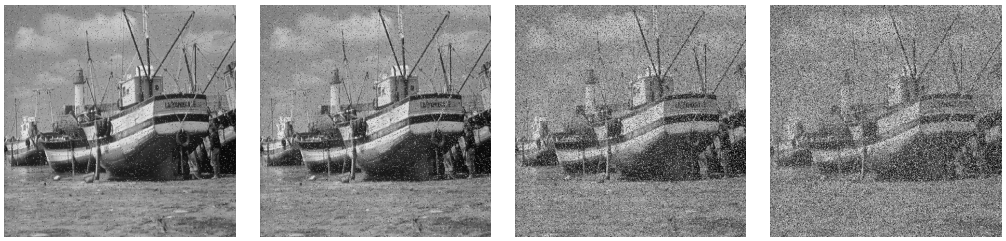
Figure 12. Clipping attack
图 12. 裁剪攻击

2) 噪声攻击分析

椒盐噪声是图像领域中较为常见的一类噪声。图 13 展示了密文在添加不同强度椒盐噪声的情况下，对解密结果所产生的影响。添加的椒盐噪声密度分别为 0.05、0.1、0.3、0.5。从仿真结果可以看出，尽管受到椒盐噪声的干扰，解密后的图像有部分像素值发生了变化，但是图像依然保留了原始图像的核心信息，这充分表明该加密算法具备较为出色的抗噪声攻击能力。



(a) 添加 0.05 椒盐噪声 (b) 添加 0.1 椒盐噪声 (c) 添加 0.3 椒盐噪声 (d) 添加 0.5 椒盐噪声



(e) 0.05 噪声解密结果 (f) 0.1 噪声解密结果 (g) 0.3 噪声解密结果 (h) 0.5 噪声解密结果

Figure 13. Salt & pepper noise attack
图 13. 椒盐噪声攻击

4.2.8. 时间分析

加密时间分析是评估图像加密算法性能的重要环节，通过对加密时间的分析，可以更好地了解算法的效率。本实验在 Intel(R) Core(TM) i5-1035G1 CPU @ 1.00 GHz 1.19 GHz、8 GB 内存的笔记本电脑下运行，使用的是 MATLAB R2024b 软件。表 4 给出了本文算法和其他算法的加密、解密时间，可以看出本文算法的效率优于其他算法。

Table 4. Encryption and decryption time
表 4. 加密和解密时间

算法	图像	加密时间(秒)	解密时间(秒)
本文算法	Clock (256 × 256)	0.136164	0.117543
	Boat (512 × 512)	0.543841	0.465622
	Male (1024 × 1024)	2.186457	1.972476
文献[13]	Boat (512 × 512)	1.256375	1.289654
文献[14]	Boat (512 × 512)	0.896547	0.867421
文献[15]	Boat (512 × 512)	1.536546	1.469853

5. 结束语

本文针对图像信息安全的需求，提出了一种结合新型 HLSE 混沌映射和改进 Zigzag 变换的图像加密算法。通过设计 HLSE 混沌系统，我们获得了一个具有更宽混沌范围、更优遍历性和更强初值敏感性的混沌序列发生器。同时，提出的改进 Zigzag 变换通过两次特定路径的扫描和结果的交叉排列，显著提升了像素的置乱程度和均匀性，克服了传统 Zigzag 变换的不足。加密方案利用 SHA-256 哈希值生成与明文相关的混沌密钥，并依次执行改进 Zigzag 置乱、混沌索引置乱和混沌异或扩散，实现了对图像数据的高效混淆和扩散。

全面的性能评估，包括密钥空间分析、密钥敏感性测试、直方图分析、相关性分析、信息熵分析、抗差分攻击(NPCR 和 UACI)能力评估、抗裁剪攻击和抗噪声攻击测试以及加解密时间分析，结果均表明本文提出的算法不仅具有高度的安全性，能有效抵御各种已知的密码分析攻击，而且在运算效率上也表现良好，优于部分现有算法。

综上所述，本文所提出的图像加密算法在安全性、鲁棒性和效率方面均展现出良好的综合性能，为数字图像在不安全信道中的传输和存储提供了一种可靠和有效的保护手段。

基金项目

本研究得到了巢湖学院 2024 年度国家级大学生创新创业训练计划项目(项目编号：202410380011)、巢湖学院 2024 年校级教学改革与研究项目(项目编号：x24jyxm02)的支持。

参考文献

[1] Long, B., Chen, Z., Liu, T., Wu, X., He, C., Wang, L., *et al.* (2024) Improved Fractal Coding and Hyperchaotic System for Lossless Image Compression and Encryption. *Nonlinear Dynamics*, **113**, 12233-12262. https://doi.org/10.1007/s11071-024-10671-2

[2] Deng, Y., Tian, X., Chen, Z., Xiao, Y. and Xiao, Y. (2024) An Image Encryption Algorithm Based on a Novel Two-Dimensional Hyperchaotic Map and Difference Algorithm. *Nonlinear Dynamics*, **113**, 3801-3828. https://doi.org/10.1007/s11071-024-10415-2

[3] Feng, W., Yang, J., Zhao, X., Qin, Z., Zhang, J., Zhu, Z., *et al.* (2024) A Novel Multi-Channel Image Encryption Algorithm Leveraging Pixel Reorganization and Hyperchaotic Maps. *Mathematics*, **12**, Article 3917. https://doi.org/10.3390/math12243917

[4] Etem, T. and Kaya, T. (2024) Modified Bernoulli Map-Based Scramble and S-Box Supported Colour Image Encryption. *Signal, Image and Video Processing*, **19**, Article No. 59. https://doi.org/10.1007/s11760-024-03572-9

[5] Belazi, A., Kharbech, S., Aslam, M.N., Talha, M., Xiang, W., Iliyasu, A.M., *et al.* (2022) Improved Sine-Tangent Chaotic Map with Application in Medical Images Encryption. *Journal of Information Security and Applications*, **66**, Article ID: 103131. https://doi.org/10.1016/j.jisa.2022.103131

[6] Xiao, Y., Tong, X., Zhang, M. and Wang, Z. (2022) Image Lossless Encoding and Encryption Method of SPECK Based on 1D Chaotic Map. *Physica Scripta*, **97**, Article ID: 055211. https://doi.org/10.1088/1402-4896/ac6544

[7] Liu, H. and Wang, X. (2011) Color Image Encryption Using Spatial Bit-Level Permutation and High-Dimension Chaotic System. *Optics Communications*, **284**, 3895-3903. https://doi.org/10.1016/j.optcom.2011.04.001

[8] Wang, X., Su, Y., Xu, M., Zhang, H. and Zhang, Y. (2021) A New Image Encryption Algorithm Based on Latin Square Matrix. *Nonlinear Dynamics*, **107**, 1277-1293. https://doi.org/10.1007/s11071-021-07017-7

[9] Vidhya, R. and Brindha, M. (2020) A Novel Dynamic Chaotic Image Encryption Using Butterfly Network Topology Based Diffusion and Decision Based Permutation. *Multimedia Tools and Applications*, **79**, 30281-30310. https://doi.org/10.1007/s11042-020-09462-9

[10] Yang, F., Mou, J., Cao, Y. and Chu, R. (2020) An Image Encryption Algorithm Based on BP Neural Network and Hyperchaotic System. *China Communications*, **17**, 21-28. https://doi.org/10.23919/jcc.2020.05.003

[11] Wang, X., Liu, C. and Jiang, D. (2021) A Novel Triple-Image Encryption and Hiding Algorithm Based on Chaos, Compressive Sensing and 3D DCT. *Information Sciences*, **574**, 505-527. https://doi.org/10.1016/j.ins.2021.06.032

[12] Zheng, J. and Lv, T. (2022) Image Encryption Algorithm Based on Cascaded Chaotic Map and Improved Zigzag Transform. *IET Image Processing*, **16**, 3863-3875. https://doi.org/10.1049/ipr2.12600

[13] Patel, S., Bharath K P, and Rajesh Kumar M, (2020) Symmetric Keys Image Encryption and Decryption Using 3D Chaotic Maps with DNA Encoding Technique. *Multimedia Tools and Applications*, **79**, 31739-31757. https://doi.org/10.1007/s11042-020-09551-9

[14] Ye, G., Wu, H., Jiao, K. and Mei, D. (2021) Asymmetric Image Encryption Scheme Based on the Quantum Logistic Map and Cyclic Modulo Diffusion. *Mathematical Biosciences and Engineering*, **18**, 5427-5448. https://doi.org/10.3934/mbe.2021275

[15] Patro, K.A.K., Soni, A., Netam, P.K. and Acharya, B. (2020) Multiple Grayscale Image Encryption Using Cross-Coupled Chaotic Maps. *Journal of Information Security and Applications*, **52**, Article ID: 102470. https://doi.org/10.1016/j.jisa.2020.102470