Statistics and Application 统计学与应用, 2025, 14(5), 141-157
Published Online May 2025 in Hans. https://www.hanspub.org/journal/sa
https://doi.org/10.12677/sa.2025.145133

Hans汉斯

基于二次定比分形插值的图像加密算法

宋李文静，叶瑞松*

汕头大学数学系，广东 汕头

收稿日期：2025年4月23日；录用日期：2025年5月15日；发布日期：2025年5月27日

摘　要

本文提出一个二次定比分形插值的模型，由其逆函数构造了一个新的分形动力系统，并从数值上验证了该动力系统的混沌特性。利用该分形混沌系统所生成的性能优良的伪随机数序列设计了一个图像加密算法，算法包括置乱和扩散两个阶段，置乱阶段应用约瑟夫遍历和排序算法打乱图像的行列像素位置。扩散阶段应用分形动力系统生成的混沌序列对图像行列进行按位加取模的双向扩散操作。论文对加密算法作了详细的性能分析，结果表明该算法具有优良的安全性能，可以抵抗多种攻击。

关键词

图像加密，信息安全，分形插值，迭代函数系统，约瑟夫遍历，扩散

Image Encryption Algorithm Based on Quadratic Proportional Fractal Interpolation

Liwenjing Song, Ruisong Ye*

Department of Mathematics, Shantou University, Shantou Guangdong

Received: Apr. 23rd, 2025; accepted: May 15th, 2025; published: May 27th, 2025

Abstract

A quadratic proportional fractal interpolation model is proposed, and a novel fractal dynamical system based on its inverse function is derived, whose chaotic properties are numerically analyzed and verified. Pseudo-random number sequences with excellent performance generated by the derived fractal chaotic system are employed to design an image encryption algorithm. The proposed image

*通讯作者。

文章引用: 宋李文静, 叶瑞松. 基于二次定比分形插值的图像加密算法[J]. 统计学与应用, 2025, 14(5): 141-157.
DOI: 10.12677/sa.2025.145133

encryption algorithm consists of permutation stage and diffusion stage. In the first stage, row-column scrambling based on adaptive Josephus traversal and sorting of chaotic sequence is performed. In the second stage, the chaotic sequence generated by the fractal chaotic dynamical system performs a bit-wise addition-modulo diffusion operation on the rows and columns of the processed image. The detailed performances of the proposed image encryption algorithm are carried out. Experimental results show that the proposed algorithm has excellent security performance and can resist various attacks.

Keywords

Image Encryption, Information Security, Fractal Interpolation, Iterated Function System, Josephus Traversal, Diffusion

1. 引言

在网络技术快速的时代，大数据信息具有极高的价值，图像是承载信息的一个重要载体，其传输、存储、访问等过程需要图像加密技术的保护[1]。常见的图像加密方案主要采用两类策略：一类是重点关注加密系统中伪随机序列密钥流的生成来源和方式，构造新型混沌系统，对传统的混沌系统及其生成的混沌序列进行各种改进；另一类是关注加密算法的结构设计，设计性能优良的加密算法，构造新颖有效的置乱算法和扩散函数，从而获得具有更好性能和安全性的图像加密算法。

在第一类图像加密方案中，随机数序列主要采用混沌系统生成[2]。1998 年，Fridrich 首次提出使用二维的 Baker 映射和 Cat 映射进行像素位置的变换，这是混沌系统在图像加密中的首次应用[3]。在基于混沌系统的图像加密方案中，研究人员大多关注混沌映射的构造和混沌系统性质的应用，赵耿等人提出一种变参数 Logistic 系统的图像加密算法[4]；叶瑞松等人提出基于帐篷映射迭路和 Baker 映射迭路的图像加密算法[5] [6]；黄佳鑫等人提出了一种复合混沌系统[7]，将三个一维混沌系统进行耦合生成新的混沌系统，扩大了参数范围，从而使得图像加密算法具有较大的密钥空间；Hu 等人构造了一种基于确定单位变换的耦合混沌系统，该系统可以结合任意两个一维混沌映射，生成性能更好的新混沌映射[8]。一般来讲，一维混沌映射具有轨道点分布不均匀、混沌参数范围较窄等缺点。因此，研究加密算法的学者针对一维混沌系统及其生成的伪随机序列进行进一步改进，提升系统的混沌性能和所生成的混沌序列的随机性能。曾祥秋等人通过模运算对 Logistic 映射进行改进，将产生的小数进行二进制移位操作以生成性能更好的伪随机数[9]。Alawida 等人提出一种通过翻转混沌状态值的分数位顺序的方法来修改混沌状态值，验证了该方法确实可以使改进的混沌映射具有更好的混沌性能、更高的复杂度和更大的混沌参数范围，并利用该方法设计了基于级联混沌映射的伪随机比特生成器[10]。Sharma 等人提出一种通过对序列尾数位之间进行异或操作，从而对混沌序列进一步随机化[11]。Zheng 提出了一种新的位循环移位方法解决随机数动态退化问题，增强数字混沌序列值的随机性[12]。

在第二类图像加密策略中，学者们设计了一系列的图像加密算法，从置乱算法和扩散机制上改进传统的算法，使得加密算法获得更好的安全性能。Zhang 等人提出了明文关联的“扩散－置乱－扩散”的图像加密算法，其中扩散算法使用明文无关的密码，置乱算法借助明文关联的密码[13]。丁玮等人提出了一种基于 Arnold 变换的图像加密方法，该方法在位置空间和色彩空间上对图像进行置乱，过程简便易行，

可以用来作为数字图像隐藏和伪装的预处理[14]。洪炎等人对传统 Arnold 变换置乱方式进行改进，使其能够加密任意大小的图像，并通过加入行列按位异或运算，有效破坏明文图像的相邻像素相关性，提升了图像在传输时的抗攻击能力[15]。Azimi 和 Ahadpour 提出了一种基于混沌映射和 DNA 动态编码的图像加密算法，该算法结合成对耦合混沌映射对彩色图像 RGB 三通道的像素值进行 DNA 扩散加密，实现了对彩色图像的加密[16]。牛莹等人提出了一种变步长的约瑟夫遍历和 DNA 动态编码的图像加密方法，将混沌映射产生的随机序列作为约瑟夫遍历的步长，实施变步长的约瑟夫遍历置乱，并且动态选择 DNA 编码规则对图像像素进行扩散，通过增强密钥敏感性来提高算法的安全性[17]。尹思文等人利用明文图像的哈希值进行密钥扩展。提出“一像素一规则”思想，并利用 DNA 运算有效地提高算法的加密和解密效率，使加密算法能够有效抵御各种常规的密码攻击[18]。孙鹤鹏等人提出了一种基于 DNA 编码的多图像加密算法，利用混沌映射产生的序列生成混沌图像，将置乱图像与 DNA 编码的混沌密钥图像进行加法运算完成扩散过程，该算法可以同时对任意数量的图像进行加密[19]。

分形几何是一种研究自然界中不规则几何形状的数学工具，它突破了传统欧几里得几何对规则形状的限制，能够描述和分析自然界中广泛存在的复杂、不规则对象。分形插值技术作为分形几何理论的重要应用分支，通过深度结合自相似性原理和迭代函数系统的数学框架，实现了对离散数据点的非线性插值重构。该技术突破传统插值范式，通过引入自相似性映射机制，将全局几何特征分解到局部数据区间，从而在插值过程中完整保留数据点间的非线性关联和复杂变化细节。1890 年 Peano 发现可以使用迭代函数系统(IFS)的方法生成填充单位正方形的曲线(Penao 填充曲线)，其本质是该 IFS 的分形为单位正方形[20]。由于 IFS 的压缩性，可以诱导得到单位正方形上的分形混沌动力系统。近年来，叶瑞松等人基于 IFS 和分形插值方法，开展了序列的研究工作，利用分形理论方法构造了新型的具有优良混沌性能的动力系统，并用所生成的混沌序列作为密钥流设计图像加密算法。文献[21]和文献[22]分别基于二维和三维仿射变换的分形插值方法，构造了新型的二维和三维分形混沌系统，并将其用于生成控制加密过程的伪随机数密钥流，实现了很好的加密效果[21] [22]。文献[23]和文献[24]分别通过两参数和三参数的 IFS 诱导得到新的分形动力系统，性能分析表明所得到的分形动力系统具有实现简单，生成的混沌序列具有超混沌性等诸多优良性能，并设计了具有优良性能的图像加密算法[23] [24]。

本文将从两方面入手设计一种新的图像加密算法。首先构造一种基于二次定比分形插值的分形动力系统，并将其用于生成控制加密过程的密钥流。基于分形插值理论，通过插值数据集生成对应的迭代函数系统，并由此诱导得到其分形动力系统。与文献[21]和文献[22]所应用的分形插值模型不同，本文通过增加分形插值模型中迭代函数系统的二次项，导致分形动力系统具有更多的参数选项，扩大了基于分形混沌系统的图像加密算法的密钥空间和安全性。通过分岔图、李雅普诺夫指数、自相关函数等对系统生成的混沌序列进行性能分析，结果表明所构造的分形动力系统具有优良的混沌特性，通过该系统生成的序列具有更好的遍历性、初值敏感性、伪随机性等混沌特性。其次，基于该分形动力系统生成的混沌序列密钥流设计了一种新的“置乱－扩散”的图像加密算法，其中置乱操作通过自适应的约瑟夫遍历和基于混沌序列排序实现，增强了算法抵御明文攻击的性能；扩散操作通过行列按位加取模的扩散机制实现，进一步获得更好的扩散效果。论文对所提出的图像加密算法进行了详细的性能分析，结果表明该算法具有优良的安全性能，可以抵抗多种攻击。

本文的剩余部分安排如下。第二节构造了一个基于二次定比分形插值的新型分形动力系统，并对分形动力系统生成的序列进行性能分析和随机性验证。第三节提出一个基于约瑟夫遍历和混沌序列排序的自适应置乱操作以及加取模运算的双向扩散的图像加密算法。第四节对图像加密算法作仿真实验，并验证算法的各种性能。第五节作一个总结。

2. 二次定比分形插值及其伴随分形动力系统

2.1. 二次定比分形插值

考虑如公式(1)所示的非线性变换，用于生成经过插值数据集 $\{(x_i,y_i)\in R^2:i=0,1,\cdots,N\}$ 的分形插值函数。

$$W_n(x,y)=\left(a_nx+e_n,c_nx+d_ny+p_nx^2+t_nxy+f_n\right),n=1,2,\cdots,N \tag{1}$$

其中 a_n,e_n,c_n,d_n,p_n,t_n 和 f_n 都是实参数，并且垂直因子 $|d_n|<1$，需要满足

$$\begin{cases}W_n(x_0,y_0)=(x_{n-1},y_{n-1}),\\ W_n(x_N,y_N)=(x_n,y_n),n=1,2,\cdots,N.\end{cases} \tag{2}$$

设 d_n,p_n,t_n 为自由参量，令 $L=x_N-x_0$，从公式(2)得到其它系数，如公式(3)所示。

$$\begin{cases}a_n=L^{-1}(x_n-x_{n-1}),e_n=L^{-1}(x_Nx_{n-1}-x_0x_n),\\ c_n=L^{-1}\left[y_n-y_{n-1}-d_n(y_N-y_0)-p_n(x_N^2-x_0^2)-t_n(x_Ny_N-x_0y_0)\right],\\ f_n=L^{-1}\left[x_Ny_{n-1}-x_0y_n-d_n(x_Ny_0-x_0y_N)+p_n(x_0x_N^2-x_0^2x_N)-t_nx_0x_N(y_0-y_N)\right],\\ n=1,2,\cdots,N.\end{cases} \tag{3}$$

设插值数据集为 $\{(0,0),(0.3,0.7),(0.5,0.4),(0.6,0.58),(1,1)\}$，改变 $d=[d_1,d_2,\cdots,d_N];p=[p_1,p_2,\cdots,p_N];t=[t_1,t_2,\cdots,t_N]$ 三组参数中某组的数值，观察显示的分形插值曲线。对于初始设定参数为 $d=[0.81,0.84,0.76,0.69];p=[0.52,0.27,0.93,0.16];t=[0.44,0.39,0.67,0.83]$ 的分形插值函数，图 1 显示了分别修改自然参数 $d=[0.5,0.5,0.5,0.5]$ 和 $p=[0.5,0.5,0.5,0.5]$ 的插值曲线。二次定比分形插值通过引入非线性变换，在细节刻画和参数控制上比一次分形插值更丰富，生成的分形插值曲线的结构更复杂，使得其诱导的混沌系统的动力学性质更复杂。

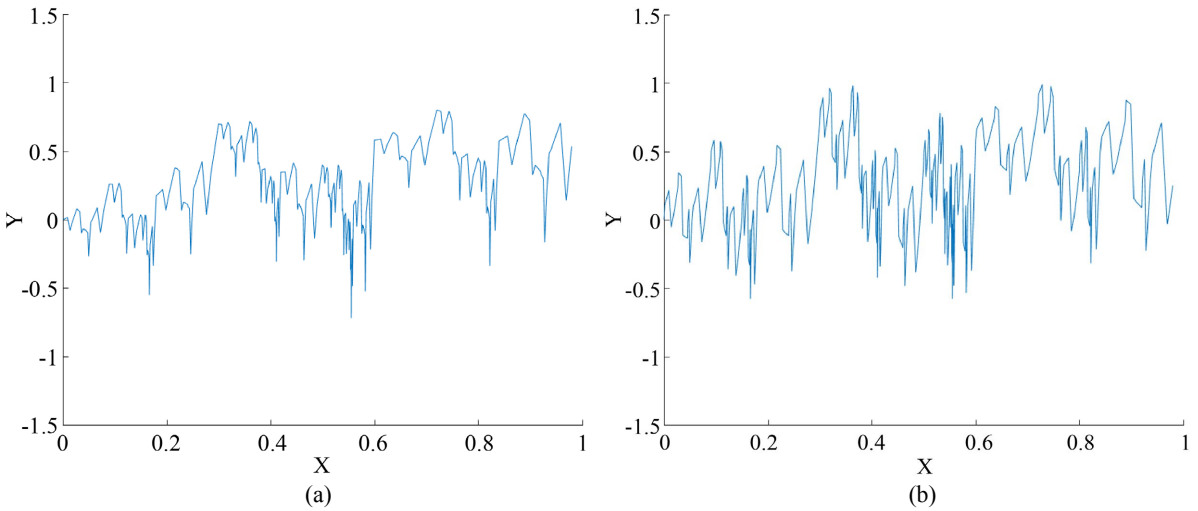

Figure 1. Quadratic proportional fractal interpolation curve
图 1. 二次定比分形插值曲线

2.2. 二次定比分形插值的伴随分形动力系统

考虑给定 $N+1$ 个插值点以及自由参量 d_n,p_n,t_n，可以通过公式(3)计算得到该迭代函数系统的参数

$a_n, c_n, e_n, f_n, n = 1, \cdots, N$。根据 IFS 理论，得到了一个伴随动力系统，如公式(4)所示。

$$\begin{cases} z_{k+1} = (z_k - e_n)/a_n, z_k \in [x_{n-1}, x_n], k = 0,1,2,\cdots \\ w_{k+1} = \left(w_k - p_n z_{k+1}^2 - c_n z_{k+1} - f_n\right)/\left(d_n + t_n z_{k+1}\right). \end{cases} \tag{4}$$

对于给定的初始值$(z_0, w_0), z_0 \in [x_0, x_N]$，随着迭代次数的增加，$z_k$ 会保持在$[x_0, x_N]$之间，而 w_k 则有可能发散，因此增加模 1 运算的操作，确保 w_k 保持在$[0,1]$之间。增加模 1 运算的操作见公式(5)，其中 mod 是模运算，$\mathrm{mod}(u,v)$ 返回一个余数 r，满足 $u = kv + r, r \in [0, v)$。本文将插值数据局限在单位区间上，所以采用模 1 的运算。分形动力系统(5)即是本文所构造的基于分形插值的新型分形动力系统。

$$\begin{cases} z_{k+1} = (z_k - e_n)/a_n, z_k \in [x_{n-1}, x_n], k = 0,1,2,\cdots \\ w_{k+1} = \mathrm{mod}\left(\left(w_k - p_n z_{k+1}^2 - c_n z_{k+1} - f_n\right)/\left(d_n + t_n z_{k+1}\right), 1\right). \end{cases} \tag{5}$$

2.3. 性能分析

设插值数据集、动力系统(5)的初始值和自由参数如公式(6)所示。

$$\begin{aligned} &\{(0,0),(0.3,0.7),(0.5,0.4),(0.6,0.58),(1,1)\}, z_0 = 0.22, w_0 = 0.57 \\ &d = [0.81, 0.84, 0.76, 0.69]; p = [0.52, 0.27, 0.93, 0.16]; t = [0.44, 0.39, 0.67, 0.83] \end{aligned} \tag{6}$$

迭代二次定比分形插值的伴随分形动力系统(5) 10^6 次，产生两个状态值序列 X, Y，用于分析分形动力系统(5)在单位正方形的混沌特性。

2.3.1. 相图

根据给定的初始值、系统参数和自由参数，系统(5)的前 10000 个轨迹点的二维相图如图 2 所示，可以看出该系统迭代生成的点均匀地分布在单位正方形内。

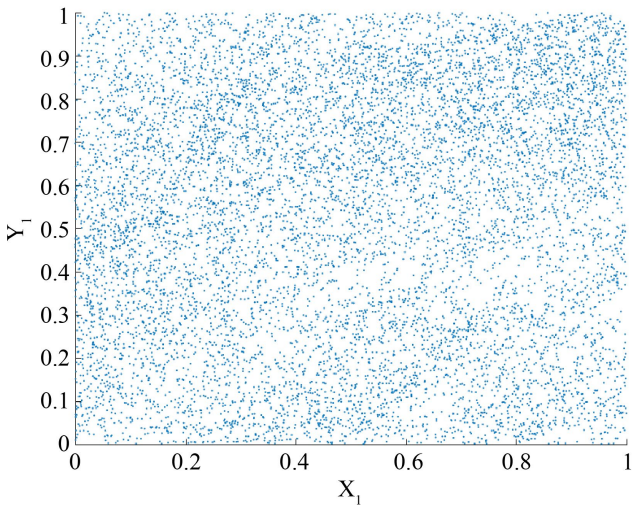

Figure 2. Phase diagram of the generated two-dimensional sequence with 10,000 iterations
图 2. 迭代 10,000 次生成的二维序列的相图

2.3.2. 分岔图

分岔是动力系统理论中的一个重要概念，它用于展示动力系统随着参数变化的动力学行为。在分岔图中，通常横轴表示系统的某个参数，而纵轴表示系统的状态。从分岔图可以观察系统在什么参数范围

为混沌状态。固定 p,t 的值，图 3(a)刻画了状态 z 的序列值 Y 随 d 变化的分岔；固定 d,t 的值，图 3(b)刻画了序列 Y 随 p 变化的分岔。当 t 变化时，也有类似的分叉图，意味着参数 $d,p,t\in[0,1]$ 时，分形动力系统(5)均具有很好的遍历性。

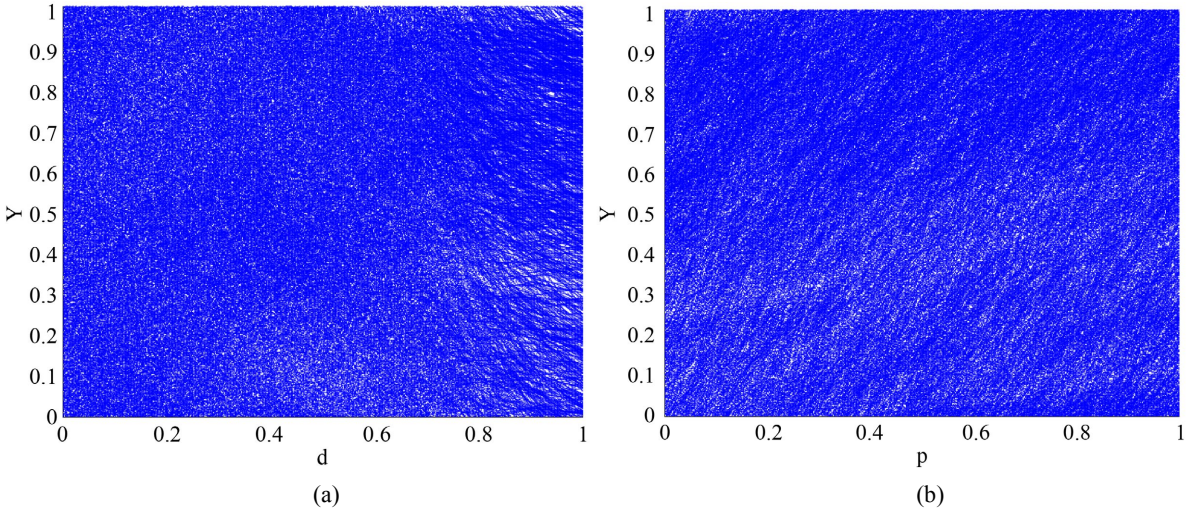

Figure 3. Bifurcation of sequence with parameter variation
图 3. 序列随参数变化的分岔

2.3.3. 李雅普诺夫指数

李雅普诺夫指数量化系统对初始条件敏感性的程度。如果一个动力系统的最大李雅普诺夫指数大于零，则系统对初值具有敏感依赖性。若多维混沌系统最大的李雅普诺夫指数大于 0，则认为系统具有混沌特性。混沌动力系统的李雅普诺夫指数计算，可以参考文献[21]。当自然参量 d,p,t 改变时，系统(5)的最大的李雅普诺夫指数均大于 0。图 4(a)，图 4(b)分别显示动力系统(5)关于 p,t 的李雅普诺夫指数，进一步验证了当参量 p,t 取值在[0, 1]之间时，该系统具有优良的混沌行为。

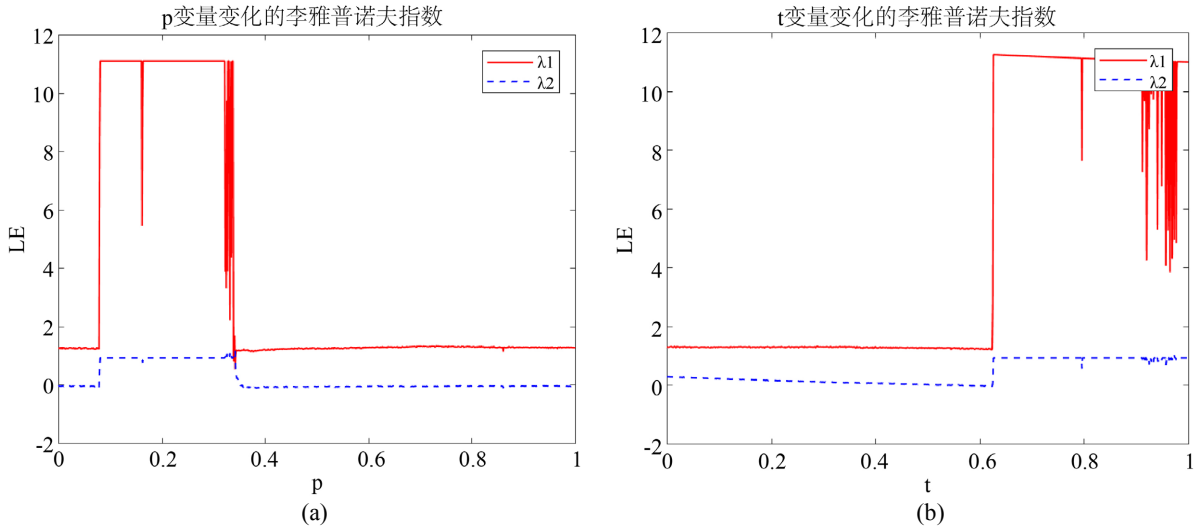

Figure 4. Lyapunov exponent of parameters for power system (5)
图 4. 动力系统(5)关于参数的李雅普诺夫指数

2.3.4. 序列的相关性

一个时间序列的延迟 k 期的自相关系数用于衡量同一个时间序列相隔 k 个时刻的序列值之间的相关性大小。互相关系数衡量两个不同时间序列之间的相关性，延迟 k 阶的互相关系数刻画一个时间序列与延迟 k 个时刻的另一个序列的值之间的相关程度。具体计算公式可参考文献[22]。分别对初始值为 $z_0=0.22, w_0=0.57$ 和 $z_0=0.22+10^{-6}$， $w_0=0.57$ 的混沌动力系统(5)产生的序列 Y_1, Y_2 计算自相关系数和互相关系数。序列 Y_1 的延迟 0-200 期的自相关系数分别如图 5(a)所示，序列 Y_1, Y_2 的延迟 0-200 期的互相关系数如图 5(b)所示。

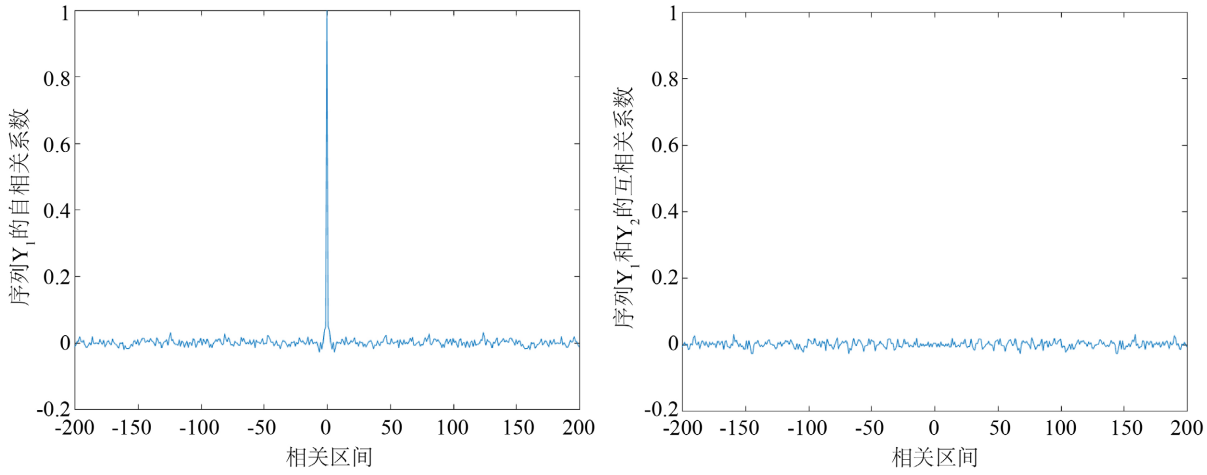

Figure 5. Sequence correlation analysis results
图 5. 序列相关性分析结果

2.3.5. SP800 随机数检验

NIST 发布的一套密码学模块检测标准 SP800-22 Rev1a 中，给出了 15 种测试方法，用于检验混沌系统所生成的比特序列的随机特性。根据 SP800-22 Rev1a，对预处理后的长度为 10^6 序列 Y 进行测试，测试的结果如表 1 所示，每项测试的 P 值均大于 0.01，通过随机性检测。参与检测的 0~1 比特序列通过公式(7)量化得到。

$$Y=\mathrm{mod}\left(\mathrm{floor}\left(Y\times 10^6\right),2\right) \tag{7}$$

其中 floor 是向下取整操作，返回不大于 x 的最大整数。

Table 1. SP800-22 Rev1a random characteristics test results
表 1. SP800-22 Rev1a 随机特性测试结果

NIST 统计检验	P 值(序列 Y)	结果
单比特频率测试	0.3692	通过
块内频率测试	0.9978	通过
游程测试	0.7315	通过
块内最长 1 游程	0.0635	通过
二进制矩阵秩测试	0.1194	通过

续表

离散傅里叶测试	0.5045	通过
非重叠模板匹配测试	0.4921	通过
重叠模板匹配测试	0.0157	通过
Maurer 通用统计测试	0.9025	通过
线性复杂度测试	0.3151	通过
序列测试	0.0609 0.0279	通过
近似熵测试	0.2429	通过
累加和测试	左：0.5156，右：1.0000	通过
随机旅行测试	0.3830，0.7130，0.7909，0.1876，0.8482，0.4207，0.3922，0.1824	通过
随机旅行变种测试	0.8635，0.9150，0.7062，0.5487，0.4270，0.4214，0.2596，0.3338，0.8439，0.8903，0.4668，0.2414，0.1927，0.1640，0.2124，0.2031，0.2036，0.1631	通过

3. 图像加密算法

本文设计的图像加密算法包括两个阶段，自适应约瑟夫遍历算法和排序变换算法结合的行列置乱和基于分形插值的伴随动力系统生成的密钥流所控制的行列按位扩散。加密的流程图见图 6。

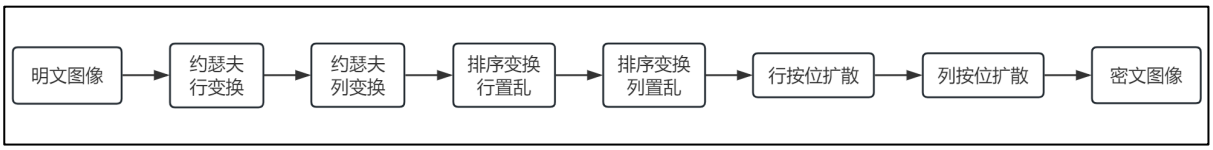

Figure 6. Encryption algorithm flowchart
图 6. 加密算法流程图

3.1. 基于自适应约瑟夫遍历的置乱

约瑟夫遍历问题是一个著名的数学和计算机科学问题。问题描述如下：有 n 个人站成一个圈，从第 1 个人开始报数，每数到第 l 个数的人会被排除圈外，然后从被排除的人的下一个人开始，继续重复这个过程，直到圈中只剩下一个人。将约瑟夫遍历用函数表达，即 $ysf(n,l)$，这里 n 为元素个数，l 为步长。约瑟夫遍历的结果相当于对一个元素间隔为 l 的序列进行重排，每个元素按照规定的顺序出现一次。例如，函数 $ysf(10,3)$ 是将序列 $[1,2,3,4,5,6,7,8,9,10]$ 变为 $[3,6,9,2,7,1,8,5,10,4]$。

图像置乱是通过数学变换或算法对图像的像素位置进行重新排列，使得图像内容变得难以辨认，从而达到加密的效果。本文采用约瑟夫遍历分别对图像进行行置乱和列置乱。对大小为 $M\times N$ 明文图像 P，首先对其每一行像素进行置乱，由于置乱只修改像素位置而不改变像素值，若每行置乱采用的约瑟夫遍历的步长通过式(8)给出，置乱前后步长 l_i 都可以通过处理的图像得到，从而保证加密图像能够被还原。

$$l_i = \mathrm{mod}\left(\sum_{j=1}^{N}\left(P(i,j)\right), \mathrm{ceil}(N/4)\right)+10 \tag{8}$$

其中 i 为进行置乱操作的行序数，N 为图像的列数，$\mathrm{ceil}(x)$ 是向上取整函数，返回不小于 x 的最小整数。每行置乱采用的约瑟夫遍历的步长与明文图像相关，能够根据明文图像的特性或加密需求自动调整加密

过程，以提高加密效果和安全性。算法具有自适应性，可以使加密算法更加灵活和强大，从而更好地抵抗各种攻击，如差分攻击和选择明文攻击。

同理，对进行行置乱后的图像 P_1 进行列置乱，每列置乱采用的约瑟夫遍历的步长 l_j 通过式(9)给出。

$$l_j = \mathrm{mod}\left(\sum_{i=1}^{M}\left(P_1(i,j)\right), \mathrm{ceil}\left(M/4\right)\right)+10, \tag{9}$$

其中 j 为进行置乱操作的列序数， M 为图像的行数。得到列置乱处理后图像 P_2 进行下一步加密操作。

3.2. 具体的加密算法

设定二次定比分形插值的参数(6)，迭代分形混沌系统(5)，生成长度为 $4MN$ 的序列，取序列前面的 MN 个数转化成大小为 $M\times N$ 的矩阵 S；对原序列进行量化处理，得到 4 个大小为 $M\times N$ 的二维矩阵 A,B,C,D，如公式(10)所示。

$$\begin{aligned}
S &= \mathrm{reshape}\left(Y(1:MN), M, N\right),\\
A &= \mathrm{reshape}\left(\mathrm{mod}\left(\mathrm{floor}\left(Y(1:MN)\times 10^6\right), 256\right), M, N\right),\\
B &= \mathrm{reshape}\left(\mathrm{mod}\left(\mathrm{floor}\left(Y(MN+1:2MN)\times 10^6\right), 256\right), M, N\right),\\
C &= \mathrm{reshape}\left(\mathrm{mod}\left(\mathrm{floor}\left(Y(2MN+1:3MN)\times 10^6\right), 256\right), M, N\right),\\
D &= \mathrm{reshape}\left(\mathrm{mod}\left(\mathrm{floor}\left(Y(3MN+1:4MN)\times 10^6\right), 256\right), M, N\right),
\end{aligned} \tag{10}$$

其中 S 用于图像像素的基于排序的置乱， A,B 用于行按位扩散， C,D 用于列按位扩散。

加密算法：

输入：大小为 $M\times N$ 的明文图像 P。

输出：大小为 $M\times N$ 的密文图像 T。

Step 1. 利用明文图像 P 的哈希值更新初外部密钥。将明文图像 P 输入 SHA-256 散列函数得到长度为 256 bit 的散列序列 H，生成 32 个 8 bit 的 Hash 值，记为 $K_1,K_2,\cdots,K_{32}$，通过式(11)生成与明文相关的 $h_1,h_2,\cdots,h_{16}$，再通过式(12)更新外部密钥，得到新的密钥 z_0,w_0,d,p,t。

$$h_i = \frac{K_{2(i-1)+1}\oplus K_{2i}}{256},\ i=1,\cdots,16 \tag{11}$$

$$\begin{cases}
d = \left[\dfrac{d_1+h_1}{2}, \dfrac{d_2+h_2}{2}, \dfrac{d_3+h_3}{2}, \dfrac{d_4+h_4}{2}\right], p = \left[\dfrac{p_1+h_5}{2}, \dfrac{p_2+h_6}{2}, \dfrac{p_3+h_7}{2}, \dfrac{p_4+h_8}{2}\right],\\
t = \left[\dfrac{t_1+h_9}{2}, \dfrac{t_2+h_{10}}{2}, \dfrac{t_3+h_{11}}{2}, \dfrac{t_4+h_{12}}{2}\right], z_0 = \dfrac{z_0+h_{13}+h_{14}}{3}, w_0 = \dfrac{w_0+h_{15}+h_{16}}{3}.
\end{cases} \tag{12}$$

Step 2. 对于明文图像 P，通过公式(8)计算每行约瑟夫遍历的步长，实施自适应行置乱，如公式(13)所示，得到置乱图像 P_1。

$$P_1\left(i,[1,2,\cdots,N]\right) = P\left(i, ysf\left(N, l_i\right)\right),\ i=1,2,\cdots,M. \tag{13}$$

Step 3. 对于置乱图像 P_1，通过公式(9)计算每列约瑟夫遍历的步长，实施自适应列置乱，如公式(14)所示，得到置乱图像 P_2。

$$P_2\left([1,2,\cdots,M], j\right) = P_1\left(ysf\left(M, l_j\right), j\right),\ j=1,2,\cdots,N \tag{14}$$

Step 4. 通过更新的密钥值和插值数据集，计算伴随动力系统(5)，得到序列值，并转换为五个 $M\times N$ 的矩阵 S,A,B,C,D，如公式(10)所示。

Step 5. 对置乱图像 P_2，对混沌密钥矩阵 S 的每行数据进行排序，得到地址变换码，如公式(15)所示，$i=1,2,\cdots,M$，$\mathrm{sort}(\,)$ 为排序函数，得到图像 P_3。

$$\begin{aligned}&[\sim,\mathrm{index1}]=\mathrm{sort}\left(S(i,:)\right),\\&P_3\left(i,[1,2,\cdots,N]\right)=P_2\left(i,\mathrm{index1}\right).\end{aligned}\tag{15}$$

Step 6. 对置乱图像 P_3，对 S 的每列排序，得到索引地址，如公式(16)所示，$j=1,2,\cdots,N$，得到图像 R。

$$\begin{aligned}&[\sim,\mathrm{index2}]=\mathrm{sort}\left(S(:,j)\right),\\&R\left([1,2,\cdots,M],j\right)=P_3\left(\mathrm{index2},j\right).\end{aligned}\tag{16}$$

Step 7. 利用矩阵 A,B 对置乱图像 R 进行双向行按位扩散得到扩散图像 U，行按位扩散过程如公式(17)~(18)所示。

正向扩散操作中，对于 $i=1,2,\cdots,M$，

$$\begin{cases}U_1(i,j)=\mathrm{mod}\left(R(i,j)+A(i,j)+R(i,j+1),256\right),j=1,2,\cdots,N-1,\\U_1(i,N)=\mathrm{mod}\left(R(i,N)+A(i,N)+255,256\right).\end{cases}\tag{17}$$

反向扩散操作中，对于 $i=M,M-1,\cdots,1$，

$$\begin{cases}U(i,j)=\mathrm{mod}\left(U_1(i,j)+B(i,j)+U_1(i,j-1),256\right),j=N,N-1,\cdots,2,\\U(i,1)=\mathrm{mod}\left(U_1(i,1)+B(i,1)+255,256\right).\end{cases}\tag{18}$$

Step 8. 利用矩阵 C,D 对图像 U 进行双向列按位扩散得到密文图像 T，列按位扩散过程如公式(19)~(20)所示。

正向扩散操作中，对于 $j=1,2,\cdots,N$，

$$\begin{cases}T_1(i,j)=\mathrm{mod}\left(U(i,j)+C(i,j)+U(i+1,j),256\right),i=1,2,\cdots,M-1,\\T_1(M,j)=\mathrm{mod}\left(U(M,j)+C(M,j)+255,256\right).\end{cases}\tag{19}$$

反向扩散操作中，对于 $j=N,N-1,\cdots,1$，

$$\begin{cases}T(i,j)=\mathrm{mod}\left(T_1(i,j)+D(i,j)+U_1(i-1,j),256\right),i=M,M-1,\cdots,2,\\T(1,j)=\mathrm{mod}\left(T_1(1,j)+D(1,j)+255,256\right).\end{cases}\tag{20}$$

加密算法完成，算法的解密过程为加密的逆过程，可以无失真解密。

3.3. 加密结果

依次读入明文图像 Lena、Baboon、Peppers，设定系统外部密钥为 $z_0=0.22,w_0=0.57$，系统参量为 $d=[0.81,0.84,0.76,0.69];p=[0.52,0.27,0.93,0.16];t=[0.44,0.39,0.67,0.83]$，经过加密和解密操作后生成的图像由图 7 所示，其中(a)~(c)为明文图像，(d)~(f)为密文图像，(g)~(i)为还原后的图像。

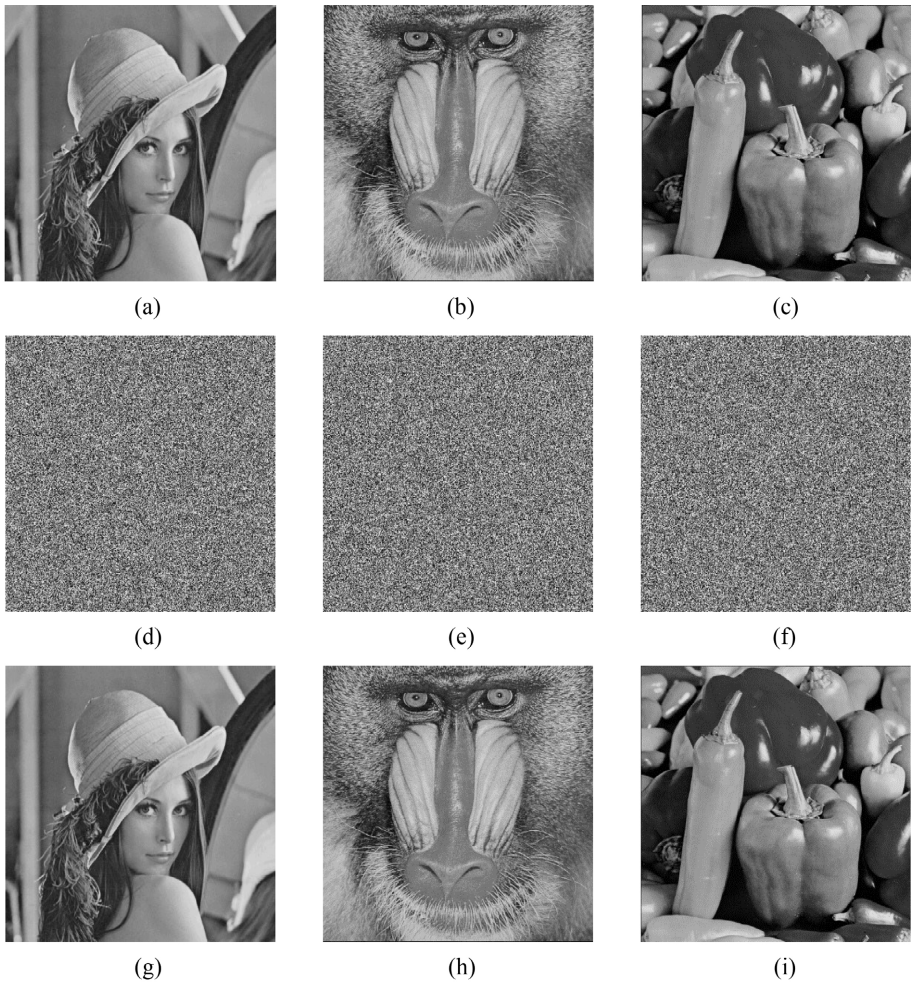

Figure 7. Experimental results of image encryption
图 7. 图像加密实验结果

4. 性能分析

4.1. 密文统计特性

直方图分析是一种统计方法，用于评估图像加密算法的直方图统计性能。在图像加密中，直方图显示了图像中每个灰度值的概率分布。一个理想的加密算法应该使得密文图像的直方图均匀分布，没有明显的模式或规律，这样才能够抵抗统计分析攻击。针对本文所提出的图像加密系统，绘制 Lena、Baboon 和 Peppers 明文图像以及密文图像的直方图，结果如图 8 所示。根据图 8 所示，直观上密文图像具有均匀的直方图，而明文图像的直方图跌宕起伏，进一步使用 χ^2 检验(单边假设检验)在数量上衡量两者的差别。给定一幅图像样本，其频数分布为 $f_i, i=1,\cdots,n$。若理论频数分布为 $g_i, i=1,\cdots,n$，作假设 H_0：样本来自理论分布。当假设 H_0 成立时，χ^2 统计量 $\chi^2=\sum_{i=1}^{n}\frac{(f_i-g_i)^2}{g_i}$ 服从自由度为 $n-1$ 的 χ^2 分布。

对于图像大小为 $M\times N$ 的 8 比特灰度图像而言，假设其直方图中像素灰度值的频数 f_i，而理论分布为 $g_i=g=MN/256, i=0,\cdots,255$。给定显著性水平 α，使得 $P\{\chi^2\geq\chi_\alpha^2(n-1)\}=\alpha$，即 $\chi^2<\chi_\alpha^2(n-1)$ 时接收假设 H_0。取显著性水平 α 为 0.01，0.05，0.1 时，$\chi_{0.01}^2(255)=310.457$，$\chi_{0.05}^2(255)=293.247$，

$\chi^2_{0.1}(255)=284.335$。计算 Lena，Baboon 和 Peppers 明文图像以及密文图像的 χ^2 统计量值，结果如表 2 所示。

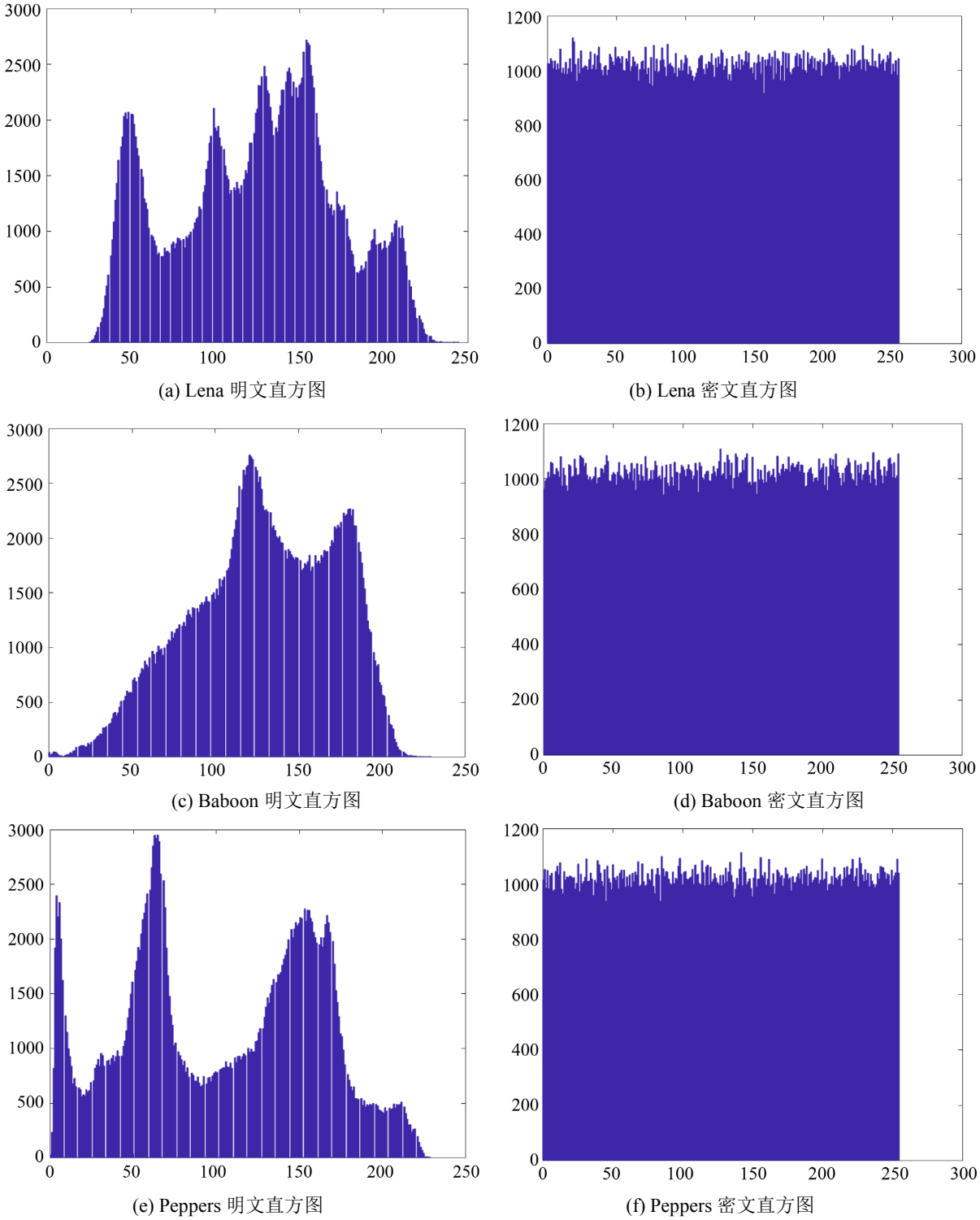

Figure 8. Histogram analysis of plaintext and ciphertext images
图 8. 明文图像和密文图像的直方图分析

Table 2. Chi square test results
表 2. 卡方检验结果

图像	Lena	Baboon	Peppers
明文	1.58024×10^5	1.87598×10^5	1.38836×10^5
密文	237.6465	270.8125	273.6191

由表 2 得知，3 个明文图像的 χ^2 统计量的数值明显大于 $\chi_\alpha^2(255)$，而对应的密文图像的 χ^2 统计量的计算值小于 $\chi_\alpha^2(255), \alpha = 0.01, 0.05, 0.1$，可认为在这 3 种显著水平下，3 个密文图像的直方图均近似均匀分布。除了图像直方图外，还需要考察密文图像的相邻像素的相关性。一般的，明文图像在水平、垂直、正对角和反对角方向上的相邻像素点间均具有较强的相关性，而密文图像的相邻像素点间应具有很弱的相关性。假设从考察的图像中任意选取 6000 对相邻的像素点，记其灰度值为 $(u_i, v_i), i = 1, \cdots, N$，则向量 $u = \{u_i\}$ 和向量 $v = \{v_i\}$ 间的相关系数 r_{xy} 可通过公式(21)~(22)计算，计算明文图像和密文图像的相关系数见表 3。由表 3 可知，明文图像相邻像素的相关性较强，而密文图像相邻像素的相关性接近于 0，近似无相关性。

$$r_{xy} = \frac{cov(u,v)}{\sqrt{D(u)}\sqrt{D(v)}},\ cov(u,v) = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - E(u)\right)\left(y_i - E(v)\right) \tag{21}$$

$$D(u) = \frac{1}{N}\sum_{i=1}^{N}\left(u_i - E(u)\right)^2,\ E(u) = \frac{1}{N}\sum_{i=1}^{N}u_i. \tag{22}$$

Table 3. Correlation coefficient between adjacent pixels of plaintext image and ciphertext image
表 3. 明文图像和密文图像的相邻像素的相关系数

图像	水平	垂直	正对角	反对角
Lena 明文	0.987950	0.970747	0.967985	0.968091
Lena 密文	−0.007119	−0.002071	0.018741	−0.013085
Baboon 明文	0.752005	0.864266	0.733154	0.725095
Baboon 密文	0.004918	−0.001829	−0.002690	−0.006558
Peppers 明文	0.982332	0.976975	0.971109	0.967218
Peppers 密文	−0.005856	−0.001264	−0.002762	0.008542

4.2. 密钥敏感性

密钥敏感性衡量加密算法对密钥变化的敏感程度。在图像加密中，理想的加密算法应该对密钥非常敏感，以确保安全性。密钥敏感性的评估通常使用像素数变化率(NPCR)、统一平均变化强度(UACI)和块平均变化强度(BACI)三个参数来衡量。NPCR 表示两幅加密图像之间变化像素数的比例，UACI 表示两幅加密图像之间平均变化强度的度量，而 BACI 表示两幅加密图像之间每个小图像块中平均变化强度的度量，其计算方式可参考文献[1]。NPCR、UACI 和 BACI 的理论期望值分别为 99.6094%、33.4635%和 26.7712%。现以大小为 512 × 512 的 Lena、Baboon 和 Peppers 灰度图像为例，对本文的加密方法进行密钥敏感性的分析。对已知的外部密钥 z_0 改变 10^{-16}，d_1, p_1, t_1 改变 10^{-16}，分别计算同一明文图像加密之后的密文图像对应的 NPCR、UACI 和 BACI，结果如表 4 所示，可以看出 NPCR、UACI 和 BACI 的测试值均接近理论期望值，表明本文提出的算法具有良好的密钥敏感性。

Table 4. Sensitivity analysis results when the key change amount is 10^{-16}
表 4. 密钥改变量为 10^{-16} 时敏感性分析结果

指标		Lena (%)	Baboon (%)	Peppers (%)	理论值(%)
z_0	NPCR	99.6094	99.6109	99.6166	99.6094
	UACI	33.4803	33.4332	33.4404	33.4635
	BACI	26.7742	26.7853	26.7240	26.7712
d_1	NPCR	99.6147	99.5975	99.6105	99.6094
	UACI	33.5587	33.5084	33.5034	33.4635
	BACI	26.8245	26.7588	26.7766	26.7712
p_1	NPCR	99.5911	99.6071	99.6101	99.6094
	UACI	33.5180	33.4949	33.4827	33.4635
	BACI	26.8086	26.8084	26.7685	26.7712
t_1	NPCR	99.6117	99.6052	99.6181	99.6094
	UACI	33.4383	33.5206	33.4908	33.4635
	BACI	26.8400	26.7996	26.8487	26.7712

4.3. 密钥空间

密钥空间是指所有合法的密钥构成的集合。图像密钥系统的密钥空间应该足够大，从而可以有效地对抗穷举攻击，密钥长度应该至少为$128b$。本文所提出的加密算法的密钥为z_0, d, p, t，其中z_0是 0 到 1 之间的实数值，而d, p, t均有 4 个分量。根据 4.2 节的密钥敏感性分析得出，其中密钥z_0的最小改变量为10^{-16}，密钥d, p, t每个分量的最小改变量为10^{-16}，因此本文所提出算法的密钥空间的大小为$\log_2\left(10^{16}\times\left(10^{16}\right)^4\times\left(10^{16}\right)^4\times\left(10^{16}\right)^4\right)=\log_2\left(10^{208}\right)\approx 691b$，远大于$128b$，所以本文所提出的图像加密算法能有效地抵抗暴力攻击。

4.4. 明文敏感性

明文敏感性分析是指使用同一密钥加密差别微小的两个明文图像，得到两个相应的密文图像，比较这两个密文图像的差别。如果这两个密文图像的差别较大，则称该图像密码系统具有较好的明文敏感性。现在以大小为 512 × 512 的 Lena、Baboon 和 Peppers 灰度图像为例，对本文的加密方法进行明文敏感性的分析，对明文图像进行加密得到密文图像 1，并随机选取明文图像的 1 个像素点，改变该像素点值，变换量为 1，使用同一密钥对其进行加密得到密文图像 2，计算密文图像 1 和密文图像 2 的 NPCR、UACI 和 BACI，实验结果如表 5 所示。可以看出 NPCR、UACI 和 BACI 的测试值均接近理论期望值，表明本文提出的算法具有良好的明文敏感性，可以有效地抵抗差分攻击。即使攻击者知道某些明文－密文对，由于本算法明文敏感性强导致相似明文的密文无规律可循，难以通过插值或外推破解其他密文。并且明文敏感性使得攻击者无法通过精心构造的明文序列获取密钥的统计特征。因此该加密算法也能够有效地抵抗已知明文攻击和选择明文攻击。

Table 5. Plaintext sensitivity analysis results
表 5. 明文敏感性分析结果

指标	Lena (%)	Baboon (%)	Peppers (%)	理论值(%)
NPCR	99.6095	99.6142	99.5998	99.6094
UACI	33.4917	33.4832	33.4071	33.4635
BACI	26.8011	26.7792	26.7743	26.7712

4.5. 密文敏感性

密文敏感性分析旨在分析密文图像发生微小变化时，解密还原的图像与原始明文图像的差别。如果这两个明文图像的差别较大，则称该图像密码系统具有较好的密文敏感性。以大小为 512 × 512 的 Lena、Baboon 和 Peppers 灰度图像为例，对本文的加密方法进行密文敏感性的分析，对明文图像进行加密得到密文图像 1，并随机选取密文图像 1 的 1 个像素点，改变该像素点值，变换量为 1，使用同一密钥对其进行解密得到明文图像 2，计算明文图像 1 和明文图像 2 的 NPCR、UACI 和 BACI，实验结果如表 6 所示。可以看出 NPCR、UACI 和 BACI 的测试值均接近理论期望值，表明本文提出的算法具有良好的密文敏感性，可以有效地抵抗选择密文攻击。

Table 6. Ciphertext sensitivity analysis results
表 6. 密文敏感性分析结果

指标	Lena		Baboon		Peppers	
	测试值/%	理论值/%	测试值/%	理论值/%	测试值/%	理论值/%
NPCR	99.6136	99.6094	99.6214	99.6094	99.6152	99.6094
UACI	28.8875	28.6237	28.2534	27.8429	30.9176	30.9762
BACI	21.0134	21.3216	20.1898	20.6225	23.1317	23.2168

4.6. 信息熵

信息熵反映了图像信息的不确定性，一般地认为，信息熵越大，不确定越大，图像包含的信息量越大，可视信息越少。对于 $L=256$ 的灰度随机图像，信息熵 H 具有最大值 8。图像的信息熵计算公式为 $H=-\sum_{i=0}^{L-1} p_i \log_2 p_i$，其中 L 表示图像的灰度值级数，p_i 表示灰度值 i 的频率。分别计算明文图像 Lena、Baboon 和 Peppers 灰度图像及其相应密文图像的信息熵，结果列于表 7，可以看出密文图像的信息熵均非常接近随机图像的最大信息熵 8，意味着密文的随机性和不确定性高，加密系统的安全性较高，可以有效地抵抗信息熵的密码分析攻击。

Table 7. Experimental results of information entropy
表 7. 信息熵实验结果

Lena 明文	Lena 密文	Baboon 明文	Baboon 密文	Peppers 明文	Peppers 密文
7.445568	7.999308	7.357949	7.999283	7.571478	7.999353

4.7. 性能对比

以大小 256 × 256 和 512 × 512 的 Lena 图像为例，对比本文算法和参考文献中 4 种算法得到的密文图像性能结果，如表 8 和表 9 所示。从结果可看出，本文算法所得性能总体上优于文献的算法所得结果。

4.8. 加密和解密速度

使用一台配置 AMD 锐龙 5-3550H、16G 内存的笔记本电脑用 MATLAB R2017a 语言实施本文的加密算法。测试图像大小为 256 × 256，用不同的密钥加密明文图像 100 次，记录每次加密耗时，然后取平均值，加密的平均速度为 0.5139 s，而相应的解密平均速度为 0.4870 s。这说明算法具有较快的加密及解密速度，可适用于实际通信环境。

Table 8. Comparison of cipher performance results for Lena images with a Size of 256 × 256
表 8. 大小为 256 × 256 的 Lena 图像密文性能结果对比

算法	NPCR (%)	UACI (%)	信息熵	相关系数		
				水平	垂直	正对角
本文	99.604691	33.491189	7.997226	0.008314	0.000056	−0.017331
文献[4]	99.612366	33.477064	7.997479	−0.026234	−0.009887	−0.006287
文献[8]	99.610474	33.798463	7.603058	0.023834	−0.012035	−0.005798
文献[15]	99.612656	33.475881	7.997125	−0.003917	−0.003496	−0.019516
文献[17]	99.608459	33.486934	7.997075	−0.017735	0.020275	0.004567

Table 9. Comparison of cipher performance results for Lena images with a Size of 512 × 512
表 9. 大小为 512 × 512 的 Lena 图像密文性能结果对比

算法	NPCR (%)	UACI (%)	信息熵	相关系数		
				水平	垂直	正对角
本文	99.609665	33.478715	7.999308	−0.002652	−0.008136	−0.003647
文献[4]	99.608021	33.459501	7.999267	0.021702	0.026257	0.031013
文献[8]	99.610535	33.469607	7.491935	−0.002245	0.009089	0.006437
文献[15]	99.608170	33.465217	7.999322	−0.009831	0.010076	0.007293
文献[17]	99.609688	33.456008	7.999185	−0.001069	−0.012652	−0.009815

5. 结论

本文提出一个二次定比分形插值函数模型，由其逆运算构造了一个新的分形动力系统，并且从数值上分析验证了该动力系统具有优良的混沌特性。由该分形混沌系统生成性能优良的随机序列通过了SP800 随机数检测，基于该随机序列设计了一个新的图像加密算法。该算法包括两个阶段，第一阶段利用明文图像的像素灰度值进行一轮自适应的基于约瑟夫遍历的行列置乱，并由分形动力系统生成的随机序列进行第二轮的基于排序的行列置乱。第二阶段基于分形动力系统产生的随机序列分别对图像行列进行按位加取模的扩散操作，该操作进行正向和反向两次扩散，最终得到密文图像。实验结果表明，该算法具有够大的密钥空间，优良的密钥敏感性、明文敏感性和密文敏感性，密文图像也具有优良的统计性能，可以有效抵抗蛮力攻击，差分攻击，选择密文攻击和明文攻击，具有优良的安全性能，而且计算速度较快。该模型所诱导的分形动力系统在某些参数区域只有一个 Lyapunov 指数为正，在这些参数范围中，系统不具有超混沌性质，如何构造在所有参数的可选范围内具有超混沌性质的分形插值模型是一个值得进一步研究的课题，希望在以后的研究中可以解决这一问题。

基金项目

广东省基础与应用基础研究基金(No. 2023A1515030199)资助项目。

参考文献

[1] 张勇. 混沌数字图像加密[M]. 北京: 清华大学出版社, 2016.

[2] Matthews, R. (1989) On the Derivation of a “Chaotic” Encryption Algorithm. *Cryptologia*, **13**, 29-42. https://doi.org/10.1080/0161-118991863745

[3] Fridrich, J. (1998) Symmetric Ciphers Based on Two-Dimensional Chaotic Maps. *International Journal of Bifurcation and Chaos*, **8**, 1259-1284. https://doi.org/10.1142/s021812749800098x

[4] 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.

[5] 叶瑞松, 庄乐仪. 基于帐篷映射迭路的置乱方法[J]. 计算机应用, 2009, 29(10): 2713-2715.

[6] 叶瑞松, 庄乐仪. 基于 Baker 映射迭路的图像加密算法[J]. 汕头大学学报: 自然科学版, 2010, 25(1): 54-60.

[7] 黄佳鑫, 赵凯悦, 李佳文, 等. 基于 Logistic-Sine-Cosine 映射的图像加密算法[J]. 科学技术与工程, 2023, 23(27): 11713-11721.

[8] Hu, G. and Li, B. (2021) Coupling Chaotic System Based on Unit Transform and Its Applications in Image Encryption. *Signal Processing*, **178**, Article 107790. https://doi.org/10.1016/j.sigpro.2020.107790

[9] 曾祥秋, 叶瑞松. 基于改进 Logistic 映射的混沌图像加密算法[J]. 计算机工程, 2021, 47(11): 158-165+174.

[10] Alawida, M., Samsudin, A. and Teh, J.S. (2020) Enhanced Digital Chaotic Maps Based on Bit Reversal with Applications in Random Bit Generators. *Information Sciences*, **512**, 1155-1169. https://doi.org/10.1016/j.ins.2019.10.055

[11] Sharma, M., Ranjan, R.K. and Bharti, V. (2022) A Pseudo-Random Bit Generator Based on Chaotic Maps Enhanced with a Bit-XOR Operation. *Journal of Information Security and Applications*, **69**, Article 103299. https://doi.org/10.1016/j.jisa.2022.103299

[12] Zheng, J. and Hu, H. (2022) Bit Cyclic Shift Method to Reinforce Digital Chaotic Maps and Its Application in Pseudorandom Number Generator. *Applied Mathematics and Computation*, **420**, Article 126788. https://doi.org/10.1016/j.amc.2021.126788

[13] Zhang, Y. (2014) Plaintext Related Image Encryption Scheme Using Chaotic Map. *TELKOMNIKA Indonesian Journal of Electrical Engineering*, **12**, 635-643.

[14] 丁玮, 闫伟齐, 齐东旭. 基于 Arnold 变换的数字图像置乱技术[J]. 计算机辅助设计与图形学学报, 2001, 13(4): 338-341.

[15] 洪炎, 王艺杭, 苏静明, 等. 基于行列异或的 Arnold 双置乱图像加密方法[J]. 科学技术与工程, 2024, 24(2): 649-657.

[16] Azimi, Z. and Ahadpour, S. (2019) Color Image Encryption Based on DNA Encoding and Pair Coupled Chaotic Maps. *Multimedia Tools and Applications*, **79**, 1727-1744. https://doi.org/10.1007/s11042-019-08375-6

[17] 牛莹, 张勋才. 基于变步长约瑟夫遍历和 DNA 动态编码的图像加密算法[J]. 电子与信息学报, 2020, 42(6): 1383-1391.

[18] 尹思文, 刘云皓, 周磊超. 基于 Lorenz 超混沌系统和 DNA 计算的三维图像加密算法[J]. 中国新技术新产品, 2024(3): 1-5.

[19] 孙鹤鹏, 张晓强. 基于 DNA 编码的多图像加密算法[J]. 计算机工程与设计, 2018, 39(10): 3050-3054+3099.

[20] 陈颙, 陈凌. 分形几何学[M]. 北京: 地震出版社, 2005.

[21] 叶瑞松, 陈月明. 一个迭代函数系统的分形混沌特性及其应用[J]. 汕头大学学报: 自然科学版, 2023, 38(2): 3-30.

[22] 高曼钰, 叶瑞松. 基于分形混沌系统的多图像加密算法[J]. 计算机科学与应用, 2024, 14(4): 83-104.

[23] Ye, R., Lan, H. and Wu, Q. (2018) A Fractal Interpolation Based Image Encryption Scheme. 2018 *IEEE International Conference on Computer and Communication Engineering Technology* (*CCET*), Beijing, 18-20 August 2018, 291-295. https://doi.org/10.1109/ccet.2018.8542341

[24] Ye, R., Li, Y. and Li, Y. (2018) An Image Encryption Scheme Based on Fractal Interpolation. *Proceedings of the* 3*rd International Conference on Multimedia and Image Processing*, Guiyang, 16-18 March 2018, 52-56. https://doi.org/10.1145/3195588.3195596