Computer Science and Application 计算机科学与应用, 2024, 14(4), 83-104
Published Online April 2024 in Hans. https://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2024.144080

Hans汉斯

基于分形混沌系统的多图像加密算法

高曼钰，叶瑞松*

汕头大学数学系，广东 汕头

收稿日期：2024年3月5日；录用日期：2024年4月5日；发布日期：2024年4月16日

摘　要

构造了一个迭代函数系统，生成充满整个单位正方形的填充曲线。由迭代函数系统生成一个单位正方形上的分形混沌系统，并从混沌系统的轨迹、李亚普诺夫指数和0~1测试等方面验证了该系统具有优良的混沌性能。基于构造的二维分形混沌系统，提出了密钥相关的Z字形变换，并结合自适应Arnold变换和有限域运算设计了一个针对多个灰度图像的混沌图像加密算法，详细分析了该加密算法的安全性。

关键词

迭代函数系统，分形，混沌，填充曲线，Z字形变换，多图像加密

Multi-Image Encryption Algorithm Based on Fractal Chaotic System

Manyu Gao, Ruisong Ye*

Department of Mathematics, Shantou University, Shantou Guangdong

Received: Mar. 5th, 2024; accepted: Apr. 5th, 2024; published: Apr. 16th, 2024

Abstract

An iterated function system is constructed to generate the filling curve on the unit square. One fractal chaotic system is derived by the iterated function system on the unit square. The chaotic natures of the fractal chaotic system are proved by the orbits, the Lyapunov exponents and 0~1 test, etc. Based on the constructed two-dimensional chaotic system, a chaotic image encryption algorithm for multiple gray images is designed by key-determined zigzag transformation, Arnold transformation and finite field operations. The security and performance of the proposed image encryption algorithm is analyzed in detail.

*通讯作者。

文章引用: 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): 83-105.
DOI: 10.12677/csa.2024.144080

Keywords

Iterated Function System, Fractal, Chaos, Filling Curve, Zigzag Transformation, Multi-Image Encryption

1. 引言

随着科学技术的不断进步，多媒体的信息安全已经成为人们越来越关心的问题，其中图像信息作为一种具有显著信息的载体，在军事、医学、教育和商业等方面具有广泛应用。所以图像加密已经成为信息安全领域的研究热点。由于图像信息的数据量大，冗余度高和相邻像素相关性强等特点，因此传统的加密方法如 AES、DES 等不适合数字图像的加密。因为混沌系统具有对初始值的敏感性、遍历性和随机性的特性，1989 年 R. Matthews 提出了用混沌序列生成伪随机数用于数据加密。1998 年，Fridrich 提出了一种基于混沌的图像加密体系结构，利用混沌序列生成伪随机数，主要框架为置乱和扩散的数字图像加密方法被广泛利用在数字图像加密领域中[1]。

常用于图像加密的一维混沌系统有 Logistic 映射、Sine 映射和 Tent 映射等，它们结构简单，易于实现[2]。但是由于计算设备精度有限，截断和舍入误差会使混沌系统陷入周期态，所以密码学家在一维混沌映射的基础上，提出了许多复合型的混沌系统。文献[3]提出了改进的 Logistic-Tent 混沌系统，文献[4]提出了复合的 Logistic-Sine 混沌系统，比原映射有更好的随机性和遍历性。文献[5]提出一个新的正弦－幂函数混沌系统，映射具有更长的周期窗口，更好的混沌特性。此外，高维 Liu 系统和 Lorenz 系统等也常常被用作图像加密[6] [7]。高维的混沌系统比起低维的混沌系统具有更大的密钥空间，用于加密时更不容易被暴力破解。但常常运算量大，耗时长，难以复现[8]。二维的混沌系统相较传统的低维系统安全性能更好，运算耗时和实现难度又优于高维系统，是密码学家用来图像加密的高效选择。文献[9]构造了一个具有大混沌范围的二维 Logistic-Gaussian 超混沌映射；文献[10]提出了一种新的二维正弦混沌系统，实验结果表明该系统比传统的系统具有更大的参数空间。

分形几何学用数学公式描述自然界中混沌、无序的复杂事物，使得分形与混沌之间有着紧密的天然联系。1890 年科学家 Peano 发现可以使用迭代函数系统(IFS)生成能够充满平面的曲线(填充曲线) [11]，这样的迭代函数系统在单位正方形内存在唯一的吸引子，由于 IFS 的压缩性，可以诱导得到分形吸引子上具有混沌特性的动力系统。本文对[12]的分形混沌系统进行改进，提出了一个二维三参数的分形混沌系统，给出了分形的迭代函数系统，并生成单位正方形的填充曲线。本文时序图，李雅普诺夫指数图和 0~1 测试等方面分析了该分形混沌系统的混沌特性。所提出的新分形混沌系统与低维系统相比具有更好的动力学特性，并且拥有运算速度快的优点；生成的混沌序列具有更好的遍历性和初值敏感性，适合生成用于图像加密的混沌序列。

置乱操作是通过打乱数字图像矩阵像素点的位置，实现图像的加密。矩阵置乱方法是直接用相应大小的矩阵，对图像数字矩阵位置进行变换。因为像素位置是整数，所以要求变换的矩阵的值是整数。著名的 Arnold 矩阵是整数矩阵且逆矩阵仍然是整数矩阵，一般应用在混沌加密中，相较于其他置乱方法来说，其置乱效果较好[13]。文献[14]将 Arnold 矩阵推广到高维情况；文献[15]分析了图像尺寸和 Arnold

变换周期的关系，为了改进周期性，提出了一种利用高维的 Arnold 变换加密彩色图像的置乱算法；文献[16]提出了一种基于 Arnold 的加密算法，在变换过程中加入密钥用来加密彩色图像；文献[17]运用三维 Arnold 映射结合混沌序列的算法对图像进行加密，算法取得了较好的加密效果。本文在[18]自适应图像加密算法的基础上，将分块之后的图像经过 Arnold 变换，结合与混沌序列的运算，以扩散的形式混淆每块图像的像素值，在有限次的变换后实现良好的加密效果。基于异或加法模运算和 Arnold 变换的扰乱和图像的明文相关，具有自适应性。

Zigzag 变换方法是用 Z 字形的扫描办法扫描想要加密的图像矩阵，然后按照顺序放入新矩阵，即加密后的矩阵，是一种像素级的置乱方法。因为 Z 形扫描方法容易实现，加密效果好，所以被广泛使用。文献[19]使用随机置乱和 Zigzag 形置乱方法加密图像；文献[20]提出了四个不同方向的 Zigzag 扫描算法；文献[21]基于神经网络算法，提出任意起点的 Z 字形扫描方式；文献[22]将传统算法改进，提出了三维的 Zigzag 扫描方法，周期性更大，安全性更好。本文提出了适用于任何大小矩阵的 Zigzag 型扫描，在加密多个灰度图像的算法中，使用明文图像 Hash 函数生成的密钥决定了每幅图像 Zigzag 型变换的起点和终点，使算法具有更好的明文敏感性和随机性。

扩散算法是在不改变像素位置的基础上，改变像素值的大小，使用有限域实现图像加密算法的扩散，是安全又高效的选择。基于有限域上的多项式运算，其运算规律和结构，生成的有限域上的四则运算表在模运算的结果下，个数有限，大小有限制，所以其在计算机科学与信息理论方面都有较为广泛的应用[23]。在有限域理论中 GF(257)的算术运算以 257 为模，此集合共包含 257 个元素。在乘法运算时，剔除元素 0 以减少因其造成的信息损失，这时集合中元素的个数为 256，正好与图像像素点灰度值的取值范围对应[24]。文献[25]构造了 GF(2^8)的加法、减法表，扩散加密图像；文献[26]构造了 GF(257)的乘法表，与混沌序列结合实现图像的扩散；本文构造了 GF(257)的乘法、除法表和加法、减法表，在查表法的基础上，对多个灰度图像合成的大图像进行扩散。利用构造的分形迭代系统生成的混沌序列，将明文信息扩散加密，加密速度和效果良好。

本文算法包含三点创新性：(1) 构造了一个二维三参数的基于迭代函数系统的分形混沌系统，该系统具有优良的混沌性能；(2) 设计了 Arnold 变换相关的自适应性加密方法；(3) 提出了一个由密钥决定的 Zigzag 扫描方法，加密方法具有很好的明文相关性；(4) 算法使用三个阶段的混淆、置乱和扩散构成，适用于由任意大小组成的多个灰度图像的加密，加密效果和加密速度优良。本文的剩余部分安排如下：第二节构造了一个基于迭代函数系统的动力系统，并从数值上验证其混沌性能；第三节提出一个基于所构造的分形混沌系统的多图像的加密算法；第四节仿真实验验证了算法的性能；第五节为结语。

2. 单位正方型上的迭代函数系统及其分形混沌系统

2.1. 迭代函数系统

给定参数 $0<a,b,c<1$，考虑下面的迭代函数系统 IFS $\{R^2;w_1,w_2,w_3,w_4\}$：

$$w_1\begin{pmatrix}x\\y\end{pmatrix}=\begin{pmatrix}0 & a\\ b & 0\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix};\quad w_2\begin{pmatrix}x\\y\end{pmatrix}=\begin{pmatrix}c & 0\\ 0 & 1-b\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}+\begin{pmatrix}0\\b\end{pmatrix};$$

$$w_3\begin{pmatrix}x\\y\end{pmatrix}=\begin{pmatrix}1-c & 0\\ 0 & 1-b\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}+\begin{pmatrix}c\\b\end{pmatrix};w_4\begin{pmatrix}x\\y\end{pmatrix}=\begin{pmatrix}0 & -(1-a)\\ -b & 0\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}+\begin{pmatrix}1\\b\end{pmatrix} \tag{1}$$

由于 $0<a,b,c<1$，IFS(1)是一个压缩的迭代函数系统，因此在 R^2 中有唯一的吸引子分形。由于单位正方形 $A=[0,1]^2$ 满足

$$W(A)=w_1(A)\cup w_2(A)\cup w_3(A)\cup w_4(A)=A$$

因此，IFS 的分形为单位正方形 A。用确定性算法，当选择不同的初始集合 B_0 进行迭代得到集合则有 $B_k = W^k(B_0), k = 0,1,2,\cdots$, 分形几何理论知道 $\lim_{k\to\infty} B_k = A$。图 1 为参数 (a,b,c) 取值为 $(0.5,0.5,0.5)$ 和 $(0.3,0.51,0.6)$ 迭代 6 次后得到的单位正方形内的填充曲线。可以看出曲线可以充满整个区域。

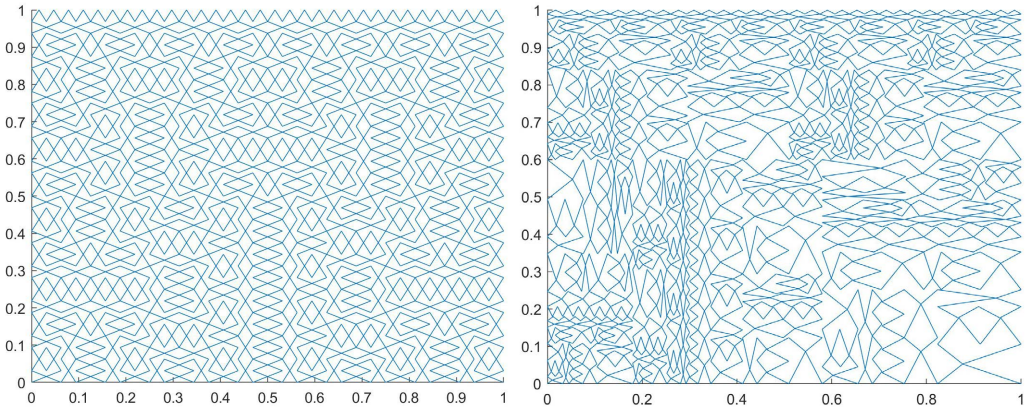


Figure 1. Filling curves generated by IFS (1)
图 1. IFS (1)生成的填充曲线

该迭代函数系统的分形 A 上有一个伴随的位移动力系统 $\{A;S\}$。$\{A;S\}$ 可以表示为公式(2)

$$S(x,y)=\begin{cases} w_1^{-1}(x,y),(x,y)\in w_1(G)\{(a,y):0\le y\le b\}, \\ w_2^{-1}(x,y),(x,y)\in w_2(G)\{(x,b):0\le x\le c\}, \\ w_3^{-1}(x,y),(x,y)\in w_3(G)\{(c,y):b\le y\le 1\}, \\ w_4^{-1}(x,y),(x,y)\in w_4(G)\{(x,b):a\le x\le 1\}. \end{cases} \tag{2}$$

分形几何理论表明 $S(A)=A$，A 是 S 的排斥吸引子，分形 A 上的动力系统 $\{G;S\}$ 具有混沌特性。推导得到定义在 A 上的动力系统 $S(x,y)$ 的具体形式如(3)所示：

$$S(x,y)\begin{cases} \left(\frac{x}{b},\frac{x}{a}\right),(x,y)\in[0,a)\times[0,b], \\ \left(\frac{x}{c},\frac{y-b}{1-b}\right),(x,y)\in[0,c]\times(b,1], \\ \left(\frac{x-c}{1-c},\frac{y-b}{1-b}\right),(x,y)\in(c,1]\times[b,1], \\ \left(\frac{b-y}{b},\frac{1-x}{1-a}\right),(x,y)\in\{[a,1]\times[0,b),(a,b)\}. \end{cases} \tag{3}$$

2.2. 性能分析

下面选定初始值 $x_0=0.313$， $y_0=0.519$，系统参数 $a=0.313$， $c=0.633$， $b=0.718$，迭代 10,000 次，产生序列 X，Y 分析分形混沌系统(3)在单位正方形的混沌特性。

2.2.1. 轨迹分析

在给定的初始值和参数下，分形动力系统迭代产生的轨迹图和序列 X，Y 的时序图如图 2 所示。可以看出系统迭代生成的点，随机且均匀的遍布在整个单位正方形内，因此提出的动力系统(3)在相空间内，具有良好的遍历性。

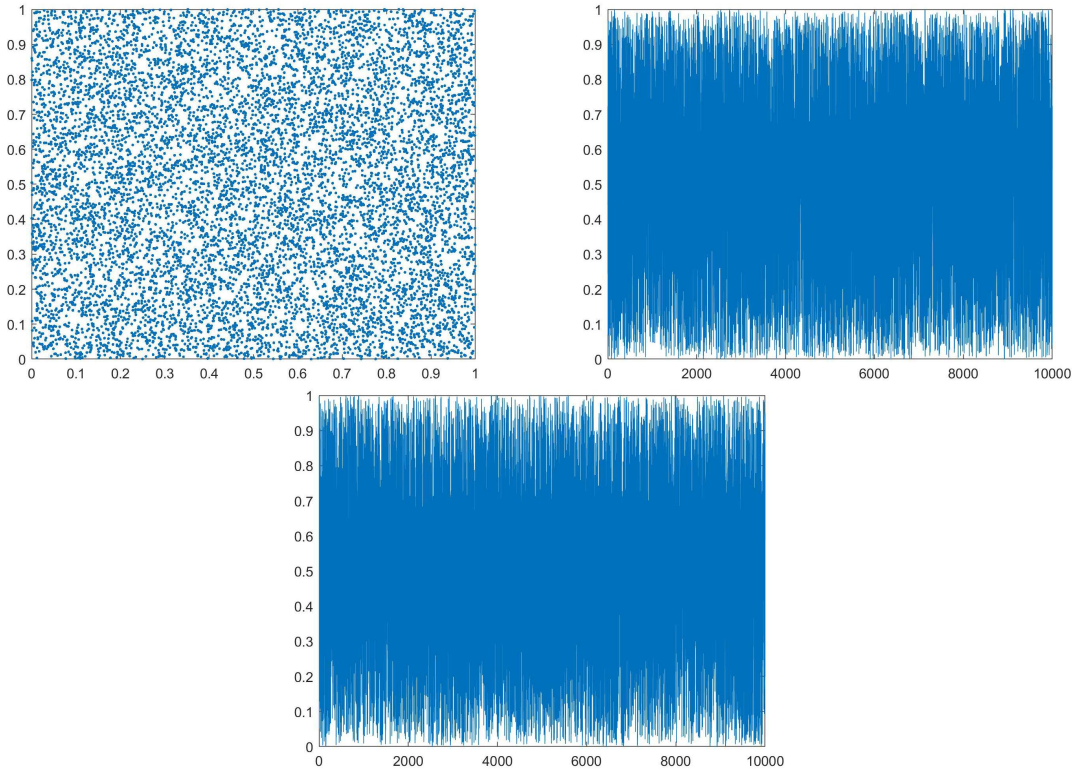


Figure 2. Chaotic orbit and time series diagram
图 2. 轨迹图和时序图

2.2.2. 分叉图

动力系统的分叉图是描述迭代序列随着参数选择的变化而变化的图像，分叉图可以直观地观察出生成序列的周期点或周期窗口，混沌序列的分叉图应该具有很好的随机性和遍历性，即具有较大的混沌参数范围。分别固定 b,c 的值，参数取值范围 $a\in(0,1)$，刻画序列 X,Y 随 a 的变换而变化的图像；固定 a,c 的值，参数取值范围 $b\in(0,1)$，刻画序列 X,Y 随 b 的变换而变化的图像；固定 a,b 的值，参数取值范围 $c\in(0,1)$，刻画序列 X,Y 随 c 的变换而变化的图像。所得结果如图 3 所示，可以看出分形混沌系统的混沌参数范围均是 $(0,1)$。

2.2.3. Lyapunov 指数

混沌的动力系统应该具有对初始值的敏感性，Lyapunov 指数可以衡量动力系统的初值敏感性，从而判断系统是否混沌。若一维的系统具有正的李雅普诺夫值，则认为系统是混沌的；n 维的系统具有 n 个 Lyapunov 指数值，若 n 维系统的正的最大李亚普诺夫指数值大于 0，则认为系统具有混沌特性，高维度的混沌系统具有超混沌性，一般来说，超混沌系统比一般的混沌系统具有更加复杂的动力学行为，在实际应用中更能满足加密信息的需求。下面探究当参数变换时，二维分形动力系统的 Lyapunov 指数变换，从而确定系统是否混沌，计算混沌范围。

对于二维混沌系统，

$$(x_i,y_i)=f^i(x_0,y_0) \tag{4}$$

(x_0,y_0) 是系统的初始值，i 表示迭代次数，$i=1,2,\cdots,n$。将 i 时刻系统 $f(x,y)$ 的 Jacobi 矩阵记为 J_i，迭代产生的 Jacobi 矩阵为 $J_n,J_{n-1},\cdots,J_1$，$Q_0=I$。对矩阵 $J_n,J_{n-1},\cdots,J_1$，进行 QR 分解：

$$\begin{aligned} qr\left[J_n, J_{n-1}, \cdots, J_1\right] &= qr\left[J_n, J_{n-1}, \cdots, \left(J_1 Q_0\right)\right] = qr\left[J_n, J_{n-1}, \cdots, \left(J_2 Q_1\right)\right]\left[R_1\right] \\ &= qr\left[J_n, J_{n-1}, \cdots, J_4\left(J_3 Q_2\right)\right]\left[R_2 R_1\right] \\ &= \cdots = qr\left[J_n, J_{n-1}, \cdots, J_{i+1}\left(J_i Q_{i-1}\right)\right]\left[R_{i-1} R_{i-2} \cdots R_2 R_1\right] \\ &= \cdots = Q_n\left[R_n \cdots R_2 R_1\right] = Q_n R \end{aligned}$$

其中 $qr[\cdot]$ 表示 QR 分解。从 J_1 开始，在第 i 步中，得到用 Q_{i-1} 右乘 J_i 得到 $B_i = J_i Q_{i-1}$，再做 QR 分解 $B_i = Q_i R_i$，$i = 1, 2, \cdots, n$。得到阶数为 2 × 2 的对角矩阵 $R = R_n \cdots R_2 R_1$，其对角线上的每一个元素是所有二阶矩阵 R_i 对角线上对应元素的乘积。

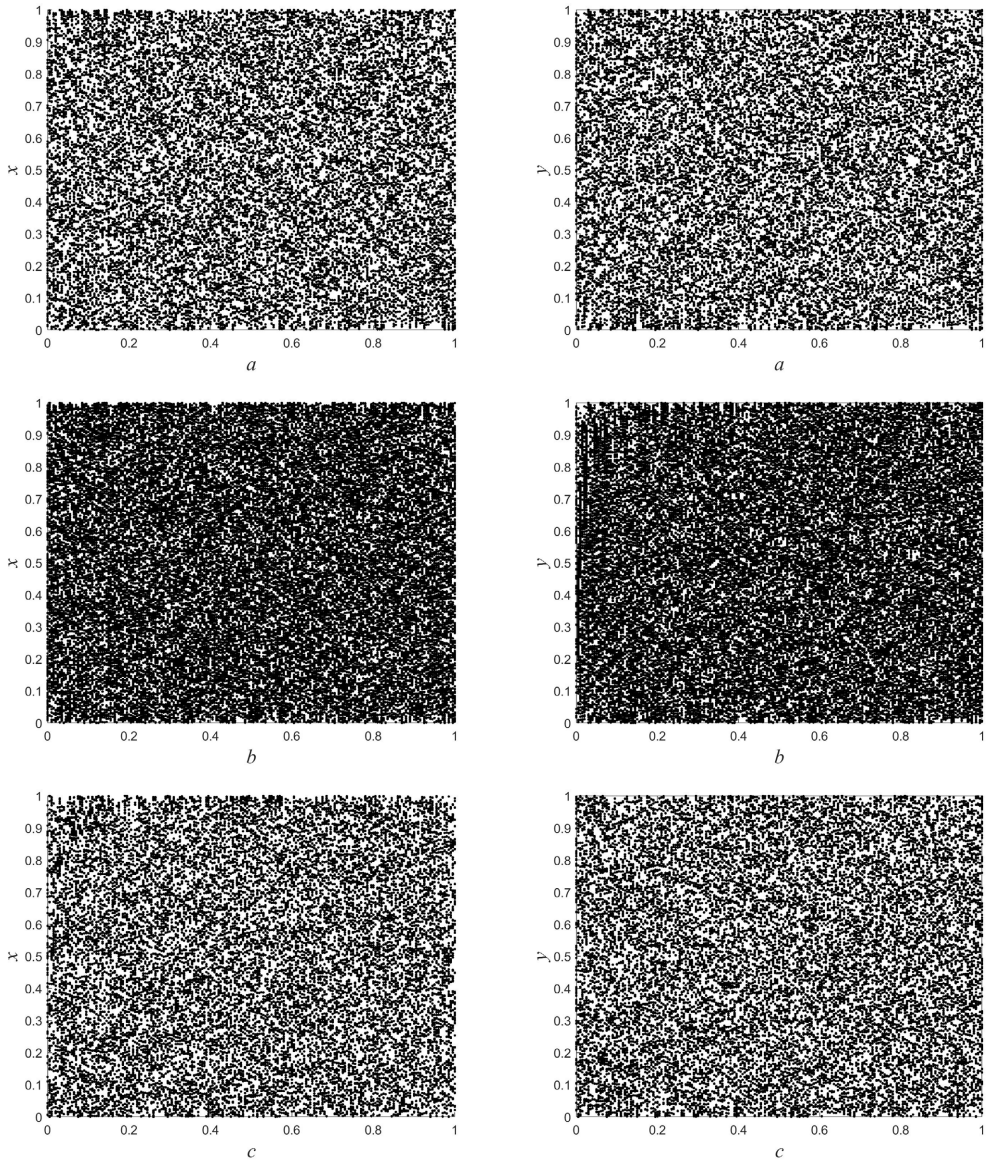


Figure 3. Bifurcation diagram
图 3. 分叉图

混沌系统 $f(x, y)$ 的两个 Lyapunov 指数可以近似计算得到：

$$\lambda_1 = \lim_{n\to\infty}\frac{1}{n}\sum_{i=1}^{n}\left|R(1,1)\right|, \lambda_2 = \lim_{n\to\infty}\frac{1}{n}\sum_{i=1}^{n}\left|R(2,2)\right| \tag{5}$$

分别固定 b,c 的值，参数取值范围 $a\in(0,1)$，刻画 Lyapunov 指数值随 a 的变换而变化的图像；固定 a,c 的值，参数取值范围 $b\in(0,1)$，刻画 Lyapunov 指数值随 b 的变换而变化的图像；固定 a,b 的值，参数取值范围 $c\in(0,1)$，刻画 Lyapunov 指数值随 c 的变换而变化的图像。如图 4 所示，加入参数 c 前后分形动力系统 Lyapunov 指数值的图像，可以明显的看出，当三个参数变化时，产生序列的 Lyapunov 指数值都大于 0，所以分形混沌系统具有超混沌性。相比较本文的分形混沌系统具有更大的 Lyapunov 指数值，一些序列在整个区间包括端点的值都很稳定，具有更好的初值敏感性。

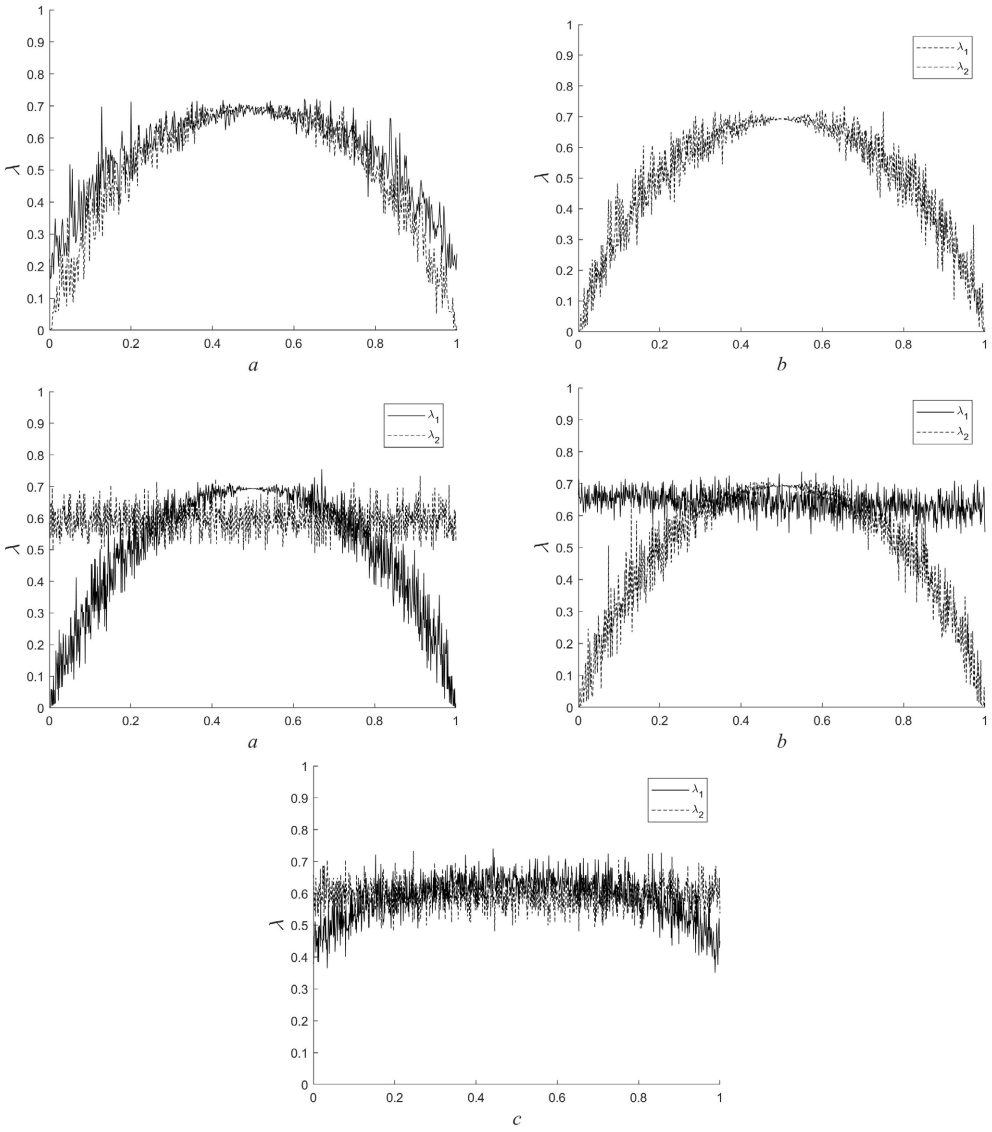


Figure 4. Lyapunov exponent
图 4. Lyapunov 指数

2.2.4. 自相关分析

时间序列 $X=\{x_1,\cdots,x_n\}$ 与其 k 期延迟序列 $Y=\{x_{k+1},\cdots,x_{n+k}\}$ 的自相关系数 ρ_k 的定义如下：

$$\rho_k = \frac{\sum_{i=k+1}^{n}\left(x_i - \overline{x}\right)\left(x_{i-k} - \overline{x}\right)}{\sum_{i=1}^{n}\left(x_i - \overline{x}\right)} \tag{6}$$

其中 n 表示序列的长度，k 是延迟期数，x_i 表示时间序列在时刻 i 的值，$\overline{x}$ 表示序 X 的平均值。自相关系数是描述一个序列 X 与其延迟了 k 期的序列之间的相关程度，可以用来刻画序列的噪声性质。具有伪随机性的序列类似白噪声，序列的其延迟了 $k\left(k \neq 0\right)$ 期的自相关系数应该接近 0，也就是序列与自身的时间序列的相关系数图与 δ 函数一致[12]。如图 5 所示，分形混沌系统产生的两个序列 X,Y 与自身的时间延迟序列的自相关系数图与 δ 函数极其近似，说明产生的序列具有很好的伪随机性、混沌性。

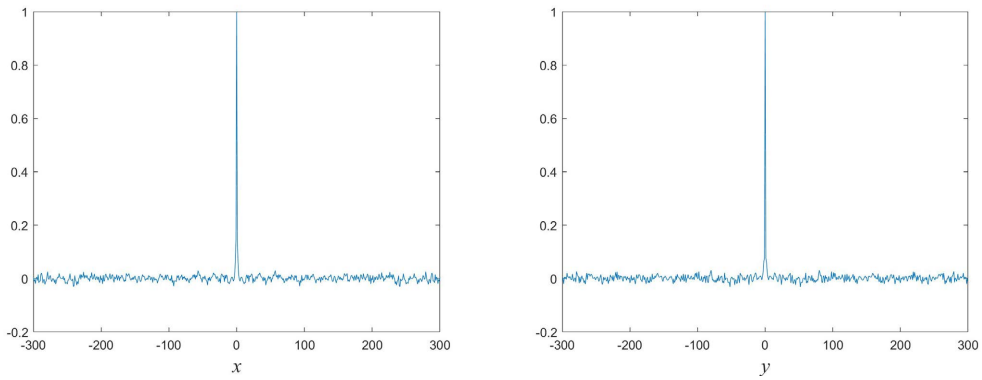


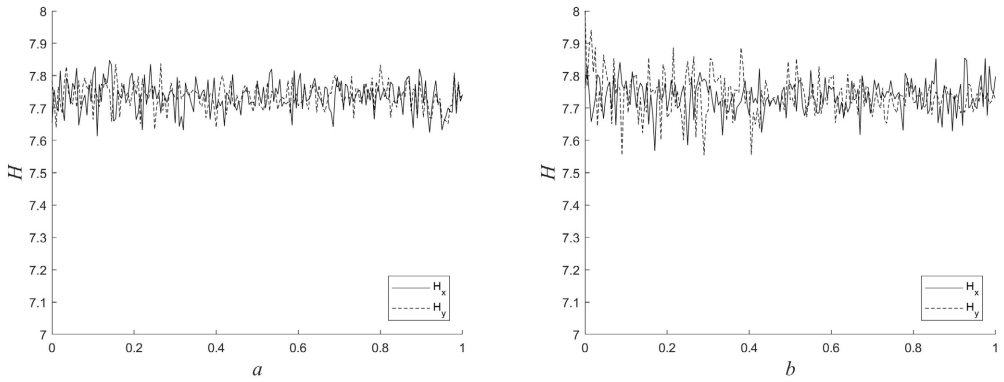
Figure 5. Autocorrelation coefficient diagram
图 5. 自相关系数图

2.2.5. 信息熵

信息熵(香农熵)反应了信息的不确定性，一般来说，熵值越大，不确定性越大。可以用来描述混沌映射生成的序列的随机性[27]，序列 X 的信息熵可以定义为：

$$H = -\sum_{i=1}^{n} p\left(x_i\right)\log_2 p\left(x_i\right) \tag{7}$$

其中，$p\left(x_i\right)$ 表示 x_i 出现的概率，n 表示将序列分割的区间个数，在实验中，设置 n = 256。计算理论值时，假设序列中的随机数落入区间内的概率都相等，则信息熵的理论值 $H = \log_2 256 = 8$。如图 6 所示，当三个参数值分别变化时，信息熵值都接近序列的最大值，所以序列的随机性良好[4]。



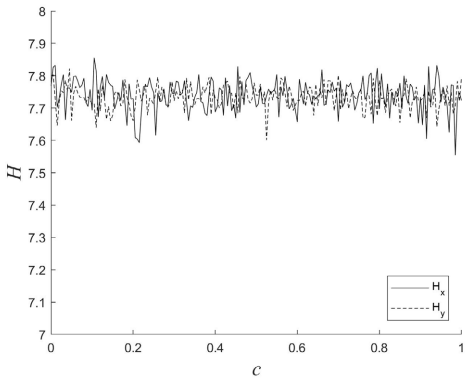


Figure 6. Information entropy diagram
图 6. 信息熵图

2.2.6. 0~1 测试

0~1 测试可以用来检验非线性系统是否处于混沌状态[28]。考虑动力系统生成的序列 $\phi(n), n=1,2,\cdots,N$，计算相关系数：

$$K=\operatorname{corr}(\alpha,\beta)=\frac{\operatorname{cov}(\alpha,\beta)}{\sqrt{\operatorname{var}(\alpha)\operatorname{var}(\beta)}}\in[-1,1] \tag{8}$$

其中 $\alpha=(1,2,\cdots,n)$，$\beta=(D(1),D(2),\cdots,D(n))$，

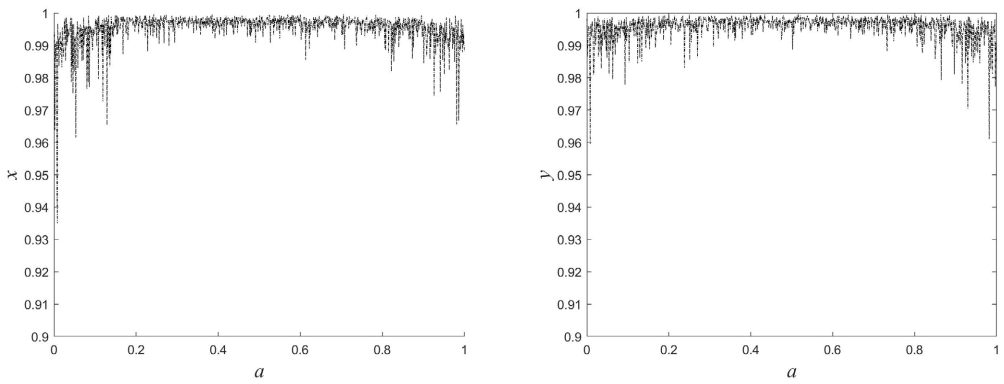
$$\operatorname{cov}(\alpha,\beta)=\frac{1}{n}\sum_{j=1}^{n}(\alpha(j)-\bar{\alpha})(\beta(j)-\bar{\beta})，\ \bar{\alpha}=\frac{1}{n}\sum_{j=1}^{n}\alpha(j)，\ \operatorname{var}(\alpha)=\operatorname{cov}(\alpha,\alpha)，$$

$$D(n)=M(n)-\left(\lim_{N\to\infty}\frac{1}{N}\sum_{j=1}^{N}\phi(j)^2\right)\frac{1-\cos(nc)}{1-\cos(c)}，\ c\in(0,\pi)，$$

$$M(n)=\lim_{N\to\infty}\frac{1}{N}\sum_{j=1}^{N}\left(\left[p(j+n)-p(j)\right]^2+\left[q(j+n)-q(j)\right]^2\right)，$$

$$p(n)=\frac{1}{n}\sum_{j=1}^{N}\phi(j)\cos(jc)，\ q(n)=\frac{1}{n}\sum_{j=1}^{N}\phi(j)\sin(jc)。$$

只有当 $K\approx1$ 时，认为非线性系统是混沌的，迭代次数 $N=1000$，$c\in(\pi/5,4\pi/5)$。对分形混沌系统，可以从图 7 看到，当控制参数在 $(0,1)$ 区间变化时，相关系数 $K\approx1$，说明序列的混沌性能良好。



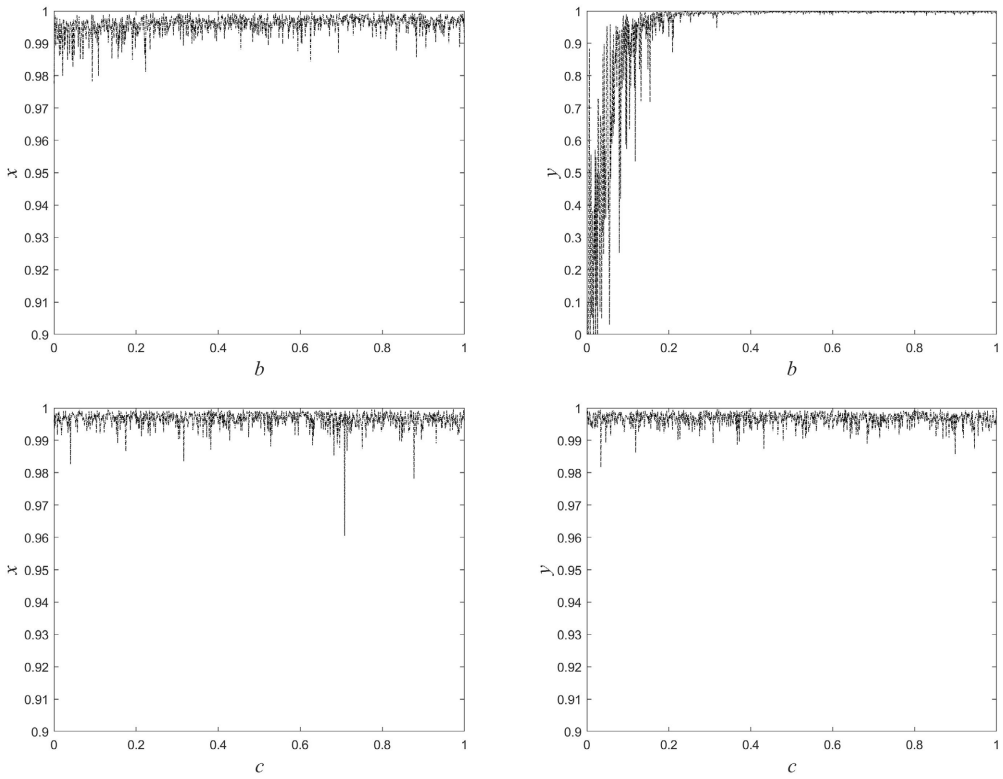


Figure 7. 0~1 test
图 7. 0~1 测试

2.2.7. 排列熵

排列熵[29]是一种动力系统的分析标准，能够准确地揭示混沌映射迭代序列的伪随机性。设迭代序列为$\{x_t\}_{t=1}^{T}$加入嵌入维度 n 和时间延 $l=1$，将序列$\{x_t\}$按递增排序：$x_t=\left[x_t,x_{t+l},\cdots,x_{t+(n-1)l}\right]$。对于 n 维向量可能出现的排序方式有 $n!$种，π 表示排列方式，$f(\pi)$表示它在时间序列中的概率，每种排序出现的概率$P(\pi)=\dfrac{f(\pi)}{T-(n-1)l}$，排列熵的定义为：$H_p(\pi)=-\sum_{n=1}^{n!}P(\pi)\ln P(\pi)$，归一化为：

$$H_p=\frac{H_p(n)}{\ln(n!)}\in[0,1] \tag{9}$$

排列熵越小，输出值越有规律；反之，排列熵越大，输出值的随机性越大。当排列熵接近 1 时，混沌性能最好。测试序列长度 $N=2000$，嵌入维度 $n=3$，时间延迟 $l=1$。结果如图 8 所示，当参数在区间$(0,1)$变化时，排列熵稳定接近 1，因此分形系统生成的序列伪随机性较好，表现出较强的混沌行为。

2.2.8. 统计性能分析

先对分形位移动力系统迭代 10^6 次生成的混沌序列 X 和 Y 进行预处理：

$$X=\mathrm{mod}\left(\mathrm{floor}\left(X,10^9\right),2\right),Y=\mathrm{mod}\left(\mathrm{floor}\left(Y,10^{11}\right),2\right), \tag{10}$$

生成 0~1 比特流，再对比特流序列进行 NIST SP800-22 测试，测试这段数据的统计特性，以此反应数据的随机性。生成 P 值期望值为[0.1,1]。实验结果如表 1 所示，分形系统生成的序列满足所有测试的标准。

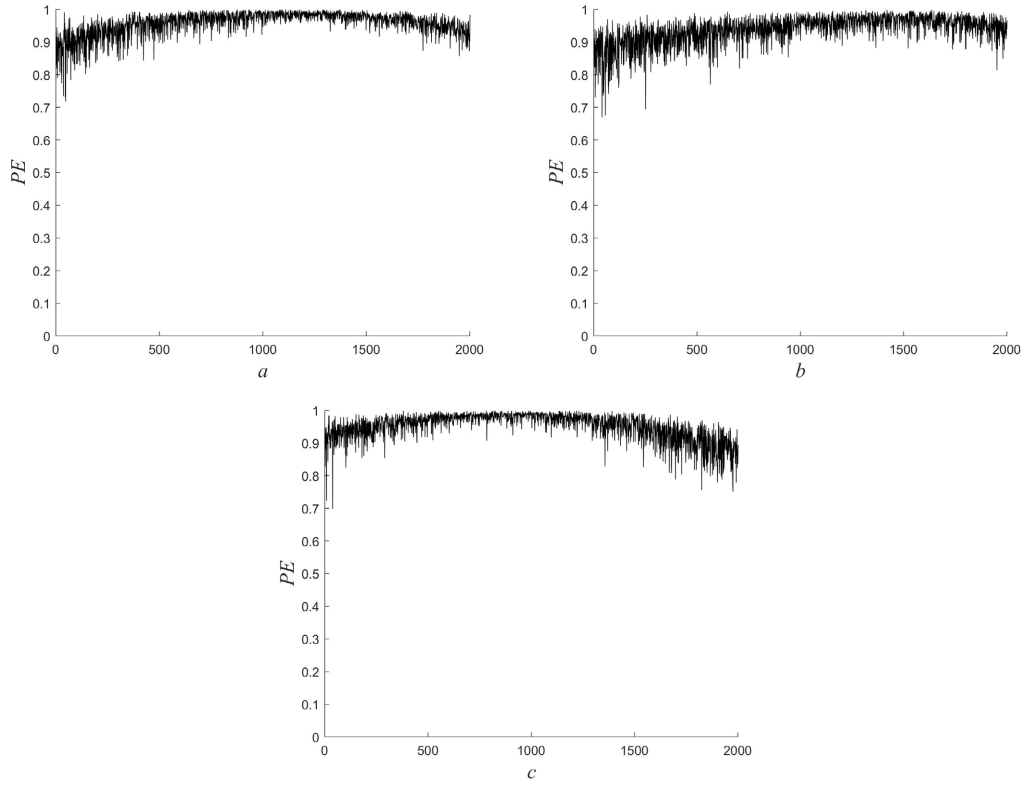


Figure 8. Permutation entropy diagram
图 8. 排列熵图

Table 1. NIST SP800-22 test
表 1. NIST SP800-22 测试结果

NIST 统计检验	P 值(序列 X)	P 值(序列 Y)	结果
单比特频率测试	0.2187	0.5906	通过
块内频率测试	0.0666	0.0184	通过
游程测试	0.1335	0.0990	通过
块内最长 1 游程测试	0.5966	0.3797	通过
二进制矩阵秩测试	0.2777	0.0646	通过
离散傅里叶测试	0.9306	0.2830	通过
非重叠模板匹配测试	0.6969	0.1835	通过
重叠模板匹配测试	0.3014	0.3902	通过
Muarer 通用统计测试	0.2978	0.4777	通过
线性复杂度测试	0.9572	0.1843	通过
序列测试	0.0883 0.0060	0.7633 0.0149	通过 通过
近似熵测试	0.4061	0.1470	通过
累加和测试	0.6942 0.2375	0.9925 0.3290	通过 通过
随机旅行测试	0.4537 0.9922 0.7238 0.3748 0.3005 0.2622 0.6761 0.1384	0.5976 0.5725 0.0829 0.8191 0.9911 0.5026 0.1594 0.0526	通过

续表

随机旅行变种测试	0.5422 0.4980 0.6614 0.8040 0.8124 0.8532 0.6761 0.3756 0.1971 0.0530 0.0830 0.2366 0.0632 0.0051 0.0084 0.0131 0.0107 0.0184	0.6397 0.8378 0.7963 0.6776 0.8994 0.8757 0.7000 0.4496 0.2701 0.5126 0.9207 0.6773 0.7153 0.3011 0.3443 0.6191 0.7895 0.7698	通过

3. 图像加密算法

本文提出的加密算法包括三个阶段，下面介绍加密时要用到的算法。

3.1. Arnold 变换

传统的 Arnold 变换，是将需要加密的图像和参数矩阵通过矩阵的乘法运算，进行加密。改进的 Arnold 映射是将需要置乱的图像矩阵展开为一个一维向量，其交换位置只需要考虑列标的变动，不需要考虑行标的变动，因为此时所有像素点位置的行标皆为 1。对向量中的任意一点坐标 $(1, j)$ 进行 Arnold 映射置换后得到新的坐标位置 (p, q)，其中 a, b 是参数，公式如下：

$$\begin{bmatrix} p \\ q \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \begin{bmatrix} 1 \\ j \end{bmatrix} \tag{11}$$

3.2. Zigzag 扫描

Zigzag 扫描方法是利用 Z 字形的扫描顺序扫描矩阵，将得到的一维向量重新放入新矩阵的置乱方法。本文提出了一种由密钥决定扫描起点和长度的 Zigzag 扫描方法。密钥由多个灰度图像的 Hash 函数决定，生成每个图像不同的扫描始终点。如图 9 所示，选择需要加密矩阵的节点(又密钥量化之后的值决定)，将元素选择之后进行 Z 字形变换，再按照节点的顺序放入原矩阵。最后加密完成的各个矩阵合成大矩阵，长度不足的地方再后方补 0，方便后续的计算。这种扫描方式比起传统的变换具有很好的明文敏感性。

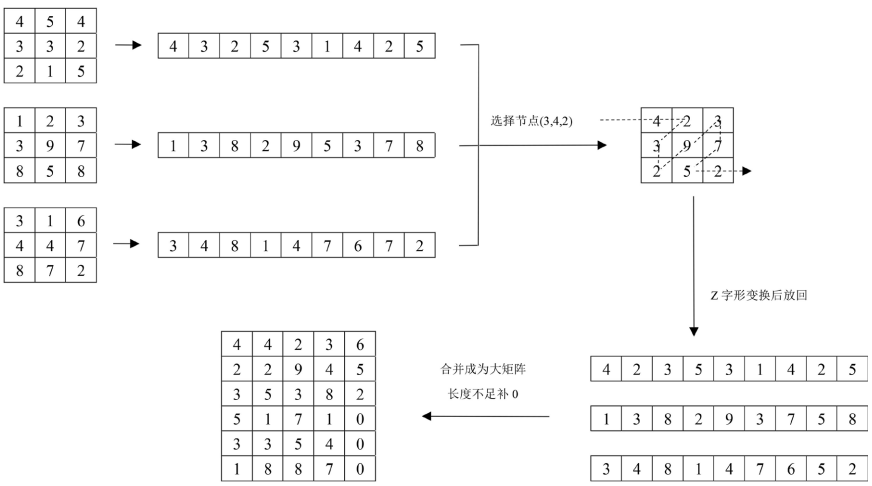


Figure 9. Flow diagram of Zigzag transformation determined by secret key
图 9. 密钥决定的 Z 字形变换流程图

3.3. 有限域扩散

基于有限域上的多项式运算生成的数域 GF(P^n)称为 P^n 阶的伽罗瓦域，其中 P 是素数。伽罗瓦域中有四则运算的定义，其中 GF(257)域的算术运算以 257 为模，剔除会造成信息损失的元素 0 之后，集合包含 256 个元素，与数字图像像素点的灰度值的取值范围 $[0,255]$ 刚好对应。所以 GF(257)适合用于图像加密的扩散算法。将加法和乘法作为加密表，减法和除法作为解密表，使用查表法进行加密。运算速度快且加密效果优良。

3.4. 图像加密算法

本文提出了一个基于分形混沌映射图像加密算法，算法的流程如图 10 所示。使用分形混沌系统生成的序列决定各个环节的加密，经过 Arnold 变换，Zigzag 扫描和有限域扩散后得到加密后的图像。

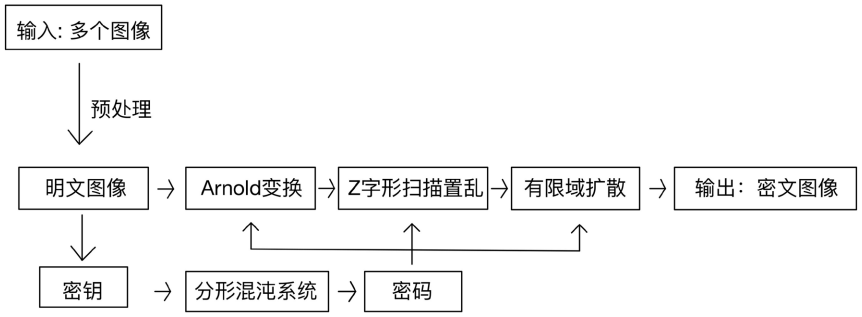


Figure 10. Flow chart of encryption algorithm
图 10. 加密算法流程

1) 图像预处理

输入多个灰度图 $P_1,P_2,\cdots,P_k$，先将组合成为大矩阵：

$$P=\begin{pmatrix} P_1 & P_2 & \cdots & P_{k_2} \\ P_{k_2+1} & P_{k_2+2} & & P_{2k_2} \\ & \vdots & \ddots & \vdots \\ P_{(k_1-1)k_2+1} & P_{(k_1-1)k_2+2} & \cdots & P_{k_1\times k_2} \end{pmatrix} \tag{12}$$

其中 $k=k_1\times k_2$，P_i 图像的大小是 $M_i\times N_i$，P 的大小为 $M\times N$。

2) 密钥和混沌序列生成

利用大矩阵 P 和 Hash 函数生成 256 位的密钥 $k=k_1k_2\cdots k_{32}$，选择动力系统的初值和参数：初始值 $x_0=0.313$，$y_0=0.519$，系统参数 $a=0.313$，$c=0.633$，$b=0.718$，迭代 $M\times N+t$ 次，过渡态长度 t。得到两个长度为 $M\times N$ 的混沌序列 X 和 Y。

3) 自适应性的 Arnold 扰乱

设 P_1 图像的大小是 $M_i\times N_i$ 选择序列 $S=X\left(1:M_1\times N_1\right)$，

$$S_1=\mathrm{mod}\left(\mathrm{floor}\left(S\times 10^{13}\right),256\right) \tag{13}$$

重新组合成为大小为 $M_1\times N_1$ 的矩阵 S_1，对 P_1 进行一次 Arnold 变换后，组合扩散如下：

$$R_1=\mathrm{mod}\left(\mathrm{Arnold}\left(P_1,1\right)+S_1,256\right) \tag{14}$$

再用 R_1 和 P_2 异或运算扰乱下一个图像 P_2，$P_2=\mathrm{bitxor}\left(R_1,P_2\right)$ 用扩散之后的 P_2 加密 $P_3=\mathrm{bitxor}\left(P_2,P_3\right)$

以此类推，直到

$$P_k = \text{bitxor}\left(P_{k-1}, P_k\right) \tag{15}$$

最后再用 P_k 改变 P_1 的像素值： $P_1 = \text{bitxor}\left(P_1, P_k\right)$。混淆每块图像的像素值，在有限次的变换后实现良好的加密效果。基于异或加运算和 Arnold 变换的扰乱和图像的明文相关，具有明文敏感性。

4) Zigzag 型扫描

使用明文相关的密钥决定每个图像的扫描起点和长度，以 $k=4$ 为例

$$D = k_{21} + k_{22} + k_{23} + k_{24} + k_{25} + k_{26};$$

$$d_1 = \text{mod}\left(D \times 2^8 + k_{21} + k_{24}, M_1 \times N_1\right);$$

$$d_2 = \text{mod}\left(d_1 + D \times 2^7 + k_{22} + k_{25}, M_1 \times N_1\right);$$

$$d_3 = \text{mod}\left(d_2 + D \times 2^6 + k_{23} + k_{26}, M_1 \times N_1\right);$$

得到三个扫描起点 d_1, d_2, d_3。按从小到大排序，分别作为各个图像的扫描长度。若 $d_1 < d_2 < d_3$，则图像 P_1 从 $(1,1)$ 开始扫描，扫描长度为 d_1，图像 P_2 从 d_1 开始扫描，扫描长度为 $d_2 - d_1, \cdots$，以此类推，直到图像 P_4 被扫描完成。再将所有的图片按照顺序组合为密文图像 C_1 使用明文图像 Hash 函数生成的密钥决定了每幅图像 Zigzag 型变换的起点和终点，使算法具有更好的明文敏感性和密钥敏感性。

5) 有限域扩散

整数集合 $\{0,1,\cdots,P-1\}$ 按通常的加法(减法)、乘法(除法)代数运算在模 P 意义下构成一个有限域 GF(P)。即：对于加法，如果 $a,b \in \text{GF}(P)$，则 $a+b \equiv r\left(\text{mod}\, P\right)$，$r \in \text{GF}(P)$；对于乘法，如果 $a,b \in \text{GF}(P)$，则 $a \cdot b \equiv s\left(\text{mod}\, P\right)$，$s \in \text{GF}(P)$。本文构造了 GF(257)的乘法表和除法表，剔除元素 0，用乘法表加密，除法表解密。能够达到无损解密。选择序列 $T = Y\left(M \times N + 1 : 2 \times M \times N\right)$，

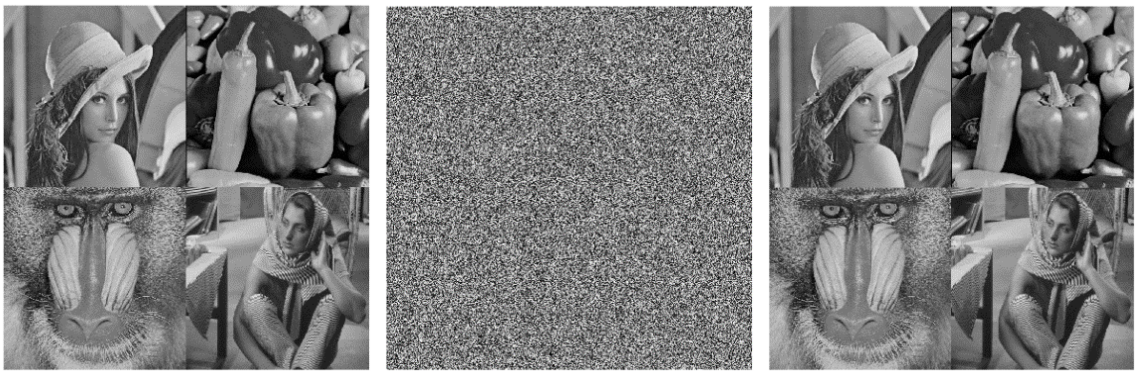
$$S_2 = \text{mod}\left(\text{floor}\left(T \times 10^{10}\right), 256\right) \tag{16}$$

将 C_1 展开成为一维向量，利用混沌序列 S_2，进行正向和逆向的扩散。将明文信息扩散加密，加密速度和效果良好。

算法的解密过程为加密的逆过程。

4. 安全性分析

4.1. 仿真实验结果



(a) (b) (c)

Figure 11. Encryption and decryption test results. (a) Plaintext image; (b) cipher text image; (c) decrypt image
图 11. 加密及解密测试结果。(a) 明文图像；(b) 密文图像；(c) 解密图像

本文使用 MATLAB2017b 进行实验仿真，选择大小为 512 × 512 的 Lena、Peppers、Baboon 和 Barbara 进行加密和解密，结果如图 11 所示。加密图像呈现随机均匀分布的噪声，利用算法图像能够无损解密。

4.2. 密钥敏感性分析

密钥敏感性分析是分析同一明文图像在密钥发生微小变化时，得到的两个密文图像之间的差别。如果两个密文图像之间的差别显著，则表示图像密码系统的密钥敏感性强；若两个密文图像之间差别较小，则称密钥敏感性差。良好的图像密码系统应该具有颇强的密钥敏感性。

衡量两幅相同大小图像 P_1, P_2 的差别有两种方法，分别是计算图像的 NPCR 和 UACI 值。NPCR 是计算两幅图像之间不同像素点值所占的比例：

$$\mathrm{NPCR}\left(P_1, P_2\right) = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N}\left|\mathrm{Sign}\left(P_1(i,j) - P_2(i,j)\right)\right| \times 100\% \tag{17}$$

其中 Sign 是符号函数，$\mathrm{Sign}(x) = \begin{cases} 1, x > 0 \\ 0, x = 0 \\ -1, x < 0 \end{cases}$。UACI 是计算两幅图像不同像素点值的差别程度：

$$\mathrm{UACI}\left(P_1, P_2\right) = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N}\left|\frac{P_1(i,j) - P_2(i,j)}{255}\right| \times 100\% \tag{18}$$

理论值分别为 NPCR = 99.6094%，UACI = 33.4635%。

对组合之后的大图像进行密钥敏感性测试。本文的密钥由外部参数 x_0, y_0, a, b, c 和加密算法的密钥 d_1, d_2, d_3 组成。对密钥分别改变 10^{-15} 单位，分别计算同一明文图像加密之后的密文图像的 NPCR 和 UACI，实验结果如表 2 所示。可以看出 NPCR 和 UACI 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 2. Key sensitivity test
表 2. 密钥敏感性测试

密钥	NPCR	UACI
x_0	99.6099%	33.4897%.
y_0	99.6067%	33.4500%
a	99.6235%	33.4715%
b	99.6132%	33.4696%
c	99.6017%	33.4908%

4.3. 密钥空间

Table 3. Comparison of key space
表 3. 密钥空间大小比较

本文算法	文献[5]	文献[30]	文献[31]
10^{75}	3×10^{43}	10^{60}	10^{45}

密钥空间是指所有合法密钥可构成的空间，图像密码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。本文混沌系统的控制参数为 $K=\{x_0,y_0,a,b,c\}$，初值和参数的取值范围为 $(0,1)$。测试中计算精度为 10^{-15}，所以算法的密钥空间大小为 $10^{15\times5}=10^{75}\gg10^{30}$ 其中 $2^{100}\approx10^{30}$ 是能够抵抗穷举攻击的最小值。所以本文的算法可以抵抗暴力攻击。与其他算法的密钥空间比较如表 3 所示。

4.4. 直方图统计分析

方差和标准差是度量数据的离散度，支撑直方图用来衡量图像数据，图形直方图越均匀，直方图的方差越低。将区间分为 256 份，方差计算公式为：

$$\alpha=\frac{1}{256}\sum_{i=1}^{256}(x_i-\bar{x}) \tag{19}$$

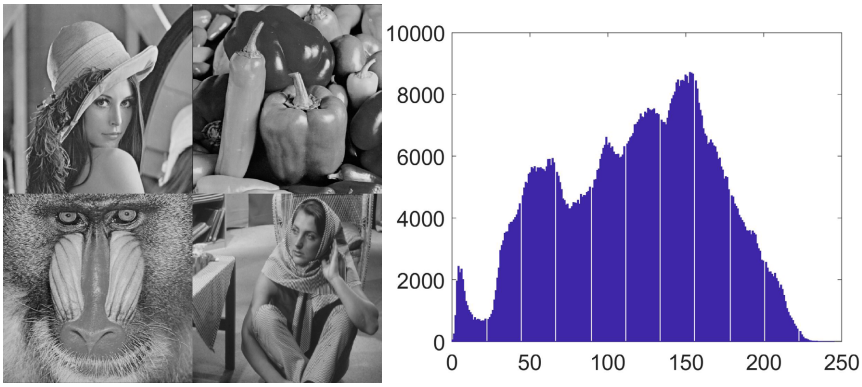
其中，均值 $\bar{x}=\dfrac{M\times N}{256}$，图像大小为 $M\times N$，x_i 为直方图中各值出现的频率。 图像的标准差为 $\beta=\sqrt{\alpha}$ 。对明文图像和密文图像分别画出图像直方图，从图 12 可以看出，加密后的图像变得非常均匀，破坏了图像的统计特征。

4.5. 相关性分析

数字图像的特点就是相邻像素之间有较大的相关性，加密算法的效果希望能够消除这种相关性。从需要考察的图像中任取 $N=3000$ 对相邻的像素点。记它们的灰度值为 (u_i,v_i)，$i=1,2,\cdots,N$，则向量 $\boldsymbol{u}=\{u_i\}$和 $\boldsymbol{v}=\{v_i\}$间的相关系数计算如下：

$$r_{uv}=\frac{\operatorname{cov}(\mathbf{u},\mathbf{v})}{\sqrt{D(\mathbf{u})}\sqrt{D(\mathbf{v})}},\ \operatorname{cov}(\mathbf{u},\mathbf{v})=\frac{1}{N}\sum_{i=1}^{N}\big(u_i-E(\mathbf{u})\big)\big(v_i-E(\mathbf{v})\big) \tag{20}$$

$$D(\mathbf{u})=\frac{1}{N}\big(u_i-E(\mathbf{u})\big)^2,\ D(\mathbf{v})=\frac{1}{N}\big(v_i-E(\mathbf{v})\big)^2 \tag{21}$$



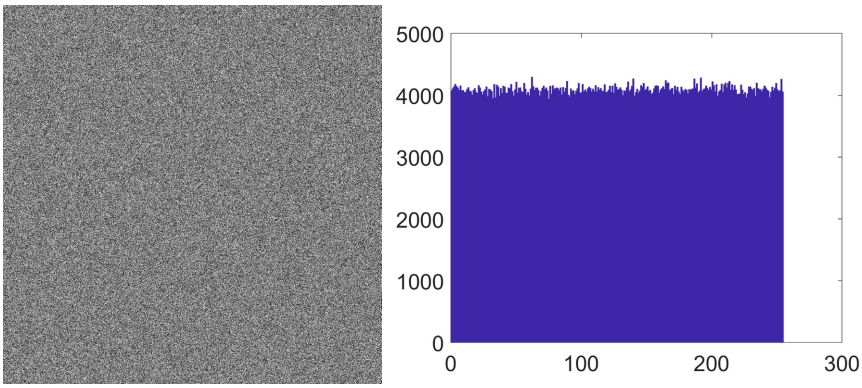


Figure 12. Histogram of plaintext image and cipher text image
图 12. 明文和密文图像的直方图

分析明文图像(Lena, Peppers, Baboon, Barbara)和密文图像水平、垂直和对角方向上的像素间的相关性，加密前后图像的相关系数的计算结果如表 4 示。实验结果表明，明文图像水平、垂直和对角方向的相关系数接近 1，而密文图像在各个方向的相关系数接近 0，本文的加密算法可以有效地破坏相邻像素之间地相关性，保护明文图像的信息。以 Lena 图像为例，密文图像相关系数的比较如表 5 示。

Table 4. Correlation coefficient of adjacent pixels
表 4. 相邻像素的相关系数

方向	水平	垂直	对角
Lena	0.9851	0.9719	0.9523
Peppers	0.9856	0.9780	0.9675
Baboon	0.7575	0.8665	0.7329
Barbara	0.9564	0.8491	0.8366
大图像	0.9350	0.9333	0.9014
密文图像	0.0015	0.0074	0.0193

Table 5. Correlation coefficient of Lena cipher text image
表 5. Lena 图像密文图像的相关系数比较

方向	水平	垂直	对角
本文加密算法	0.0091	−0.0026	−0.0204
文献[32]	0.0144	0.0102	0.0021
文献[33]	0.0130	0.0141	−0.0258

4.6. 信息熵分析

信息熵可以反应图像信息的不确定性。信息熵越大，不确定性越大，可视信息越少，信息熵的计算公式为：

$$H = -\sum_{i=1}^{L} p(i)\log_2 p(i) \tag{22}$$

其中 L 为图像的灰度等级数，$p(i)$表示灰度值 i 出现的概率。在实验中，对于 $L = 256$ 的灰度随机图像，

信息熵的理论值 $H = \log_2 256 = 8$。明文图像和加密图像的信息熵如表 6 所示，算法的信息熵接近 8。因此，通过分析加密图像的信息来获取明文信息近乎不可能。

Table 6. Information entropy of plaintext image and cipher text image
表 6. 明文图像和密文图像的信息熵

图像名称	明文图像	密文图像
Lena	7.4455	7.9994
Peppers	7.5714	7.9991
Baboon	7.3579	7.9993
Barbara	7.4664	7.9993
大图像	7.5963	7.9998

4.7. 差分攻击分析

差分攻击是在明文信息发生细微变化时，使用同一密钥得到的两幅密文图像之间的差别，如果两个密文图像的差别迥异，则称该图像密码系统具有优良的明文敏感性；如果这两个密文图像的差别不大，则称该图像密码系统具有较弱的明文敏感性。使用 NPCR 和 UACI 的值来衡量图像之间的差异。

本文对明文图像随机选取 200 个像素，在每一次实验中只改变一个像素位置灰度值一个单位，用相同的密钥进行加密，得到密文图像。计算原始密文图像和新的密文图像的 NPCR 和 UACI 值，计算其平均值。测试结果 NPCR = 99.6031%，UACI = 33.4500%。NPCR 和 UACI 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抵抗差分攻击的能力。

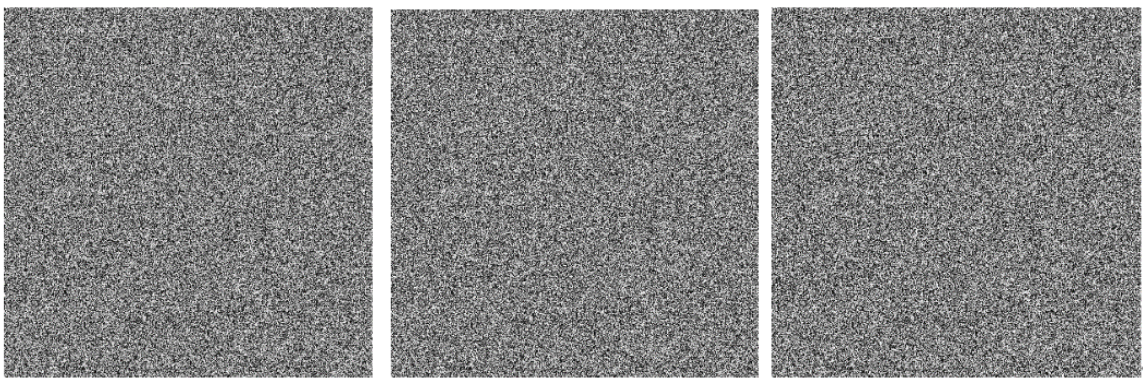
4.8. 鲁棒性分析

在真实应用环境中，图像信息传输时，会受到噪声信息干扰或者损失部分图像信息，一个好的算法要能够拥有抵抗这些攻击的能力。

4.8.1. 噪声攻击

在密文图像中加入不同强度的椒盐噪声，并用正确的密钥解密，结果如图 13 所示。结果表明，解密后的图像仍然可以被识别，说明算法能够抵抗噪声攻击。

4.8.2. 裁剪攻击

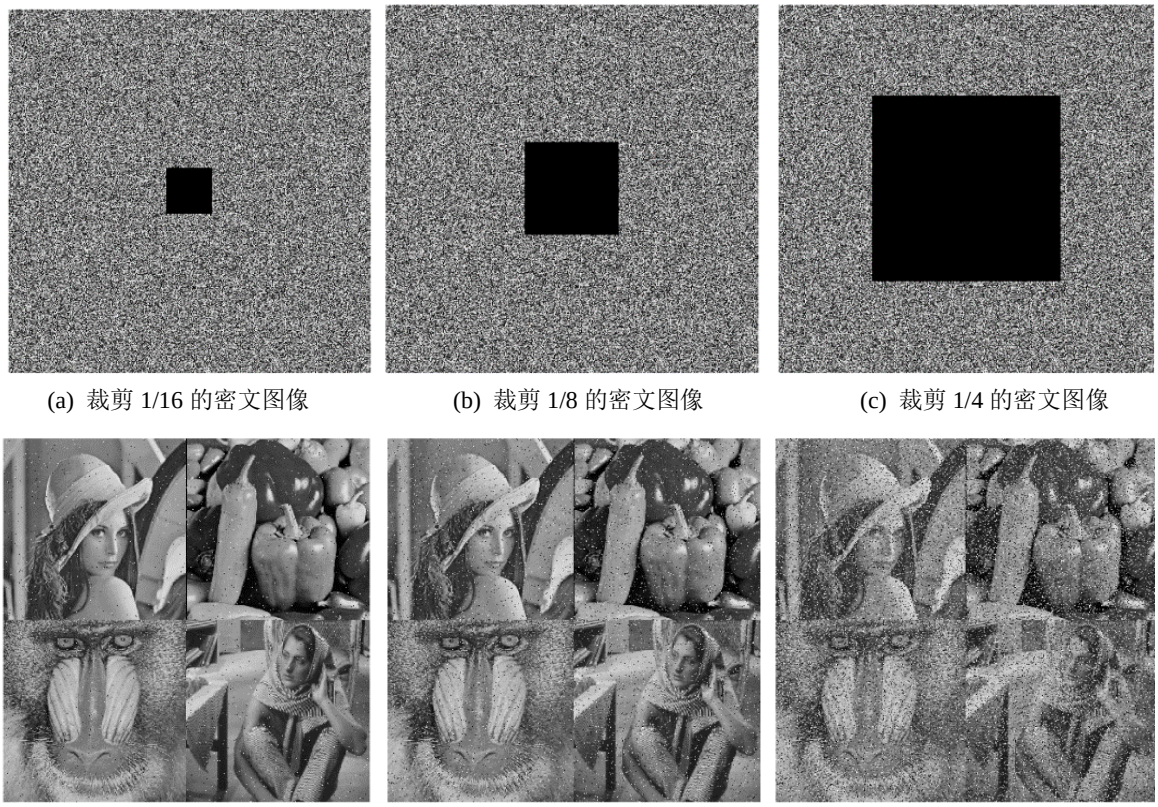


(a) 噪声强度 0.01 的密文图像　(b) 噪声强度 0.05 的密文图像　(c) 噪声强度 0.1 的密文图像

(d) 噪声强度 0.01 的解密图像　(e) 噪声强度 0.05 的解密图像　(f) 噪声强度 0.1 的解密图像

Figure 13. Cipher text images and decrypted images after pepper and salt noise attack
图 13. 椒盐噪声攻击后的密文图像和解密后图像

对密文图像进行不同程度的裁剪攻击，用正确的密钥解密，实验结果如图 14 所示。明文图像能够得到较大程度的还原，说明本文的算法能够抵抗裁剪攻击。



(a) 裁剪 1/16 的密文图像　(b) 裁剪 1/8 的密文图像　(c) 裁剪 1/4 的密文图像

(d) 裁剪 1/16 的解密图像　(e) 裁剪 1/8 的解密图像　(f)裁剪 1/4 的解密图像

Figure 14. Cipher text images and decrypted images after clipping attack
图 14. 裁剪攻击后的密文图像和解密后图像

4.8.3. PSNR 和 SSIM

均方误差(MSE)和峰值信噪比(PSNR)可以用来评价图像的质量，PSNR 表示一副图像加入噪声后和原图像的差距程度。PSNR 越高，图像与原始图像差别越小，效果越好。均方差用 MSE 表示，是各数据偏

离真实值的距离平方和的平均数，均方差值越小越好。对大小为 $M \times N$，数据类型为 uint8 的原始图像 X 和处理后的图像 Y，灰度值最大值为 255，均方误差定义为：

$$\mathrm{MSE}(X,Y)=\frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}\left|X(i,j)-Y(i,j)\right|^2 \tag{23}$$

峰值信噪比定义为：

$$\mathrm{PSNR}=10\times\log_{10}\left(\frac{255\times 255}{\mathrm{MSE}(X,Y)}\right) \tag{24}$$

与 MSE 和 PSNR 衡量两幅数字图像之间的绝对差异不同，SSIM 模拟人眼的视觉感受，考虑图像的亮度、对比度和结构来评价图像数据[34]：

$$\mathrm{SSIM}(X,Y)=\frac{(2\mu_X\mu_Y+C_1)(2\sigma_{XY}+C_2)}{(\mu_X^2+\mu_Y^2+C_1)(\sigma_X^2+\sigma_Y^2+C_2)} \tag{25}$$

其中 μ_X 和 μ_Y 分别表示图像 X 和 Y 的样本均值，σ_X 和 σ_Y 表示图像 X 和 Y 的标准差，σ_{XY} 为 X 和 Y 之间的协方差，C_1 和 C_2 是分母趋于零时稳定除法的常数，一般取 $C_1 = 0.01$，$C_2 = 0.03$。SSIM 的取值范围是 $[0,1]$，当 $X = Y$ 时 SSEM = 1。

将测试的明文图像加密之后加入噪声或剪切攻击，再用同一密钥解密，计算原明文图像和差分攻击后的明文图像之间的 PSNR 和 SSIM 值，用来衡量收到攻击之后明文图像信息的损失程度。测试结果如表 7 所示，本文提出的算法得到的 PSNR 值较大，高于 30 dB；在裁剪攻击下的 SSIM 值都较大，甚至接近 1；说明明文图像失真程度较小，两个图像在人眼观察下区别较小，本文提出的算法能够抵抗噪声和裁剪攻击，其中抗裁剪攻击能力较好。以 Lena 图像为列，与其他算法的 PSNR 和 SSIM 值比较为表 8 所示。

Table 7. PSNR (dB) and SSIM of the image
表 7. 图像的 PSNR (dB)和 SSIM

噪声攻击强度	0.01	0.05	0.1
PSNR	43.1356	36.3011	33.5321
SSIM	0.7010	0.3158	0.1897
剪切攻击强度	1/16	1/8	1/4
PSNR	51.7461	45.7866	39.8400
SSIM	0.9457	0.8096	0.5132

Table 8. Comparison of PSNR and SSIM values (512 × 512 Lena image)
表 8. PSNR 和 SSIM 值比较(512 × 512 的 Lena 图像为例)

噪声攻击强度	0.01	0.05	0.1
PSNR	42.8364	36.0367	33.2956
文献[4]	42.0917	35.2071	32.6197
文献[9]	41.4933	34.8478	32.2479
SSIM	0.6434	0.2327	0.1281
文献[4]	0.7626	0.3347	0.1829
文献[9]	0.5639	0.1796	0.0981

剪切攻击强度	1/16	1/8	1/4
PSNR	51.8584	45.7447	39.8421
文献[4]	45.6663	39.8850	34.2626
文献[9]	50.8890	45.2576	39.5052
SSIM	0.9401	0.7853	0.4493
文献[4]	0.8846	0.6483	0.2762
文献[9]	0.9327	0.7713	0.4332

4.9. 加密及解密速度

实验使用一台配置 AMD R7-5800H、16 G 内存的笔记本电脑，算法基于 MATLAB2017b 语言实现。加密及解密速度测试使用尺寸为 1024 × 1024 的图像。加密速度测试中，对同一图像加密 100 次，记录每次加密耗时，取计算平均值，解密速度测试也采取相同的方式。测试结果算法加密平均速度为 0.2081773 s，解密平均速度为 0.2347666 s。这说明算法具有有效的加密及解密速度，可适用于实际通信环境。与其他算法的运算时间比较如表 9，本文的算法具有优势。

Table 9. Comparison of encryption and decryption time
表 9. 运算时间比较

本文	文献[30]	文献[33]	文献[35]
0.443 s	11.8 s	3.012 s	1.71 s

5. 结语

本文构造了一个新的分形混沌系统，并且从数值上的分析验证了该动力系统的混沌特性，改进之后的动力系统具有更好的混沌特性。利用该分形位移动力系统所生成的混沌序列，设计了一个针对多个灰度图像的扩散－置乱－扩散的加密算法。加密算法包括三个阶段，第一阶段利用改进的 Arnold 变换将首图像加密，再利用前一个图像加密下一个图像，以此类推，将混沌序列的信息扩散；第二阶段用明文图像的密钥决定扫描起点和长度的 Zigzag 变换置乱图像；第三阶段使用 Galois 有限域扩散多个图像组成的大图像。实验结果表明，该算法能有效抵抗蛮力攻击，统计攻击和差分攻击，也能抵抗噪声和裁剪攻击，具有优良的安全性能，而且计算速度较快。

致　谢

本文为广东省基础与应用基础研究基金资助项目(No. 2020B1515310018, 2023A1515030199)。

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] Zhou, W., Wang, X., Wang, M. and Li, D.A. (2022) New Combination Chaotic System and Its Application in a New Bit-Level Image Encryption Scheme. *Optics and Lasers in Engineering*, **149**, Article 106782. https://doi.org/10.1016/j.optlaseng.2021.106782

[3] Amina, S. and Mohamed, F.K. (2018) An Efficient and Secure Chaotic Cipher Algorithm for Image Content Preservation. *Communications in Nonlinear Science and Numerical Simulation*, **60**, 12-32. https://doi.org/10.1016/j.cnsns.2017.12.017

[4] Wang, Q., Zhang, X. and Zhao, X. (2022) Image Encryption Algorithm Based on Improved Zigzag Transformation and Quaternary DNA Coding. *Journal of Information Security and Applications*, **70**, Article 103340.

https://doi.org/10.1016/j.jisa.2022.103340

[5] Wang, X., Chen, X., Feng, S. and Liu, C. (2022) Color Image Encryption Scheme Combining Cross-Plane Zigzag Scrambling and Pseudo-Random Combination RGB Component Diffusion. *Optik*, **269**, Article 169933. https://doi.org/10.1016/j.ijleo.2022.169933

[6] Tang, M., Zeng, G., Yang, Y. and Chen, J. (2022) A Hyperchaotic Image Encryption Scheme Based on the Triple Dislocation of the Liu and Lorenz System. *Optik*, **261**, Article 169133. https://doi.org/10.1016/j.ijleo.2022.169133

[7] Xiao, Y., Tong, X., Zhang, M. and Wang, Z. (2022) Image Lossless Encoding and Encryption Method of EBCOT Tier1 Based on 4D Hyperchaos. *Multimedia Systems*, **28**, 727-748. https://doi.org/10.1007/s00530-021-00868-5

[8] Sheela, S.J., Sanjay, A., Suresh, K.V., Tandur, D. and Shubha, G. (2022) Image Encryption Based on 5D Hyperchaotic System Using Hybrid Random Matrix Transform. *Multidimensional Systems and Signal Processing*, **33**, 579-595. https://doi.org/10.1007/s11045-021-00814-8

[9] Lai, Q., Hu, G., Erkan, U. and Toktas, A. (2023) High-Efficiency Medical Image Encryption Method Based on 2D Logistic-Gaussian Hyperchaotic Map. *Applied Mathematics and Computation*, **442**, Article 127738. https://doi.org/10.1016/j.amc.2022.127738

[10] Hua, Z., Zhou, Y. and Bao, B. (2020) Two-Dimensional Sine Chaotification System with Hardware Implementation. *IEEE Transactions on Industrial Informatics*, **16**, 887-897. https://doi.org/10.1109/TII.2019.2923553

[11] 陈颙, 陈凌. 分形几何学[M]. 北京: 地震出版社, 2005: 22-25.

[12] 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.

[13] 谷利泽, 郑世慧, 杨义先. 现代密码学教程[M]. 北京: 北京邮电大学出版社, 2009.

[14] Qi, D., Zou, J. and Han, X. (2000) A New Class of Scrambling Transformation and Its Application in the Image Information Covering. *Science in China Series E*: *Technological Sciences*, **43**, 304-312. https://doi.org/10.1007/BF02916835

[15] 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.

[16] 张义, 宛楠. 一种基于 Arnold 变换的数字图像加解密算法[J]. 安徽工程大学学报, 2013, 28(3): 66-68.

[17] 杜翠霞, 张定会. 一种新的三维 Arnold 变换和混沌序列相结合的图像加密算法[J]. 数据通信, 2014(1): 51-54.

[18] 李莉, 韦鹏程, 杨华千. 云计算图像加密算法研究[M]. 北京: 科学出版社, 2021: 51-53.

[19] Wang, X. and Chen, X. (2021) An Image Encryption Algorithm Based on Dynamic Row Scrambling and Zigzag Transformation. *Chaos, Solitons & Fractals*, **147**, Article 110962. https://doi.org/10.1016/j.chaos.2021.110962

[20] 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

[21] 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

[22] 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

[23] 胡向东. 应用密码学教程[M]. 北京: 电子工业出版社, 2005.

[24] 王越, 安新磊, 施倩倩, 刘思洋. 基于一个复混沌系统的图像加密算法[J/OL]. 复杂系统与复杂性科学, 2023, 1-9. https://link.cnki.net/urlid/37.1402.N.20230914.1039.002, 2023-09-15.

[25] 黄清梅, 阿孜古丽·伊克木, 李国东. 基于有限域与 Arnold 映射结合的医学图像快速加密算法[J]. 计算机应用与软件, 2023, 40(5): 319-323.

[26] 刘思洋, 王越, 李寒. 基于超混沌系统及有限域的图像加密算法[J]. 河北师范大学学报(自然科学版), 2024, 48(2): 129-140.

[27] Duan, C.,-F., Zhou, J., Gong, L.-H., Wu, J.-Y. and Zhou, N.-R. (2022) New Color Image Encryption Scheme Based on Multi-Parameter Fractional Discrete Tchebyshev Moments and Nonlinear Fractal Permutation Method. *Optics and Lasers in Engineering*, **150**, Article 106881. https://doi.org/10.1016/j.optlaseng.2021.106881

[28] Gottwald, G.A. and Melbourne, I. (2005) Testing for Chaos in Deterministic Systems with Noise. *Physica D*: *Nonlinear Phenomena*, **212**, 100-110. https://doi.org/10.1016/j.physd.2005.09.011

[29] Li, X., Ouyang, G. and Richards, D.A. (2007) Predictability Analysis of Absence Seizures with Permutation Entropy. *Epilepsy Research*, **77**, 70-74. https://doi.org/10.1016/j.eplepsyres.2007.08.002

[30] Zhu, L., *et al*. (2020) A Robust Meaningful Image Encryption Scheme Based on Block Compressive Sensing and SVD Embedding. *Signal Processing*, **175**, Article 107629. https://doi.org/10.1016/j.sigpro.2020.107629

[31] Xiao, D., Zhao, M. and Wang, M. (2021) Low-Cost and Secure Multi-Image Encryption Scheme Based on P-Tensor Product Compressive Sensing. *Optics & Laser Technology*, **140**, Article 107077. https://doi.org/10.1016/j.optlastec.2021.107077

[32] Demirtaş, M. (2022) A Novel Multiple Grayscale Image Encryption Method Based on 3D Bit-Scrambling and Diffusion. *Optik*, **266**, Article 169624. https://doi.org/10.1016/j.ijleo.2022.169624

[33] Wang, X., Zhao, M., Feng, S. and Chen, X. (2023) An Image Encryption Scheme Using Bit-Plane Cross-Diffusion and Spatiotemporal Chaos System with Nonlinear Perturbation. *Soft Computing*, **27**, 1223-1240. https://doi.org/10.1007/s00500-022-07706-4

[34] Armijo-Correa, J.O., Murguía, J.S., Mejía-Carlos, M., Arce-Guevara, V.E. and Aboytes-González, J.A. (2020) An Improved Visually Meaningful Encrypted Image Scheme. *Optics & Laser Technology*, **127**, Article 106165. https://doi.org/10.1016/j.optlastec.2020.106165

[35] Zhang, X. and Hu, Y. (2021) Multiple-Image Encryption Algorithm Based on the 3D Scrambling Model and Dynamic DNA Coding. *Optics & Laser Technology*, **141**, Article 107073. https://doi.org/10.1016/j.optlastec.2021.107073