Computer Science and Application 计算机科学与应用, 2025, 15(9), 202-216
Published Online September 2025 in Hans. https://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2025.159238

Hans汉斯

基于超混沌系统和动态DNA编码的图像加密

邓一灵，姑丽加玛丽·麦麦提艾力

新疆师范大学数学科学学院，新疆 乌鲁木齐

收稿日期：2025年8月10日；录用日期：2025年9月9日；发布日期：2025年9月17日

摘　要

基于混沌系统和DNA编码相结合的图像加密是目前研究的热点。针对传统低维混沌系统存在复杂度有限、安全性不足等问题，本文提出一种将超混沌系统和动态DNA编码相结合的彩色图像加密算法。首先，利用明文的哈希值构造混沌系统的初始密钥；然后，通过四维和五维超混沌系统生成的多个混沌序列，对图像像素进行选择、扩散和重组操作。其中，四维混沌系统生成的混沌序列使DNA编码规则动态化，不同的像素值实时选择DNA碱基运算方式；五维混沌系统生成的混沌序列则与DNA编码共同用于图像灰度值的置乱。接着，两个混沌系统生成的混沌序列分别作用于DNA域和像素域，进而完成双重扩散，最后实现图像的加密。根据图像加密的逆过程，可得到解密后的图像。经过实验验证，该算法密钥空间大，复杂度较高，加密效果好。

关键词

超混沌系统，图像加密，置乱扩散，动态DNA编码

Image Encryption Based on Hyperchaotic Systems and Dynamic DNA Coding

Yiling Deng, Gulijiamali Maimaiti Aili

School of Mathematical Sciences, Xinjiang Normal University, Urumqi Xinjiang

Received: Aug. 10th, 2025; accepted: Sep. 9th, 2025; published: Sep. 17th, 2025

Abstract

Image encryption based on the combination of chaotic systems and DNA coding is a current research hotspot. To address the limited complexity and insufficient security of traditional low-dimensional chaotic systems, this paper proposes a color image encryption algorithm that combines hyperchaotic systems with dynamic DNA coding. First, the initial key of the chaotic system is constructed using the hash value of the plaintext. Then, image pixels are selected, diffused, and reassembled using

文章引用: 邓一灵, 姑丽加玛丽·麦麦提艾力. 基于超混沌系统和动态 DNA 编码的图像加密[J]. 计算机科学与应用, 2025, 15(9): 202-216. DOI: 10.12677/csa.2025.159238

multiple chaotic sequences generated by four-dimensional and five-dimensional hyperchaotic systems. The chaotic sequence generated by the four-dimensional chaotic system makes the DNA coding rules dynamic, allowing different pixel values to select DNA base operations in real time. The chaotic sequence generated by the five-dimensional chaotic system is used together with the DNA coding to scramble the image grayscale values. Next, the chaotic sequences generated by the two chaotic systems act on the DNA domain and the pixel domain, respectively, completing double diffusion and ultimately achieving image encryption. The decrypted image is obtained by inversely following the image encryption process. Experimental verification shows that the algorithm has a large key space, high complexity, and good encryption performance.

Keywords

Hyperchaotic System, Image Encryption, Scrambling Diffusion, Dynamic DNA Encoding

1. 引言

随着社会的不断发展，云计算、大数据和人工智能等技术已深入到城市生活的方方面面，而信息安全则成为这些新技术顺利应用的基础[1]。在享受技术进步带来的便利的同时，人们也面临着信息盗窃和隐私泄露的风险。在这些新技术的应用中，数字图像因其直观性强、信息量大而被广泛传输和存储在各种网络和设备上。图像加密作为信息安全的重要手段，已被广泛应用于多媒体系统、卫星遥感、军事通信、互联网传输和医学图像等领域[2]。目前，已有多种图像加密技术被提出。其中，传统加密算法如 RSA、DES、3DES 及 AES [3]在处理图像时存在一定局限性，例如加密速度较慢、图像加密后视觉效果不足、依赖固定块处理结构，难以满足现实应用中对大尺寸图像的高速、高质量加密需求[4]。为克服这些问题，研究者提出了基于混沌系统的图像加密方法。混沌系统具有高度的随机性与初值敏感性，能够生成遍历性强的密钥序列，因而更适合用于图像的快速、无损且高安全性的加密处理[5]。近年来，基于混沌映射的加密方案已经成为密码学及图像安全领域的主流研究方向之一。混沌系统通常分为一维混沌系统和高维混沌系统[6]。文献[7]将 Logistic 映射和正弦映射相结合，提出一种新的改进的一维正弦混沌系统，有效增强了混沌序列的复杂性与随机性。文献[8]提出一种新的分数阶一维混沌映射，在广泛参数区间内表现出强混沌性，适用于实时图像加密与通信，并在密码学中不受暴力攻击。为进一步提升系统性能，文献[9]设计了一种具有优良混沌特征的二维混沌模型，解决现有混沌映射中混沌轨迹分布不均和混沌范围有限的问题。早在 1963 年，Lorenz 在分析蝴蝶效应时首次利用三维非线性常微分方程构建了 Lorenz 混沌系统，用于描述天气系统对初始条件的敏感依赖[10] [11]。2007 年王等在三维 Lorenz 系统基础上，设计了一种四维超混沌 Lorenz 系统[12]，其混沌特性更为复杂。此后，贾和陈等学者又设计了多种改进型的四维 Lorenz 系统[13] [14]，进一步拓展了其在图像加密中的应用。文献[15]通过在传统 Lorenz 系统中引入两个控制器，构建了一种新的五维多带多翼混沌系统，具有更强的混沌行为和密钥生成能力。高维混沌系统相较于低维系统在计算复杂度、安全性和密钥空间等方面具有显著优势，因此成为图像加密研究的一个重要方向。然而，一些文献仍存在混沌性能不强、密钥空间较小、加密图像扩散性不足等问题。针对上述问题。本文提出一种新型混沌图像加密方案，通过融合多个高维超混沌系统对图像进行加密。首先，利用四维超混沌系统生成的混沌序列构造密钥矩阵、规则矩阵、动态运算规则矩阵以及规则编号

矩阵。在密钥矩阵与规则矩阵的作用下，将图像像素值映射为对应的 DNA 碱基对，并通过五维混沌系统生成的混沌序列结合规则矩阵实现碱基之间的置乱操作。随后，利用四维超混沌系统和五维超混沌系统生成的混沌序列，结合动态运算规则，对图像在 DNA 域和像素域上分别进行扩散处理，从而完成双重扩散，最终实现图像加密。该方法通过将多维混沌系统与 DNA 编码策略有机结合，使加密过程更具复杂性和随机性，显著提升了图像加密的安全性。多维混沌系统带来的大密钥空间和强抗攻击能力，为高效、安全的图像保护提供了有力支持。

2. 基本理论

2.1. 安全哈希算法(SHA-256)

哈希函数在信息安全领域发挥着重要作用，不仅能够保障数据完整性，还可结合数字签名和消息认证码(MAC)算法，实现身份认证等安全服务。其中，SHA-256 作为一种广泛应用的密码学哈希函数，能够生成固定长度为 256 位的二进制哈希值，通常以 64 位十六进制字符串的形式表示。研究表明，该算法具有显著的雪崩效应，即使输入数据仅发生单个像素的微小变化，生成的哈希值也会出现明显差异。在本文提出的方案中，256 位的外部密钥 K 被表示为包含 8 个十进制整数的数组，每个整数对应一个 32 位的分段密钥(因为 8 个十六进制字符等价于 32 位二进制)，从而得到 8 个 32 位的分段密钥，记为 K_i，其中 i = 1, 2, ..., 8。

2.2. 扩散原理

扩散是指在加密的过程中，图像像素的位置保持不变，通过一定的规则改变像素的数值，将明文图像的信息隐藏在密文图像中，从而达到混淆效果。常见的扩散算法包括基于异或(XOR)操作和加取模运算的算法。异或运算能够有效改变图像的像素值，从而隐藏图像中的有效信息，这种改变通常可以通过直方图分析显现。在本文扩散操作中，我们采用将混沌序列与扩散相结合的方法，将原始图像像素与混沌序列值进行异或运算，以实现对图像像素值的隐藏和保护。

2.3. DNA 序列编码

在生物学中，DNA 是由四种脱氧核苷酸组成的长链分子，四种脱氧核苷酸分别为腺嘌呤(A)、胞嘧啶(C)、鸟嘌呤(G)和胸腺嘧啶(T)。根据 DNA 碱基互补配对规律，A 与 T 互补配对，G 与 C 互补配对。由于二进制系统中的“0”和“1”具有互补关系，因此可以将 DNA 碱基对与二进制编码相对应。表 1 为 DNA 碱基之间互补规则的 8 种编码方式。

Table 1. 8 encoding methods of DNA
表 1. DNA 的 8 种编码方式

		1	2	3	4	5	6	7	8
DNA 编解码方式	A	00	00	01	01	10	10	11	11
	G	01	10	00	11	00	11	01	10
	T	11	11	10	10	01	01	00	00
	C	10	01	11	00	11	00	10	01

3. 超混沌系统

3.1. 四维超混沌系统

1994 年，Sprott 构建了 19 个不同的简单三维混沌系统，这些系统均包含两个二次非线性元和五个

项。其中，混沌 Sprott-B 系统可由以下常微分方程(1)表示：

$$\begin{cases} \dot{x} = ayz \\ \dot{y} = b(x-y) \\ \dot{z} = c - xy \end{cases} \tag{1}$$

在三阶 Sprott-B 混沌系统的基础上，引入忆阻器可构建一个四阶超混沌忆阻器系统。根据忆阻器理论，一个广义的压控忆阻器可由式(2)表示为：

$$\begin{cases} i = W(x)v \\ \dfrac{dx}{dt} = f(x,v) \end{cases} \tag{2}$$

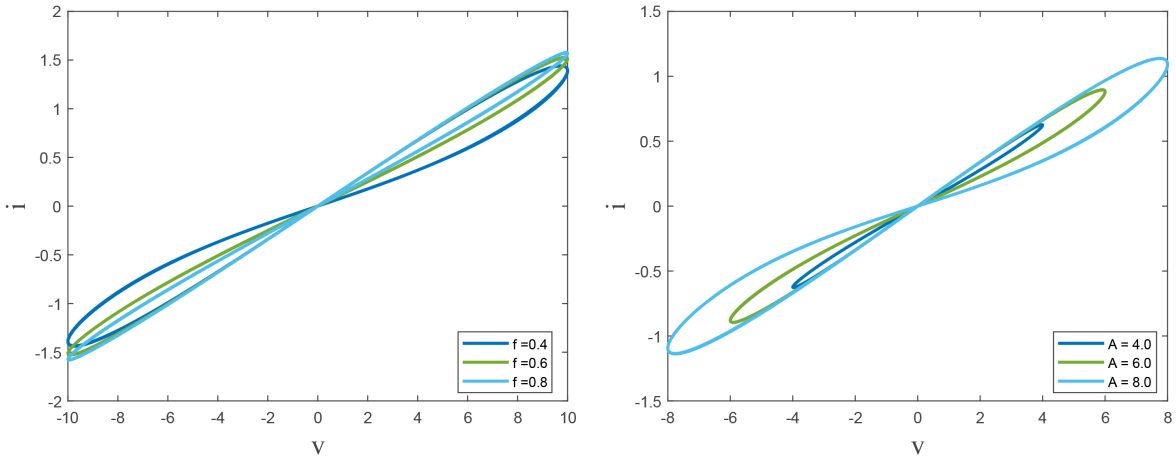
其中，$W(x)$ 为忆导，是一个以状态变量 x 为自变量的连续函数；v 为施加在忆阻器两端的输入电压；i 为流经忆阻器的电流；x 为忆阻器的内部状态变量。由该表达式可知，一个新的广义压控忆阻器可由式(3)表示为：

$$\begin{cases} i = \left(0.3e^{-x} - \tan x\right)v \\ \dfrac{dx}{dt} = (1-\cos x)v \end{cases} \tag{3}$$

其中，为磁通量，$\tan(\cdot)$ 为正切函数。

对该忆阻器在不同激励信号幅度与频率下的伏－安(V－I)特性曲线进行分析。

在新的忆阻器两端施加周期激励信号 v = Asin(2πft)，其中 A 为幅值，f 为频率，t 为时间。当固定 A = 10 时并改变频率 f 时，所得伏－安特性曲线如图 1(a)所示。可以观察到，随着频率 f 的增大，忆阻器的滞回曲线面积逐渐减小，最终趋近于一条直线。当固定频率 f = 0.6 时并改变幅值 A 时，对应的伏－安特性曲线如图 1(b)所示。结果显示，随着幅值 A 的增大，滞回曲线的面积明显增大，且曲线均通过原点。由此可见，该模型满足忆阻器的基本特性。



(a) A = 10 时，不同 f 下的滞回曲线　　(b) f = 0.6 时，不同 A 下的滞回曲线

Figure 1. Input signal frequency/amplitude dependent volt-ampere characteristic curve
图 1. 输入信号频率/振幅相关的伏－安特性曲线

结合混沌 Sprott B 系统和新的忆阻器，我们得到新的四阶超混沌忆阻系统如式(4)所示：

$$\begin{cases} \dot{x} = ayz + kW(u)z \\ \dot{y} = b(x - y) + cu^2 \\ \dot{z} = 1 - xy + du \\ \dot{u} = (1 - \cos u)z \end{cases} \tag{4}$$

其中参数 a = 1，b = 1，c = 7，d = 1.2，k = 0.1，初始值选为(0.1, 0.1, 0.1, 0.1)时，该系统产生的相图如图 2 所示。

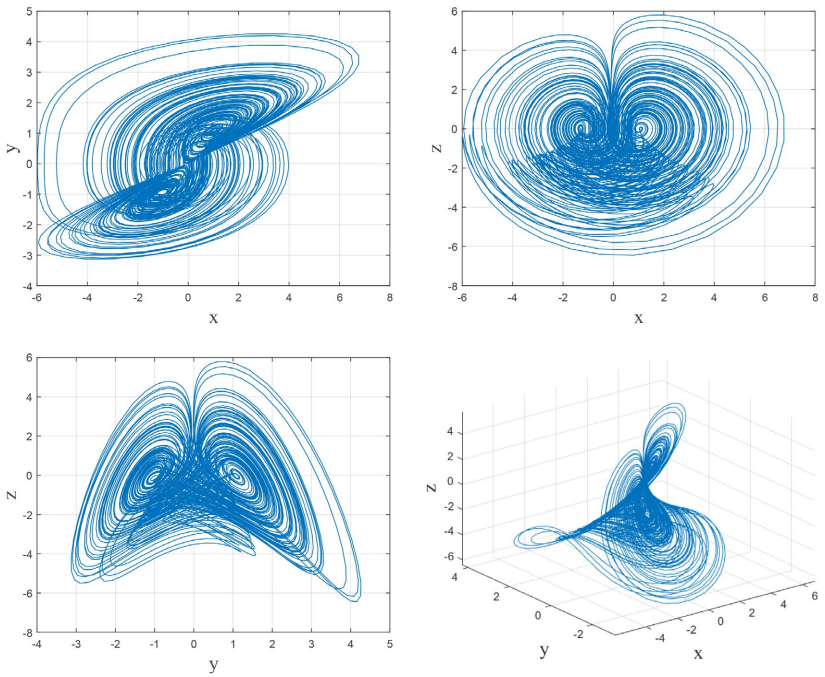


Figure 2. Phase diagram of a four-dimensional hyperchaotic system
图 2. 四维超混沌系统相图

其中，该系统的 Lyapunov 指数谱如图 3 所示，其 Lyapunov 指数分别为 LE1 = 0.21358，LE2 = 0.10165，LE3 = 0.01670，LE4 = −1.21400，有三个状态变量的 Lyapunov 指数大于 0，因此该系统为超混沌系统。

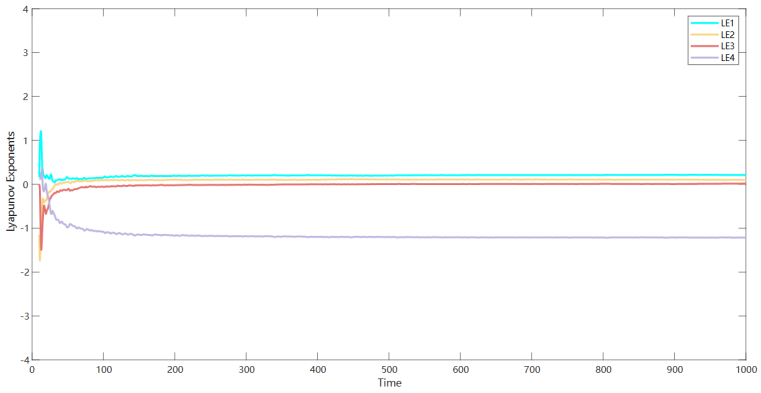


Figure 3. Lyapunov exponent spectrum
图 3. Lyapunov 指数谱

李雅普诺夫指数是衡量混沌系统对初始条件敏感性的重要指标。当最大李雅普诺夫指数(MLE)大于零时，系统对初始微扰呈指数级放大，表现出混沌特性；若所有指数均小于零，则系统稳定，轨迹趋于收敛。此外，李雅普诺夫指数之和反映系统相空间体积的演化趋势：耗散系统该值为负，混沌吸引子至少存在一个正值。通过分析其分布，可评估系统的可预测性与复杂度。对所研究的四维混沌系统进行李雅普诺夫指数计算，结果分别为：LE1 = 0.21358，LE2 = 0.10165，LE3 = 0.01670，LE4 = −1.21400。由于该系统存在三个正的李雅普诺夫指数，故可判定其为超混沌系统。同时，引入 Lyapunov 维数 D_L (又称 Kaplan-Yorke 维数)，该概念由 Kaplan 和 Yorke 首次提出，用以估算系统吸引子的分形维数。系统(2)的 Lyapunov 维数计算如式(5)所示：

$$d_L = r + \frac{1}{\left|LE_{r+1}\right|}\sum_{k=1}^{r} LE_k = 3 + \frac{LE_1 + LE_2 + LE_3}{\left|LE_4\right|} \approx 3.2734 \tag{5}$$

其中，由于 Lyapunov 维数是大于 3 的非整数，则系统具有非周期性运动轨迹。

3.2. 五维超混沌系统

文献[16] Lorenz 于 1963 年提出了著名的三维经典混沌模型。Lorenz 系统作为一个连续动力系统，自提出以来受到了广泛的关注和极大的发展，其具体微分方程组如式(6)所示：

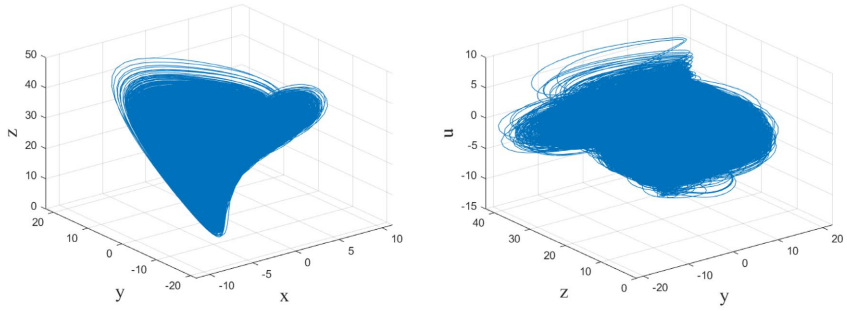
$$\begin{cases} \dot{x} = a(y - x) \\ \dot{y} = bx - zx - y \\ \dot{z} = xy - cz \end{cases} \tag{6}$$

其中，x、y、z 为状态变量。当参数 a = 10，b = 8/3，c = 28 时，该系统呈混沌状态。

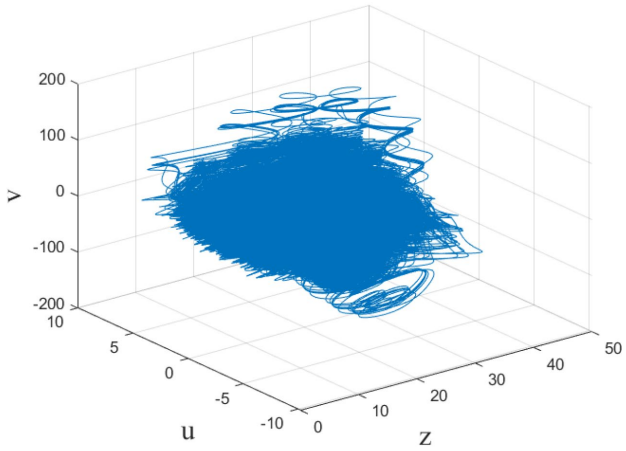
由于高维混沌系统相较于低维系统具有更加丰富的动力学特性，因而成为众多研究领域的关注焦点。本文基于爱德华·洛伦兹提出的经典三维混沌系统，向系统中引入两个新的状态变量和两个非线性项，将原三维系统扩展为五维系统[17]。该五维系统的具体形式如式(7)所示：

$$\begin{cases} \dot{x} = a(y - x) + u \\ \dot{y} = bx - cxz - v \\ \dot{z} = dx^2 - gz \\ \dot{u} = hyz \\ \dot{v} = kv + zu \end{cases} \tag{7}$$

其中，x、y、z、u、v 为状态变量；a，b，c，d，g，h，k 为系统参数且为正实数。当 a、b、c、d、g、h、k 系统参数分别为(10, 40, 3, 4, 2.5, 0.1, 0.2)时，初始条件取为(1, 1, 1, 1, 1)，系统(7)表现出超混沌行为。其对应的相图、Lyapunov 指数谱和分叉分别如图 4、图 5 所示。



(a) x-y-z 平面　　(b) y-z-u 平面



(c) z-u-v 平面

Figure 4. Phase diagram of five-dimensional hyperchaotic image
图 4. 五维超混沌图像的相图

由图 4 可以看出该系统具有很强的随机性，混沌性。

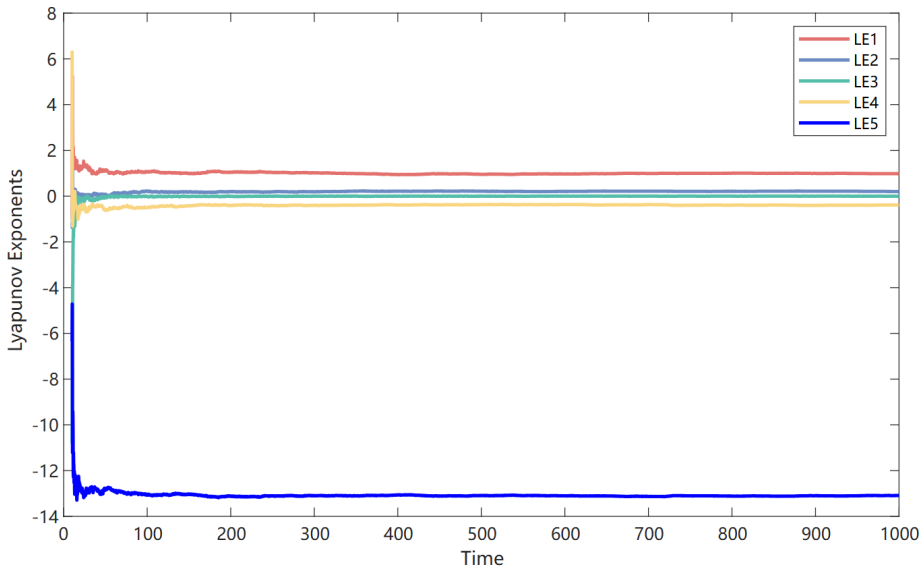


Figure 5. Lyapunov exponent spectrum of the five-dimensional hyperchaotic image
图 5. 五维超混沌图像的 Lyapunov 指数谱

由图 5 可知，可以得到三个正 Lyapunov 指数，该系统呈现出超混沌状态。

由式(7)可知，当 a = 10，b = 40，c = 3，d = 4，g = 2.5 ，h = 0.1，k = 0.2 时，系统求解得出 4 个 Lyapunov 指数值且 Lyapunov 维数是大于 4 的非整数，则系统具有非周期性运动轨迹。由此可知，系统(7)正处于超混沌状态。

4. 图像加密方案

图像加密方案包含一轮置乱、两轮扩散，两轮扩散包括 DNA 域内的扩散以及像素域内扩散，图像加解密方案整体结构示意图如图 6 所示。

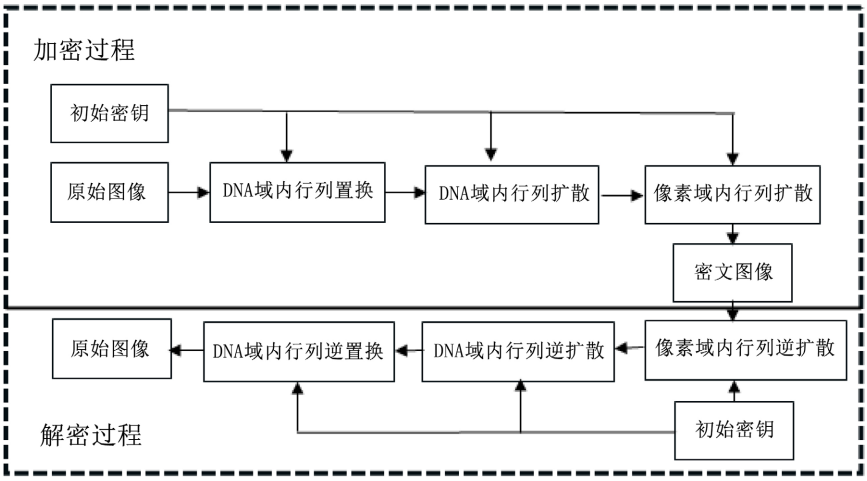


Figure 6. Schematic diagram of the overall structure of the image encryption and decryption solution
图 6. 图像加解密方案整体结构示意图

该方案将彩色数字图像分解为RGB三个二维矩阵，利用四维混沌系统生成的混沌序列动态调整DNA编码规则，实现不同像素值对应实时选择的DNA碱基运算方式；随后，基于五维混沌系统生成的混沌序列结合DNA编码对图像灰度值进行置乱。最后，将两个混沌系统生成的混沌序列在DNA域和像素域内分别进行双重扩散操作，完成加密后将三个通道合并，得到彩色加密图像。

解密过程首先是对加密图像分解为RGB三个二维矩阵，利用四维混沌系统生成的混沌序列动态调整DNA编码规则，实现不同像素值对应实时选择的DNA碱基运算方式；将两个混沌系统生成的混沌序列在像素域和DNA域内分别进行双重逆扩散操作，然后，基于五维混沌系统生成的混沌序列结合DNA编码对图像灰度值进行逆置乱，最后将解密后的三个通道合并，得到彩色解密图像。

4.1. 基于四维－五维混沌模型的图像加密算法

加密算法由DNA域内行列置乱、扩散以及像素域内扩散组成，其中的加密示意图如图7所示。

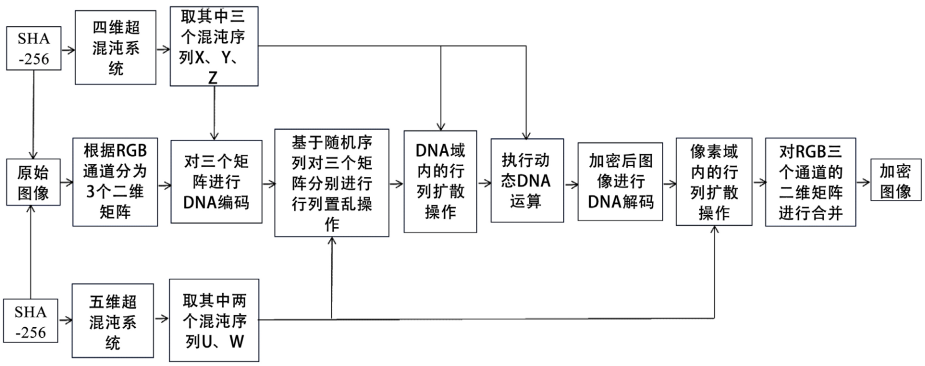


Figure 7. Schematic diagram of image encryption
图 7. 图像加密示意图

详细的加密步骤如下：

步骤一：给定一张M * N * 3的彩色图像P，其对应矩阵的大小的长度为M和宽度为N，将彩色图像P转换为灰度图像，三个通道的图像分别记为R、G和B。

步骤二：利用与彩色图像相关的哈希值构造两个混沌系统的初始值。利用 sha-256 计算得到与原始图像相关的 hash 值，将 hash 值分为 8 组，记为 $h=\{h_1,h_2,\cdots,h_8\}$，

$$\begin{cases} x_1=\mathrm{mod}\left(\dfrac{h'(1)+h'(2)}{h'(3)+h'(4)},1\right) \\ y_1=\mathrm{mod}\left(\dfrac{h'(2)+h'(3)}{h'(4)+h'(5)},1\right) \\ z_1=\mathrm{mod}\left(\dfrac{h'(4)+h'(5)}{h'(6)+h'(7)},1\right) \\ u_1=\mathrm{mod}\left(\dfrac{h'(6)+h'(7)}{h'(1)+h'(8)},1\right) \end{cases} \tag{8}$$

$$\begin{cases} x_2=\mathrm{mod}\left(\dfrac{h'(1)\times h'(5)+h'(2)\times h'(6)}{h'(4)\times h'(7)},1\right) \\ y_2=\mathrm{mod}\left(\dfrac{h'(8)\times h'(4)+h'(3)\times h'(1)}{h'(5)\times h'(3)},1\right) \\ z_2=\mathrm{mod}\left(\dfrac{h'(7)\times h'(1)+h'(8)\times h'(2)}{h'(1)\times h'(5)},1\right) \\ u_2=\mathrm{mod}\left(\dfrac{h'(6)\times h'(1)+h'(4)\times h'(3)}{h'(8)\times h'(2)},1\right) \\ w=\mathrm{mod}\left(\dfrac{h'(3)\times h'(7)+h'(5)\times h'(8)}{h'(6)\times h'(4)},1\right) \end{cases} \tag{9}$$

将 $h=\{h_1,h_2,\cdots,h_8\}$ 十六进制数转换为十进制，记得到的十进制数为 $h'=\{h_1',h_2',\cdots,h_8'\}$，通过公式(8)得到初始值 x1、y1、z1、u1 并且通过公式(9)得到初始值 x2、y2、z2、u2、w。之后，将得到的密钥和大小定向到四维和五维超混沌系统，分别迭代$(300+\max(M,N))$和$(700+\max(M,N))$次，去掉前 300 次和 700 次，以消除暂态效应，从而生成更加稳定和随机的混沌序列，分别得到四维混沌系统的四个混沌序列和五维混沌系统的五个混沌序列，取四维混沌系统的前三个混沌序列和五维混沌系统的后两个混沌序列，记为 X、Y、Z、U、W。

步骤三：通过式(8)和式(9)对 X、Y、Z、U、W 分别进行处理，通过式(10)得到序列 X_1，Y_1，Z_1，U_1，W_1。

$$\begin{cases} X_1=\mathrm{mod}\left(\mathrm{floor}\left(x*10^{14}\right),256\right) \\ Y_1=\mathrm{mod}\left(\mathrm{floor}\left(y*10^{14}\right),256\right) \\ Z_1=\mathrm{mod}\left(\mathrm{floor}\left(z*10^{14}\right),256\right) \\ U_1=\mathrm{mod}\left(\mathrm{floor}\left(u*10^{14}\right),256\right) \\ W_1=\mathrm{mod}\left(\mathrm{floor}\left(w*10^{14}\right),256\right) \end{cases} \tag{10}$$

步骤四：设置混沌序列 seq1 = X1(1:M * N)；seq2 = Y1(1:M * N)；seq3 = Z1；seq4 = U1(1:M + 4N)；seq5 = W1(1:4 * M * N)。

步骤五：其中，seq1 用于生成密钥矩阵 K；seq2 用于生成规则矩阵；seq3 用于生成动态运算规则。

步骤六：根据规则矩阵，将原始图像 P 中的像素值转换为对应的 DNA 碱基，得到碱基矩阵 P1。

步骤七：利用混沌序列 seq4 对碱基矩阵 P1 进行行列置乱，得到矩阵 P2。

步骤八：将 P2 与密钥矩阵 K 在 DNA 域内执行扩散操作，得到矩阵 P3。

步骤九：对 P3 进行动态 DNA 编码运算，得到矩阵 S。

步骤十：根据规则矩阵，对矩阵 S 进行 DNA 解码操作，转换成像素值矩阵 Q。

步骤十一：利用混沌序列 seq5 对矩阵 Q 进行最终扩散操作，包括行方向的链式模加和列方向的循环移位。

步骤十二：最后，合并加密后的 R、G、B 通道，输出加密后的彩色图像。

4.2. 解密算法

解密算法包括像素域内行列逆扩散、DNA 域内行列逆扩散以及 DNA 域内行列逆置乱。首先，将两个混沌系统生成的混沌序列在像素域和 DNA 域内分别进行双重逆扩散操作，然后，基于五维混沌系统生成的混沌序列结合 DNA 编码对图像灰度值进行逆置乱，最后得到彩色解密图像。

Figure 8. Digital image encryption and decryption experiment diagram
图 8. 数字图像加解密实验图

5. 实验仿真与测试

5.1. 实验结果

本节概述了在配备 2.40GHzCPU 和 16GBRAM 的 Windows11 操作系统平台上，基于软件 MatlabR2023b 仿真环境对提出的加密算法进行了性能评估。实验随机选择图像 Lena (512 × 512)、Pepper (512 × 512)作为测试样本。仿真结果表明，原始明文图像经过加密处理后转变为具有噪声特性的密文图像，在视觉上完全不可辨认。值得注意的是，当使用正确的密钥解密后，图像能够无损地恢复出与原始图像完全一致的视觉效果。本文随机选择 Lena (512 × 512)和 Pepper (512 × 512)两幅彩色图像进行测试，直观地验证了该加密算法的有效性和可靠性，加解密图像效果如图 8 所示。

5.2. 密钥空间分析

密钥空间指的是密码系统中所有有效且互不相同的密钥组成的集合，秘钥空间的大小决定了密码系统的安全性。密码系统的安全性与密钥空间的大小呈正相关。密钥空间越大，截获的密文越能抵御暴力

攻击，因为攻击者需要尝试所有可能的密钥组合来破解信息。在本文图像加密研究中，图像密码系统的密钥由九个初始值和十二个系统参数组成，这确保了即使采用暴力攻击手段，攻击者在有限时间内难以遍历整个密钥空间，从而确保加密系统的安全性。由于计算机准确度为10^{-15}，始密钥空间如式(11)所示。

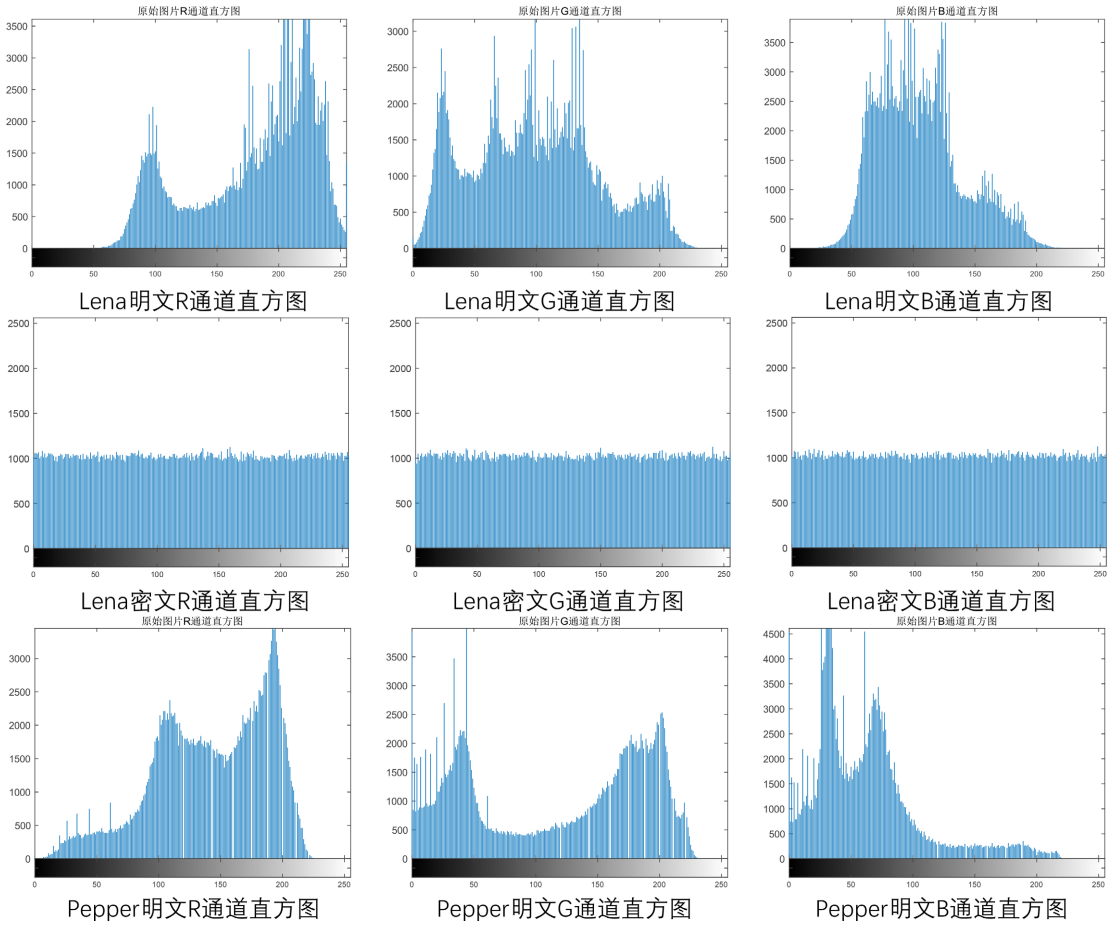
$$秘钥空间=\prod_{t=1}^{21}10_t^{15} \tag{11}$$

式(11)的结果为10^{315}，远大于2^{100}。对于安全的彩色图像加密算法，其密钥空间充足。因此，该系统的密钥空间足以挫败穷举攻击。

5.3. 直方图分析

密文图像的直方图反映了像素值的分布情况，是评估加密算法是否能抵抗统计分析攻击的一个重要指标。统计分析攻击指攻击者通过分析加密图像的统计特征，进而获取密钥信息或明文信息，从而实施选择性密文攻击。图中显示，密文图像的 R、G、B 三个通道的直方图均呈均匀分布，这表明加密后图像的统计特征被有效的成功隐藏，攻击者难以从中提取有用信息。由此，密文图像与明文图像在统计特征上存在显著差异，增强了算法抵抗统计攻击的能力。

本文选取了“Lena”和“Pepper”两幅不同图像进行加密实验，实验结果如图 9 所示。从结果可以看出，加密前的明文图像直方图呈现明显的不均匀分布，而加密后的图像直方图则趋于平坦，显示出较好的均匀性。



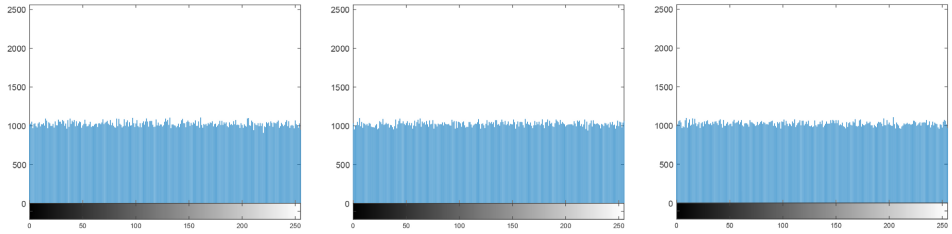


Figure 9. Comparison of histograms on each channel before and after image encryption
图 9. 图像加密前后在各个通道上的直方图对比

5.4. 信息熵分析

信息熵是衡量给定消息不确定性的重要指标。对于灰度图像，其理论最大值为 8。当信息熵越接近 8 时，表示图像的不确定性越强，像素的随机性越大，从而反映出其具有更好的加密效果。本文以 Lena 彩色图像作为实验对象，将本文图像加密后的信息熵与文献资料[18]-[20]加密后图像的信息熵进行对比，结果如表 2 所示。信息熵的计算公式如式(12)所示：

$$M(x)=-\sum_{k=0}^{2^N-1}p(x_k)\log_2 p(x_k) \tag{12}$$

Table 2. Test of color image information entropy
表 2. 彩色图像信息熵的检验

测试图像	R 通道	G 通道	B 通道
Lena 图像	7.9994	7.9993	7.9993
Pepper 图像	7.9992	7.9993	7.9994
Baboon 图像	7.9993	7.9993	7.9992
文献[18] (Lena)	7.9992	7.9993	7.9993
文献[19] (Lena)	7.9993	7.9992	7.9993
文献[20] (Lena)	7.9912	7.9917	7.9912

表 2 可以看出，本文获得的值更接近理论值 8。

5.5. 相关性分析

图像像素之间通常具有较强的相关性，这种相关性使得图像更容易被破解，特别是相邻像素的相关性，这描述了相邻像素之间的水平、垂直或对角关系。在原始图像中，图像中的像素在水平、垂直和对角线三个方向上都具有很强的相关性，相关系数接近于 1。对于加密图像来说，打破源图像中相邻像素之间的相关性非常重要，理想情况下，密码图像的相关性为零，但这通常无法实现。相关系数可以通过以下式(13)定量计算：

$$\begin{cases} r_{xy}=\dfrac{\operatorname{cov}(x,y)}{\sqrt{D(x)}\bullet\sqrt{D(y)}} \\ \operatorname{cov}(x,y)=\dfrac{1}{n}\sum_{k=1}^{n}E\left(x_k-E(x)\right)\left(y_k-E(y)\right) \\ E(x)=\dfrac{1}{n}\sum_{k=1}^{n}x_k \\ D(x)=\dfrac{1}{n}\sum_{k=1}^{n}\left(x_k-E(x)\right)^2 \end{cases} \tag{13}$$

其中 x_k 和 y_k 表示两个相邻像素。n 是像素数。 $E(x)$ 和 $D(x)$ 分别表示图像的期望值和方差。在本文中，从明文图像和密文图像中随机选择了 10000 对相邻像素进行测试，得到了三个通道不同方向上的相关性。明文图像和加密图像的相关性分布如图 10 所示。很明显，明文图像表现出很强的相关性，而密文图像破坏了这些相关性。本文以 Lena、Pepper 和 Baboon 彩色图像作为实验对象，将图像加密后的相邻像素点相关性(取绝对值)与与原图的相邻像素点相关性(取绝对值)分别从水平、垂直、对角线三个方向进行对比，结果如表 3 所示。表 3 说明该加密算法将图像相邻像素点的高相关性(接近 1)成功破坏至接近 0 的水平，显著增强了安全性。

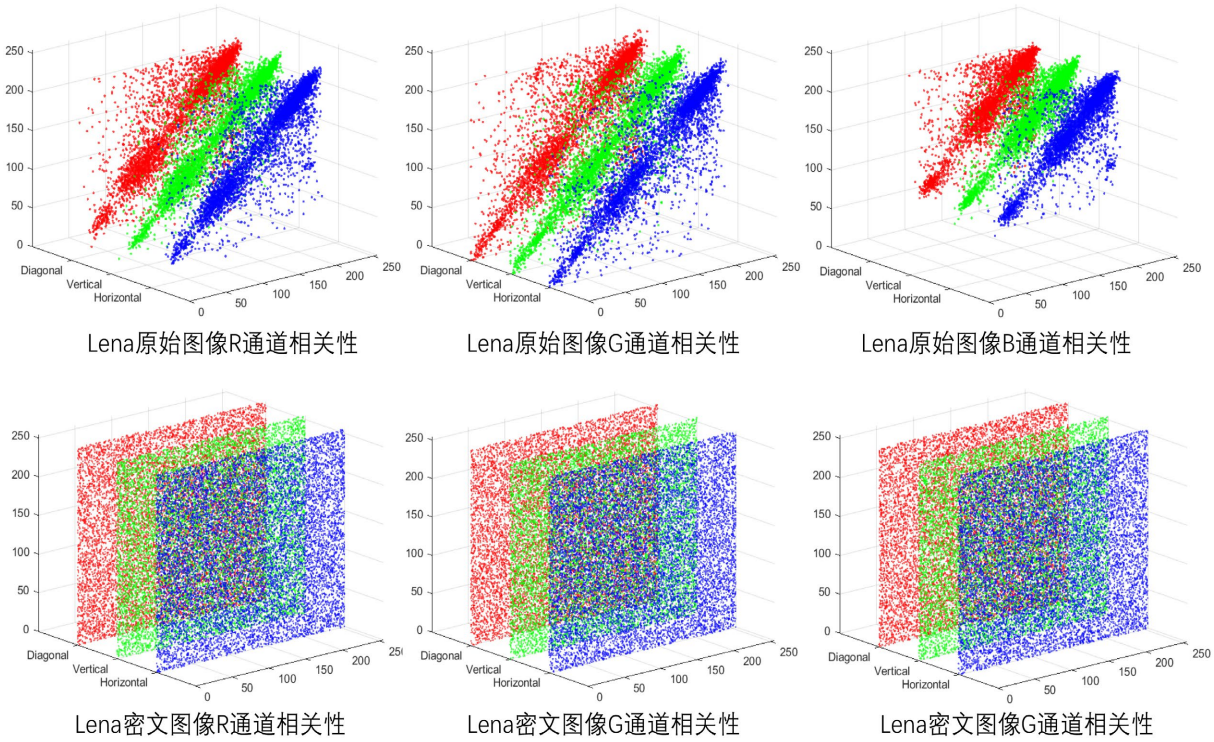


Figure 10. Correlation comparison of the R, G, and B channels of the Lena image in different directions before and after encryption
图 10. Lena 图像 R、G、B 三个通道加密前后不同方向上相关性对比

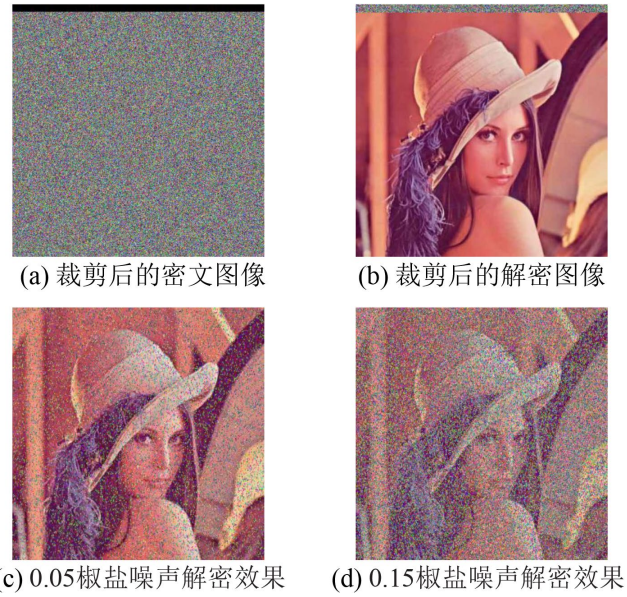
Table 3. Correlation of adjacent pixels (absolute value)
表 3. 相邻像素点相关性(取绝对值)

测试图像	明文			密文		
	水平	垂直	对角线	水平	垂直	对角线
Lena	0.9038	0.8796	0.8290	0.0102	0.0036	0.0066
Pepper	0.8997	0.8807	0.8268	0.0088	0.0062	0.0077
Baboon	0.9041	0.8750	0.8206	0.0083	0.0055	0.0102

5.6. 抗剪切能力分析和抗噪声能力分析

目前，图像在传输过程中受到的攻击主要有两种，即裁剪攻击和噪声攻击。为了鲁棒性测试，对所提出算法获得的密文图像进行裁剪攻击和噪声攻击。裁剪攻击测试如图 11 所示。这表明，即使将密文图

像裁剪一部分，解密图像仍然能够恢复大量信息。另外，本文对 Lena 密文图像分别加入 0.05 和 0.15 的椒盐噪声来模拟传输过程受到干扰的情形。图 11 显示了测试结果。因此，随着椒盐噪声强度的逐渐增加，解密过程中仍然可以恢复大部分信息。



(a) 裁剪后的密文图像　(b) 裁剪后的解密图像

(c) 0.05椒盐噪声解密效果　(d) 0.15椒盐噪声解密效果

Figure 11. Test results of cropping attack and noise attack
图 11. 裁剪攻击与噪声攻击测试结果

6. 结束语

本文基于四维－五维超混沌系统、DNA 编码、置乱和扩散技术，设计了一种新的图像加密方案。该方案根据四维超混沌系统产生的混沌系列，使 DNA 编码规则动态化，不同的像素值实时选择 DNA 碱基运算方式；再基于五维混沌系统生成的混沌序列和 DNA 编码对图像灰度值进行置乱。随后，将两个混沌系统生成的混沌序列在 DNA 域和像素域内分别进行双重扩散操作，最后合并三个通道得到彩色加密图像。该算法相较于低维系统，复杂度更高，密钥空间更大。通过实验证明，该算法加密后的图像，具有像素关联度低、直方图均衡，抗密钥攻击性能好等优点，可以用于实际图像加密工作中。

参考文献

[1] Usmonov, M. (2021) Basic Concepts of Information Security. *International Journal of Academic and Applied Research*, **5**, 5-8.

[2] Rashid, F.B., Rankothge, W., Sadeghi, S., Mohammadian, H. and Ghorbani, A. (2024) Privacy-Preserving for Images in Satellite Communications: A Comprehensive Review of Chaos-Based Encryption. Elsevier.

[3] Subhedar, M.S. and Mankar, V.H. (2014) Current Status and Key Issues in Image Steganography: A Survey. *Computer Science Review*, **13**, 95-113. https://doi.org/10.1016/j.cosrev.2014.09.001

[4] Hamadi, S.J. and Mohammed, E.A. (2025) Chaotic Systems in Cryptography: An Overview of Feature-Based Methods. *Al-Salam Journal for Engineering and Technology*, **4**, 164-172.

[5] Saberi Kamarposhti, M., Ghorbani, A. and Yadollahi, M. (2024) A Comprehensive Survey on Image Encryption: Taxonomy, Challenges, and Future Directions. *Chaos, Solitons & Fractals*, **178**, Article 114361. https://doi.org/10.1016/j.chaos.2023.114361

[6] Gao, Z., Liu, Z. and Wang, L. (2021) An Image Encryption Algorithm Based on the Improved Sine-Tent Map. *Discrete Dynamics in Nature and Society*, **2021**, 1-16. https://doi.org/10.1155/2021/9187619

[7] Wang, X.Y., Li, Y.P. and Jin, J. (2020) A New One-Dimensional Chaotic System with Applications in Image Encryption. *Chaos*, *Solitons & Fractals*, **139**, Article 110102. https://doi.org/10.1016/j.chaos.2020.110102

[8] Talhaoui, M.Z. and Wang, X.Y. (2021) A New Fractional One Dimensional Chaotic Map and Its Application in High-Speed Image Encryption. *Information Sciences*, **550**, 13-26. https://doi.org/10.1016/j.ins.2020.10.048

[9] Zhao, M., Li, L. and Yuan, Z. (2024) An Image Encryption Approach Based on a Novel Two-Dimensional Chaotic System. *Nonlinear Dynamics*, **112**, 20483-20509. https://doi.org/10.1007/s11071-024-10053-8

[10] Lorenz, E.N. (2017) Deterministic Nonperiodic Flow. In: *Universality in Chaos*, CRC Press, 367-378. https://doi.org/10.1201/9780203734636-38

[11] Holmes, P. (1995) The Essence of Chaos (E. N. Lorenz). *SIAM Review*, **37**, 129-131. https://doi.org/10.1137/1037031

[12] 王兴元, 王明军. 超混沌 Lorenz 系统[J]. 物理学报, 2007, 56(9): 5136-5141.

[13] Jia, Q. (2007) Hyperchaos Generated from the Lorenz Chaotic System and Its Control. *Physics Letters A*, **366**, 217-222. https://doi.org/10.1016/j.physleta.2007.02.024

[14] Yang, Q.G., Zhang, K.M. and Chen, G.R. (2009) Hyperchaotic Attractors from a Linearly Controlled Lorenz System. *Nonlinear Analysis*: *Real World Applications*, **10**, 1601-1617. https://doi.org/10.1016/j.nonrwa.2008.02.008

[15] Zhuang, Z.B., Zhuang, Z.B. and Wang, T. (2024) Medical Image Encryption Algorithm Based on a New Five-Dimensional Multi-Band Multi-Wing Chaotic System and QR Decomposition. *Scientific Reports*, **14**, Article No. 402. https://doi.org/10.1038/s41598-023-50661-9

[16] Lorenz, E.N. (2017) Deterministic Nonperiodic Flow. In: *Universality in Chaos*, CRC Press, 367-378. https://doi.org/10.1201/9780203734636-38

[17] 李瑞梅, 周艳, 崔壮. 新五维超混沌系统的动力学和自适应同步分析[J]. 内蒙古农业大学学报(自然科学版), 2025, 46(2): 81-89.

[18] 张成龙, 张朝霞, 刘芊伟. 基于四维混沌系统的彩色图像加密算法[J]. 现代信息科技, 2024, 8(15): 142-148+153.

[19] 张淑霞, 李珊珊, 白牡丹, 等. 基于混沌系统的数字彩色图像加密技术[J]. 科学技术与工程, 2022, 22(13): 5291-5298.

[20] 张赛男, 李千目. 一种基于 Logistic-Sine-Cosine 映射的彩色图像加密算法[J]. 计算机科学, 2022, 49(1): 353-358.