# DNA 序列和分数阶 Chen 超混沌系统彩色图像加密

姚丽莎[1] 朱珍元[2] 程家兴[1]

[1]安徽新华学院信息系统软件研究所，安徽 合肥 230088

[2]安徽警官职业学院信息管理系，安徽 合肥 230088

**摘要** 针对彩色图像加密的特点，为了减弱图像相关性、加大密钥空间、提高安全性，提出 DNA 序列和分数阶 Chen 超混沌系统彩色图像加密算法。该算法将三维的彩色图像转换成三个二维 DNA 序列矩阵，利用分数阶 Chen 超混沌系统产生的混沌序列将三个 DNA 序列矩阵进行位置置乱，将置乱的三个 DNA 序列矩阵分别分成相等的小块，利用分数阶 Chen 混沌系统和 DNA 序列加法法则将块相加，重新组合小块并利用 DNA 解码规则得到彩色加密图像。仿真结果和安全性分析表明，与其他图像加密算法对比，该算法降低了算法空间和时间需求，相关性低，密钥空间大，密钥敏感性高，安全性更高，具有更强的抵御各种攻击能力。

**关键词** 图像处理；图像加密；DNA 序列；分数阶 Chen 超混沌系统；彩色图像

**中图分类号** TP309.7 **文献标识码** A

**doi**：10.3788/LOP53.091003

# Color Image Encryption Algorithm Based on DNA Sequence Operation and Fractional Order Chen Hyper-Chaotic System

Yao Lisha[1] Zhu Zhenyuan[2] Cheng Jiaxing[1]

[1] *Institute of Information and Software, Anhui Xinhua University, Hefei, Anhui* 230088, *China*

[2] *Department of Information Management, Anhui Vocational College of Police Officers, Hefei, Anhui* 230088, *China*

**Abstract** According to the characteristics of color image encryption, in order to reduce the correlation of images, increase the key space and improve the security, the color image encryption algorithm based on DNA sequence operation and fractional order Chen hyper-chaotic system is proposed. The three-dimensional color image is transformed into three two-dimensional DNA sequence matrices. The chaotic sequences which is generated by fractional order Chen chaotic system are used to scramble the locations of elements from three DNA sequence matrices, and then divide three DNA sequence matrices into some equal blocks respectively. The proposed algorithm adds these blocks by using fractional order Chen chaotic system and DNA sequence addition operation. The encrypted color image by decoding the DNA sequence matrices and recombining the blocks. The simulation results and security analysis show that the proposed algorithm has the advantages of low space, short time, low correlation, big space of the key, high sensitivity of the key, high security and strong resist attacks ability compared with other image encryption algorithms.

**Key words** image processing; image encryption; DNA sequence; fractional order Chen hyper-chaotic system; color image

**OCIS codes** 100.2960; 100.4998; 100.6890

## 1 引 言

随着计算机和网络技术的飞速发展，人们的沟通方式发生了巨大变化，大量的图像等多媒体信息在网络上频繁传输，在传输过程中图像等多媒体信息的安全性问题受到了威胁[1-2]。由于开发的网络环境，在传输

**收稿日期**：2016-05-10；**收到修改稿日期**：2016-05-22；**网络出版日期**：2016-08-29

**基金项目**：国家级大学生创新训练计划项目(201512216007，201512216008)、安徽省高校自然科学重点项目(KJ2015A309)

**作者简介**：姚丽莎(1986—)，女，硕士，讲师，主要从事图像处理与模式识别方面的研究。E-mail：jsjyaolisha@163.com

过程中,人们必须更加注重图像等多媒体信息的安全与保密。

经典的加密算法有 RSA 公钥加密算法、数据加密标准(DES)算法、国际数据加密(IDEA)算法等,但是由于图像数据量大、冗余度高、相邻像元相关性强等特点,传统加密算法用于图像加密效率和安全性不高。混沌系统是一个非线性的动力系统,因其初始值敏感性、参数敏感性、状态遍历性、混合和相似随机性的特点,其结构复杂,难以分析预测,可以提高加密系统的安全性,故在图像加密领域得到了广泛应用。基于混沌系统的图像加密算法包括置乱和扩散两个部分。在置乱部分中,虽然图像加密的视觉效果不错,但由于其不改变图像的像元值,加密图与原图的直方图一致,不能改变原图的统计特性,所以安全性受到统计分析的威胁。在扩散部分中,原图像元值被混沌序列改变,可以有效地改变原图的统计特性,与置乱相比,扩散安全性高,但加密的视觉效果不好。因此,在实际应用中,常常将置乱与扩散结合互相弥补不足,可以有效地抵御统计攻击。Pareek 等[3]提出基于一维 Logistic 混沌映射的图像加密,但单一一维的混沌映射密钥空间小,安全性低。随后一些高效的图像加密算法被提出,Wang 等[4]提出基于混合混沌序列的图像加密算法,虽然算法密钥空间大,灵敏度高,但其安全性不够高;Kanso 等[5]提出一种新的基于三维混沌图像加密算法,抗攻击能力强,但相关性不够弱;Luo 等[6]提出基于时空混沌和遍历矩阵的自适应图像加密算法,该算法将时空混沌系统和遍历矩阵结合用于大小相同的不同图像块加密,可以获取不同的图像加密密码,可以有效地进行图像加密,但抗攻击性有待提高;Wang 等[7]提出一种新的快速图像加密算法,该算法加密速度快,但安全性能有待提高。

1994 年,Adleman[8]完成第一个 DNA 计算实验,为信息时代开启了新纪元。在随后的研究中,研究者发现 DNA 计算具有大量平行性、低功耗、大存储的优点。DNA 计算研究继续深入,DNA 作为信息的载体,新的密码学领域即 DNA 加密产生。Gehani 等[9]提出基于 DNA 的图像加密算法。目前,一次一密是最安全的加密方法,但实际应用的基于一次一密的密码系统受到传统电子媒体的限制,要保存一个巨大的一次一密乱码本因存储容量而变得困难。而 DNA 拥有高信息密度,恰能解决一次一密存储容量的难题,使其在保持一次一密高安全性的同时,操作简单,且易于实现。1999 年,Celland 等[10]实现了利用 DNA 作为信息的载体,成功地将“June 6 invasion:Normandy”隐藏在 DNA 中。但目前基于 DNA 的加密方案的研究仍侧重于理论,虽取得了一些成果,但因生物计算难题、编码过程复杂、实验成本高等因素的影响,无法完全满足实用。Zhang 等[11]提出基于 DNA 序列和两个 Logistic 混沌映射的图像加密新方案;Liu 等[12]提出利用 DNA 互补规则和混沌映射用于图像加密,但以上两种算法的密钥空间小,相关性有待提高。

针对混沌加密和 DNA 加密方案的密钥空间小、相关性强、抗攻击能力弱等不足,考虑到实际应用中大多数为彩色图像,而三维彩色图像的计算空间大、时间长等因素,本文提出 DNA 序列和分数阶 Chen 超混沌系统的彩色图像加密方案。该方案结合分数阶 Chen 超混沌系统产生的混沌序列进行置乱操作,使得加密算法密钥空间加大、相关性减弱、伪随机性增强、安全性更高,具有较强的抵御各种攻击能力。

## 2 分数阶 Chen 超混沌系统

超混沌系统可以克服低维混沌系统的不足,产生结构更复杂的混沌序列。超混沌系统拥有多个正 Lyapunov 指数,密钥空间更大,可在更大空间进行置乱和扩散,加密安全性提高,同时超混沌系统可以减弱像元间的相关性。

通过对整数阶和分数阶 Chen 系统的分析可知,分数阶 Chen 系统的混沌序列的互相关性和自相关性的幅值均小于整数阶 Chen 系统[13]的混沌序列。由此可知,分数阶 Chen 系统的伪随机性更佳、相关性更低、动力学特性更复杂。

综上所述,本文加密方案利用分数阶 Chen 超混沌系统产生混沌序列用于图像加密。分数阶 Chen 超混沌系统模型[14]描述为

$$\begin{cases}\dfrac{\mathrm{d}^{\alpha}}{\mathrm{d}t^{\alpha}}x_1=a(x_2-x_1)+x_4\\ \dfrac{\mathrm{d}^{\alpha}}{\mathrm{d}t^{\alpha}}x_2=bx_1-x_1x_3+cx_2\\ \dfrac{\mathrm{d}^{\alpha}}{\mathrm{d}t^{\alpha}}x_3=x_1x_2-dx_3\\ \dfrac{\mathrm{d}^{\alpha}}{\mathrm{d}t^{\alpha}}x_4=x_2x_3+ex_4\end{cases},\tag{1}$$

式中 $a$、$b$、$c$、$d$、$e$ 为系统参数，当 $a=35$、$b=7$、$c=12$、$d=3$、$e=0.6$ 时，系统处于混沌状态，并存在 4 个混沌序列 $x_1$、$x_2$、$x_3$、$x_4$。超混沌系统有两个正的 Lyapunov 指数为 $\lambda_1=0.567$、$\lambda_2=0.126$。超混沌系统的预测时间往往比单一混沌系统短，因此安全性更高。利用四阶龙格-库塔算法对(1)式进行离散化，当 $\alpha=0.95$ 时，混沌吸引子如图 1 所示。

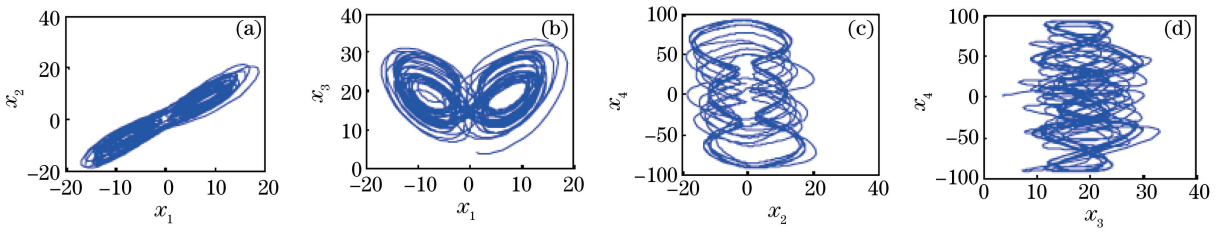


图 1 分数阶 Chen 超混沌系统吸引子。(a) $x_1-x_2$ 平面；(b) $x_1-x_3$ 平面；(c) $x_2-x_4$ 平面；(d) $x_3-x_4$ 平面

Fig. 1 Attractors of fractional order Chen hyper-chaotic system. (a) $x_1-x_2$ plane; (b) $x_1-x_3$ plane; (c) $x_2-x_4$ plane; (d) $x_3-x_4$ plane

## 3 DNA 序列

### 3.1 DNA 编码和解码

DNA 序列中包括 A、T、C、G4 个核酸基，其中，A 与 T、C 与 G 是互补基对。在二进制中 0 和 1 是互补的，因此 00 和 11，01 和 10 也是互补的。在 4！=24 种编码中，只有 8 种满足互补规则，表 1 为满足互补规则的 8 种 DNA 编码。

表 1 满足互补规则的 8 种 DNA 编码

Table 1 Eight kinds of DNA encoding meet the complementary rule

| Type | 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 |

将三维的彩色图像用 DNA 序列进行编码，那么一幅三维彩色图像可以分成 R、G、B 三个频道。每个频道像元值长度是 8 位，每两位用一个 DNA 碱基表示，那么 8 位的二进制像元值便可转换为长度为 4 的 DNA 序列。例如，一个单频通道的像元值为 150，则相应的 8 位二进制编码为 10010110，如采用表 1 的 DNA 编码规则 3 进行编码，那么将 8 位二进制序列转换为长度为 4 的 DNA 序列为 TAAT。在解码时同样用 DNA 编码规则 3 对 DNA 序列进行解码，可得到二进制序列 10010110，但若用 DNA 编码规则 1 对 DNA 序列进行解码，则会得到另一个二进制序列 11000011。

### 3.2 汉明距离

在 DNA 编码中，汉明距离[15]表示两个长度相同的 DNA 序列相应位置不同编码的数目，DNA 编码中的汉明距离通常用以作为 DNA 序列相似性的约束条件。

序列 $x=(x_1,x_2,\cdots,x_n)$ 和 $y=(y_1,y_2,\cdots,y_n)$ 的汉明距离 $H(x,y)$ 定义为

$$\begin{cases} H(x,y)=\sum_{i=1}^{n}h(x_i,y_i) \\ h(x_i,y_i)=\begin{cases}0, x_i=y_i \\ 1, x_i\neq y_i\end{cases}\end{cases}。 \tag{2}$$

例如，图 2 中的两个 DNA 序列的汉明距离为 4。

```
A T C C T A G T
| | | | | | | |
T T A C C A G G
---------------
1 0 1 0 1 0 0 1
```

图 2 两个 DNA 序列的汉明距离

Fig. 2 Hamming distance of two DNA sequences

### 3.3 DNA 序列的加减法操作

DNA 的加减法是按照二进制每两位数值对应一个 DNA 碱基的二进制传统加减法规则进行的。8 种 DNA 编码规则，便相应的有 8 种 DNA 加法和减法规则。

如采用 DNA 编码规则 1 对两个 DNA 序列 TGAC 和 ACCT 进行加法运算，其结果为 TTCG，如图 3 所示。相同地，DNA 序列 TTCG 减去 TGAC 的结果为 ACCT，如图 3 所示。

| | | | |
|---|---|---|---|
| TGAC | 11010010 | TTCG | 11111001 |
| +) ACCT | 00101011 | −) TGAC | 11010010 |
| TTCG | 11111001 | ACCT | 00101011 |

图 3 两个 DNA 序列的加减法示例

Fig. 3 Example of the addition and subtraction of two DNA sequences

以此类推，采用 DNA 编码规则 1 对应的 DNA 加法和减法运算规则如表 2、3 所示。从表 2 和表 3 可以看出，每行每列的碱基是唯一的，即 DNA 序列的加减法运算结果是唯一的，那么可以将 DNA 序列的加减法运算用于彩色图像的像元置乱。

表 2 采用 DNA 编码规则 1 的加法运算

Table 2 Addition operation of DNA encoding rule 1

| + | A | G | C | T |
|---|---|---|---|---|
| A | A | G | C | T |
| G | G | C | T | A |
| C | C | T | A | G |
| T | T | A | G | C |

表 3 采用 DNA 编码规则 1 的减法运算

Table 3 Subtraction operation of DNA encoding rule 1

| − | A | G | C | T |
|---|---|---|---|---|
| A | A | T | C | G |
| G | G | A | T | C |
| C | C | G | A | T |
| T | T | C | G | A |

## 4 DNA 序列和分数阶 Chen 超混沌系统彩色图像加密方案

针对混沌加密和 DNA 加密方案的密钥空间小、相关性强、抗攻击能力弱等不足，考虑到实际应用中大多数为彩色图像，而三维彩色图像的计算空间大、时间长等因素，提出 DNA 序列和分数阶 Chen 超混沌系统的彩色图像加密方案。该方案采用简单的伪 DNA 序列理论将三维彩色图像转换成三个二维 DNA 序列矩阵，降低了算法的计算空间和时间的需求，利用分数阶 Chen 超混沌系统产生的混沌序列将三个 DNA 序列矩阵进行位置置乱，将置乱的三个 DNA 序列矩阵分别分成相等的小块，利用分数阶 Chen 混沌系统和 DNA 序列加法法则将块相加，重新组合小块并利用 DNA 解码规则得到彩色加密图像，使得加密算法密钥空间加

大、相关性减弱、伪随机性增强、安全性更高，具有较强的抵御各种攻击能力。

### 4.1 密钥生成

本文加密方案将分数阶 Chen 超混沌系统产生的混沌序列的初始值 $x_{1_1}$、$x_{2_1}$、$x_{3_1}$、$x_{4_1}$作为加密密钥。将三维彩色图像转换为三个 DNA 编码的序列，便可得到三个汉明距离，作为 DNA 序列相似性的约束条件。将得到的三个汉明距离变换成三个十进制小数，然后将这三个十进制小数依次加入分数阶 Chen 超混沌系统产生的混沌序列的初始值中得到新的初始值替换原来的初始值。密钥生成的伪代码设计如下：

$$\text{if } H<1 \text{ then } H=H/10;$$
$$\text{else } x_{1_1}=x_{1_1}+H;$$
$$\text{end if.}$$

### 4.2 加密过程

彩色图像加密过程分成两部分：置乱和扩散。分数阶 Chen 超混沌系统产生 4 个混沌序列 $x_1$、$x_2$、$x_3$、$x_4$，其中，混沌序列 $x_1$、$x_2$、$x_3$ 用于图像置乱操作，混沌序列 $x_1$、$x_2$、$x_4$ 用于图像扩散操作。本文加密算法结构图如图 4 所示，将三维的彩色图像转换成三个二维 DNA 序列矩阵，利用分数阶 Chen 超混沌系统产生的混沌序列将三个 DNA 序列矩阵进行位置置乱，将置乱的三个 DNA 序列矩阵分别分成相等的小块，利用分数阶 Chen 混沌系统和 DNA 序列加法法则将块相加，重新组合小块并利用 DNA 解码规则得到彩色加密图像。

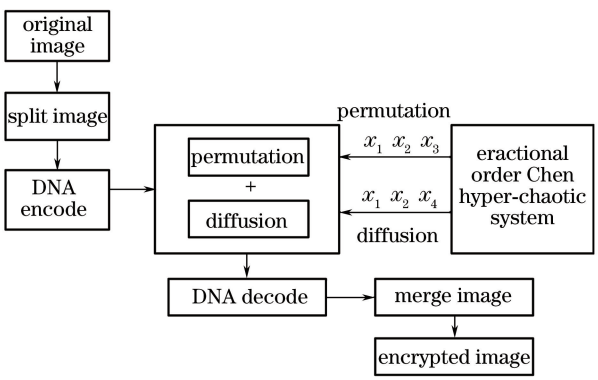


图 4 加密算法结构图

Fig. 4 Structure chart of encryption algorithm

具体加密步骤如下：

1) 将 $m\times n$ 的三维彩色图像 $\boldsymbol{I}(m,n,3)$转换成三个二维灰度图像矩阵 $\boldsymbol{R}(m,n)$、$\boldsymbol{G}(m,n)$、$\boldsymbol{B}(m,n)$。

2) 将三个二维灰度图像矩阵 $\boldsymbol{R}(m,n)$、$\boldsymbol{G}(m,n)$、$\boldsymbol{B}(m,n)$的十进制灰度值转换为 8 位二进制数，按照表 1 中 DNA 编码的规则 3 每两位二进制数转换为 1 位 DNA 碱基，则每一个灰度值将转换为长度为 4 的 DNA 序列，那么，三个二维灰度图像矩阵 $\boldsymbol{R}(m,n)$、$\boldsymbol{G}(m,n)$、$\boldsymbol{B}(m,n)$将转换为三个 DNA 编码矩阵 $\boldsymbol{R}(m,n\times4)$、$\boldsymbol{G}(m,n\times4)$、$\boldsymbol{B}(m,n\times4)$。

3) 利用分数阶 Chen 超混沌系统，设置好初始值密钥 $x_{1_1}$、$x_{2_1}$、$x_{3_1}$、$x_{4_1}$及混沌状态的系统参数 $a$、$b$、$c$、$d$、$e$，生成 4 个混沌序列 $x_1=(x_{1_1},x_{1_2},\cdots,x_{1_{4n}})$、$x_2=(x_{2_1},x_{2_2},\cdots,x_{2_{4n}})$、$x_3=(x_{3_1},x_{3_2},\cdots,x_{3_{4n}})$、$x_4=(x_{4_1},x_{4_2},\cdots,x_{4_{4n}})$。

4) 将分数阶 Chen 超混沌系统生成 4 个混沌序列按升序重新排列，得到重排后的新序列 $fx_1$、$fx_2$、$fx_3$、$fx_4$，表示为

$$\begin{cases}[lx_1,fx_1]=\text{sort}(x_1)\\ [lx_2,fx_2]=\text{sort}(x_2)\\ [lx_3,fx_3]=\text{sort}(x_3)\\ [lx_4,fx_4]=\text{sort}(x_4)\end{cases},\tag{3}$$

式中 $lx_1$、$lx_2$、$lx_3$、$lx_4$ 为 $fx_1$、$fx_2$、$fx_3$、$fx_4$ 的位置指示值。

5) 利用混沌序列 $fx_1$、$fx_2$、$fx_3$ 将三个 DNA 编码矩阵 $\boldsymbol{R}(m,n\times4)$、$\boldsymbol{G}(m,n\times4)$、$\boldsymbol{B}(m,n\times4)$进行像

元置乱操作：

$$\begin{cases}\boldsymbol{R}(i,j)\leftrightarrow\boldsymbol{R}\,[lx_1(i),lx_2(j)]\\ \boldsymbol{G}(i,j)\leftrightarrow\boldsymbol{G}\,[lx_1(i),lx_3(j)]\\ \boldsymbol{B}(i,j)\leftrightarrow\boldsymbol{B}\,[lx_2(i),lx_3(j)]\end{cases},\tag{4}$$

式中 $\boldsymbol{R}(i,j)$、$\boldsymbol{G}(i,j)$、$\boldsymbol{B}(i,j)$表示 R、G、B 三个频道在$(i,j)$处的灰度值，$i=1,2,\cdots,m$，$j=1,2,\cdots,n\times4$。

6) 将置乱的三个 DNA 编码矩阵 $\boldsymbol{R}(m,n\times4)$、$\boldsymbol{G}(m,n\times4)$、$\boldsymbol{B}(\mathbf{m},\mathbf{n}\times4)$分成大小为 $4\times4$ 的小块 $\boldsymbol{Rb}<i,j>$、$\boldsymbol{Gb}<i,j>$、$\boldsymbol{Bb}<i,j>$。

7) 利用分数阶 Chen 超混沌系统的混沌序列 $fx_1$、$fx_2$、$fx_4$ 和 DNA 序列加法法则按下式将块相加得

$$\begin{cases}\boldsymbol{Rb}<i,j>\leftarrow\boldsymbol{Rb}<i,j>+\boldsymbol{Rb}<lx_1(i),lx_2(j)>\\ \boldsymbol{Gb}<i,j>\leftarrow\boldsymbol{Gb}<i,j>+\boldsymbol{Gb}<lx_1(i),lx_4(j)>\\ \boldsymbol{Bb}<i,j>\leftarrow\boldsymbol{Bb}<i,j>+\boldsymbol{Bb}<lx_2(i),lx_4(j)>\end{cases},\tag{5}$$

式中 $i=1,2,\cdots,m/4$，$j=1,2,\cdots,n$。

8) 重新组合小块得到三个新的 DNA 序列矩阵 $\boldsymbol{R}'(m,n\times4)$、$\boldsymbol{G}'(m,n\times4)$、$\boldsymbol{B}'(m,n\times4)$。

9) 将新的 DNA 序列矩阵 $\boldsymbol{R}'(m,n\times4)$、$\boldsymbol{G}'(m,n\times4)$、$\boldsymbol{B}'(m,n\times4)$按照 DNA 编码规则 4 进行解码得到三个二值矩阵，合并 R、G、B 三个频道得到彩色加密图像 $\boldsymbol{E}(m,n,3)$。

图像的解密过程是加密的逆过程。

## 5 仿真实验及安全性分析

### 5.1 仿真实验效果

实验选用大小为 $256\times256\times3$ 的标准彩色图像“Lena”和“pepper”为实验图像，如图 5(a)、(d)所示。仿真实验中，分数阶 Chen 超混沌系统的参数设置为 $a=35$、$b=7$、$c=12$、$d=3$、$e=0.6$，混沌序列的初始值设为 $x_{1_1}=0.3$、$x_{2_1}=-0.4$、$x_{3_1}=1.2$、$x_{4_1}=1$。在 Matlab2007b 平台编程完成 DNA 序列和分数阶 Chen 超混沌系统的彩色图像加密和解密，图 5(b)、(e)为加密图像，图 5(c)、(f)为解密图像。从仿真实验结果可见，本文加密方案的原图与加密图无任何关联，加密和解密的视觉效果较好。


图 5 实验结果。(a) Lena 原图；(b) 加密图；(c) 解密图；(d) pepper 原图；(e) 加密图；(f) 解密图

Fig. 5 Experimental results. (a) Original image of Lena; (b) encrypted image; (c) decrypted image; (d) original image of pepper; (e) encrypted image; (f) decrypted image

### 5.2 密钥分析

1) 密钥空间分析

在本文算法中，分数阶 Chen 超混沌系统的初始值 $x_{1_1}$、$x_{2_1}$、$x_{3_1}$、$x_{4_1}$以及参数 $e$、$\alpha$ 可作为系统加密密钥，如精确度设定为 $10^{-14}$，则密钥空间为 $10^{14\times6}=10^{84}$。而整数阶 Chen 超混沌系统因无参数 $\alpha$，其密钥空间为 $10^{70}$。显然，分数阶 Chen 超混沌系统的密钥空间要比整数阶大，安全性更高。

2) 密钥敏感性分析

因分数阶 Chen 超混沌系统对初始值和参数敏感，故任何一个密钥的细微差别将造成其解密图像与原图完全不同。图 6(a)为原始 Lena 图像，图 6(b)为加密图像，修改一个解密密钥 $x_{1_1}+0.000000000001=0.300000000001$，其他解密密钥保持不变对加密图进行解密，解密结果如图 6(c)所示，原图与解密图完全不同。显然，这是分数阶 Chen 超混沌系统对初始值和参数敏感所致。综上，该算法密钥敏感性高。

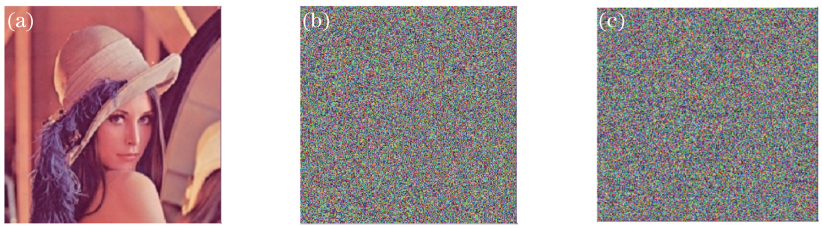


图 6 密钥敏感性实验结果。(a) Lena 原图；(b) 加密图；(c) 错误解密图

Fig. 6 Experimental results of secret key sensitivity. (a) Original image of Lena; (b) encrypted image; (c) error decrypted image

### 5.3 统计分析

对加密算法的统计分析主要是分析算法在置乱和扩散上抵御统计攻击的能力，主要通过直方图分析和相邻像元相关性分析进行。

1) 直方图分析

原始彩色 Lena 图像 R、G、B 三层直方图分布不均、波动大、易被攻击，如图 7(a)～(c)所示。经过加密后，图像 R、G、B 三层直方图分布较均匀，具有伪随机性，可隐藏统计特性，如图 7(d)～(f)所示。由此可见，本文加密方案可有效抵御统计攻击。

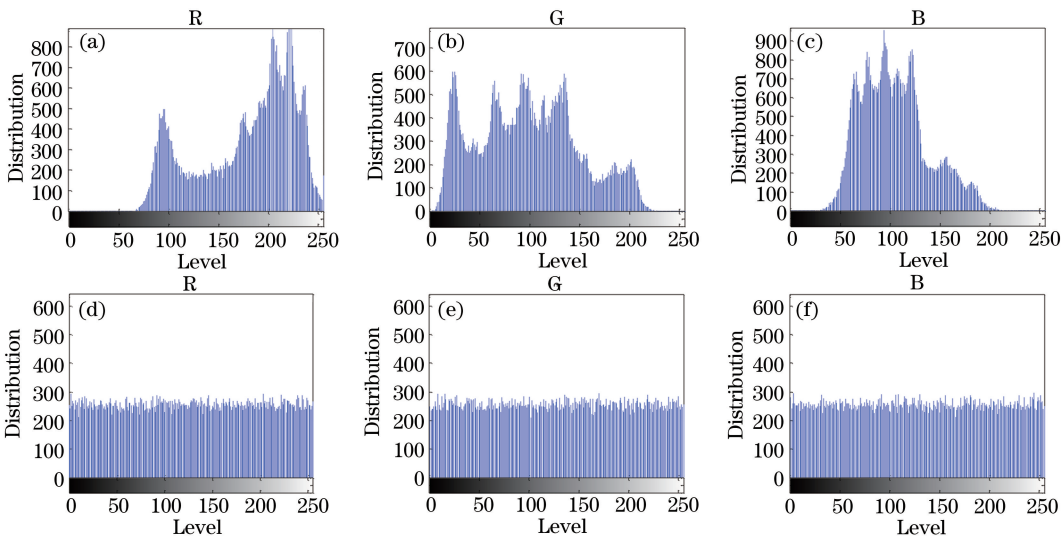


图 7 原图与加密图直方图。(a)(b)(c) 原图 R,G,B 直方图；(d)(e)(f) 加密图 R,G,B 直方图

Fig. 7 Histograms of original image and encrypted image. (a) (b) (c) Histograms in R, G, B channel of original image; (d) (e) (f) histograms in R, G, B channel of encrypted image

2) 相邻像元相关性分析

相邻像元相关性越小，则其抵御攻击能力越强。为了测试原图与加密图相邻像元相关性，实验分别选取水平、垂直和对角线方向相邻的 3000 对像元来分析。计算公式为

$$r_{xy}=\frac{\operatorname{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}},\tag{6}$$

其中，

$$E(x)=\frac{1}{N}\sum_{i=1}^{N}x_i,\tag{7}$$

$$D(x)=\frac{1}{N}\sum_{i=1}^{N}[x_i-E(x)]^2,\tag{8}$$

$$\operatorname{cov}(x,y)=\frac{1}{N}\sum_{i=1}^{N}[x_i-E(x)][y_i-E(y)],\tag{9}$$

式中 $x$、$y$ 为相邻像元灰度值，$N$ 为像元总数，$E(x)$为像元平均值，$D(x)$为方差，$\mathrm{cov}(x,y)$为协方差，$r_{xy}$为相关性系数，其绝对值越大表示相关性越强。

图 8(a)～(c)分别为 Lena 原图 R、G、B 三个通道水平相邻像元相关性，图 8(d)～(f)分别为加密图 R、G、B 三个通道水平相邻像元相关性，其他相关性结果如表 4 所示。

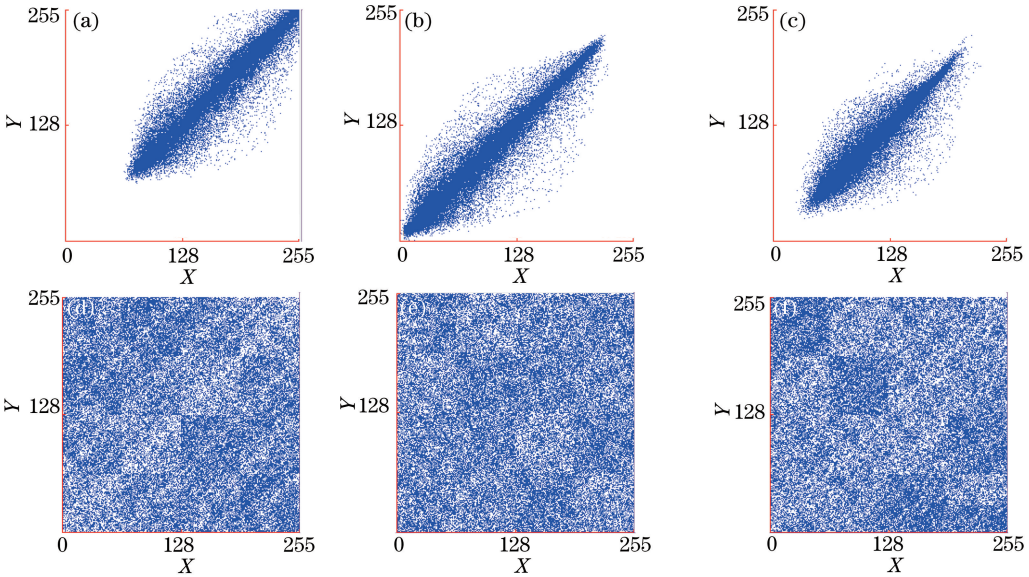


图 8 原图与加密图水平相关性。(a)(b)(c) 原图 R,G,B 水平相关性；(d)(e)(f) 加密图 R,G,B 水平相关性

Fig. 8 Horizontal correlation of original image and encrypted image. (a) (b) (c) Horizontal correlations in R, G, B channel of original image; (d) (e) (f) horizontal correlations in R, G, B channel of encrypted image

由图 8 和表 4 可知，原图相邻像元相关性高，需降低相邻像元相关性以提高抗统计攻击能力。加密图的相邻像元相关性接近于 0，因此本文加密方案抵御统计攻击的能力较强。

采用文献[5]和文献[11]的图像加密算法进行对比分析，选取通道 G 相关系数作比较，对比结果如表 5 所示。由表 5 可知，本文算法的水平、垂直和对角相关系数均小于其他两种算法，故本文加密算法的抗统计攻击的能力更强。

表 4 原图与加密图相关性系数

Table 4 Correlation coefficients of original image and encrypted image

| | Original image | | | Encrypted image | | |
|---|---|---|---|---|---|---|
| | Horizontal | Vertical | Diagonal | Horizontal | Vertical | Diagonal |
| R | 0.9678 | 0.9821 | 0.9471 | −0.1219 | 0.0061 | 0.0092 |
| G | 0.9699 | 0.9830 | 0.9525 | −0.0096 | −0.0044 | 0.0020 |
| B | 0.9470 | 0.9675 | 0.9176 | −0.0894 | −0.0220 | −0.0299 |

表 5 加密算法相关性系数对比

Table 5 Correlation coefficients contrast of encryption algorithms

| | Horizontal | Vertical | Diagonal |
|---|---|---|---|
| Proposed algorithm | −0.0096 | −0.0044 | 0.0020 |
| Ref. [5] algorithm | 0.0651 | −0.0884 | 0.0535 |
| Ref. [11] algorithm | −0.0098 | 0.0203 | 0.0414 |

### 5.4 差分攻击分析

攻击者通常对原始图像作细微改变，然后应用加密算法对改变前后的图像进行加密，通过比较这两幅加密图像，寻找原图与加密图的关系，这类攻击称为差分攻击。如果原图的细微改变使得加密图在置乱和扩散中引起巨大改变，则差分攻击几乎无效，换言之，其抗差分攻击能力强。

本文加密方案采用汉明距离生成加密密钥来抵御差分攻击。彩色图像有 R、G、B 三个通道，因此有三个对应的汉明距离。当 DNA 序列差别不大时汉明距离并不能完全改变，因此所提方法并不能完全抵御差分

攻击。然而,因原图图像像元间相关性高,故本文方法便可以有效抵御差分攻击。

为评价抗差分攻击能力,分析整个加密图中一个像元改变的影响,常用像元改变率(NPCR)和一致平均改变强度(UACI)来评价,这两个值越高说明对原图的细微改变越敏感,抗差分攻击能力越强。

测试实验修改原 Lena 图 R 通道的第一个像元值后,比较修改前后的两幅加密图,结果如表 6 所示。

表 6 NPCR 和 UACI 结果

Table 6 Results of NPCR and UACI

| | NPCR /% | UACI /% |
|---|---|---|
| R | 99.5865 | 33.4835 |
| G | 99.2172 | 33.4640 |
| B | 98.8480 | 33.2689 |

采用文献[5]和文献[11]的图像加密算法进行对比分析,选取通道 G 的 NPCR 和 UACI 作比较,对比结果如表 7 所示。由表 6 和表 7 可知,本文算法较其他两种算法对原图的细微改变更敏感,故本文加密算法的抗差分攻击的能力更强。

表 7 NPCR 和 UACI 对比结果

Table 7 Contrast results of NPCR and UACI

| | NPCR /% | UACI /% |
|---|---|---|
| Proposed algorithm | 99.2172 | 33.4640 |
| Ref. [5] algorithm | 84.5997 | 27.6630 |
| Ref. [11] algorithm | 93.8241 | 30.8981 |

## 5 结 论

针对混沌加密和 DNA 加密方案的密钥空间小、相关性强、抗攻击能力弱等不足,考虑到实际应用中大多数为彩色图像,而三维彩色图像的计算空间大、时间长等,提出了 DNA 序列和分数阶 Chen 超混沌系统的彩色图像加密方案。该方案主要工作如下:

1) 将分数阶 Chen 超混沌系统和 DNA 序列进行结合用于像元置乱,利用分数阶 Chen 混沌系统和 DNA 序列加法法则进行扩散操作,扩大密钥空间,减弱相关性;

2) 采用简单的伪 DNA 序列理论将三维彩色图像转换成三个二维 DNA 序列矩阵,降低了算法的计算空间和时间的需求;

3) 利用分数阶 Chen 超混沌系统产生混沌序列的初始值,并通过汉明距离约束调整初始值生成密钥,提高抗差分攻击能力。

仿真实验通过对密钥分析、统计分析、差分攻击分析表明,此加密方案与其他两种加密算法相比,其密钥空间大、密钥敏感性高、相关性减弱、伪随机性增强、安全性更高,具有更强的抵御各种攻击能力。

## 参 考 文 献

1 Chen Yixiang, Wang Xiaogang. Nonlinear double images encryption based on double random phase encoding[J]. Acta Optica Sinica, 2014, 34(7): 0710001.
陈翼翔, 汪小刚. 基于双随机相位编码的非线性双图像加密方法[J]. 光学学报, 2014, 34(7): 0710001.

2 Chen Yixiang, Wang Xiaogang. Image encryption based on iterative amplitude-phase retrieval and nonlinear double random phase encoding[J]. Acta Optica Sinica, 2014, 34(8): 0810003.
陈翼翔, 汪小刚. 一种基于迭代振幅-相位恢复算法和非线性双随机相位编码的图像加密方法[J]. 光学学报, 2014, 34(8): 0810003.

3 Pareek N K, Patidar V, Sud K K. Image encryption using chaotic logistic map[J]. Image and Vision Computing, 2006, 24(9): 926-934.

4 Wang M L, Liu Q, Li Y. An image encryption algorithm based on the mixed chaotic sequence[J]. Optoelectronics Letters, 2010, 6(4): 310-313.

5 Kanso A, Ghebleh M. A novel image encryption algorithm based on a 3D chaotic map[J]. Commun Nonlinear Sci Numer Simulat, 2012, 17(7): 2943-2959.

6 Luo Y L, Du M H. A self-adapting image encryption algorithm based on spatiotemporal chaos and ergodic matrix[J]. Chinese Physics B, 2013, 22(8): 080503.

7 Wang X Y, Wang Q. A fast image encryption algorithm based on only blocks in cipher text[J]. Chinese Physics B, 2014, 23(3): 030503.

8 Adleman L M. Molecular computation of solutions to combinatorial problems[J]. Science, 1994, 266(11): 1021-1024.

9 Gehani A, LaBean T H, Reif J H. DNA-based cryptography[M]. Cambridge: Springer, 2000, 2950: 167-188.

10 Celland C T, Risca V, Bancroft C. Hiding messages in DNA microdots[J]. Nature, 1999, 399(6736): 533-534.

11 Zhang Q, Guo L, Wei X. Image encryption using DNA addition combining with chaotic maps[J]. Mathematical and Computer Modelling, 2010, 52(11-12): 2028-2035.

12 Liu H, Wang X, Kadir A. Image encryption using DNA complementary rule and chaotic maps[J]. Applied Soft Computing, 2012, 12(5): 1457-1466.

13 Zhu Wei, Yang Geng, Chen Lei, *et al*. An improved image encryption algorithm based on double random phase encoding and chaos[J]. Acta Optica Sinica, 2014, 34(6): 0607001.
朱 薇, 杨 庚, 陈 蕾, 等. 基于混沌的改进双随机相位编码图像加密算法[J]. 光学学报, 2014, 34(6): 0607001.

14 Wang Xingyuan. Synchronization of chaotic system and its application in secure communication[M]. Beijing: Science Press, 2011.
王兴元. 混沌系统的同步及在保密通信中的应用[M]. 北京: 科学出版社, 2011.

15 Wang Bin. Research and application of chaotic theory in image encryption[D]. Dalian: Dalian University of Technology, 2013.
王 宾. 混沌理论在图像加密中的研究与应用[D]. 大连: 大连理工大学, 2013.