Interdisciplinary Science Letters 交叉科学快报, 2025, 9(3), 380-393
Published Online May 2025 in Hans. https://www.hanspub.org/journal/isl
https://doi.org/10.12677/isl.2025.93048

Hans汉斯

基于广义Gray码变换和广义Arnold映射的彩色图像加密算法

郭蓉蓉，陈　星，赵红旗，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16日；发布日期：2025年5月27日

摘　要

本文通过结合混沌系统与数据编码，提出了一种新型彩色图像加密算法。该算法通过离散型广义Arnold映射对明文像素位置进行非线性置乱，破坏相邻像素相关性；引入广义Gray码变换对置乱后图像颜色分量值实施编码，初步隐藏视觉信息；利用连续型广义Arnold映射生成伪随机密钥流，对编码图像完成扩散运算，进一步破坏明文统计特征。加密算法融合了广义Gray码变换的局部混淆能力和广义Arnold映射的全局扩散特性，构建双重安全机制。一方面，离散型广义Arnold映射和广义Gray编码协同增强像素位置与灰度值的动态扰乱效果；另一方面，连续型广义Arnold映射扩展了加密算法的密钥空间。数值实验表明，该图像加密算法具有优良的加密性能，可以抵御蛮力攻击、统计分析攻击以及差分攻击等。

关键词

图像加密，广义Gray码，广义Arnold映射，混沌映射

Color Image Encryption Algorithm Based on Generalized Gray Code Transformation and Generalized Arnold Map

Rongrong Guo, Xing Chen, Hongqi Zhao, Ruisong Ye*

Department of Mathematics, Shantou University, Shantou Guangdong

Received: Apr. 23rd, 2025; accepted: May 16th, 2025; published: May 27th, 2025

Abstract

The paper proposes a novel image encryption algorithm by integrating chaotic system with data

*通讯作者。

文章引用: 郭蓉蓉, 陈星, 赵红旗, 叶瑞松. 基于广义 Gray 码变换和广义 Arnold 映射的彩色图像加密算法[J]. 交叉科学快报, 2025, 9(3): 380-393. DOI: 10.12677/isl.2025.93048

coding. The algorithm employs a discrete generalized Arnold map to nonlinearly scramble plain image's pixel positions, effectively disrupting adjacent pixel correlations. A generalized gray code transformation is introduced to perform encoding on color component values of the scrambled image, achieving preliminary visual information concealment. Subsequently, a continuous generalized Arnold map generates pseudo-random keystreams to execute diffusion operations on the encoded image, further eliminating statistical features of the plain image. Combining the local confusion capability of generalized gray code transformation with the global diffusion nature of generalized Arnold map, the encryption algorithm establishes a dual security mechanism. On the one hand, the collaborative effect of discrete generalized Arnold map and generalized gray coding enhances dynamic disruption of pixel positions and grayscale values; on the other hand, the continuous generalized Arnold map significantly expands the key space of the proposed encryption. Numerical experiments demonstrate that the proposed image encryption algorithm exhibits excellent performance and security, showing strong resistance against differential analysis attack, statistical attacks and brute-force attack, etc.

Keywords

Image Encryption, Generalized Gray Code, Generalized Arnold Map, Chaos

1. 引言

在数字化时代，图像数据已成为信息传递的重要载体，并在公共网络上广泛传输共享，使得图像数据安全成为信息安全领域的热点问题。然而，图像数据的高冗余特性与像素间的强相关性，使得传统加密算法(如 AES、DES)在处理图像时面临效率低下、安全性不足等问题，特别是在大规模图像传输与存储场景中，如何实现高效且安全的图像加密成为亟待解决的技术难题[1]。混沌系统具有对初始条件的极端敏感性、混沌序列的伪随机性、轨迹遍历性以及容易实现等性质，而这些混沌特性与密码的混淆与扩散的要求高度相似，基于混沌的图像加密算法也因此成为图像信息安全领域的研究热点，混沌系统被视为设计图像加密系统的理想工具[2] [3]。

Arnold 映射成熟应用于经典的图像置乱技术之中，通过像素位置的非线性变换实现图像的视觉混淆。Arnold 映射最初由 Vladimir Arnold 在遍历理论研究中提出，俗称“猫脸映射”，通过像素的位置移动实现图像的置乱效果[4]。传统离散型 Arnold 映射在数字图像加密中存在明显的局限性，主要表现在仅适用于等长图像，且其周期性特性使得攻击者可以通过暴力攻击恢复原始图像，降低了加密的安全性。为克服这些局限性，学者们提出了广义 Arnold 映射(Generalized Arnold Map, GAM)。GAM 通过引入可变参数、非线性项以及离散映射的形式，扩展了 Arnold 映射的普适性和复杂性，使得映射能够适用于非等长图像，并且映射的周期和混沌参数选择范围更大，有效降低了周期性特性带来的安全风险[5]-[7]。洪炎等人提出了一种基于行列异或的 Arnold 双置乱图像加密方法，通过改进 Arnold 映射和行列按位异或操作，实现了对任意类型图像的灰度空间和位置空间的双重置乱效果[8]。文献[9] [10]通过将 Arnold 映射推广到高维情形，提出了基于 RGB 色彩空间的图像置乱方法，通过高维 Arnold 映射对图像的 RGB 颜色分量进行置乱，从而实现彩色图像的置乱加密。Gray 码技术最初由 Frank Gray 在 1940 年代提出，主要用于减少模拟信号传输中的误码率[11]。传统 Gray 码通过最小化相邻像素值的差异，确保在传输过程中，相邻像素值的变化最小化，从而有效减少了传输误码对图像质量的影响。然而，传统 Gray 码基于二进制实现，其

像素亮度值变化能力有限，难以满足现代图像加密技术的安全性需求。为克服这一局限性，广义 Gray 码(Generalized Gray Code, GGC)通过引入更复杂的变换矩阵和运算规则，实现了像素值的变化更加随机化，能够有效提高图像的混淆和扩散效果，增强图像的安全性。王广超等人提出了一种新的广义 Gray 码，即置乱广义 Gray 码，通过定义新的变换规则，进一步提高了图像置乱的效率和安全性[12]。邹建成等人讨论了广义 Gray 码在数字图像置乱中的应用，并给出了图像置乱变换的周期公式，进一步推广了丁玮等人的相关结果[13]。文献[14]综合了 Gray 码和 Arnold 映射的特性，提出了一种非等长 Arnold 映射并结合 Gray 码变换的双重加密算法。利用非等长 Arnold 映射破坏相邻像素的相关性，再利用广义 Gray 码算法改变图像的灰度值，使得密文图像像素灰度值分布近似均匀分布，从而弥补了 Arnold 映射不能修改灰度值的缺陷，使得加密算法具有更好的安全性。

本文提出了一种基于广义 Gray 码变换和广义 Arnold 映射的图像加密算法，目的在于改进传统加密算法的效率，密钥空间以及性能等。已有的 Gray 码或广义 Gray 均是基于二进制实现，加密效率较低，改变像素亮度值或颜色分量值的效果有待提升[15]。本文将广义的 Gray 码变换从二进制推广到十六进制，节约了运算量，提高了加密效率。通过结合广义 Gray 码的任意进制编码特性与非等长 Arnold 映射的扩展置乱能力，设计了一个采用非等长 Arnold 置乱、广义 Gray 码变换扩散、像素颜色分量值按位比特和加取模扩散的图像加密算法。在应用非等长离散型广义 Arnold 置乱时，该算法不仅支持任意尺寸图像的加密，而且通过引入明文相关的动态参数生成机制，使得置乱过程与明文相关，具有自适应性，能实现一图一密的效果，增强了置乱效果和抗差分攻击能力。在扩散过程的第一阶段，首先利用四位比特分离方法对图像的颜色分量值分离成高四位和低四位，然后应用十六进制的广义 Gray 码变换对彩色图像的三颜色 R，G，B 分量值进行交叉融合。由于广义 Gray 码变换的参数由连续型广义 Arnold 映射生成，具有动态的特点，改进了传统的二进制 Gray 码或广义二进制 Gray 码的固定变换的缺陷，提升了算法的安全性。在扩散过程的第二阶段，利用连续型广义 Arnold 映射生成的混沌序列对彩色图像的三颜色 R，G，B 分量值实施按位异或和加取模的扩散操作，使得加密算法的安全性得到进一步提高。实验结果表明，该图像加密算法具有优良的安全性能，为图像信息安全提供了一种有效且安全的方案。

2. 相关知识

2.1. 广义 Arnold 映射

实参数映射。实参数广义 Arnold 映射是一种基于经典 Arnold 映射的扩展形式，广泛应用于图像加密领域。该映射通过引入两个实数控制参数 p 和 q，扩展了混沌系统的动态范围和复杂性，具体如公式(1)所示：

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & p \\ q & 1+p\times q \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} \bmod 1 \tag{1}$$

其中系统参数 p,q 可以选为实数，初始值 $x_0, y_0 \in (0,1)$，系统参数 p,q 和初始值 x_0, y_0 可作为加密算法的密钥。公式(1)生成实数混沌序列 x_n 与 y_n，而 mod 1 操作确保了该混沌序列中的值始终位于单位区间内，可用于生成整数参数型广义 Arnold 映射的参数 b 和 e，以及控制加密算法中三颜色分量值的扩散过程的密钥流。这种实参数广义 Arnold 映射显著扩大了参数的选择范围，从而扩大了加密算法的密钥空间，使得加密算法能够更好地抵抗统计攻击和暴力破解攻击，为数字图像加密提供了更可靠的伪随机数密钥流。

整数参数型映射。整数参数型广义 Arnold 映射通过引入参数 b,c,e 以及非线性项，改善了图像像素位置置乱效果，并提高加密算法的安全性；另一方面，该广义 Arnold 映射可以实现任意大小的图像加密，使得置乱算法具有普适性。本文采用的整数参数型广义 Arnold 映射如公式(2)所示[5]：

$$\begin{cases} x_{n+1} = (x_n + by_n) \bmod M \\ y_{n+1} = \left(cx_n + (1+bc)y_n + ef(x_{n+1})\right) \bmod N \end{cases} \tag{2}$$

其中 $c=kN\cdot\left(\gcd\left(M,N\right)\right)^{-1}, b\in\left\{1,2,\cdots,M-1\right\}$， k 选取为正整数且 $\mathrm{mod}\left(c,N\right)\neq 0, e\in\left\{1,2,\cdots,N-1\right\}$，函数 $f\left(x\right)=x^3$。公式(2)的逆映射如公式(3)所示，可以实现快速解密。

$$\begin{cases} y_n=\left(y_{n+1}-cx_{n+1}-ef\left(x_{n+1}\right)\right)\bmod N \\ x_n=\left(x_{n+1}-by_n\right)\bmod M \end{cases} \tag{3}$$

2.2. 比特平面分解与重构

四位比特分离方法。在图像加密领域，像素的灰度值或颜色分量值的比特操作是一种常用的技术，用于增强加密算法的复杂性和安全性。四位比特分离方法是一种有效的比特操作技术，能够将图像像素值的高四位与低四位分离处理，再将它们重新组合，从而实现更精细的加密控制[16]。本文使用四位比特分离方法，并将其应用于图像加密算法的设计。首先对图像的每个像素的灰度值或颜色分量值进行高四位和低四位的分离，然后分别对这两部分进行加密操作。四位比特分离方法的引入，使得图像加密算法能够更有效地处理图像信息，同时增强了算法对明文攻击的抵抗能力。表 1 举例说明了四位比特的分解。

Table 1. Decomposition of 8-bit integer
表 1. 8 比特整数的分解

像素值	运算	高四比特位	低四比特位
88	88/16 = 5…8	5	8
150	150/16 = 9…6	9	6
215	215/16 = 13…7	13	7

广义 Gray 码变换及其逆变换。广义 Gray 码变换是一种基于传统 Gray 码的扩展变换，通过引入可逆的变换矩阵，将传统 Gray 码的二进制变换推广到任意 q 进制，这样的 Gray 码推广使得数字图像置乱加密具有很好的安全性和普适性。其定义如下：对于任意非负整数 u，其 q 进制码表示为 $u=\left(u_{n-1}u_{n-2}\cdots u_1u_0\right)_q$，定义如公式(4)所示的广义 Gray 码变换。

$$\begin{bmatrix} g_{n-1} \\ g_{n-2} \\ \vdots \\ g_0 \end{bmatrix}=\begin{bmatrix} a_{0,0} & a_{0,1} & \cdots & a_{0,n-1} \\ a_{1,0} & a_{1,1} & \cdots & a_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n-1,0} & a_{n-1,1} & \cdots & a_{n-1,n-1} \end{bmatrix}\begin{bmatrix} u_{n-1} \\ u_{n-2} \\ \vdots \\ u_0 \end{bmatrix}\bmod q, \tag{4}$$

其中 $q\geq 2$ 为正整数，$a_{i,j}$ 为整数，$i,j=1,2,\cdots,n-1$，当变换矩阵的行列式与 q 互素时，该变换称为 u 的 q 进制广义 Gray 码变换，$g\left(u\right)=\left(g_{n-1}g_{n-2}\cdots g_1g_0\right)_q$ 称为 u 的 q 进制广义 Gray 码。广义 Gray 码变换算法简单，置乱效率较高，在数字图像安全性方面有较好的应用前景。

3. 加密算法

加密算法包括了置乱与扩散两部分，其中置乱部分对像素的位置进行变换；扩散部分实现对像素的灰度值或颜色分量值的改变。本文的加密算法使用连续型广义 Arnold 映射所生成的混沌序列构造整数参数型广义 Arnold 映射对图像进行置乱，再使用广义 Gray 码变换进行第一次扩散；利用连续型广义 Arnold 映射所生成的混沌序列的量化序列，对图像实行进一步扩散，最终得到密文图像。加密的流程图如图 1 所示，具体步骤包括 Step 1-Step 5。

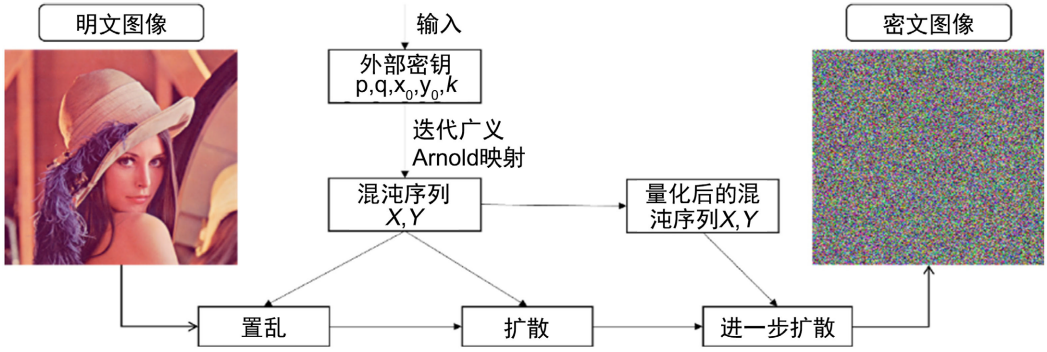


Figure 1. Flowchart of encryption process
图 1. 加密流程图

Step 1. 读取彩色图像 PI 的 R，G，B 分量(大小均为 $M\times N$)，接着将三者拼接为 $M\times 3N$ 的矩阵 $RGB=[R,G,B]$，利用公式(5)计算图像所有分量相关的特征值 s，用于丢弃连续型广义 Arnold 映射所生成的混沌序列的前面部分过渡点，使得基于离散型广义 Arnold 映射的位置置乱与明文相关，可以增强加密算法抵御差分攻击的性能。

$$s=\mathrm{mod}\left(\sum_{i=1}^{M}\sum_{j=1}^{3N}RGB(i,j),70\right)+30. \tag{5}$$

Step 2. 选取系统参数 $p=2.31,q=29.67$ 及初始值 $x_0,y_0\in(0,1)$ 作为密钥。迭代连续型广义 Arnold 映射 (1) 生成混沌序列 $x_n,y_n\left(n=0,1,2,\cdots,100+3MN\right)$。再保留后面 $3MN$ 个 x_n,y_n，记为 X,Y：$X=\left(x_{101},\cdots,x_{100+3MN}\right),Y=\left(y_{101},\cdots,y_{100+3MN}\right)$。

Step 3. 对 x_{s+1},y_{s+1} 用公式(6)量化得到整数参数型广义 Arnold 映射的参数 b 和 e，

$$\begin{aligned}b&=\mathrm{mod}\left(floor\left(x_{s+1}\times 10^{10}\right),M-1\right)+1,\\ e&=\mathrm{mod}\left(floor\left(y_{s+1}\times 10^{10}\right),3\times N-1\right)+1.\end{aligned} \tag{6}$$

选取参数 $c=KN\cdot\left(\gcd(M,N)\right)^{-1},k=1$，令 $f(x)=x^3$，利用整数参数型广义 Arnold 映射(2)对 RGB 进行像素位置的置乱，得到 RGB1。

Step 4. 将 RGB1 再分割为三个大小为 $M\times N$ 的矩阵 $R1,G1,B1$，获取三者的高 4 位比特与低 4 位比特，组成 16 进制的二维矩阵，分别记为 R_H,R_L,G_H,G_L,B_H,B_L，如公式(7)所示：

$$\begin{aligned}R_H&=floor(R/16),R_L=\mathrm{mod}(R,16),\\ G_H&=floor(G/16),G_L=\mathrm{mod}(G,16),\\ B_H&=floor(B/16),B_L=\mathrm{mod}(B,16).\end{aligned} \tag{7}$$

将 R_H,R_L,G_H,G_L,B_H,B_L 的元素值使用广义 Gray 变换进行交叉融合，获取矩阵 $R1_H,R1_L,G1_H,G1_L,B1_H,B1_L$，如公式(8)所示，其中 $a_{ij}=\mathrm{mod}\left(floor\left(x_{100+(i-1)\times 6+j}\times 10^{10}\right),16\right)$。

$$\begin{pmatrix}R1_H\\ B1_L\\ G1_H\\ G1_L\\ B1_H\\ R1_L\end{pmatrix}=\begin{pmatrix}1 & a_{12} & a_{13} & a_{14} & a_{15} & a_{16}\\ & 1 & a_{23} & a_{24} & a_{25} & a_{26}\\ & & 1 & a_{34} & a_{35} & a_{36}\\ & & & 1 & a_{45} & a_{46}\\ & & & & 1 & a_{56}\\ & & & & & 1\end{pmatrix}\begin{pmatrix}R_H\\ R_L\\ G_H\\ G_L\\ B_H\\ B_L\end{pmatrix}\mathrm{mod}16. \tag{8}$$

将 $R1_H, R1_L, G1_H, G1_L, B1_H, B1_L$ 进行重新组合，形成新的三颜色分量矩阵 $RGBnew$，如公式(9)所示。

$$\begin{aligned} &Rnew = R1_H \times 16 + R1_L, Gnew = G1_H \times 16 + G1_L, \\ &Bnew = B1_H \times 16 + B1_L, RGBnew = [Rnew, Gnew, Bnew]. \end{aligned} \tag{9}$$

Step 5. 使用实参数 Arnold 映射生成的混沌序列 $X = (x_{101}, \cdots, x_{100+3MN})$， $Y = (y_{101}, \cdots, y_{100+3MN})$ 实施 Step 5.1 和 Step 5.2 的像素值扩散。

Step 5.1. 利用公式(10)，形成伪随机的灰度值序列密钥流。

$$X = \mathrm{mod}\left(floor\left(X \times 10^{10}\right), 256\right), Y = \mathrm{mod}\left(floor\left(Y \times 10^{10}\right), 256\right). \tag{10}$$

用 Reshape 函数将 X, Y 重塑为大小为 $M \times 3N$ 的矩阵，如公式(11)所示。

$$X = reshape\left(X, [M, 3 * N]\right), Y = reshape\left(Y, [M, 3 * N]\right). \tag{11}$$

Step 5.2. 将 X 与 $RGBnew$ 实施按位异或运算得到 $C0$，将 Y 与 $C0$ 实施加取模运算得到 $C1$，具体如公式(12)所示：

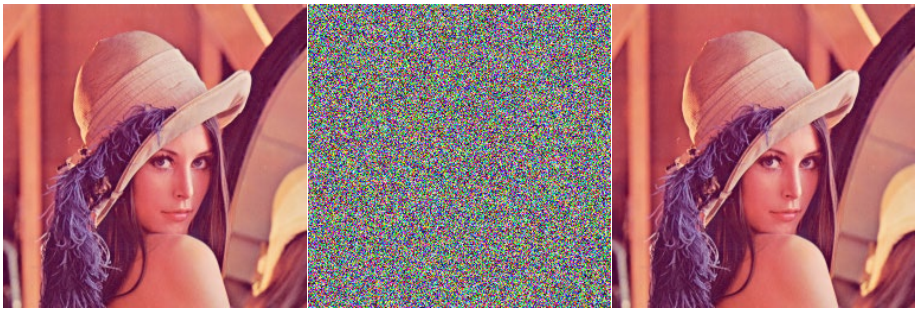
$$C0 = bitxor\left(X, RGBnew\right), C1 = \mathrm{mod}\left(C0 + Y, 256\right). \tag{12}$$

把 $C1$ 用公式(13)分割为三颜色分量，得到最后的彩色密文图像矩阵 C。

$$\begin{aligned} &C(:,:,1) = C1(:,1:N), C(:,:,2) = C1(:,N+1:2*N), \\ &C(:,:,3) = C1(:,2*N+1:3*N). \end{aligned} \tag{13}$$

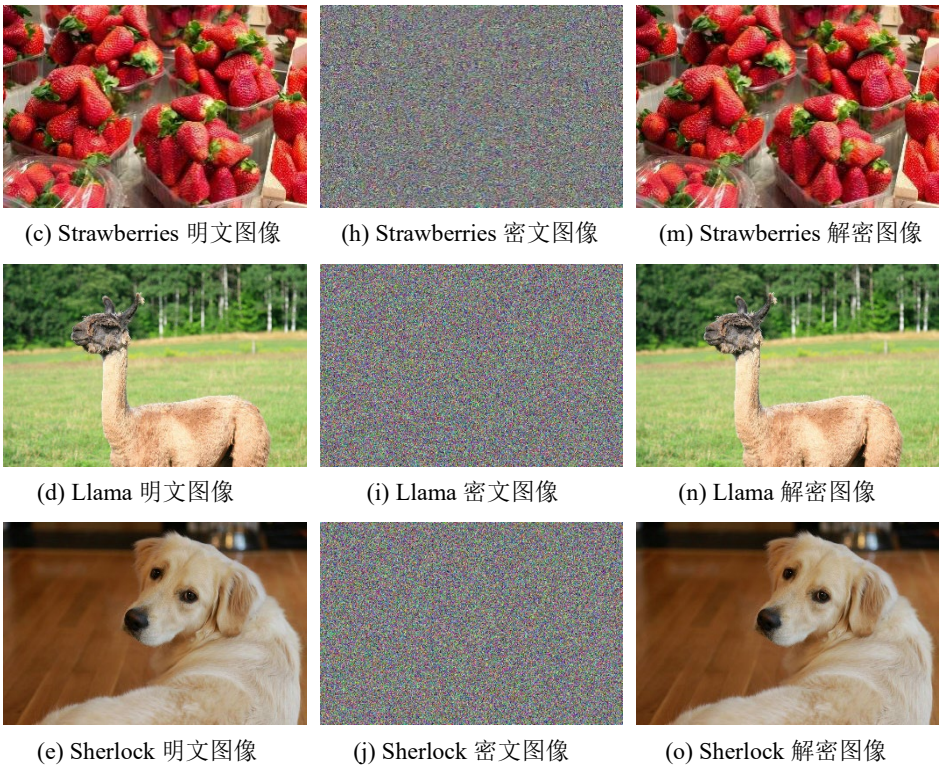
4. 仿真结果与性能分析

实验使用的计算机配置为 Windows 11，在 MATLAB R2023a 平台上进行图像加密算法的仿真实验。将加密算法中连续广义 Arnold 映射的初始值和系统参数设为 $x_0 = 0.2, y_0 = 0.1$， $p = 2.31, q = 29.67, k = 1$。选取 Lena，Onion，Strawberries，Llama，Sherlock 五幅不同大小的彩色图像作为明文图像，解密和解密结果如图 2 所示。明文图像如图 2(a)~(e)，密文图像如图 2(f)~(j)，解密图像如图 2(k)~(o)，经验证，解密图像与明文图像完全一致，可知加密后的图像均很杂乱，类似噪声，较好地隐藏了明文图像的信息，加密效果良好，算法无失真解密。



(a) Lena 明文图像　(f) Lena 密文图像　(k) Lena 解密图像

(b) Onion 明文图像　(g) Onion 密文图像　(l) Onion 解密图像



(c) Strawberries 明文图像　(h) Strawberries 密文图像　(m) Strawberries 解密图像

(d) Llama 明文图像　(i) Llama 密文图像　(n) Llama 解密图像

(e) Sherlock 明文图像　(j) Sherlock 密文图像　(o) Sherlock 解密图像

Figure 2. The simulation experiment results
图 2. 仿真实验结果

4.1. 抗攻击能力分析

本研究创新性地引入了两种形式的非等长广义 Arnold 映射，以构建安全性高、抗攻击能力强的图像加密算法。具体而言。研究中首先采用实参数形式的广义 Arnold 映射生成混沌序列，再融合混沌序列与明文像素值所生成的特征值 s 以生成置乱阶段的参数 b、e，最终运用整数参数的广义 Arnold 映射进行图像置乱操作，实现图像像素的随机分布。由此可知，该加密策略的核心优势在于对任意尺寸的广泛适用性，及引入明文相关的动态参数生成机制所实现的自适应性。本研究采用的做法，使得在置乱过程中明文相关参数生成与明文密切相关，能够实现“一图一密”的效果。此算法对明文高敏感性决定了图像优良的抵御差分攻击、选择明文攻击和已知明文攻击能力。

4.2. 密钥空间分析

密钥空间包含了加密算法允许使用的全部合法密钥，是衡量加密系统安全性的基础指标，其大小直接影响抗暴力攻击能力。本文所采用的密钥为实参数 $K=\{p,q,x_0,y_0\}$，为了能更好的抵抗穷举的攻击，密钥空间必须是大于 2^{100}，在计算机的精度 10^{-15}，该算法的密钥空间为 $\left(10^{15}\right)^4=10^{60}$，远大于 2^{100}。因此，加密算法的密钥空间足够大，能够有效抵御穷举攻击。

4.3. 直方图分析

直方图是图像中每个灰度级(通常为 0~255)的像素数量的统计图，用于展示图像中灰度值的分布特征。当直方图分布趋于均匀时，图像信息的不确定性显著增加，从而能够有效抵御基于直方图的攻击。以 Lena 图像为例，分别绘制明文图像和密文图像在 RGB 三个通道上的直方图。从图 3 中可以清晰地观察到，

Lena 明文图像的灰度值分布波动较大，呈现出明显的起伏特征；而密文图像的灰度值分布则较为均匀，直方图曲线相对平缓。这一对比表明，密文图像的灰度直方图分布更加均衡，能够更好地保障图像信息的安全性。

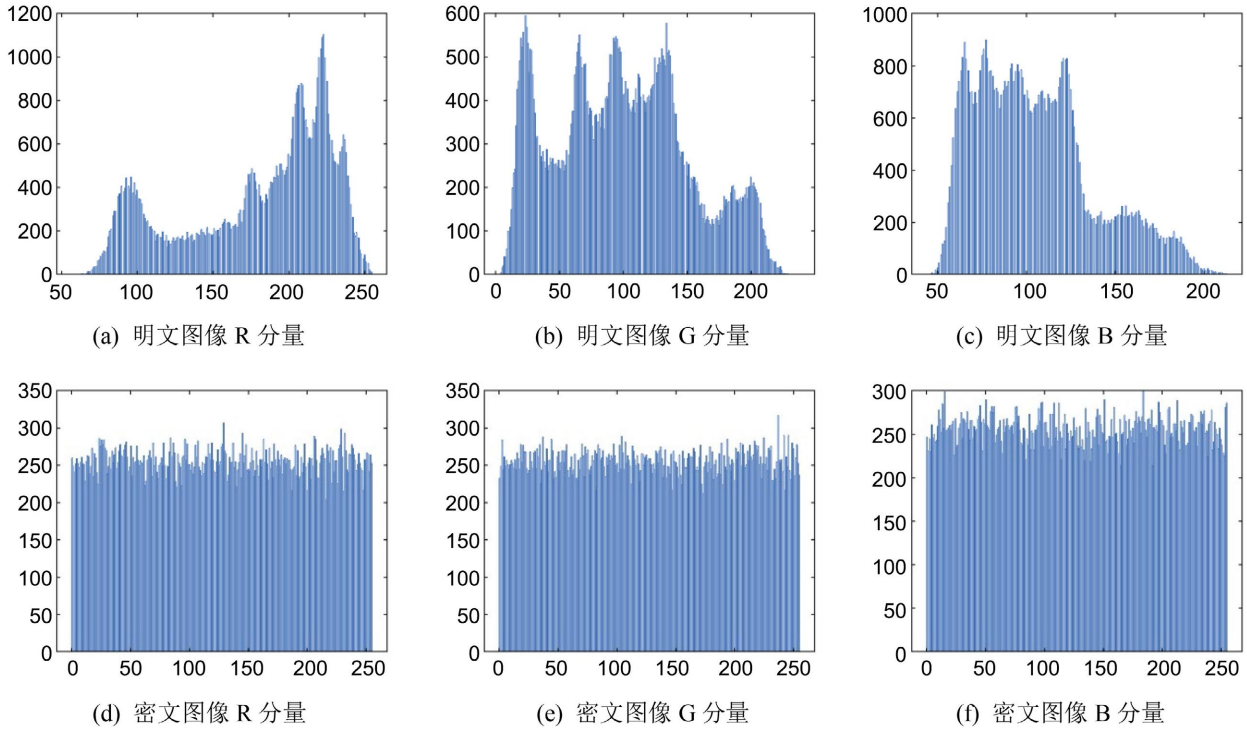


Figure 3. Histograms of three color components
图 3. 三颜色分量的直方图

为了进一步定量刻画明文图像和密文图像的区别，本文采用 Pearson χ^2 检验对两者的差别在数值上进行分析。给定一组观察到的频数分布，记为 $f_i, i=1,\cdots,n$，假设理论频数分布为 $g_i, i=1,\cdots,n$，作假设 H_0：样本来自该理论分布。当假设 H_0 成立时，$\chi^2=\sum_{i=1}^{n}\frac{(f_i-g_i)^2}{g_i}$ 服从自由度为 $n-1$ 的 χ^2 分布。对于灰度等级为 256 的图像而言，应用公式(14)计算服从自由度为 255 的 χ^2 分布统计量，来检验直方图是否服从均匀分布。

$$\chi^2=\sum_{i=1}^{255}\frac{(f_i-g)^2}{g} \tag{14}$$

其中 f_i 代表直方图中每个灰度值的频数，$g=\frac{MN}{256}$，取显著性水平 α，$\chi_\alpha^2(n-1)$ 满足 $P\{\chi^2\geq\chi_\alpha^2(n-1)\}=\alpha$，则当 $\chi^2<\chi_\alpha^2(n-1)$ 时，接收假设 H_0。

Table 2. The χ^2 results for Lena image and its cipher image
表 2. Lena 图像和密文图像的 χ^2 结果

图像	*R*	*G*	*B*
明文图像	65305.64	30665.70	91939.87
密文图像	276.72	252.49	265.88

当以 Lena 图像为例，并实施加密，得到其密文图像，计算明文图像和密文图像的 χ^2 统计量，结果如表 2。可以看出明文图像三个颜色分量的 χ^2 统计量的值远大于 $\chi^2_{0.01}(255)=310.457$，而对应密文图像的 χ^2 统计量的值均小于 $\chi^2_{0.01}(255)$。加密后的密文图像近似均匀分布，图像信息难以被预测，确保了其安全性。

4.4. 相关系数分析

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相关性。为了确保图像信息的安全性，加密后获得的密文图像的相邻像素间的相关性应当呈现较低水平，接近 0。计算两组相邻像素的相关性系数公式如公式(15)所示。

$$\begin{cases} r_{xy}=\dfrac{\operatorname{cov}(u,v)}{\sqrt{D(u)}\sqrt{D(v)}}, \\ \operatorname{cov}(x,y)=\dfrac{1}{T_0}\sum_{i=1}^{T_0}\left(x_i-E(u)\right)\left(y_i-E(v)\right), \\ D(u)=\dfrac{1}{T_0}\sum_{i=1}^{T_0}\left(u_i-E(u)\right)^2, \\ D(v)=\dfrac{1}{T_0}\sum_{i=1}^{T_0}u_i. \end{cases} \tag{15}$$

以 Lena 图像为例，根据公式(15)计算得到的明文图像和密文图像的各方向的相关系数如表 3 所示。根据表 3 的实验数据对比分析可知，原始明文图像在水平、垂直及对角方向上的相邻像素间均呈现出显著的相关性特征。密文图像在相应方向的相关系数均显著趋近于零的理想值。该结果表明，加密算法有效消除了图像像素间的空间关联特性，使密文图像的统计特征与随机噪声趋于一致。这对原始图像统计特性的彻底破坏，使得攻击者难以通过频率分析、相关性分析等统计手段获取有效信息，从而显著提升了算法抵御统计攻击的安全性能。

Table 3. Adjacent pixels' correlation coefficients of Lena image and its cipher image
表 3. Lena 图像和密文图像相邻像素的相关系数

Lena 图像相关系数		水平	垂直	对角	反对角
R 分量	明文图像	0.9557	0.9774	0.9316	0.9560
	密文图像	−0.0186	−0.0083	−0.0051	0.0003
G 分量	明文图像	0.9378	0.9697	0.9152	0.9376
	密文图像	0.0011	−0.0134	−0.0061	0.0071
B 分量	明文图像	0.9166	0.9509	0.8982	0.9146
	密文图像	0.0065	0.0175	0.0040	−0.0075

4.5. 信息熵

信息熵作为评估图像随机性的量化指标，反映了图像的复杂程度和信息量，其数值与数据不确定性呈正相关关系。一般认为，信息熵越大，图像的不确定性越高，可视信息越少，从而能够更有效地保护图像信息的安全性。信息熵的计算见公式(16)：

$$H=-\sum_{i=0}^{L-1}p(i)\log_2 p(i) \tag{16}$$

其中 $L=256$ 为灰度等级数，$p(i)$ 表示像素值 i 的分布概率。根据公式(16)计算 Lena 图像信息熵，得到表 4 的结果。对于 8 位灰度图像，理论最大熵值为 8。观察表 4 发现，各个明文图像的 RGB 分量的信息熵均小于 8，且与理论值差异较大，而密文图像十分接近理论值 8。实验结果验证了加密算法能够有效消除像素分布规律性，大幅降低可视信息泄露风险。

Table 4. Information entropy results
表 4. 信息熵结果

指标	*R* 分量		*G* 分量		*B* 分量	
	明文图像	密文图像	明文图像	密文图像	明文图像	密文图像
Lena	7.2353	7.9969	7.5683	7.9969	6.9176	7.9971
Onion	7.2208	7.9930	7.5104	7.9938	6.7218	7.9940
Strawberries	7.6486	7.9998	7.4473	7.9997	7.2258	7.9997
Llama	7.6660	7.9999	7.2524	7.9998	7.3467	7.9999
Sherlock	7.2534	7.9997	7.3716	7.9997	7.3014	7.9997

4.6. 密钥敏感性分析

密钥敏感性分析主要用于衡量加密算法对密钥微小变化的响应能力，通过对比同一明文图像在使用两个仅有微小差距的密钥加密后生成的密文图像，量化两者之间的差异程度。当加密密钥发生微小变化时，若生成的密文图像表现出显著差异，则表明该算法具有较强的密钥敏感性，能够有效抵抗暴力破解攻击。该特性通常用 NPCR (像素变化率)和 UACI (归一化平均变化强度)来反映，如公式(17)和公式(18)所示：

$$\begin{cases} \mathrm{NPCR}=\dfrac{1}{M\times N}\sum_{i,j}D(i,j)\times 100\% \\ \mathrm{UACI}=\dfrac{1}{255\times M\times N}\sum_{i}^{M}\sum_{j}^{N}\left|C_1(i,j)-C_2(i,j)\right|\times 100\% \end{cases} \tag{17}$$

$$D(i,j)=f(x)=\begin{cases}1, C_1(i,j)\neq C_2(i,j)\\ 0, \text{otherwise}\end{cases} \tag{18}$$

其中 $C_1(i,j)$ 和 $C_2(i,j)$ 分别为使用两个微小差异密钥加密后的密文图像在位置 (i,j) 的灰度值或颜色分量值，$M\times N$ 为图像尺寸。

两幅随机图像之间的 NPCR 和 UACI 的理论期望值分别为 NPCR = 99.6094%， UACI = 33.4635%。两幅密文图像之间的实验结果越接近理论期望值，则两幅图片之间差别越大，说明密钥的敏感性更好。以图像 Lena、Onion、Strawberries、Llama、Sherlock 为例，对密钥的 4 个参数依次进行敏感性分析，分别对其进行微小扰动，改变 10^{-14} 后得到 NPCR 和 UACI 值，如表 5 所示。观察到，NPCR 和 UACI 均十分接近理论期望值，从而说明该算法具有较强的密钥敏感性。

4.7. 明文敏感性分析

为了提升算法抵抗差分攻击的能力，算法的密钥应具有较强的明文敏感性。对原始明文图像进行单像素修改，采用相同密钥对修改前后的图像分别执行加密操作，算得 NPCR 和 UACI 的值，重复操作 100 次后取平均值。通过广义 Arnold 映射生成的混沌序列驱动像素扩散过程，结合 Gray 码的比特平面交叉重组，使得微小明文差异可以得到明显的密文差异。结果见表 6，观察发现实验结果非常接近期望值，这说明加密算法具有良好的明文敏感性，具有良好的抵御差分攻击能力。

Table 5. Key sensitivity analysis results (%)
表 5. 密钥敏感性分析结果(%)

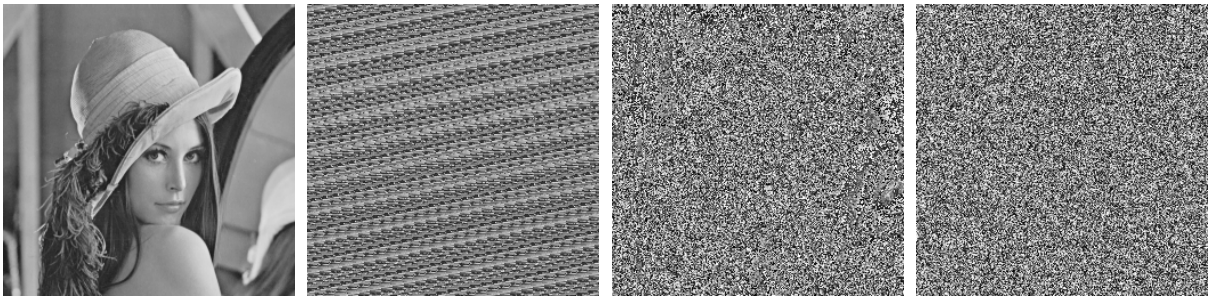
指标		x_0		y_0		p		q	
		NPCR	UACI	NPCR	UACI	NPCR	UACI	NPCR	UACI
Lena	*R* 分量	99.58	33.32	99.61	33.47	99.58	33.44	99.59	33.33
	G 分量	99.65	33.41	99.61	33.54	99.66	33.54	99.61	33.42
	B 分量	99.62	33.61	99.58	33.58	99.59	33.47	99.65	33.47
Onion	*R* 分量	99.58	33.17	99.58	33.35	99.57	33.50	99.64	33.51
	G 分量	99.61	33.69	99.59	33.35	99.58	33.30	99.61	33.39
	B 分量	99.63	33.78	99.63	33.49	99.60	33.56	99.61	33.64
Strawberries	*R* 分量	99.61	33.47	99.59	33.51	99.60	33.41	99.60	33.41
	G 分量	99.60	33.42	99.62	33.50	99.61	33.39	99.59	33.41
	B 分量	99.60	33.52	99.60	33.46	99.61	33.44	99.61	33.46
Llama	*R* 分量	99.60	33.43	99.62	33.50	99.61	33.45	99.60	33.44
	G 分量	99.61	33.47	99.60	33.43	99.61	33.46	99.60	33.43
	B 分量	99.61	33.43	99.62	33.51	99.60	33.46	99.61	33.49
Sherlock	*R* 分量	99.61	33.43	99.62	33.50	99.60	33.45	99.60	33.44
	G 分量	99.61	33.47	99.60	33.43	99.62	33.46	99.60	33.43
	B 分量	99.61	33.43	99.62	33.46	99.61	33.46	99.61	33.49
理论值		99.61	33.46	99.61	33.46	99.61	33.46	99.61	33.46

Table 6. Plaintext sensitivity analysis results (unit: %)
表 6. 明文敏感性分析结果(单位：%)

图像		指标	
	理论值	NPCR	UACI
		99.6094	33.4635
Lena	*R* 分量	99.54	33.54
	G 分量	99.55	33.45
	B 分量	99.52	33.48
Onion	*R* 分量	99.59	33.50
	G 分量	99.63	33.44
	B 分量	99.64	33.58
Strawberries	*R* 分量	99.58	33.42
	G 分量	99.61	33.45
	B 分量	99.59	33.40
Llama	*R* 分量	99.61	33.49
	G 分量	99.60	33.44
	B 分量	99.61	33.44
Sherlock	*R* 分量	99.60	33.41
	G 分量	99.61	33.47
	B 分量	99.60	33.42

4.8. 性能比较

为进一步验证本文提出的加密算法的性能优势，本文选取了两篇相关文献进行对比分析：基于文献[2]实现等长广义 Arnold 变换图像加密，并设置参数 $a=11, b=123$；基于文献[12]实现广义 Gray 码的图像置乱。同时，为了更具针对性地比较，本文在实现广义 Arnold 变换加密和广义 Gray 码加密算法的基础上，对图像进行了双重加密处理，即先进行 Arnold 变换加密，再进行广义 Gray 码加密。本文以 Lena 图像为例进行上述实验，结果见图 4(a)~(d)。



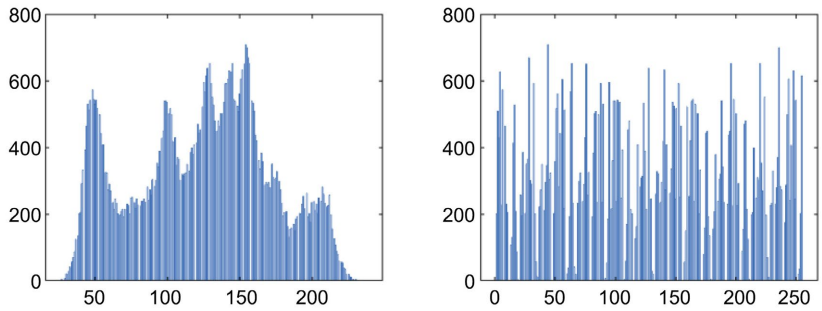
(a) 明文图像　(b) 广义 Arnold 映射加密图像　(c) 广义 Gray 码加密图像　(d) 双重加密图像

Figure 4. Encrypted experiment results
图 4. 加密实验结果

为了能更好地反映该算法的统计特性和空间结构破坏能力，以及扩散性和抗差分攻击能力，本文以 Lena 图像例，选择直方图、相关系数、信息熵和明文敏感性四个指标进行评估。

(1) 直方图分析

分别对图 4(a)、图 4(d)进行直方图分析，得到图 5(a)、图 5(b)。该密文图像直方图(b)柱形高度差异较大，说明不同值出现的频率差异明显，分布不均匀，易被利用这种频率差异进行统计分析，破解部分信息。而本文提出的图像加密算法的密文图像直方图中柱形高度相对较为均衡，表明密文的像素值分布更均匀，攻击者难以从密文直方图中获取关于明文的统计特征，抗统计分析能力更强。



(a) Lena 明文图像　(b) Lena 双重加密图像

Figure 5. Histogram distribution of the Lena image before and after double encryption
图 5. 双重加密前后 Lena 图像的直方图分布

(2) 相关系数分析

在图像加密中，较优的加密算法应能破坏明文图像相邻像素间的相关性，使密文图像相邻像素相关性趋近于 0，降低攻击者通过像素相关性分析破解的可能性。观察表 7 发现，与双重加密算法的相关性系数虽均大幅降低，但本文的加密算法的密文图像的相邻像素的相关性整体上优于双重加密。

Table 7. Correlation coefficients of double encryption
表 7. 双重加密的密文图像的相关系数

Lena 图像相关系数	水平	垂直	正对角	反对角
明文图像	0.9461	0.9691	0.9241	0.9406
密文图像	−0.0065	0.0015	−0.0082	0.0108

(3) 信息熵

通过计算发现，双重加密 Lena 图像的信息熵与明文图像的信息熵均为 7.24，未发生改变。这表明此加密算法未能显著提升密文图像的随机性和信息量。从信息熵的角度来看，此加密算法无法通过增加信息熵来提高密文图像的随机性，从而未能有效增强其安全性和抗破解能力。

(4) 明文敏感性分析

观察表 8 发现，该双重加密算法在 NPCR 和 UACI 指标上与理想值偏差更大，相较于本文提出的图像加密算法，在明文敏感性表现上存在明显不足，加密性能更差。

Table 8. Plaintext sensitivity analysis results (unit: %)
表 8. 明文敏感性分析结果(单位：%)

双重加密 Lena 图像		理论值
NPCR	UACI	99.6094
0.0015	6.4996e−04	33.4635

通过本节的性能比较分析，发现本文提出的图像加密算法不仅覆盖了灰度图像的加密，还成功扩展至彩色图像，从而显著提升了算法的应用范围和实用性。与文献[2]和文献[12]中主要针对灰度图像设计的算法相比，本文算法在随机性、相关性破坏、信息保留和明文敏感性等关键性能指标上展现出更优的性能。此外，本文算法在加密效率和安全性方面具有显著优势。通过结合置乱和扩散机制，本文算法不仅提高了加密过程的效率，还增强了加密结果的安全性。

5. 结论

本文结合广义 Gray 码变换和广义 Arnold 混沌映射，提出了一种新的彩色图像加密算法。该算法利用混沌序列对离散型广义 Arnold 映射与广义 Gray 变换的参数进行动态设置，使得参数与外部密钥高度相关，具有较强的敏感性，可以更好地抵御选择明文、已知明文攻击。加密算法将像素的颜色分量值的高四位比特平面和低四位比特平面实施随机交叉置换，很好地隐藏了图像信息。为了进一步提升密文图像的统计性能和算法的安全性，加密算法在第一次扩散之后，又使用量化后的混沌序列进行进一步的按位比特异或和加取模的扩散。结果表明，本文所设计的加密算法具有很好的安全性和加密性能，可以统计分析攻击、暴力攻击和明文攻击等。

基金项目

论文研究资助项目为广东省大学生创新创业项目以及广东省基础与应用基础研究基金项目(No. 2023A1515030199)。

参考文献

[1] Shannon, C.E. (1949) Communication Theory of Secrecy Systems. *The Bell System Technical Journal*, **28**, 656-715. https://doi.org/10.1002/j.1538-7305.1949.tb00928.x

[2] Ye, R. (2011) A Novel Chaos-Based Image Encryption Scheme with an Efficient Permutation-Diffusion Mechanism. *Optics Communications*, **284**, 5290-5298. https://doi.org/10.1016/j.optcom.2011.07.070

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

[4] Arnold, V.I. and Avez, A. (1968) Ergodic Problems of Classical Mechanics. Benjamin.

[5] 吴成茂. 二维不等长变换改进及其应用[J]. 计算机辅助设计与图形学学报, 2015, 27(8): 1530-1538.

[6] 兰红, 方毅. 非等长 Arnold 变换图像加密算法研究[J]. 江西理工大学学报, 2019, 40(1): 88-94.

[7] 邵利平, 覃征, 高洪江, 等. 二维非等长图像置乱变换[J]. 电子学报, 2007, 35(7): 1290-1294.

[8] 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.

[9] 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.

[10] 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): 339-341.

[11] Gray, F. (1953) Pulse Code Communication. United States Patent 2,632,058.

[12] 王广超, 罗来鹏. 一种广义 Gray 码及其在数字图像置乱中的应用[J]. 赣南师范学院学报, 2007, 28(3): 41-44.

[13] 邹建成, 李国富, 齐东旭. 广义 Gray 码及其在数字图像置乱中的应用[J]. 高校应用数学学报 A 辑, 2002, 17(3): 363-370.

[14] 张帅, 杨雪霞. 非等长 Arnold 变换与 Gray 码相融合的图像加密算法[J]. 太原师范学院学报(自然科学版), 2019, 18(3): 68-72.

[15] 谢国波, 朱柳. 双混沌和广义 Gray 码相融合的图像加密算法[J]. 计算机工程与应用, 2018, 54(16): 197-202.

[16] 梁杰涛, 苏杰彬, 王俊刚, 叶瑞松. 基于混沌和位平面交换的彩色图像加密算法[J]. 图像与信号处理, 2021, 10(2): 88-98.