**文章编号：** 1671-7449(2024)05-0487-13

# 基于2D-SFHM混沌系统和改进DNA编码的彩色图像加密

段玮鹏，胡红萍*

（中北大学 数学学院，山西 太原 030051）

**摘　要：** 为改善一维混沌系统密钥空间较小、安全性能较低而超混沌系统初始参数要求较高且效率较低等问题，提出了一种基于二维正弦函数超混沌映射(2D-SFHM)混沌系统和改进DNA编码的彩色图像加密方法。首先通过2D-SFHM混沌系统与Logistic系统生成混沌序列，将彩色图像分为RGB 3个通道，再基于混沌序列对每个通道分块进行DNA编码、解码、扩散和置乱，并在动态DNA编码的基础上提出基因突变机制，一定程度上丰富了DNA编码规则，最后合并3个通道得到彩色加密图像。实验结果表明，所提方法对密文图像直方图统计特性均匀平滑，相关性分析性能良好，实现了图像的安全加密效果，具有良好的加密性能和安全性。

**关键词：** 彩色图像加密；超混沌系统；DNA编码；像素置乱；扩散

**中图分类号：** TP309.7；O415.5　　**文献标识码：** A　　**doi:** 10.3969/j.issn.1671-7449.2024065

**引用格式：** 段玮鹏，胡红萍．基于2D-SFHM混沌系统和改进DNA编码的彩色图像加密[J]．测试技术学报，2024，38(5)：487-499.

DUAN Weipeng，HU Hongping．A color image encryption based on 2D-SFHM chaos system and improved DNA encoding[J]．Journal of Test and Measurement Technology，2024，38(5)：487-499.

# A Color Image Encryption Based on 2D-SFHM Chaos System and Improved DNA Encoding

DUAN Weipeng，HU Hongping*

（School of Mathematics，North University of China，Taiyuan 030051，China）

**Abstract：** A method for encrypting color images based on a two-dimensional sine function hyperchaotic map（2D-SFHM）chaotic system and improved DNA encoding is proposed to address the issues of small key space and low-security performance in one-dimensional chaotic systems，as well as the high initial parameter requirements and low efficiency in hyperchaotic system. Initially，chaotic sequences are generated using a 2D-SFHM chaotic system and Logistic system. The color image is then divided into RGB channels，and each channel is block-wise encoded，decoded，diffused，and scrambled based on the chaotic sequences and dynamic DNA encoding. Additionally，a gene mutation mechanism is introduced to enrich the DNA encoding rules. Finally，the encrypted color image is obtained by combining the three channels. Experimental results show

**收稿日期：** 2024-01-10

**基金项目：** 山西省基础研究计划资助项目(20210302123019，20210302124195，20210302124212，20210302123189)；山西省回国留学人员科研资助项目(2020-104，2021-108)。

**作者简介：** 段玮鹏(2000—)，男，硕士生，主要从事图像处理研究。E-mail：d1532567434@163.com。

***通信作者：** 胡红萍(1973—)，女，教授，博士，硕士生导师，主要从事应用数学研究。E-mail：huhongping@nuc.edu.cn。

that the proposed method achieves uniform and smooth statistical characteristics of the ciphertext image histogram, good correlation analysis performance, and effectively secures the encrypted image, demonstrating excellent encryption performance and security.

**Key words**: color image encryption; hyperchaotic system; DNA encoding; pixel scrambling; diffusion

## 0 引 言

图像信息已成为网络信息传播的主要内容之一，通常需要传输这些图像进行处理或分析。在军事、远程医疗等许多领域，图像信息必须加密，以防止未经授权的人访问[1]。因此，基于混沌系统与DNA编码的彩色图像加密成为了一个备受关注的研究领域。混沌系统具有高度的随机性和不可预测性，而DNA编码则具有高度的信息容量和复杂性，这使得它们成为了图像加密领域的有力工具。

混沌系统是一种非线性动力学系统，具有复杂的运动轨迹和敏感的初值依赖性[2-3]。通过选择合适的混沌映射函数和参数，可以生成具有高度随机性的混沌序列。这些混沌序列可以用作密钥对彩色图像进行加密和解密。在加密过程中，混沌序列与图像像素进行异或运算，从而改变像素值，使得加密后的图像难以被破解。在解密过程中，使用相同的密钥对加密后的图像进行异或运算，即可还原出明文图像。

DNA编码[4]是一种将数字信息转化为DNA序列的方法。DNA序列具有高度的信息容量和复杂性，可以提供更高的加密强度。在彩色图像加密中，可以将图像的像素值转化为相应的DNA序列。通过选择合适的DNA编码规则和转换算法，可以将图像信息嵌入到DNA序列中。在解密过程中，通过逆向的DNA编码算法可以将DNA序列转化为原始的像素值，从而还原出明文图像。

基于混沌系统与DNA编码的彩色图像加密方法具有许多优势。张爱华等[5]提出了一种基于比特重排与一维混沌系统的图像加密方案，但该算法过于简单，密钥空间较小，容易被攻击。方鹏飞等[6]提出一种基于四维超混沌系统与神经网络的彩色图像加密方案，但其提出的四维超混沌系统对于初始值要求较高，只有在$a$=24，$b$=25，$c$=3及$d$=0.5时系统处于混沌状态，并且超混沌系统迭代缓慢，加密效率低下。Wang等[7]提出了一种利用半张量矩阵的安全算法。但是，这些算法在加密过程中没有考虑明文信息，容易受到明文攻击。为了克服这些问题，学者开始转向使用高维混沌系统甚至超混沌系统来实现多图像加密。赵桥等[8]提出了一种基于Chen超混沌系统和DNA编码的彩色图像加密算法，该算法通过对彩色图像分块进行DNA动态编码提升了加密算法的安全性，但超混沌系统初始参数要求高、迭代速度慢的问题仍然存在。Pak等[9]提出了一种新的彩色图像加密方法，利用一维混沌映射的组合，首先将彩色图像的红、绿、蓝分量组成一个大矩阵，然后利用索引向量对其进行加密，得到密码图像。Pak等[10]提出了一种利用一维Logistic和正弦映射进行位级彩色图像加密的方法，利用混沌序列排序得到的置换位置矩阵对普通图像进行位矩阵的加密。Gan等[11]提出了一种基于三维位平面置换的混沌图像加密算法，首先对彩色平面图像进行RGB分割和位平面分解得到三维位平面，然后利用三维Chen混沌系统的位置序列对其进行置换，最后采用密钥矩阵对混沌矩阵进行扩散得到密码图像。Gong等[12]提供了一种图像压缩加密方法，通过对Logistic-Sine系统和Logistic-Tent系统产生的混沌序列进行排序得到两个向量，一个矢量用于控制行排列，另一个矢量用于按列排列。上述排列方法有一个缺点，即置乱方法的安全性依赖于索引向量，攻击者通过分析密码图像与明文图像之间的关系，可以很容易地获得索引向量，这可能导致置乱操作的无效。因此，相比于一维混沌系统，高维混沌系统运行轨迹更加复杂，更难以被预测，从而提高了图像加密的安全性和可靠性，而与超混沌系统相比，高维混沌系统在满足图像加密安全性的前提下具有更高的加密效率。因此，高维混沌系统在多图像加密领域的研究和应用具有重要意义。

为了改善一维混沌系统与超混沌系统存在的一些问题，本文提出了一种基于二维正弦函数超混沌映射(Two-Dimensional Sine Function Hyperchaotic Map，2D-SFHM)混沌系统和改进DNA编码的彩色图像加密方法。通过2D-SFHM混沌映射和Logistic映射两种混沌模型迭代生成复杂的混沌序列，并将其与改进的DNA编码方法相结合，对图像进行加密。在该算法中，通过引入二维混沌映射模型可以生成更复杂和难以预测的混沌序列，提高了加密的安全

性，并将其与SHA-256函数相结合，在达到“一图一密”效果的同时进一步增强了密钥空间大小与加密算法的安全性。同时，利用改进的DNA编码方法可以将混沌序列与图像像素进行有效地映射和编码，从而实现对图像的高效加密。将加密过程与明文密切相关，提高密文对明文的敏感性。加密完成后，对实验结果进行分析与对比，其中密文图像直方图均匀平滑，相关性分析性能良好，抗差分攻击性能较好，实现了图像的安全加密效果。

## 1　混沌系统与DNA编码

### 1.1　Logistic映射

近年来，加密体系中最常用到一个系统就是Logistic映射，它是一种常见的非线性映射函数，定义如下[13]

$$x_n=\mu x_{n-1}(1-x_{n-1}),\tag{1}$$

式中：$\mu$为分支参数；$\{x_n\}$为得到的混沌序列。当$\mu\in[0,4]$，$x_0\in[0,1]$时，Logistic映射的模型如图1所示。

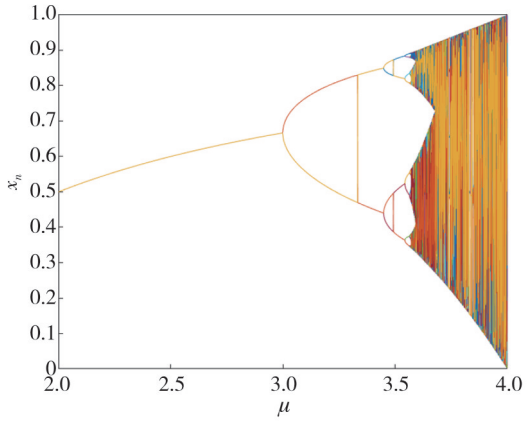



图1　Logistic映射

Fig. 1　Logistic map

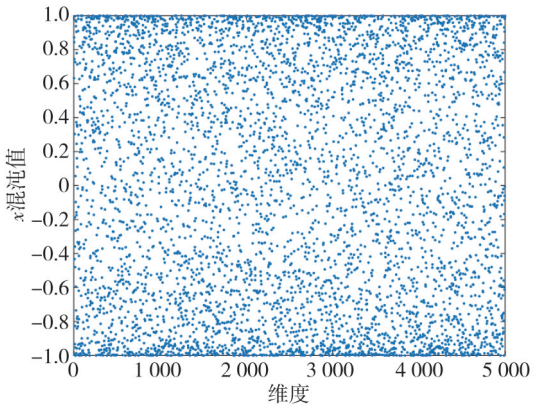
由图1可知，Logistic映射的输出序列分布对分支参数$\mu$非常依赖。当$\mu<3$时，映射的迭代结果趋于定值。如果满足3.569 945 67…$<\mu\leqslant4$，且给定一个起始值$x_0\in(0,1)$，通过连续迭代，可以产生一个非周期性且不会收敛的序列。这个序列的数值能够覆盖整个混沌区间$[0,1]$。在这种情况下，称对应的Logistic映射为混沌的[14-15]。

### 1.2　2D-SFHM混沌系统

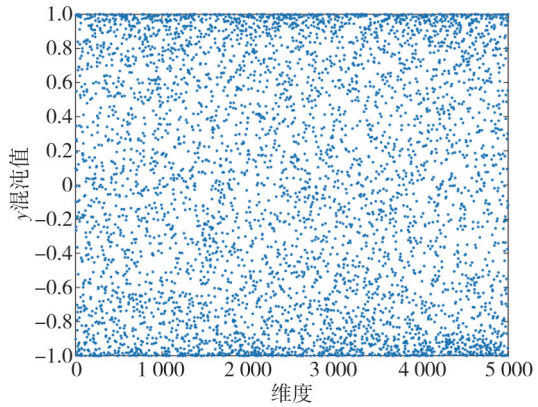
本文使用的2D-SFHM混沌映射是由经典正弦映射和数学函数耦合在模型结构中的二维混沌映射[16]，定义如下

$$\begin{cases}x_{n+1}=\sin\left(\dfrac{a\pi^2}{x_n y_n}\right),\\ y_{n+1}=\sin(b\pi^2(x_n(1-y_n)),\end{cases}\tag{2}$$

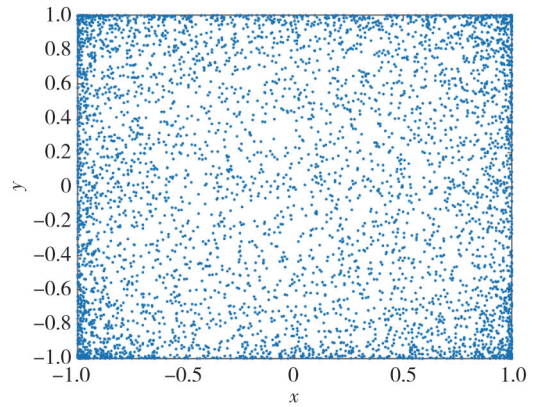
式中：$a$和$b$为递归参数，取值在$[0,100]$范围内，对初始变量$x_n$和$y_n$进行迭代生成变量$x_{n+1}$和$y_{n+1}$。当$a$和$b$取值均为50时，$x$与$y$混沌值如图2所示。




（a）$x$随迭代次数变化散点图




（b）$y$随迭代次数变化散点图

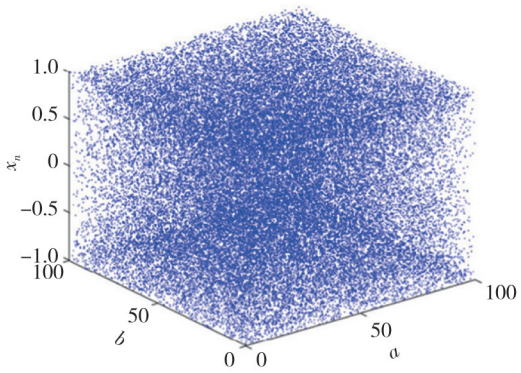



（c）$x$与$y$运行轨迹图

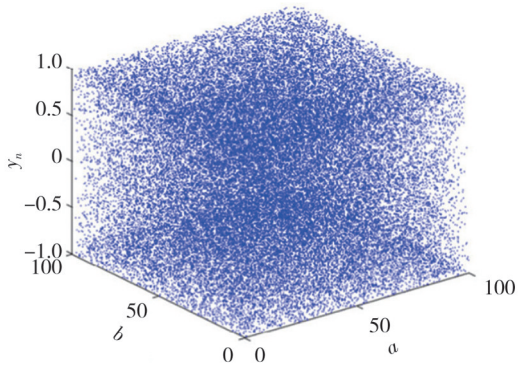
图2　$x$与$y$混沌值

Fig. 2　The chaos values of $x$ and $y$

分岔图可直观地展示时间序列在不同控制参数下的演化过程，从而决定了混沌区间的范围。图 3 显示了初始状态为$(x_0, y_0)=(0.1, 0.1)$的 2D-SFHM混沌系统中，控制参数$a$和$b$在[0, 100]范围内的分岔图。2D-SFHM的分岔图可以在整个数据范围内展开，这表明在所有参数设置下，所提出的映射具有两个迭代序列，可以在整个空间中随机分布。




(a) $x$随$a$, $b$变化分岔图



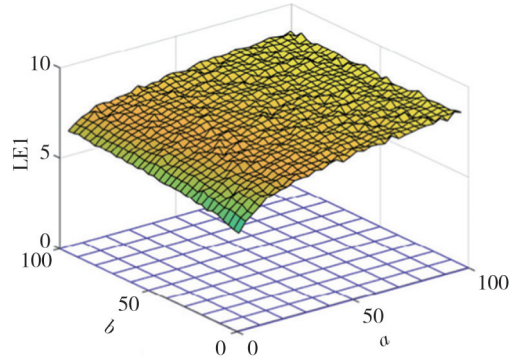

(b) $y$随$a$, $b$变化分岔图

图 3 2D-SFHM混沌系统分岔图

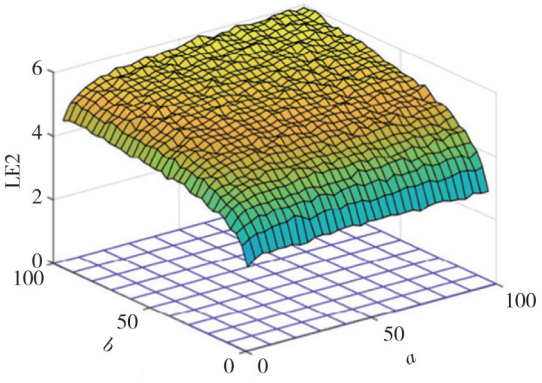
Fig. 3 Bifurcation diagrams of 2D-SFHM chaotic system

非线性系统的复杂程度可以通过李雅普诺夫指数(LE)来定量评估。动力系统的最大LE (LLE)决定了系统是否具有混沌行为。超混沌映射具有两个或两个以上的正LE，比混沌映射具有更高的随机性和更复杂的动力学行为。图 4 直观地显示了 2D-SFHM映射在参数$a$和$b$取[0, 100]区间内的2个LE，这表明所提出的映射能够表现出超混沌行为。

显然，2D-SFHM的轨迹可以分布在整个相平面上，具有很好的随机性。结合图 2～图 4 可以看出，2D-SFHM映射具有复杂的混沌行为，非常适合于图像加密等特定应用。




(a) $x$随$a$, $b$变化LE图




(b) $y$随$a$, $b$变化LE图

图 4 2D-SFHM混沌系统LE图

Fig. 4 Bifurcation diagrams of the 2D-SFHM chaotic system

### 1.3 DNA 编码

DNA，又称为脱氧核糖核酸，包含4种碱基：C(胞嘧啶)、T(胸腺嘧啶)、A(腺嘌呤)和G(鸟嘌呤)。根据DNA碱基的互补配对原理，A与T、C与G是互补的[17]。在二进制表示中，0和1也是互补关系，因此00与11，以及01与10也被视为互补。所以，可以使用A、G、C、T这4种碱基来编码00、01、10和11。根据Watson-Crick互补规则，在24种编码中，只有8种编码是符合规则的。表 1 展示了这8种符合互补规则的编码方式。

表 1 DNA编码与解码规则

Tab. 1 DNA encoding and decoding rules

| 编码方式 | A | T | G | C |
|---|---|---|---|---|
| 1 | 11 | 00 | 01 | 10 |
| 2 | 11 | 00 | 10 | 01 |
| 3 | 01 | 10 | 00 | 11 |
| 4 | 01 | 10 | 11 | 00 |
| 5 | 10 | 01 | 00 | 11 |
| 6 | 10 | 01 | 11 | 00 |
| 7 | 00 | 11 | 01 | 10 |
| 8 | 00 | 11 | 10 | 01 |

假设一个像素点的R通道值为十进制153，经过DNA编码后得到DNA序列CGCG。然后，将编码

后的DNA序列按照表1中的规则进行解码，得到二进制数01100110，再转换为十进制即为102。可见，通过一次简单的DNA编码和解码，可以使一个数值发生极大的改变，实现了对数值的加密。在此基础上，通过对DNA序列之间进行加减法、异或和同或运算等操作，可以进一步增强图像的加密效果。这种基于DNA编码解码的加密方法具有较高的安全性和可靠性，可以在数字图像加密中发挥重要作用。

## 2　本文算法

### 2.1　改进的DNA编码

表1列出了满足互补规则的8种DNA编码方式，然而在传统图像加密中，DNA编码只选取其中一种作为编码规则，同时在运算方式的选择上往往只会选择加减、同或与异或其中的一种，并且大多数基于DNA编码的图像加密算法利用DNA加法、DNA减法、DNA异或、DNA循环或DNA互补操作来实现扩散过程。但这些操作相对简单，而且存在被暴力破解的风险。与它们不同的是，DNA互补周期突变策略（DCCMS）[18]是一种用于扩散的策略，它由多个混沌序列和明文信息决定。突变原本是指生物体和病毒DNA基因组核苷酸序列的改变。在图像处理领域，突变是指图像像素的变化。例如，图像像素100（其8位二进制数为01100100），假设其二进制序列的第2位突然发生变化，01*100100→00*100100，符号*表示元素突变的位置，图像像素由100（二进制数为01100100）变换为36（二进制数为00100100）。可以看出，突变是一种可以有效修改图像像素值的扩散方法。本文基于2D-SFHM混沌系统，设计了一种改进型DNA编码方式（具体方法见2.2节步骤5～7），通过混沌系统产生的混沌序列对彩色图像不同通道的不同子块分别采用不同的DNA编码方式与运算规则，并提出了基因突变机制，在进一步扩大算法的密钥空间提升加密算法安全性的同时又在一定程度上丰富了DNA编码规则。基因突变规则如表2所示。

表2　DNA基因突变规则

Tab. 2　DNA gene mutation rules

| 编码方式 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| A | A | C | G | T |
| T | T | A | C | G |
| G | G | T | A | C |
| C | C | G | T | A |

该方法在DNA互补周期突变策略的6条DNA互补规则的基础上舍弃循环操作，保留部分互补规则，并直接作用于部分子块而非每个像素，使其更适用于大尺寸以及彩色图像加密。例如，选取表1中的规则对子块进行突变，则子块内各元素不发生改变，而选取表2中的规则进行突变，则将子块内所有元素进行DNA编码后再将其A、T、G、C分别转换为C、A、T、G。这在保证加密效率的前提下有效提高了密钥空间复杂度与加密图像抵抗明文攻击的能力。

### 2.2　算法流程

将彩色数字图像分为R、G、B 3个通道，对每个通道分块进行DNA编码和解码运算，加密后再次进行置乱，最后合并3个通道得到彩色加密图像。图像每个分块的DNA编码解码以及运算规则由2D-SFHM混沌系统生成的序列决定。为保证“一图一密”的效果，将2D-SFHM混沌系统的初始值与明文图像关联，提升了系统的抗攻击能力。利用Logistic映射迭代得到的3个不同的混沌序列，分别对明文图像进DNA编码运算、行置换、列置换，在增强密文图像的扩散与置乱效果的同时可以获得抗裁剪的特性。本文在此基础上提出了一种基于2D-SFHM混沌系统和改进DNA编码的彩色图像加密算法，该加密算法流程如图5所示。

该算法的具体步骤如下：

**步骤 1**　将大小为$M'\times N'$的明文图像$\boldsymbol{I}$按式(3)分为R，G，B 3个二维矩阵，称为$\boldsymbol{I}_1$，$\boldsymbol{I}_2$，$\boldsymbol{I}_3$。

$$\begin{cases}\boldsymbol{I}_1=\boldsymbol{I}(:,:,1),\\ \boldsymbol{I}_2=\boldsymbol{I}(:,:,2),\\ \boldsymbol{I}_3=\boldsymbol{I}(:,:,3)。\end{cases}\tag{3}$$

**步骤 2**　为加强算法普适性，填充3个二维矩阵使其尺寸均满足式(4)，填充的数据值取为0。

$$\begin{cases}mod(M,t)=0,\\ mod(N,t)=0,\end{cases}\tag{4}$$

式中：$M$和$N$为填充后的图像尺寸（$M\geqslant M'$，$N\geqslant N'$）；$t$为分块大小。通过式(4)可知，矩阵$\boldsymbol{I}_1$，$\boldsymbol{I}_2$，$\boldsymbol{I}_3$都能够均匀分成$\dfrac{(M\times N)}{t^2}$个大小为$t\times t$的块。

**步骤 3**　混沌系统初值的生成：本文使用SHA-256函数为明文图像$\boldsymbol{I}$生成一个256位的哈希密钥，将其以8位为一组组合得到$k_i$，其中$i=$

1, 2, …, 32。初始值$x_0$由明文图像的哈希密钥与外部密钥$t_1$, $t_2$, $t_3$, $t_4$得出, 如式(5)。

$$x_0=\left((t_1+t_2)/256(t_3+t_4)\right)\cdot\left(\left(k_1\oplus k_9\oplus k_{17}\oplus k_{25}\right)\bmod 1,\right. \tag{5}$$

式中: $x\oplus y$表示$x$与$y$的异或运算。

设定参数$\mu$、输入初值$x_0$, 根据式(1)对 Logistic 映射连续迭代得到序列$\{u_i\}$, 序列的长度为$M\times N$。其中, $\mu$设定为 3.999 9, 作为加密时的密钥之一。按式(6)将序列$\{u_0\}$中每个元素的值转化为0~255范围内得到序列$\{U_i\}$, 再通过式(7)将序列$\{U_i\}$转换为与$\boldsymbol{I}_1$大小相同的$M\times N$的二维矩阵, 用于与$\boldsymbol{I}_i(i=1, 2, 3)$进行 DNA 运算。

$$U=mod\left(round(u\times 10^4), 256\right), \tag{6}$$

$$R=reshape(U, M, N)。 \tag{7}$$

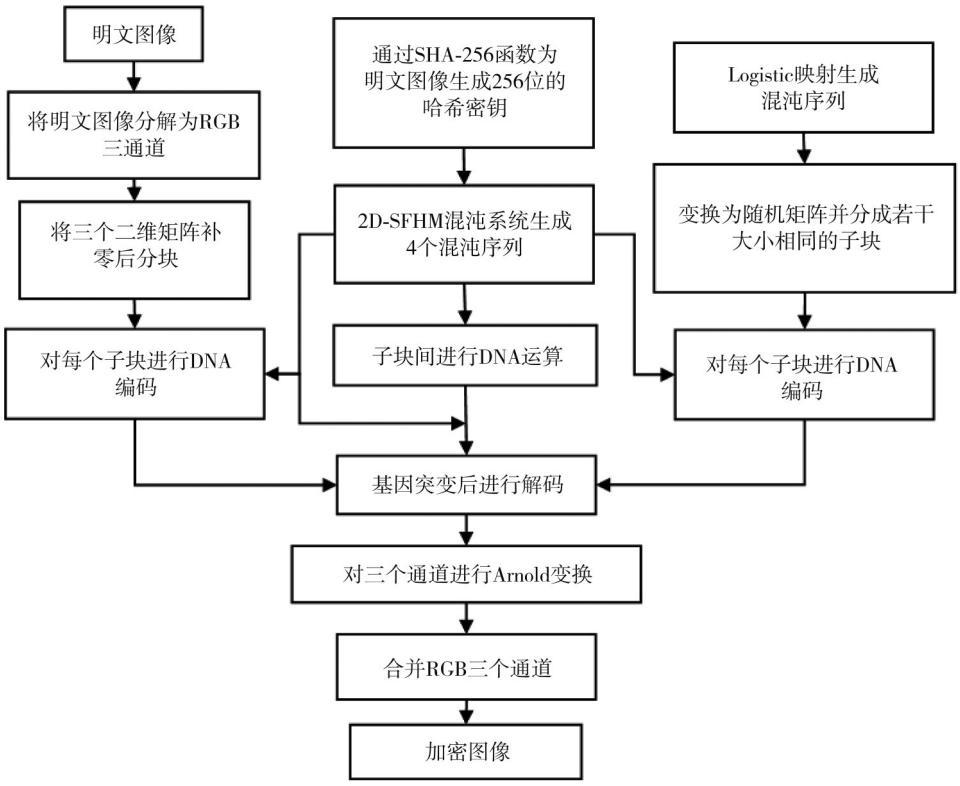



图 5 加密算法流程图

Fig. 5 Encryption algorithm flowchart

**步骤 4** 设定参数$a$和$b$, 输入初值$X_0$, $Y_0$, $Z_0$, $H_0$, 利用2D-SFHM混沌系统进行迭代, 为了消除瞬态效应去掉前$M$个值后, 得到4个长度均为$M\times N/t^2$的序列$\{X_i\}$, $\{Y_i\}$, $\{Z_i\}$, $\{H_i\}$。参数$a$和$b$取值均设定为50, 初始值由明文图像的哈希密钥与外部密钥$t_1$, $t_2$, $t_3$, $t_4$得出。

$$\begin{cases}X_0=\left((t_1+t_2)/256(t_3+t_4)\right)\left(\left(k_1\oplus k_5\oplus k_9\oplus k_{13}\oplus k_{17}\oplus k_{21}\oplus k_{25}\oplus k_{29}\right)\bmod 1,\right.\\ Y_0=\left((t_2+t_3)/256(t_4+t_1)\right)\left(\left(k_2\oplus k_6\oplus k_{10}\&k_{14}\right)\oplus\left(k_{18}\oplus k_{22}\oplus k_{26}\&k_{30}\right)\right)\bmod 1,\\ Z_0=\left((t_3+t_4)/256(t_1+t_2)\right)\left(\left(k_3\oplus k_7\&k_{11}\oplus k_{15}\right)\middle|\left(k_{19}\oplus k_{23}\&k_{27}\oplus k_{31}\right)\right)\bmod 1,\\ H_0=\left((t_4+t_1)/256(t_2+t_3)\right)\left(k_4\oplus k_8\middle|k_{12}\oplus k_{16}\right)\oplus\left(k_{20}\oplus k_{24}\&k_{28}\oplus k_{32}\right)\bmod 1,\end{cases} \tag{8}$$

式中: $x\oplus y$, $x\,|\,y$, $x\&y$分别表示$x$与$y$的异或运算, 或运算和与运算; $x\bmod y$表示取模运算。

**步骤 5** DNA编码。以$\boldsymbol{I}_1$, $\boldsymbol{I}_2$, $\boldsymbol{I}_3$的顺序排序后依次进行DNA编码, 编码方式由$\{X_i\}$决定, $\{Y_i\}$决定$\boldsymbol{R}$矩阵的各子块DNA编码方式。

将序列$\{X_i\}$和序列$\{Y_i\}$的值通过式(9)转化为范围在1~8之间的整数, 由此来决定选用的加密规则。

$$\begin{cases}X_i'=mod\left(round(X_i\times 10^4), 8\right)+1,\\ Y_i'=mod\left(round(Y_i\times 10^4), 8\right)+1,\end{cases} \tag{9}$$

式中: $i=1, 2, \cdots, \dfrac{(M\times N)}{t^2}$, 转化后的序列$\{X_i'\}$, $\{Y_i'\}$的值为1~8之间的随机整数, 选用编码方式$X_i'$对$\boldsymbol{I}_1$、$\boldsymbol{I}_2$、$\boldsymbol{I}_3$中第$i$个子块进行编码, 选用编码方式$Y_i'$对混沌矩阵$\boldsymbol{R}$中第$i$个子块进行编码。

**步骤 6**　为了减小运算复杂度，对$I_1$、$I_2$、$I_3$与$R$对应块之间采用同一种运算法则，选取的运算法则由2D-SFHM混沌系统生成的序列$\{Z_i'\}$决定。具体运算法则如式（10）所示。

$$Z_i' = mod\left(round(Z_i \times 10^4),\ 4\right)。\tag{10}$$

规定：$Z_i'=0$对应加法运算；$Z_i'=1$对应减法运算；$Z_i'=2$对应异或运算；$Z_i'=3$对应同或运算。

**步骤 7**　为了进一步扩大密钥空间，增强图像加密的安全性，在动态DNA编码的基础上加入了基因突变算法，通过2D-SFHM混沌系统生成的序列$\{H_i\}$控制编码后DNA序列发生突变的位置以及突变的规则，具体运算法则由式（11）决定。

$$\begin{cases} P_i = \sum round(H_i \times 255), \\ V_i = mod\left(round(P_i \times 10^4),\ 4\right) + 1, \end{cases}\tag{11}$$

式中：$P_i$为发生第$i$次基因突变时的位置；$V_i$为第$i$处基因突变的突变规则，如表2所示。

**步骤 8**　由序列$\{H_i\}$决定解码规则，对经过DNA运算后的矩阵进行DNA解码，再通过逆过程将A，G，C，T解码成具体的数值。

**步骤 9**　对解码后的三通道进行Arnold变换，具体变换形式如式（12）。

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \bmod(N),\tag{12}$$

式中：$x$，$y$为需要加密图像的像素坐标；$x'$，$y'$为加密后图像的像素坐标；$N$为图像的边长。

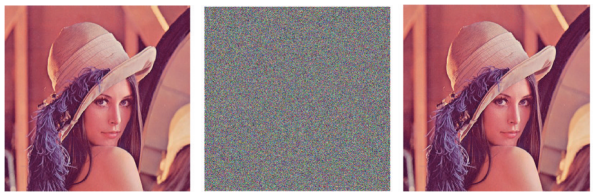
**步骤 10**　将置乱后的三通道合并得到密文图像。

## 3　仿真实验及安全性分析

本文在16 GB内存、2.50 GHz CPU的Windows11操作系统下，MatlabR2023a工具中对该算法进行仿真验证，其中图像的分块大小取为4×4，其他参数与上述加解密步骤中所选参数相同。

### 3.1　单幅图像的实验结果

本节以大小为512×512的彩色数字图像“Lena”为例作为待加密图片验证该算法的有效性。图6为明文图像“Lena”通过本文所提算法得到的密文图像和解密图像。从图6视觉角度上看，密文图像与明文图像无任何关联。



（a）明文图像　（b）密文图像　（c）解密图像

图6　本文算法的实验结果

Fig. 6　Experimental results of the algorithm in this paper

#### 3.1.1　直方图分析

图7分别为图像“Lena”的明文图像和密文图像的R，G，B通道像素直方图，其中第1行为明文图像的R，G，B通道像素直方图，第2行为密文图像的R，G，B通道像素直方图。

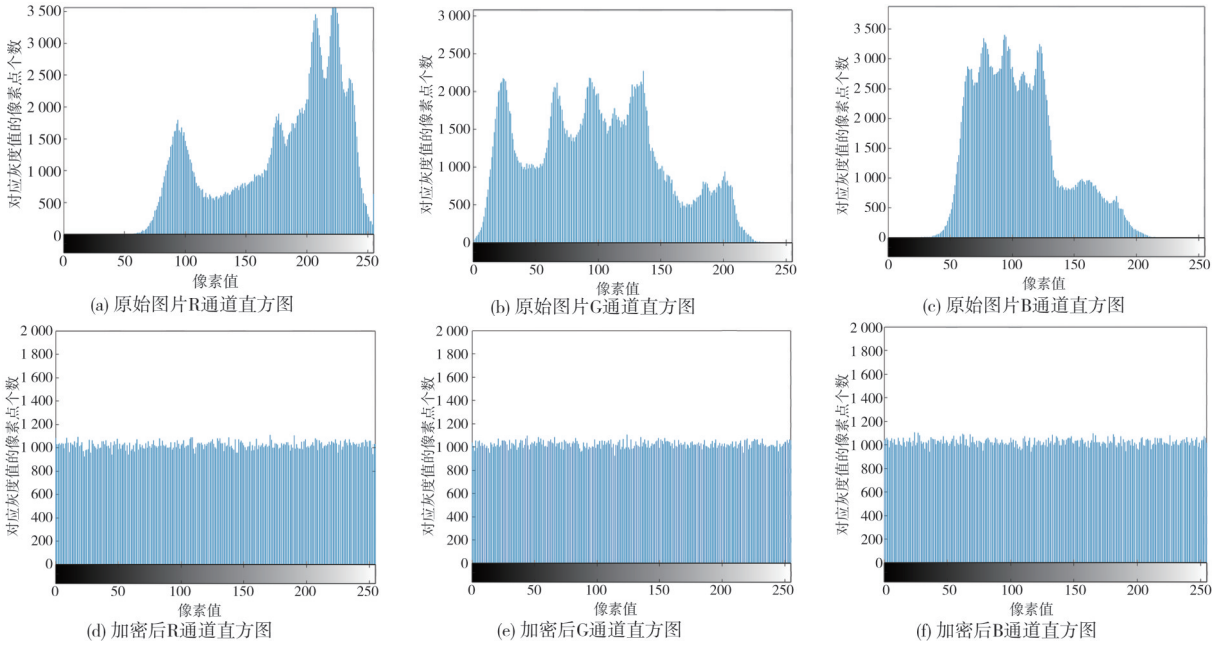



图7　原始图像和密文图像的R，G，B通道像素直方图

Fig. 7　Histograms of R, G, B channel pixels for raw images and ciphertext images

根据图 7 显示的结果，密文图像的3个通道直方图相比于明文图像分布更加均匀，表现出更强的伪随机性。这种特性使得其可以隐藏明文图像的统计特征，有效地抵御基于直方图统计的大规模图像攻击[19]。

### 3.1.2 相邻像素相关性

图像加密算法的有效性部分体现在消除明文图像像素间的高度相关性上，这是破解密码图像的关键。一个出色的加密方法应能够有效地消除相邻像素之间的相关性，从而抵御各种非法的统计攻击手段[20]。图 8 为加密前后图像相邻位置数据值的相关性系数点图，其中横坐标为随机点位置的数据值，纵坐标为该随机点相邻位置的数据值，第1行为明文图像的R，G，B三通道的水平相邻位置数据值关联性，第2行为密文图像的R，G，B三通道的水平相邻位置数据值关联性。

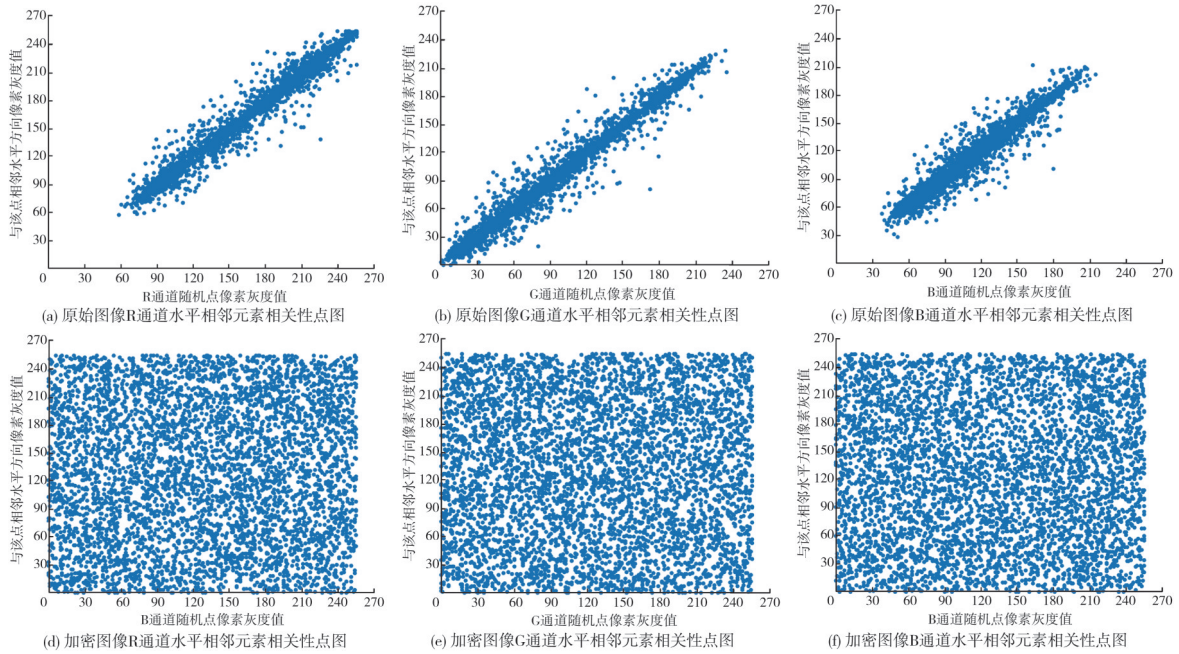



图 8 R，G，B 三通道加密前后水平相邻位置数据值关联性

Fig. 8 R, G, B three-channel encryption before and after horizontal adjacent location data value correlation

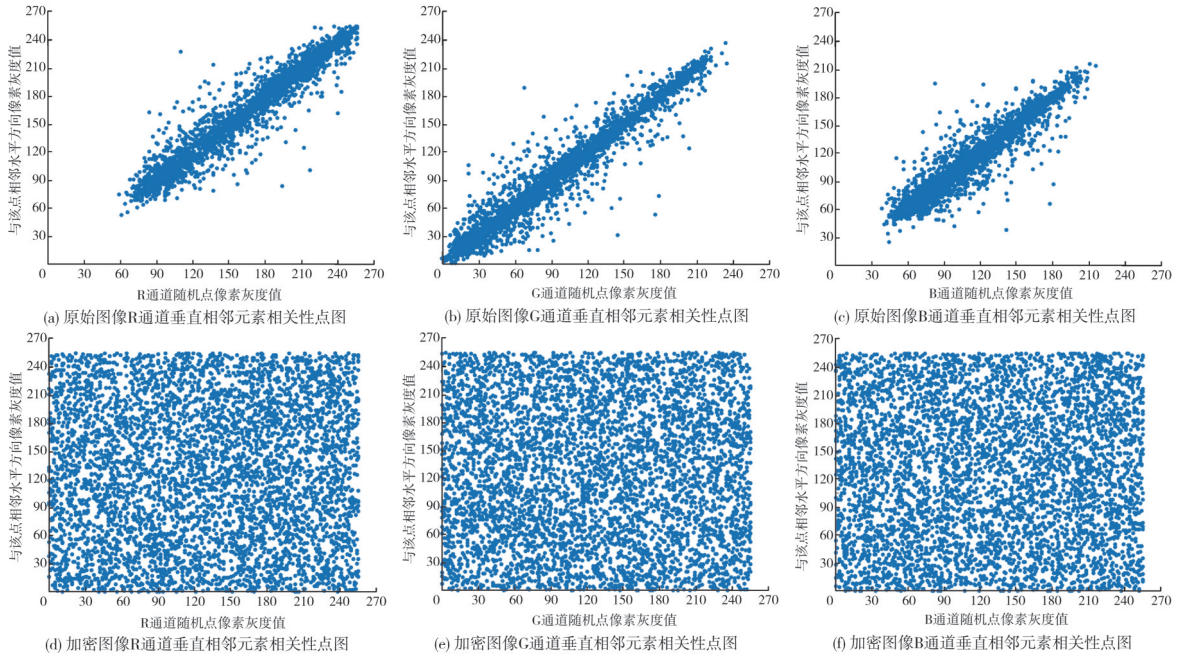



图 9 R，G，B 三通道加密前后垂直相邻位置数据值关联性

Fig. 9 R, G, B three-channel encryption before and after vertical adjacent location data value correlation

通过图 8 可以看出，数据点的分布呈线性关系，表明明文图像 3 个通道的水平相邻位置的数据值关联性很强。而密文图像的水平相邻位置数据值之间的关联性几乎为零，数据点分布完全随机。垂直与对角方向相关性同样满足此性质，如图 9 和图 10 所示。这充分说明此加密算法扩散与置乱效果较好，拥有较强的抗攻击能力。

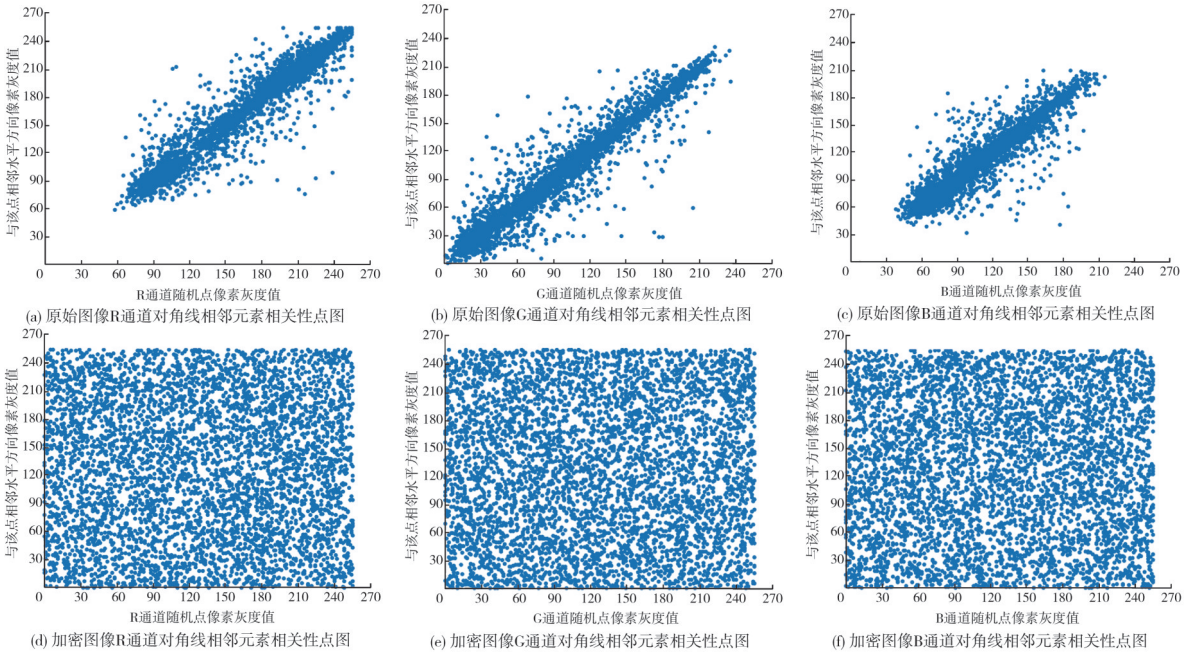



图 10　R，G，B 三通道加密前后对角线相邻位置数据值关联性

Fig. 10　Correlation of data values between diagonal adjacent locations before and after three-channel encryption

### 3.1.3　信息熵

信息熵（Information Entropy，IE）是衡量密码图像是否随机的一种定量度量[21]，定义为

$$IE(S_i)=-\sum_{J=1}^{L}Pr(J)\log_2 Pr(J), \quad (13)$$

式中：$L$ 为灰度值；$Pr(J)$ 为该灰度值的比例。加密图像的理论 $IE$ 值为 8。IE 趋近于 8 意味着密码图像的随机性更强，可以降低信息泄露的风险。

表 3 为本文算法与其他文献算法关于“Lena”图像进行加密后的信息熵结果比较。由表 3 可以看出，密文图像在 R，G，B 3 个通道的 $IE$ 值都非常接近于 8，意味着密码图像的随机性更强，可以降低信息泄露的风险。因此，本文提出的加密算法具有较高的安全性能和较低的信息泄露概率，足以抵御大多数攻击。同时本文算法在“Lena”图像的三通道的 $IE$ 值都达到了最大值，表明本文算法优于其他比较算法。

表 3　信息熵比较结果

Tab. 3　Compared the results of Information entropy

| | 信息熵 | | | | | |
|---|---|---|---|---|---|---|
| | 明文图像 | 本文算法 | 文献[8] | 文献[22] | 文献[23] | 文献[24] |
| R通道 | 7.268 2 | 7.999 4 | 7.999 3 | 7.999 3 | 7.999 3 | 7.989 5 |
| G通道 | 7.590 1 | 7.999 5 | 7.999 3 | 7.999 3 | 7.999 3 | 7.989 4 |
| B通道 | 6.995 1 | 7.999 4 | 7.999 4 | 7.999 3 | 7.999 3 | 7.989 4 |

### 3.1.4　密钥空间

本文所提算法的密钥如下：1）外部密钥 $t_1$，$t_2$，$t_3$，$t_4$；2）控制参数 $\mu$，$a$，$b$；3）SHA-256 函数生成的 256 位哈希值。在 Window11 操作系统下，每个密钥的精度为 $10^{-15}$，则本文密钥空间为 $(10^{15})^4\times(10^{15})^3=10^{105}>2^{350}$，远远大于 $2^{100}$。如果考虑 256 位哈希值，密钥空间可能更大，可以使暴力攻击无效。从表 4 可以看出，本文算法远优于比较算法。

表 4　不同算法的密钥空间比较

Tab. 4　Key space comparison of different algorithms

| | 本文算法 | 文献[25] | 文献[26] | 文献[27] | 文献[28] |
|---|---|---|---|---|---|
| 密钥空间 | $2^{350}$ | $2^{215}$ | $2^{256}$ | $2^{280}$ | $2^{270}$ |

### 3.1.5　密钥敏感性分析

密钥敏感性是指加密算法对密钥变化的敏感程度，密钥敏感性越强，意味着即使密钥发生微

小的改变，加密结果也会发生巨大的变化，无法推导出原始信息[29]。为检验本文算法的密钥敏感性，对密钥做微小改变，将密钥$\mu$由 3.999 9 改为 3.999 900 01，解密图像如图 11 所示。

(a) 密钥改变后解密图像 (b) 解密图像

图 11 初始值改变后解密图像

Fig. 11 Decrypted image after initial value change

可以看出，密钥的改动范围仅仅有 0.000 000 01 仍然无法看出其明文图像。说明此算法的密钥敏感性极强，并且其密钥数量很大，完全可以抵御穷举密钥进行的攻击。

### 3.1.6 差分攻击分析

差分攻击旨在测试算法对信息的敏感性。一个高效的加密算法应该对明文的细微变化高度敏感，即使是微小的明文变化也应该引起密文的巨大变动。算法抵抗差分攻击的能力由像素变化率(NPCR)和统一平均变化强度(UACI)表示[30]。根据不同大小图像对应的理论临界值，表 5 所示本文算法的 NPCR 和 UACI 均在有效范围内，表明该算法可以有效抵御差分攻击。

表 5 明文图像抗差分攻击实验结果均值

Tab. 5 The mean experimental results of plaintext image anti-differential attack

| 参数 | 本文算法 | 文献[8] | 文献[31] | 文献[32] |
|---|---|---|---|---|
| NPCR/% | 99.612 | 99.603 | 89.415 | 99.606 |
| UACI/% | 33.546 | 33.552 | 33.398 | 33.446 |

### 3.1.7 鲁棒性

由于网络传输过程中会导致图像丢失部分信息，因此本节通过在密文图像中添加噪声来模拟在传输过程中受到的影响，并通过峰值信噪比(PSNR)和均方误差(MSE)两个指标对其进行结果分析。图 12 显示了在不同椒盐噪声影响下的 Lena 解密图，在噪声影响下，解密后的图像信息仍然可以进行分辨，表明本文所提算法具有一定的抗噪声性能。图 13 显示了 R，G，B 三通道加入椒盐噪声后的 MSE 与 PSNR 曲线图，表明在传输过程中，椒盐噪声强度较低的情况下，此加密算法可以抵御噪声的攻击，但在噪声很大的传输环境下，此加密算法会受到噪声较大影响。

(a) 椒盐噪声密度为0.05时 (b) 椒盐噪声密度为0.1时

(c) 椒盐噪声密度为0.15时 (d) 椒盐噪声密度为0.2时

图 12 加入椒盐噪声后的解密结果

Fig. 12 Decryption result after adding salt and pepper noise

### 3.1.8 时间复杂度分析

运行时间也是评估图像压缩和加密算法性能的重要指标[33]。加密过程主要由 7 个步骤组成：即初始参数的生成(如步骤 3 所示)、混沌系统的迭代(如步骤 4 所示)、DNA 编码(如步骤 5 所示)、DNA 运算(如步骤 6 所示)、基因突变(如步骤 7 所示)、DNA 解码(如步骤 8 所示)、Arnold 变换(如步骤 9 所示)。因此，解密过程包括混沌系统的迭代、逆 DNA 编码、逆 DNA 运算、基因突变还原、逆 DNA 解码、Arnold 反变换等。通过本文算法对 512×512 彩色 Lena 图像进行操作，并对加密过程与解密过程的时间消耗进行了测试。其中，加密过程用时约为 3.863 s，解密过程用时约为 7.098 s。当图像大小从 512×512 变化到 256×256 时，加密时间从 3.863 s 变化到 1.096 s，解密时间从 7.098 s 变化到 4.237 s。运行时间与其他算法的比较列于表 6。从该表中可以看出，本文算法运行时间更快，可以满足图像加密的实时性要求。

表 6 运行时间比较

Tab. 6 Comparison on running time.

| 图像 | 运行时间/s | | | |
|---|---|---|---|---|
| | 本文算法 | 文献[34] | 文献[35] | 文献[36] |
| Lena | 1.096 | 1.26 | 1.25 | >10 |

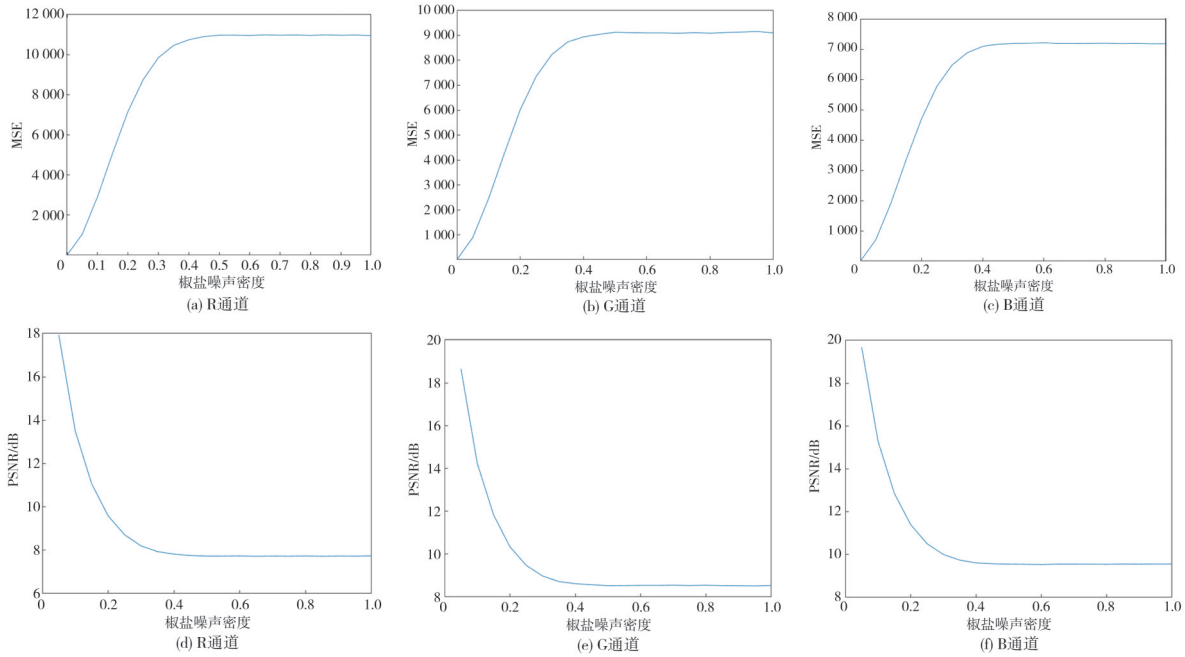



图 13　加入椒盐噪声后R，G，B 三通道的MSE与PSNR曲线图

Fig. 13　MSE and PSNR curves after adding salt and pepper noise to the R，G，and B channels

### 3.2　多幅图像的实验结果

为了直观地观测加密效果，本节对其他 4 幅图像分别进行仿真实验，结果如图 14 所示。

从图 14 中可以看出，密文图像像素值分布均匀，难以获得任何有效信息，并且本文算法为基于混沌系统与DNA 编码的无损加密，解密后图像与明文图像几乎不存在差别，因此，加密过程中可以完整保留所有图像信息，同时本文算法对于不同图像的加密都具有较好的性能。

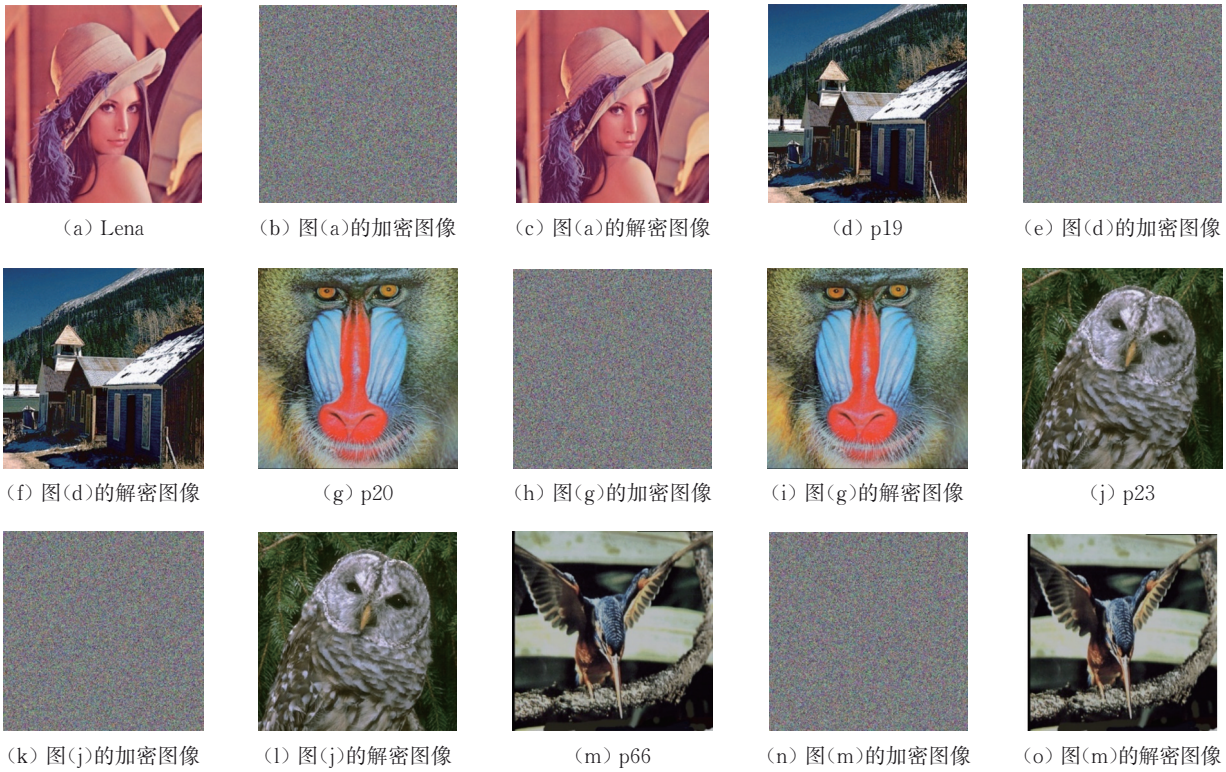



图 14　多幅图像的实验结果

Fig. 14　Experimental results of multiple images

## 4 结 论

本文提出了一种基于2D-SFHM混沌系统和改进DNA编码的彩色图像加密算法，该算法将彩色数字图像分为3个通道，再对每个通道分块进行DNA编码、解码和置乱，最后合并得到彩色加密图像。

通过仿真实验分析，本文加密算法的密文具有更加良好的像素相关性，所提算法的密钥空间足够大，并且密钥敏感性较高，可以抵抗穷举攻击。密钥空间复杂度满足加密所需条件的同时也保证了加密的效率。并且本文算法得到的密文图像在信息熵的表现上具有良好的性能。

**参考文献：**


[1] 陶云松，张丽红. 基于知识增强与注意力机制的双通道图像描述研究[J]. 测试技术学报，2021，35(1)：36-41.
TAO Yunsong，ZHANG Lihong. Research on two channel image description based on knowledge enhancement and attention mechanism[J]. Journal of Test and Measurement Technology，2021，35(1)：36-41.（in Chinese）

[2] 朱薇，杨庚，陈蕾，等. 基于小波变换和改进双随机相位编码的多图像加密算法[J]. 南京邮电大学学报(自然科学版)，2014，34(5)：87-92.
ZHU Wei，YANG Geng，CHEN Lei，et al. Multiple-image encryption based on wavelet transform and improved double random phase encoding[J]. Journal of Nanjing University of Posts and Telecommunications (Natural Science)，2014，34(5)：87-92.（in Chinese）

[3] PAN S M，WEN R H，ZHOU Z H，et al. Optical multi-image encryption scheme based on discrete cosine transform and nonlinear fractional Mellin transform[J]. Multimedia Tools and Applications，2017，76(2)：2933-2953.

[4] ZHU S，ZHU C. Secure image encryption algorithm based on hyperchaos and dynamic DNA coding[J]. Entropy，2020，22(7)：772.

[5] 张爱华，江中勤. 基于Logistic映射的混沌图像加密算法的改进[J]. 南京邮电大学学报(自然科学版)，2009，29(4)：69-73.
ZHANG Aihua，JIANG Zhongqin. Improving for chaotic image encryption algorithm based on logistic mapping[J]. Journal of Nanjing University of Posts and Telecommunications (Natural Science Edition)，2009，29(4)：69-73.（in Chinese）

[6] 方鹏飞，黄陆光，娄苗苗，等. 基于四维超混沌系统的彩色图像加密算法[J]. 计算机工程与设计，2022，43(2)：361-369.
FANG Pengfei，HUANG Luguang，LOU Miaomiao，et al. Color image encryption algorithm based on four dimensional hyper chaotic system[J]. Computer Engineering and Design，2022，43(2)：361-369.（in Chinese）

[7] WANG X，GAO S. Image encryption algorithm for synchronously updating Boolean networks based on matrix semi-tensor product theory[J]. Information Sciences，2020，507：16-36.

[8] 赵桥，李博，项融融. 基于混沌系统和动态DNA编码的彩色图像加密算法[J]. 计算机测量与控制，2024，32(3)：319-326.
ZHAO Qiao，LI Bo，XIANG Rongrong. Color image encryption algorithm based on chaos system and dynamic DNA encoding[J]. Computer Measurement & Control，2024，32(3)：319-326.（in Chinese）

[9] PAK C，HUANG L. A new color image encryption using combination of the 1D chaotic map[J]. Signal Processing，2017，138：129-137.

[10] PAK C，AN K，JANG P，et al. A novel bit-level color image encryption using improved 1D chaotic map[J]. Multimedia Tools and Applications，2019，78(9)：12027-12042.

[11] GAN Z H，CHAI X L，HAN D J，et al. A chaotic image encryption algorithm based on 3-D bit-plane permutation[J]. Neural Computing and Applications，2019，31(11)：7111-7130.

[12] GONG L，QIU K，DENG C，et al. An image compression and encryption algorithm based on chaotic system and compressive sensing[J]. Optics & Laser Technology，2019，115：257-267.

[13] 谢涛. Logistic映射在密码学中的应用研究[D]. 湘潭：湘潭大学，2014.

[14] NOSRATI K，SHAFIEE M. Fractional-order singular logistic map：stability，bifurcation and chaos analysis[J]. Chaos，Solitons & Fractals，2018，115：224-238.

[15] 武剀. 对经典logistic映射图像的加密方案的改进及数字图像的双混沌加密技术探究[D]. 乌鲁木齐：新疆财经大学，2016.

[16] 李玲，王伟男，李津杰，等. 基于Logistic映射和超混沌的自适应图像加密算法[J]. 微电子学与计算机，2012，29(1)：42-46.

LI Ling, WANG Weinan, LI Jinjie, et al. Self-adaptive image encryption algorithm based on logistic map and hyper-chaos[J]. Microelectronics & Computer, 2012, 29(1): 42-46. (in Chinese)

[17] 张璐. 基于云PACS的医学图像压缩加密技术研究[D]. 长春: 长春理工大学, 2022.

[18] CHAI X, ZHI X, GAN Z, et al. Combining improved genetic algorithm and matrix semi-tensor product (STP) in color image encryption[J]. Signal Processing, 2021, 183: 108041.

[19] 张艳鹏, 侯冬梅, 杨倩, 等. 基于混沌同步技术的图像加密算法设计研究[J]. 现代电子技术, 2021, 44(19): 39-42.
ZHANG Yanpeng, HOU Dongmei, YANG Qian, et al. Research on image encryption algorithm design based on chaos synchronization technology[J]. Modern Electronics Technique, 2021, 44(19): 39-42. (in Chinese)

[20] ZHANG X, HU Y. Multiple-image encryption algorithm based on the 3D scrambling model and dynamic DNA coding[J]. Optics & Laser Technology, 2021, 141: 107073.

[21] WANG X, GAO S. Image encryption algorithm based on the matrix semi-tensor product with a compound secret key produced by a Boolean network[J]. Information Sciences, 2020, 539: 195-214.

[22] HUA Z, JIN F, XU B, et al. 2D Logistic-Sine-coupling map for image encryption[J]. Signal Processing, 2018, 149: 148-161.

[23] WU X, KURTHS J, KAN H. A robust and lossless DNA encryption scheme for color images[J]. Multimedia Tools and Applications, 2018, 77(10): 12349-12376.

[24] CHAI X, WU H, GAN Z, et al. Hiding cipher-images generated by 2-D compressive sensing with a multi-embedding strategy [J]. Signal Processing, 2020, 171: 107525.

[25] ZHAO C F, REN H P. Image encryption based on hyper-chaotic multi-attractors[J]. Nonlinear Dynamics, 2020, 100(1): 679-698.

[26] PATRO K A K, SONI A, NETAM P K, et al. Multiple grayscale image encryption using cross-coupled chaotic maps[J]. Journal of Information Security and Applications, 2020, 52: 102470.

[27] LIU X, SONG Y, JIANG G P. Hierarchical bit-level image encryption based on chaotic map and feistel network [J]. International Journal of Bifurcation and Chaos, 2019, 29(2): 1950016-9.

[28] LIU S, GUO C, SHERIDAN J T. A review of optical image encryption techniques[J]. Optics & Laser Technology, 2014, 57: 327-342.

[29] HUANG L, CAI S, XIONG X, et al. On symmetric color image encryption system with permutation-diffusion simultaneous operation [J]. Optics and Lasers in Engineering, 2019, 115: 7-20.

[30] KUMARI M, GUPTA S, SARDANA P. A survey of image encryption algorithms [J]. 3D Research, 2017, 8(4): 37.

[31] HUA Z, ZHOU Y. Image encryption using 2D Logistic-adjusted-Sine map[J]. Information Sciences, 2016, 339: 237-253.

[32] EL ASSAD S, FARAJALLAH M. A new chaos-based image encryption system[J]. Signal Processing: Image Communication, 2016, 41: 144-157.

[33] CHAI X, FU X, GAN Z, et al. A color image cryptosystem based on dynamic DNA encryption and chaos [J]. Signal Processing, 2019, 155: 44-62.

[34] ZHANG M, TONG X. A new chaotic map based image encryption schemes for several image formats [J]. Journal of Systems and Software, 2014, 98: 140-154.

[35] WU X, LI Y, KURTHS J. A new color image encryption scheme using CML and a fractional-order chaotic system [J]. PLoS One, 2015, 10 (3): e0119660.

[36] YE R. A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism[J]. Optics Communications, 2011, 284(22): 5290-5298.