文章编号:1671-4598(2024)03-0319-08 DOI:10.16526/j.cnki.11-4762/tp.2024.03.047 中图分类号:TP309.7 文献标识码:A

基于混沌系统和动态 DNA 编码的彩色图像加密算法

赵 桥,李 博,项融融
(中北大学 仪器与动态测试教育部重点实验室,太原 030051)

摘要:为了提高图像在传输过程中的安全性,使得用户有更好的体验感,将 Chen 超混沌系统和 DNA 编码引入图像加密领域;彩色数字图像根据红、绿、蓝 3 个通道分为三个二维矩阵,并对三个二维矩阵进行 DNA 分区域编码处理,增加了编码运算的多样性,使得加密过程更加安全;由 Chen 超混沌系统生成的序列决定了每个二维矩阵的 DNA 编码解码规则和运算规则,按照相应规则进行加密,加密后由分段 Logistic 生成相应的序列再次进行行、列置换,分段的 Logistic 混沌映射可以让系统更快地进入混沌状态;合并红、绿、蓝 3 个通道的三个二维矩阵,生成三维矩阵,最终得到相应的彩色加密图像;选取相应的彩色图像进行仿真实验,最终的仿真结果表明,所提出的算法加密效果和相关性能指标良好,同时具有较强的安全性和鲁棒性。

关键词:图像加密;信息安全;Chen 超混沌系统;Logistic 混沌系统;DNA 编码;彩色图像

Color Image Encryption Algorithm Based on Chaos System and Dynamic DNA Encoding

ZHAO Qiao, LI Bo, XIANG Rongrong
(Key Laboratory of Instruments and Dynamic Testing, Ministry of Education, Central North University, Taiyuan 030051)

Abstract: In order to improve the security of images during transmission and provide users with a better experience, the Chen hyperchaos system and DNA encoding are introduced into the field of image encryption; Color digital images are divided into three two-dimensional matrices based on the red, green, and blue channels, and the DNA region encoding is performed on the three two-dimensional matrices to increase the diversity of encoding operations and make the encryption process more secure; The sequence generated by the Chen hyperchaotic system determines the DNA encoding, decoding, and operation rules of each two-dimensional matrix. It is encrypted according to the corresponding rules, and then the segmented Logistic generates the corresponding sequence for row and column permutation, the segmented Logistic chaotic mapping can make the system to enter the chaotic state faster; The three two-dimensional matrices of red, green, and blue channels are merged to generate a three-dimensional matrix, and ultimately obtain the corresponding color encrypted image. The corresponding color images are selected to simulate the simulation experiments, and the final simulation results show that the proposed algorithm has good encryption performance and related performance indicators, which has a high security and robustness.

Keywords: image encryption; information security; chen hyperchaotic system; logistic chaotic system; DNA encoding; color image

0 引言

信息技术的飞速发展推动了社会各个领域的发展,改变了人们的工作和学习方式,社会生产力也得到极大的提升。在享受这个时代带来种种便利的同时,人们自身的信息安全也会受到威胁[1]。

在这种背景下,图像加密技术开始出现。图像加密是一门融合了图像处理和密码学等领域的新型交叉学科,它可以保护图像中的敏感数据,避免非授权访问或窃取、篡改图像。通过加密,只有授权的用户才能访问受保护的图像。此外,随着信息技术的不断发展,不法分子破译的手段也在不断提升。在此背景下,研究新的图像加密技术刻不容缓[2]。

混沌系统因为其初值敏感性、有界性、不可预测性等优点,刚好被运用在图像加密领域。近几年基因工程也在飞速发展,使人们的目光同样聚焦到生物学上。科学家们将 DNA 数据链可以携带大量信息的特征与二进制数据链的特点相比较[3],将生物学和计算机科学进行了特殊的结合,凭借 DNA 序列的一些优点,如具有很高的并行性和存储空间大等优点,研究出了基于 DNA 序列的图像加密方法。同时,研究者们将目光聚焦于混沌系统和 DNA 编码技术相结合的图像加密技术,事实也证明了基于混沌系统和 DNA 的

收稿日期:2023-04-21; **修回日期**:2023-05-29。
基金项目:国家自然科学基金(61471325);国家自然科学基金青年科学基金(52006114)。
作者简介:赵 桥(1995-),男,硕士研究生。
引用格式: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.

图像加密技术是大有可为的。

针对混沌系统和 DNA 的图像加密技术，一些文献中已经提供了不同的思路和方法。文献［4］中研究者们初步将混沌系统和 DNA 序列相结合，提出一种新的图像加密技术，该算法虽然一定程度上可以保证加密图像的安全，但是没有对抗噪声和抗剪切性的分析，同时也不能很好地抵御外来攻击。文献［5］中研究者们将 Logistic 混沌系统和 DNA 编码相结合，得到了一种图像加密方案，该方案可以将 8 种 DNA 加密算法规则混合到一起，很明显地提高了算法的置乱和扩散效率，可以较好的抵御外部的明文攻击。文献［6］中研究出一种基于分块置乱和混沌系统的加密算法，该算法中的分块、分区域思想可以很好地应用到 DNA 的碱基运算过程中。文献［7］则是研究出一种同步排列扩散技术，可以在 DNA 序列的基础上对像素进行置乱和扩散。文献［8］中研究者们提出了一种基于混沌系统和 DNA 编码的图像加密算法，该算法将混沌系统和 DNA 很好的结合在一起，但是在实现过程中，DNA 编码过程不是动态编码，碱基运算的复杂程度和混沌系统的稳定性都不够高。文献［9］中利用变步长约瑟夫遍历的方法，结合动态 DNA 编码规则，提出了一种全新的算法，该算法碱基运算规则复杂，有较好的安全性。文献［10］在混沌系统和 DNA 编码结合的基础上，引入了一种哈希函数，得到一种新的算法，该算法具有很好的抗差分攻击的能力，但其缺少相关的鲁棒性能。文献［11］将超混沌系统引入图像加密领域中，该算法一定程度上提高了算法的安全性，但其密钥空间不够大，不能很好地抵御穷举攻击。文献［12］将 logistic 混沌系统和动态 DNA 编码相结合，且拓展到了彩色图像加密领域，该算法的加密效果良好，但是该算法缺少相关鲁棒性能的分析。

由上述可知，虽然目前混沌系统结合 DNA 的加密算法已经取得了一些研究成果，但是依然存在一些问题，比如密钥空间较小、密文的熵值较低、抗攻击能力弱等，本文针对上述问题进行设计算法和深入研究。本文的主要贡献如下：

1）将普通的一维和多维混沌系统升级为 Chen 超混沌系统，同时结合了分段 Logistic 混沌映射，使系统可以更快进入混沌状态的同时，也变得更加稳定，加密效果更好。采用 DNA 编码规则进行编码，且动态 DNA 编码进一步增加了编码运算的多样性，让加密过程更安全。

2）将传统灰度数字图像的加密算法扩展至彩色数字图像，使得算法的应用范围更广泛。

1 基本理论

1.1 密钥系统

密码学是一门研究信息保密的学科，涉及到加密、数字证书和其他安全计算技术等。它使用密码、密钥和数学算法等对数据进行特殊加密，以达到保护数据的目的。

现代密码学的核心思想是通过使用特定的加密算法来加密明文序列，接收者再通过特定的解密密钥对加密文件进行解密，得到最初的明文序列。具体的工作流程如图 1 所示。

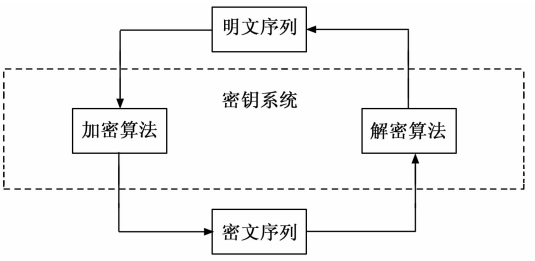


图 1 加密流程图

1.2 加密算法的性能分析

加密算法的好坏可以用不同的指标来进行衡量和比较。密钥空间越大，破解的难度就会呈几何倍的提升，抵御外来攻击的能力就会越强。直方图是否均匀分布也可以体现出加密算法的好坏，加密后的直方图分布越均匀，加密算法的效果越好。其他的一些性能指标，如相邻像素相关性、信息熵、抗差分攻击、密钥敏感性、抗噪声性能和抗剪切性能等也都可以分析出加密算法的好坏。

1.3 混沌系统

混沌理论是一个在复杂性科学领域里非常本质的理论。混沌是一种非常特殊的现象，它具有对初值的高度敏感性，有一定的边界，没有周期性。像被人们所熟知的“蝴蝶效应”理论，即“南美洲的一只蝴蝶扇一扇翅膀，就可能在佛罗里达州引起一场飓风”，这句话描述的就是一种典型的混沌现象。

混沌系统在图像加密领域中，根据不同的维度可以将其分为低维和高维混沌系统；根据混沌系统的 Lyapunov 指数是否有一个正数，可以将其分为普通混沌系统和超混沌系统。下面对一些常用的混沌系统进行介绍。

1.3.1 Logistic 混沌系统

Logistic 混沌映射[13]是一种一元二次的单峰映射，是生态学中的虫口模型，又叫 Logistic 迭代，可以用下式进行表示：

$$x_{k+1} = \mu x_k(1 - xk) \tag{1}$$

图 2 为 Logistic 的映射分叉图，从图中可以看到，当 $\mu = 3$ 时，系统开始出现分叉；当 μ 增大到 3.569 9 时，系统开始出现混沌状态；当 $\mu = 4$ 时，映射达到满映射，进入全混沌的状态。

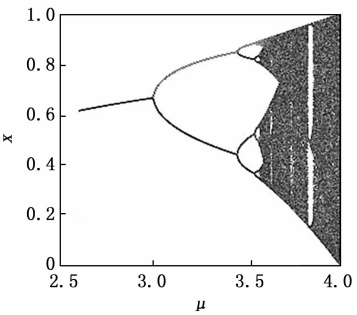


图 2 Logistic 的映射分叉图

对 Logistic 混沌映射进行分段，具体公式如下：

$$x_{n+1}=\begin{cases}1-4*\mu*(x_n+0.5)^2 & -1<x_n<0\\ 4*\mu*(x_n-0.5)^2-1 & 0\leqslant x_n<1\end{cases} \tag{2}$$

式中，$x_0\in(-1,1)$，$\mu\in[0,2]$，且分段后增加了初始值的范围，减小了映射参数，使该系统可以更快的进入混沌系统。

1.3.2　Chen 混沌系统

1999 年，我国的陈关荣教授，在 Lorenz 系统的基础上进行了改进设计，提出了结构更为复杂的 Chen 系统[14]。

$$\begin{cases}x^{\cdot}=\alpha y-\alpha x\\ y^{\cdot}=(\gamma-\alpha)x-xz+\gamma y\\ z^{\cdot}=xy-\beta z\end{cases} \tag{3}$$

根据上式可得，当 $\alpha=35$，$\beta=3$，$\gamma=28$ 时，Chen 系统进入混沌状态。

1.3.3　Chen 超混沌状态

将 Chen 混沌状态作为基础，对其进行升级改造得到了四维的 Chen 超混沌状态，其密钥空间更大，系统复杂程度更高，加密效果也更好[15]。系统的动态方程如下：

$$\begin{cases}\dot{x}=a(y-x)+q\\ \dot{y}=bx+cy-xz\\ \dot{z}=xy-dz\\ \dot{q}=yz+eq\end{cases} \tag{4}$$

上式中：a、b、c、d、e 表示该系统的参数，x、y、z、q 表示该系统的变量。当系统参数值 $a=35$，$b=7$，$c=12$，$d=3$，$e\in(0.085,0.798]$ 时，可以计算出该系统的 Lyapunov 指数存在两个正值，此时的 Chen 混沌满足了超混沌的定义，即该系统是超混沌系统。

超混沌系统相比于高维和低维系统的内部更加复杂，因此其具有更好的加密效果。

1.4　DNA 编码

DNA 编码技术是一种将分子生物技术和计算机技术结合在一起的新学科。该技术利用 DNA 的伪运算进行信息隐藏和加密。

DNA 的全称是脱氧核苷酸，是一种双链结构的高分子化合物[16]，其由 4 种脱氧核苷酸组成，分别为：腺嘌呤（A）、鸟嘌呤（G）、胞嘧啶（C）、胸腺嘧啶（T）。其中 A 和 T 互补，G 和 C 互补。因为计算机只有二进制 0 和 1，而 0 和 1 是互补的，01 和 10 互补，00 和 11 也是互补的。因此，A、G、C、T 可以用于计算机的编码，共有 24 种方案。但是由于互补原则，其中只有 8 种方案可使用，如表 1 所示。

表 1　DNA 编码和解码规则

规则	1	2	3	4	5	6	7	8
A	00	00	01	01	10	10	11	11
T	11	11	10	10	01	01	00	00
G	01	10	00	11	00	11	01	10
C	10	01	11	00	11	00	10	01

如对一像素值为 228 的像素点进行编码时，先将其变为二进制编码“11100100”，对应 8 种不同的编码规则，即：AGCT，ACGT，GTAC，GATC，CTAG，CATG，TGCA，TCGA。当对一图像进行加密时，加密算法采用一种 DNA 编码规则，解密算法采用另一种 DNA 解码规则时，像素值可以被有效的加密，无法恢复原来的图像。DNA 编码的多样特性可以使图像的加密过程更加安全。还是对像素值为 228 的图像进行加密，用规则 2 对其进行编码得到 DNA 序列为 TGCA，再使用规则 8 对其进行解码得到二级制数 00100111，其对应像素值为 39，与原图像的像素值差距很大，因此 DNA 编码可以很好的保护图像信息的安全。

2　加密算法设计

2.1　加密算法整体框架

本文所提出的新算法大致包括了以下内容：Chen 超混沌系统、DNA 的编码解码和运算、区域分块运算、分段 Logistic 混沌映射和三通道红、绿、蓝彩色图像等几部分。

首先将彩色数字图像根据红、绿、蓝 3 个通道分为三个二维矩阵，并对 3 个矩阵进行 DNA 分区域编码处理；其次由 Chen 超混沌系统生成的序列决定了每个二维矩阵的 DNA 编码解码规则和运算规则，按照相应规则进行加密，加密后由分段 Logistic 生成相应的序列再次进行行、列置换，分段的 Logistic 混沌映射可以让系统更快的进入混沌状态；合并红、绿、蓝 3 个通道的 3 个矩阵，生成三维矩阵，最终得到相应的彩色加密图像。

DNA 碱基之间的区域分块运算规则增加了编码运算的多样性，使得加密过程更加安全。分段 Logistic 混沌映射迭代得到的 3 个不同的混沌序列，一个用于与原始图像进行 DNA 运算，一个用于行置换，一个用于列置换，在增强密文图像的置乱效果的同时可以获得抗裁剪的特性，同时分段的 Logistic 混沌映射可以使系统更快进入混沌系统，更好地保证图像在传输过程中的安全性。具体加密流程如图 3 所示。

2.2　加密算法具体步骤

1）读取一张大小为 $M\times N$ 的原始图像 P，将其按照红（R）、绿（G）、蓝（B）3 个通道分为三个二维矩阵，分别为 $\boldsymbol{P}_1$、$\boldsymbol{P}_2$、$\boldsymbol{P}_3$。分离方式如下：

$$\begin{cases}\boldsymbol{P}_1=p(:,:,1)\\ \boldsymbol{P}_2=p(:,:,2)\\ \boldsymbol{P}_3=p(:,:,3)\end{cases} \tag{5}$$

2）设置分块大小 t，使 1）中的 $\boldsymbol{P}_1$、$\boldsymbol{P}_2$、$\boldsymbol{P}_3$ 矩阵都能分成 t^2 个大小的块。

3）设定参数 μ 和初值 x_0 作为加密的密钥，使 μ 为 3.999，初始值 x_0 进行如下处理：

$$x_0=\frac{sum(p_1(:))+sum(p_2(:))}{255\times 2\times M\times N} \tag{6}$$

其中：sum 表示像素的总和，x_0 为 P_1 和 P_2 的灰度平均值。

4）对分段 Logistic 混沌映射迭代得到序列 K，将 K 转

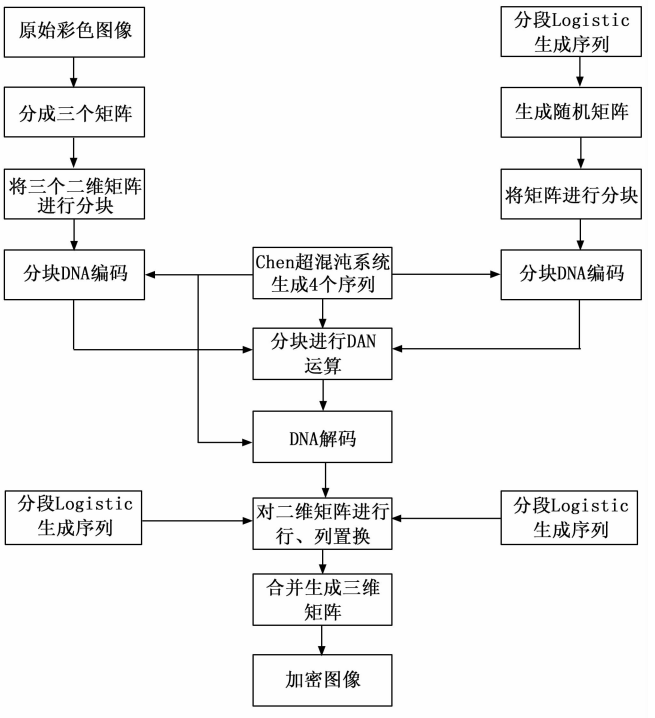


图 3 具体加密流程图

换为 $M\times N$ 的二维矩阵，其范围规定在 0 到 255。

5）计算超混沌系统，得到 4 个序列 X，Y，Z，H，其长度均为 $\frac{M\times N}{t^2}$。设定 Chen 超混沌系统的初始值分别为 X_0、Y_0、Z_0、H_0，计算方式如下式：

$$\begin{cases} X_0 = \dfrac{sum(sum(bitand(\boldsymbol{P}_1,17)))}{(17\times M\times N)} \\ Y_0 = sum\ \dfrac{(sum(bitand(\boldsymbol{P}_2,34)))}{(34\times M\times N)} \\ Z_0 = sum\ \dfrac{(sum(bitand(\boldsymbol{P}_3,68)))}{(68\times M\times N)} \\ H_0 = sum\ \dfrac{(sum(bitand(\boldsymbol{P}_1,136)))}{(136\times M\times N)} \end{cases} \tag{7}$$

X_0、Y_0、Z_0、H_0 4 个值在算法中也可以作为密钥使用。

6）DNA 共有 8 种编码方式，记为规则 1 到规则 8。由 Chen 超混沌系统产生了 4 个序列 X、Y、Z 和 H，将 4 个序列进行如式（8）处理。序列 X 决定三个二维矩阵编码的方式，序列 Y 决定 $\boldsymbol{R}$ 矩阵的 DNA 编码方式，序列 Z 决定三个二维矩阵和 $\boldsymbol{R}$ 的运算规则，序列 H 决定 DNA 的解码规则。序列 Z 决定 4 种 DNA 运算规则，序列 X、Y、Z 则是对应有 8 种 DNA 编码解码方式。

$$\begin{cases} X = mod(round(X\times 10^4),8)+1 \\ Y = mod(round(Y\times 10^4),8)+1 \\ Z = mod(round(Z\times 10^4),4) \\ H = mod(round(H\times 10^4),8)+1 \end{cases} \tag{8}$$

7）运算规则由序列 Z 决定，当 $Z=0$ 时，采用加法运算；$Z=1$ 时，采用减法运算；$Z=2$ 时，采用异或运算；$Z=3$ 时，采用同或运算。

8）采用分区域分块运算，将当前的加密结果和前一块的再次进行 DNA 运算。DNA 解码运算时 DNA 编码运算的逆过程，由序列 H 决定，把 A、G、C、T 解码成对应的数值。

9）获得两个 Logistic 混沌序列 K_1 和 K_2，过程与 3）类似。两个初值 x_{01} 和 x_{02} 根据式 9 产生。X_{01} 表示 R 通道和 B 通道的平均灰度值，x_{02} 表示 G 通道和 B 通道的平均灰度值，两个值可以作为本加密算法的密钥。

$$\begin{cases} x_{01} = \dfrac{sum(\boldsymbol{P}_1(:))+sum(\boldsymbol{P}_3(:))}{255\times 2\times M\times N} \\ x_{02} = \dfrac{sum(\boldsymbol{P}_2(:))+sum(\boldsymbol{P}_3(:))}{255\times 2\times M\times N} \end{cases} \tag{9}$$

10）对 9）中的序列 K_1 和 K_2 进行降序操作。对 $\boldsymbol{R}$、$\boldsymbol{G}$、$\boldsymbol{B}$ 这 3 个通道的矩阵进行置换，获得更好的置乱效果。

11）将三个二维矩阵进行合并成一个三维矩阵，得到加密后的图像。

2.3 解密算法设计

2.3.1 解密算法整体框架

解密过程就是加密过程的逆过程，即解密过程中采取和加密过程的相反操作。解密过程要注意：1）要使用和加密时完全相同的密钥；2）DNA 的解码是加密过程中 DNA 的编码，DNA 的编码是加密过程中的解码。正确地进行解码操作才能得到和原图完全相同的解密图像。

2.3.2 解密过程具体步骤

解密过程的步骤即为加密过程的反过程。图 4 是解密算法的具体流程图。

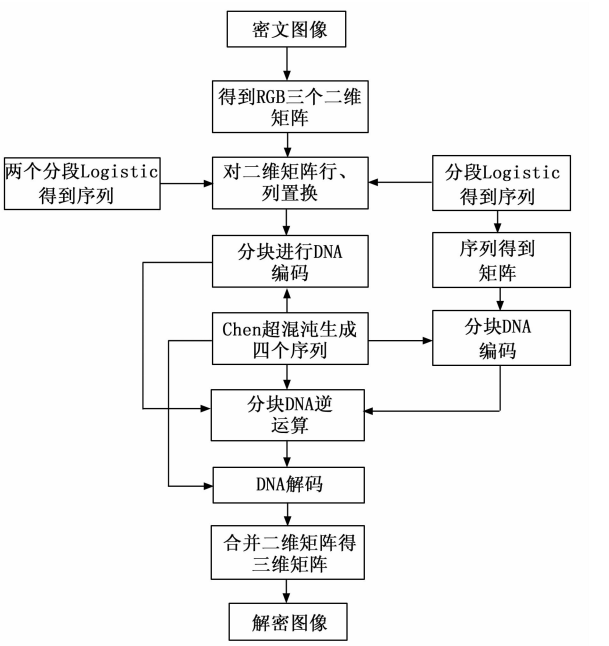
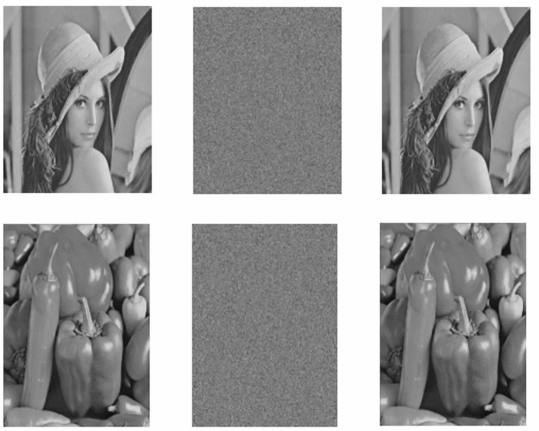


图 4 解密算法的具体流程图

3 仿真结果

本次的仿真过程借助 Matlab 2018a 平台，8 GB 内存计算机，Win7 操作系统上实现。此实验中使用了经典的 Lena

和 Peppers 两种彩色图像，像素大小均为 512 ×512 ，原图像如图 5（a）所示。经过本章算法加密后的图像如图 5（b）所示，从图像（b）我们可以清晰的看出，经过加密后的图像呈现出一种雪花状的噪声状态，完全隐藏了原始图像的信息，且通过和原图（a）的对比，看不到任何的相关信息，有很好的加密效果。解密后的图像如图 5（c）所示，和原始彩色图像完全相同。由此可以得出结论，仅从仿真角度来看，本章算法可以达到很好的加密和解密效果。



(a)原始图像　(b)加密图像　(c)解密图像

图 5　仿真结果图

3.1　仿真结果相关性能分析

3.1.1　密钥空间分析

Chen 超混沌系统中的 4 个初值 X_0、Y_0、Z_0、H_0 可以作为算法的密钥，此外运用到了三次分段 Logistic 混沌映射，参数 μ 是相同的，三次的初值则不同，分别为 x_0、x_{01} 和 x_{02}，共有 8 个值作为算法密钥。通常在 64 位计算机操作系统下，浮点数的精度为 10^{-16}，则此算法的密钥空间容量为 $10^{16}\times 10^{16}\times 10^{16}\times 10^{16}\times 10^{16}\times 10^{16}\times 10^{16}\times 10^{16}=10^{128}$。且该算法也可以设置 3 种不同的 Logistic 混沌映射的参数 μ，此时密钥空间将增大到 10^{160}。当密钥空间的大小超过 2^{100}时，说明了该算法基本满足了密钥空间的安全需求。该算法密钥空间远大于安全密钥空间的基本要求，可以很好地抵御穷举攻击，保证信息的安全性[17]。

3.1.2　直方图分析

以色彩特征更为明显的图像 Peppers 为例，该算法的直方图仿真结果如图 6 所示。原始彩色图像 R（红）、G（绿）、B（蓝）3 个通道的直方图曲线十分陡峭，高低分布显著不同。而加密图像的直方图中，各线条均匀分布，高低在一定的数值上下波动。因此可以得出结论，本文算法具有很好的抵御统计分析的能力，即使被攻击，也不会被攻击者得到有用的信息[18]。

3.1.3　信息熵分析

信息熵可以表示一个系统的复杂程度，一个系统越是有序，信息熵就越低；相反的，一个系统越是复杂混乱，信息熵就越高。信息熵越接近 8，密文信息越安全[19]，信

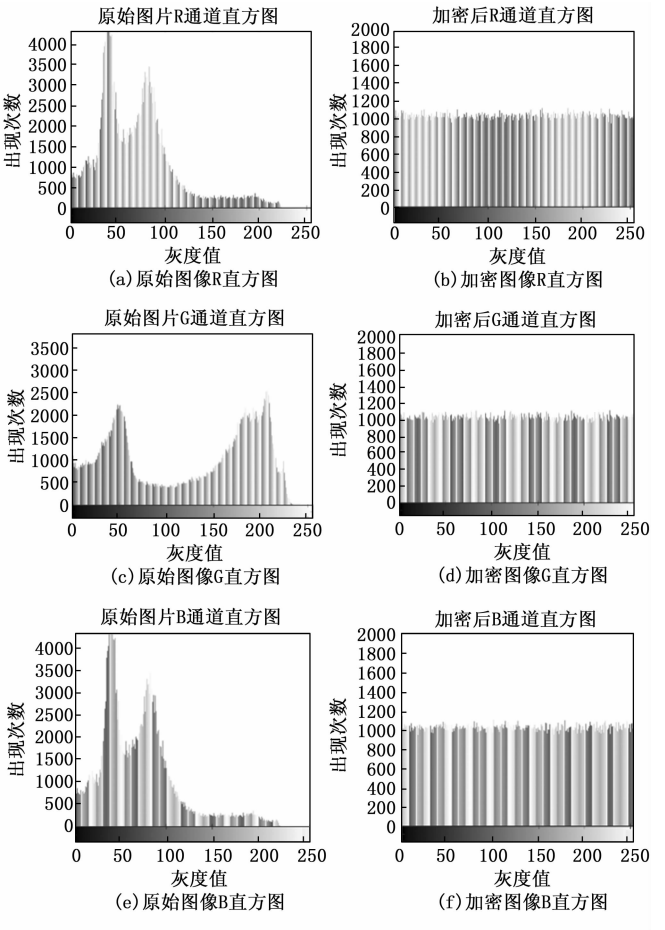


图 6　加密前后 R、G、B 三通道图像的直方图

息熵的计算公式如式（10），式中 m_i 表示图像的灰度值。

$$H_{(m)}=\sum_{i=1}^{2N-1}p(m_i)\log_2\frac{1}{p(m_i)} \tag{10}$$

彩色图像 Peppers 在加密前后的 3 个通道 R、G、B 的信息熵值，以及和其他文献算法加密图像的比较如表 2 所示。

表 2　原始图像和密文图像信息熵对比

通道	R	G	B
原始图像	7.338 8	7.496 3	7.058 3
加密图像	7.999 3	7.999 3	7.999 4
文献[20]	7.999 4	7.997 1	7.997 7
文献[21]	7.999 4	7.998 5	7.998 7

由表 2 可以看出，加密图像的信息熵相较于原始图像有很明显的增加，且都非常接近理论信息熵的最大值 8，说明了密文图像的混乱程度非常高。同时本文算法加密后的信息熵值总体大于文献［20］和文献［21］的加密算法，由此可以得出结论，该算法能够很好地抵御外部攻击，能保证密文信息的安全。

3.1.4　相邻像素点的相关性

相关性分析是分析图像像素之间的关联性强弱，一般明文图像相关系数很接近 1，说明该图像的相关性高，体现

在相关性系数点图上为图像总体呈线性分布。而加密算法则是要打破像素点之间的强关联系性，使相关系数降低。密文相关性越接近 0，加密效果越好。经过仿真实验对水平、垂直和对角线 3 个方向的分析，随机选取 5 000 对相邻像素计算其相关性，计算公式如式（11）：

$$\begin{cases} Dx = \dfrac{1}{n}\sum_{i=1}^{n}[x_i - E(x)]^2 \\ cov(x,y) = \dfrac{1}{n}\sum_{i=1}^{n}[x_i - E(x)][y_i - E(y)] \\ r_{(x,y)} = \dfrac{cov(x,y)}{\sqrt{D(x)}\ \sqrt{D(y)}} \end{cases} \tag{11}$$

式中，$E(x)$，$E(y)$ 表示相邻像素点之间的期望值，n 表示像素点的个数，$cov(x,y)$ 表示协方差，$r_{(x,y)}$ 表示相关系数。

表 3 为彩色图像 Peppers 原始图像和密文图像分别在 R（红）、G（绿）、B（蓝）3 个通道的相邻位置相关性的数据对比，即相关性系数的大小比较。

表 3 相关性系数大小比较

	原图			密图		
	R	G	B	R	G	B
水	0.959 3	0.982 1	0.966 7	−0.014 6	0.000 4	0.004 0
垂	0.965 8	0.979 9	0.966 6	0.017 8	0.019 7	0.011 5
对	0.952 5	0.967 4	0.947 5	0.003 2	0.014 2	0.027 5

由表 3 可以得出，原始图像的 R（红）、G（绿）、B（蓝）3 个通道的水平、垂直和对角线系数都很大，很接近于 1，说明加密前的图像像素点之间的相关性都很高。而密文图像的 R、G、B3 个通道的水平、垂直和对角线系数都很接近 0，说明加密后的图像像素间基本没有关联性，从加密图像上得不到一点关于原图像的有用信息，加密效果良好。

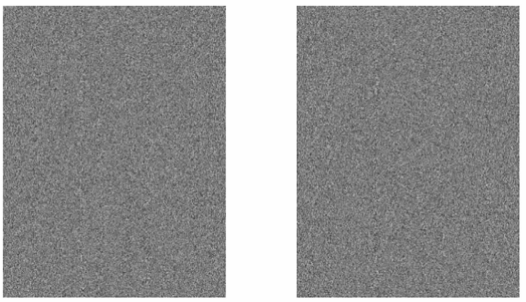
3.1.5 密钥敏感性分析

密钥敏感性[22]分析主要是通过对初始密钥进行一个极小的改变，最终导致图像解密失败，这样就可以说该算法密钥敏感性高，可以很好地保证加密图像的安全性。除了根据均方差 MSE 判断外，还可以对初始密钥进行极小的改变，观察是否能解密出清晰的图像。本章在解密过程中，让初始密钥之一的 μ 产生极其微小的变化，由 3.999 变为 3.999 000 001，利用修改后的密钥对其进行解密操作，不能得到清晰的解密图像如图 7（a）所示。再对另一初始密钥 x_0 的值进行改变，由 0.547 5 变为 0.547 499 999 9，得到错误密钥下的解密图像如图 7（b）所示。

从图 7 中可以明显看出，即使初始密钥发生了极其微小的变化，解密后得到的图像也和原始图像完全不相同，没有任何联系。说明了本章设计的算法对密钥具有极高的敏感性，同样的算法安全性也高。

3.1.6 抗差分攻击能力分析

抗差分攻击则是对原始图像的一部分特定区域进行分析和攻击，最后得到不同像素点占总体像素点的部分数。对于一个加密算法而言，像素点的变化导致加密图像发生明显的改变，对加密结果的影响大，那么它就可以有效抵御差分攻击。NPCR 和 UACI 是定量测试分析原始图像和加密图像的方法[23]，具体计算方法如式（12）和（13）。



(a) μ 改变后的解密图像　(b) x_0 改变后的解密图像

图 7 密钥改变时的解密图像

$$NPCR = \frac{\sum_{i,j} E(i,j)}{m \times n} \times 100\% \tag{12}$$

$$UACI = \frac{1}{m \times n}\sum_{i,j}\left|\frac{F_1(i,j) - F_2(i,j)}{255}\right| \times 100\% \tag{13}$$

表 4 和表 5 为本章加密算法和与其他文献算法的对比结果，且比较对象都是 Peppers 图像，表对比结果可以看出本章算法具有很好的抗差分攻击能力。

表 4 图像 NPCR 数据分析对比

通道	本章算法	文献[20]	文献[21]
R	99.624 5	99.619 0	99.618 2
G	99.611 0	99.618 2	99.617 7
B	99.614 6	99.622 2	99.627 2

表 5 图像 UACI 数据分析对比

通道	本章算法	文献[20]	文献[21]
R	33.658 2	33.612 6	33.681 3
G	33.686 8	33.648 0	33.536 4
B	33.621 1	33.613 0	33.650 6

3.1.7 抗剪切性能分析

抗剪切能力是指在进行图片加密处理过程中，加密后的图片在遭遇剪切攻击时，可以保证加密后的形态不被歪曲或改变的功能。本次实验选取一张布满文字的数字图像，对其加密得到加密后的图像，并对加密图像进行剪切性攻击，最后对该图像进行解密操作，如图 8 所示。

从图 8 可以看出，虽然对密文图像的一些区域进行了剪切，但本章算法能够将对局部区域的破坏转移到整体图像上，虽然最终的解密图像没有原始图像清晰，但是本算法能确保关键信息的不丢失。如本实验的图像，经剪切后依旧能得到每个字的信息，没有被破坏遗漏，保持了整张图像的完整性。上述结果表明本章算法的抗剪切能力强，适用于包含细节关键信息图像的加密。

3.1.8 抗噪声性能分析

为了测试本章算法的抗噪声性能，分别对密文图像加

图 8　抗剪切性能效果图

入不同程度的噪声进行干扰。加入不同程度噪声后的解密图像结果示意图如图 9 所示。从图像中可以清楚的看到，随着噪声的程度加大，图片的质量也随着变差，越来越模糊，但是仍然能分辨出图像的主要信息，没有信息的丢失，说明了本章算法的抗噪声能力强，安全性能好。

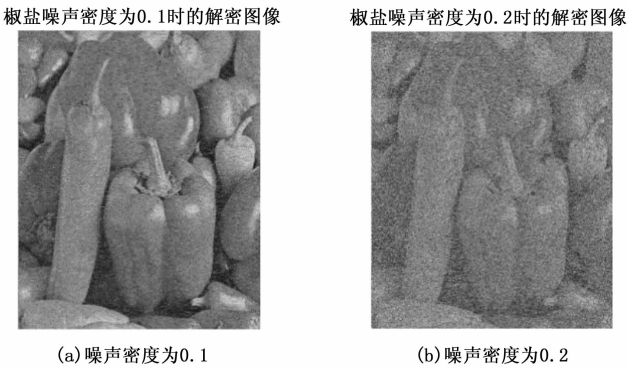


图 9　不同程度噪声下解密图像的效果图

峰值信噪比（PSNR）和均方误差（MSE）可以从抗噪声方面对图像质量进行评价。在加密后的图像中依次加入椒盐噪声密度为 0 到 1，密度间隔为 0.1 的椒盐噪声得到对应的解密图像，MSE 和 PSNR 的值分别可以由式（14）和式（15）计算，并绘制出相应的椒盐噪声密度－均方误差 MSE 曲线图和椒盐噪声密度－峰值信噪比 PSNR 曲线图如图 10 所示。

$$MSE = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N}[G(i,j) - K(i,j)]^2 \quad (14)$$

式中，用 G 和 K 分别表示原始图像和加密过后的图像的二维序列。分别可以具体表示为 $M = \{M(i,j)\}$ 和 $N = \{N(i,j)\}, i = 1,2,\cdots,M; j = 1,2,\cdots,N$。

$$PSNR = 10\lg\frac{255^2}{MSE} \quad (15)$$

由图 10 可以看出，当椒盐噪声值密度小于 0.4 时，该算法抗噪声能力强；当椒盐噪声密度达到 0.4 时，图像基本处于失真状态，受噪声影响很大。

4　结束语

本文所提出算法包括以下内容：首先将彩色数字图像

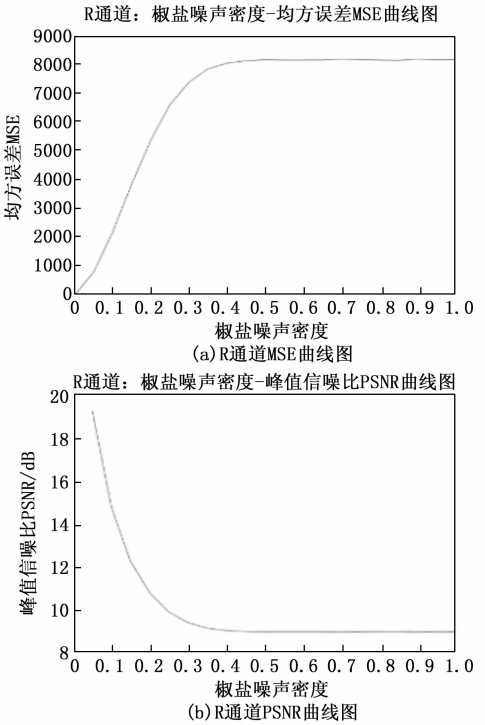


图 10　R 通道加入噪声后的 MSE 和 PSNR 曲线图

根据红、绿、蓝 3 个通道分为 3 个二维矩阵；其次由混沌系统生成的序列决定了每个二维矩阵的 DNA 编码解码规则和运算规则；合并红、绿、蓝 3 个通道的 3 个矩阵，生成三维矩阵，最终得到相应的彩色加密图像。通过仿真结果以及和其他算法的比较分析，可以得出结论：该算法和其他的算法相比，密钥空间更大，相关性系数极小，有良好的抗噪声和抗剪切性能，还能适用于彩色图像的加密，可以满足用户很高的加密需求。

未来的图像加密领域仍会有极大的发展空间，本文算法虽然能够有效保证图像加密的安全性，但是也存在着一些缺陷。该算法密钥空间很大，加密效果良好，且可以应用于彩色图像的加密设计，有良好的抗噪声和抗剪切性能，但是加密速度较慢，算法也更加复杂。以后的研究方向可以从下列几个方面进行入手：1）对算法的复杂度、安全性和加密速度之间要做出一定的平衡，做到最大程度的兼顾。2）与不同领域进行结合研究，如本文的所用到的 DNA 编码就是生物学领域的方法，还可以考虑与生态学、化学等领域相结合。3）将图像加密延伸到视频加密，图像加密是视频加密的基础，在算法方面可以朝着视频加密的方向去研究。

参考文献：

[1] 李志远，蒋爱平，沈彦琦. 基于 Chen 超混沌和 DNA 编码的图像加密算法 [J]. 黑龙江大学自然科学学报，2020，37（5）：602－609.

[2] CAO W J，MAO Y J，ZHOU Y C. Designing a 2D infinite collapse map for image encryption [J]. Signal Processing，2020，

171 (c): 107457 - 107457.
[3] M A B F, R G, A K, et al. A novel chaos based optical image encryption using fractional Fourier transform and DNA sequence operation [J]. Optics and Laser Technology, 2020, 121 (c), 105777 - 105777.
[4] ZHANG Q, GUO L, WEI X P. Image encryption using DNA addition combining with chaotic maps [J]. Mathematical and Computer Modelling, 2010, 52 (11): 2028 - 2035.
[5] ZHEN P, ZHAO G, MIN L, et al. Chaos - based image encryption scheme combining DNA coding and entropy [J]. Multimedia Tools and Applications, 2016, 75 (11): 6303 - 6319.
[6] 王 纪. 一种基于分块置乱和混合混沌的图像加密算法 [J]. 长江信息通信, 2021, 34 (10): 64 - 66.
[7] RASUL E, ABDUL H A, ISMAIL F I, et al. Image encryption using a synchronous permutation - diffusion technique [J]. Optics and Lasers in Engineering, 2017, 90 (7): 146 - 154.
[8] ZHANG X Q, WANG X S. Multiple - image encryption algorithm based on DNA encoding and chaotic system [J]. Multimedia Tools and Applications, 2019, 78 (6): 7841 - 7869.
[9] 牛 莹, 张勋才. 基于变步长约瑟夫遍历和 DNA 动态编码的图像加密算法 [J]. 电子与信息学报, 2020, 42 (6): 1383 - 1391.
[10] 蒋 刚, 郭 祥, 杨 晨, 等. 混沌和 DNA 运算结合的图像加密算法仿真 [J]. 计算机仿真, 2021, 38 (5): 176 - 180.
[11] SUN S L. A novel hyperchaotic image encryption scheme based on DNA encoding, pixel - level scrambling and bit - level scrambling [J]. IEEE Photonics Journal, 2018, 10 (2): 1 - 14.
[12] 杨吉云, 吴 昊. 基于混沌系统和动态 DNA 编码与运算的彩色图像加密算法 [J]. 计算机工程, 2018, 44 (2): 151 - 157.
[13] MAY R M. Simple mathematical models with very complicated dynamics [J]. Nature, 1976, 261 (5560): 459 - 67.
[14] 彭建奎, 俞建宁, 张建刚, 等. Chen 系统的混沌控制研究 [J]. 成都大学学报 (自然科学版), 2008 (2): 120 - 122.
[15] 张 健, 霍 达. 基于混沌系统的量子彩色图像加密算法 [J]. 西南交通大学学报, 2019, 54 (2): 421 - 427.
[16] 黄迎久, 徐 扬, 李海荣. 基于 DNA 编码和超混沌系统的图像加密算法 [J]. 内蒙古科技大学学报, 2018, 37 (3): 246 - 254.
[17] CHEN, Z., I, et al. Two - level chaos - based video cryptosystem on H. 263 codec [J]. Nonlinear Dynamics, 2011, 62 (3): 647 - 664.
[18] ZAFAR S, MARC C, WILLIAM P. Fast protection of H. 264/AVC by selective encryption of CAVLC and CABAC for I and P frames [J]. IEEE Trans. Circuits Syst. Video Techn, 2011, 21 (5): 565 - 576.
[19] 程东升, 谭旭, 许志良, 等. 结合四维超混沌系统和位分解的图像加密算法研究 [J]. 电子科技大学学报, 2018, 47 (6): 906 - 912.
[20] AKRAM B, AHMED A. A E, SAFYA B. A novel image encryption scheme based on substitution - permutation network and chaos [J]. Signal Processing, 2016, 128 (15): 155 - 170.
[21] HUA Z Y, ZHOU Y C, PUN C M, et al. 2D Sine Logistic modulation map for image encryption [J]. Information Sciences, 2015, 297 (7): 80 - 94.
[22] 田传俊, 陈关荣. 关于变参数离散 Devaney 混沌系统 [J]. 深圳大学学报, 2006 (1): 16 - 20.
[23] CHEN G R, MAO Y B, CHUI C K. A symmetric image encryption scheme based on 3D chaotic cat maps [J]. Chaos, Solitons and Fractals, 2004, 21 (3): 749 - 761.

(上接第 318 页)

[4] LIU W M, YAN P L, ZHU L L. Standardization of Maglev Technoligy inChina [A]. Maglev 2014 [C] // Rio de Janeiro, Brazil, September 28th-October 1st.
[5] 李培署, 王风洲. 我国高速动车组制动技术现状及未来技术发展探讨 [J]. 铁道车辆, 2018, 56 (9): 1 - 5.
[6] 熊嘉阳, 沈志云. 中国高速铁路的崛起和今后的发展 [J]. 交通运输工程学报, 2021, 21 (5): 6 - 29.
[7] ZHANG K, CHAI Y, LIU J. A class of category discrimination based model frameworks for multiple fault diagnosis [J]. Kongzhi Lilun Yu Yingyong/Control Theory and Applications, 2016, 33 (2): 154 - 163.
[8] ISERMANN R. Fault-diagnosis systems: An introduction from fault detection to fault tolerance [M]. Springer Berlin Heidelberg, 2006.
[9] BERNARAS A, LARESGOITI I, BARTOLOME N, et al. Ontology for fault diagnosis in electrical networks, Orlando, FL, USA, 1996 [C] // IEEE, 1996.
[10] 程建峰, 苏晓峰. 磁悬浮列车的发展及应用 [J]. 铁道车辆, 2003 (11): 14 - 17.
[11] 张 帆. 高速铁路与中国区域经济发展研究 [D]. 重庆: 重庆大学, 2019.
[12] 李培署, 王风洲. 我国高速动车组制动技术现状及未来技术发展探讨 [J]. 铁道车辆, 2018, 56 (9): 1 - 5.
[13] 吴祥明. 磁浮列车 [M]. 上海: 上海科学出版社, 2003.
[14] 苗 欣. 高速悬浮列车车载控制器综合测试平台研制 [J]. 计算机测量与控制, 2020, 28 (4): 251 - 260.
[15] 郭昭宇. 悬浮控制器故障诊断技术研究及检测维护平台研发 [D]. 长沙: 国防科学技术大学, 2014.
[16] 柳阳阳. 中低速磁浮列车悬浮控制系统在线监测与故障诊断系统研究 [D]. 成都: 西南交通大学, 2018.
[17] 李行善, 左 毅, 孙 杰. 自动测试系统集成技术 [M]. 北京: 电子工业出版社, 2004.
[18] 龙志强, 李 云, 贺 光. 磁浮列车悬浮控制系统电磁铁故障诊断技术研究 [J]. 控制与决策, 2010, 25 (7): 1004 - 1009.
[19] 谢 涛, 何怡刚. 模拟电路故障诊断新方法 [J]. 计算机工程与应用, 2014, 6 (6): 1 - 7.
[20] 朱秀娥. 模拟电路故障诊断的仿真研究 [J]. 福建工程学院学报, 2014, 2, 12 (1): 88 - 91.