文章编号：2096-1618(2022)05-0485-09

基于DNA编码和二维混沌系统的图像加密算法

唐浩哲[1]， 黄源源[1]， 任震宇[1]， 成江宇[1]， 李朝荣[2]
(1.成都信息工程大学网络空间安全学院，四川 成都 610225；2.宜宾学院人工智能与大数据学部，四川 宜宾 644000)

摘要：为解决信息在以图像加密形式传输的途中可能被不法分子截获并破译的问题，提出一种基于DNA编码和二维混沌系统组的图像加密算法，能有效解决图像信息保密问题。算法首先将输入图像转换到CIE(commission international d'eclairage，国际照明委员会) L*a*b*图像色彩空间，并将图片维度降为二维；然后通过Chen混沌系统产生混沌映射，让图像像素的位置进行置乱操作；再结合二维Logistic混沌和广义Arnold混沌系统，对图像像素进一步置乱；最后进行DNA(deoxyribo nucleic acid，脱氧核糖核酸)序列运算，得到密文图像。根据多种针对图像的安全性而做的测试结果表明，该算法不仅提高了传输过程中的安全性，还具有足够的密钥空间，有较小的图像相邻像素值相关性和较大的信息熵等。

关 键 词：图像加密；CIE L*a*b*图像空间；Chen混沌；二维混沌系统组；DNA编码
中图分类号：TP751.1 **文献标志码**：A
doi：10.16836/j.cnki.jcuit.2022.05.001

0 引言

近年来，随着移动网络时代不断地飞速发展，人们能够更便捷地获取信息。然而，在与其他人交流互动的过程中，个人信息容易泄漏这个安全问题变得层出不穷。研究人员也随之发现了网络信息安全问题，并认为解决网络信息安全以及传输中的问题刻不容缓。传统的加密方法，如DES(data encryption standard，数据加密标准)、AES(advanced encryption standard，高级加密标准)等都只能保证应用在数据量较小的环境时，能够有效保护多媒体版权，增强数据安全性[1]。

由于图像所承载的信息具有高冗余度、巨大的数据存储容量、较强的像素之间信息相关性等特点，所以使用图像信息加密技术需要使用更加快速有效的加密算法。由此，传统的图像加密编码方法(DES、AES等)已经无法满足当前的数字图像编码加密安全性需求。

该领域的研究者在对图像加密算法的实验和研究中遇到过如下一些问题。

首先，CIE L*a*b*颜色空间在图像处理和传输中都扮演了重要角色，被研究者应用到图像的实验和研究中。许莉等[2]提出了一种基于Lab颜色空间的运动目标检测方法。通过选择L*a*b*的颜色特征作为前景/背景进行分析的特征，分开处理亮度和色度，得到每个像素在各个通道上的不同信息；然后通过使用背景差和帧差相结合的查分监测模型对背景进行处理，最后通过背景差分得到运动图像目标；不同的颜色空间也被加以应用，金汉均等[3]提出一种在HSV颜色空间中结合小波变换做的图像检索应用研究方法，但由于方法没有融合图像的多特征进行检索，导致其准确度不高。

其次，通过应用DNA编码来处理图像，DNA编码是将计算机科学与分子生物学相结合而产生的一个新兴学科，通过模拟DNA生物操作，进行伪DNA计算来实现信息加密[4]。在实验过程中，遇见了以下的一些问题：Zhang等[5]提出了一种基于DNA编码和二维Logistic混沌映射的图像加密算法，但发现这种算法得到的图像难以抵挡已知明文的攻击；田海江等[6]提出一种图像加密算法通过基于普通混沌系统和DNA动态编码，结果因DNA的运算规则不够复杂，使得加密算法太过单一，图像安全性也不高；因为其加密算法的不可逆现象，Bonny B R等[7]提出了一种基于DNA编码的对称密钥加密算法，结果由于密钥长度不够，容易被暴力破解。

对于图像加密，有不少学者也尝试将混沌加密算法与人工智能领域中的DL(deep learning，深度学习)板块相结合，通过卷积神经网络的理论，使用足够多的数据集去训练加密算法或者超混沌系统，从而使算法处理后的加密图像具有很高的安全性和抗噪能力。陈炜等[8]提出一种利用深度学习来压缩重构图像，再使用复合混沌系统、滑动置乱与矢量分解组成的加密算法对图像进行加解密处理。但使用该算法加密的图像并没有得到很高的图像信息熵值，加密图像不具有足够高的随机性和安全性。

收稿日期：2022-02-02
基金项目：国家自然科学基金资助项目(62102379)；四川省科技厅资助项目(2022NSFSC0557、2021ZYD0020)

超混沌系统有很多特征:具有优秀的伪随机性、对初始状态及结构参数的极端敏感性以及其轨道具有不可预测特性等[9]。使用混沌序列成为随机密钥,能够达到一次一密的效果。这样的操作,在理论上是不可破的。然而,低维混沌序列存在许多问题,比如低维混沌序列会因计算机字节长度的限制,从而对混沌的动力学特性造成影响,使得加密算法不够成熟;而且低维混沌系统产生的混沌只可短期预测,这让其产生的混沌序列具有较差的随机性,且获得的密钥空间小,加密后的结果安全性能低[10],易于破译。相反,高维混沌系统能够通过对更多的参数进行控制变化,提高图像置乱的随机性,从而增强图像加密的安全性。因此,多维超混沌系统成为了一个很好的方法来确保混沌系统的复杂性。

为此,本文提出的基于 DNA 编码和二维混沌系统组的图像加密算法,结合了超混沌系统组(超混沌 Chen 系统、二维 Logistic 映射和广义 Arnold 映射)和 DNA 编码运算对目标加密图像进行分块加密。不仅能有效提高图像加密过程密钥的敏感性和传输过程中的安全性,还成功通过了包括差分攻击在内的攻击形式,以及灰度直方图、相关系数计算分析等,具有较高的安全性。

1 基础理论

1.1 CIE L * a * b * 色彩空间

CIE L * a * b * 是被常用来描述人眼可见的所有颜色的最完备的色彩模型[11]。即使目前绝大多数的彩色图像信息的输入和输出均是根据 RGB 三色空间作为标准的,但是由于 RGB 三色通道均包含了其亮度信息,导致彩色图像的三色间具有很强的相关性,从而影响图像在后面部分加密置乱时无法得到一个更随机安全性更高的的加密图像。

CIE L * a * b * 色彩空间是基于 1931 年的 CIE XYZ 色彩空间的一种更复杂的色彩空间,后者是采用 X、Y、Z 3 个刺激值组成。X 表示创建的非负曲线的圆锥体响应,Y 表示亮度,Z 表示蓝色分量。由于 RGB 到 CIE L * a * b * 之间没有直接的转换公式,故需要先从 RGB 到 CIE XYZ,再到 CIE L * a * b *,以 CIE XYZ 作为颜色的中间层,起到起承转合的作用。这两个转换步骤具体为

1.1.1 RGB—> CIE XYZ

RGB 和 CIE L * a * b * 色彩空间的转换公式:

$$[X,Y,Z]^{\mathrm{T}}=\begin{bmatrix}0.433953 & 0.376219 & 0.189828\\ 0.212671 & 0.715160 & 0.072169\\ 0.017758 & 0.109477 & 0.872765\end{bmatrix}\cdot\begin{bmatrix}R\\G\\B\end{bmatrix}$$

可见,XYZ 和 RGB 在互相换算时,参数之和刚好为 1。例如:$X=0.433953\times R+0.376219\times G+0.189828\times B$,其中$0.433953+0.376219+0.189828=1$,这样就做到了在转换前后能够获得同等范围的映射[12]。

1.1.2 CIE XYZ—>CIE L * a * b *

CIE(国际照明委员会)在 1964 年提出了 CIE L * a * b * 均匀颜色空间。从 XYZ 到 L * a * b * 的转换计算为

$$\begin{cases}L^{*}=116f\left(\dfrac{Y}{Y_n}\right)-16\\ a^{*}=500\left[f\left(\dfrac{X}{X_n}\right)-f\left(\dfrac{Y}{Y_n}\right)\right]\\ b^{*}=200\left[f\left(\dfrac{Y}{Y_n}\right)-f\left(\dfrac{Z}{Z_n}\right)\right]\end{cases}$$

其中:

$$f\left(\frac{X}{X_n}\right)=\left(\frac{X}{X_n}\right)^{\frac{1}{3}}\quad \text{if}\quad \left(\frac{X}{X_n}\right)>(24/116)^3$$

并且:

$$f\left(\frac{Y}{Y_n}\right)=\left(\frac{Y}{Y_n}\right)^{\frac{1}{3}}\quad \text{if}\quad \left(\frac{Y}{Y_n}\right)>(24/116)^3$$

同时:

$$f\left(\frac{Z}{Z_n}\right)=\left(\frac{Z}{Z_n}\right)^{\frac{1}{3}}\quad \text{if}\quad \left(\frac{Z}{Z_n}\right)>(24/116)^3$$

其中,X_n,Y_n,Z_n 为 CIE 标准光源照射在完全漫反射体上后,再经过完全漫反射至观察者眼中的三刺激值。通常情况下,X_n,Y_n,Z_n 为常数且值均为 255。另外,$L\in[0,100]$,$a\in[-127,127]$,$b\in[-127,127]$。真彩 Lena 图像转换至 CIE L * a * b * 色彩空间后的结果如图 1 所示。

(a)处理前Lena图 (b)处理后Lena图

图 1 CIE L * a * b * 处理前后 Lena 图

1.2 Chen 混沌

2005 年,通过状态反馈控制构建了 Chen 氏混沌系统,其方程为

$$\begin{cases}\dot{x}=a(y-x)+\omega\\ \dot{y}=dx-xz+cy\\ \dot{z}=xy-bz\\ \dot{\omega}=yz+r\omega\end{cases}$$

其中,x,y,z 和 ω 作为系统的状态变量,a,b,c,d 和 r 为系统的控制参数。根据研究显示:当$a=35$、$b=3$、$c=12$、$d=7$且$0.085\leqslant r\leqslant 0.798$时,系统将表现为超混沌运动。

1.3 Logistic 混沌系统

1.3.1 一维 Logistic 映射

单从数学式分析,一维 Logistic 映射是一个相当简单的映射,但其实它在通信传输上拥有较高的复杂度。也有不少人在此基础上研究图像的加密问题,其数学公式为

$$X_n+1=X_n\times\mu\times(1-X_n)$$

其中,μ 作为 Logistic 参数,且 $\mu\in[0,4]$,而研究表明,当变量 $X\in[0,1]$时,此系统处于混沌状态。

然而,在现在的各类攻击手法作用下,普通的一维 Logistic 系统由于参数太少,无法生成复杂的混沌系统,无法使加密算法拥有较高的安全稳定性,因此本文将应用 Logistic 映射的二维混沌系统进行图像加密。

1.3.2 二维 Logistic 映射

为保证加密后的图像具有一定的安全性,引入一个新的二维 Logistic 函数。与现有的混沌映射相比,它具有更广泛的范围内混乱,更好的遍历性和混沌性。其数学公式为

$$\begin{cases}x_{n+1}=\mu\lambda_1 x_n(1-x_n)+\gamma y_n\\ y_{n+1}=\mu\lambda_2 y_n(1-y_n)+\gamma x_n\end{cases}$$

其中,μ、λ_1、λ_2 和 γ 均为控制参数,通常情况下,取 $\mu=4$。经过计算得知:当 $\lambda_1=0.9$、$\lambda_2=0.9$、$\gamma=0.1$时,此时的二维 Logistic 系统处于混沌状态[13]。为了研究及其应用,提出一个置乱转换(CMT),以有效地改变图像的像素位置。结合二维 Logistics 与 CMT,可以进一步实现图像加密算法。

1.4 猫脸变换(Arnold)系统

1.4.1 离散 Arnold 变换

猫脸变换最早是由俄国数学家 Arnold 引入的,其数学式如公式为

$$\begin{bmatrix}x_{n+1}\\ y_{n+1}\end{bmatrix}=\begin{bmatrix}1 & 1\\ 1 & 2\end{bmatrix}\begin{bmatrix}x_n\\ y_n\end{bmatrix}\ (\mathrm{mod}\ 1)=A\begin{bmatrix}x_n\\ y_n\end{bmatrix}\ (\mathrm{mod}\ 1)$$

其中,x_n 和 y_n 均为实数且 $x_n,y_n\in(0,1)$,取模运算 mod 将(x_n,y_n)的相空间限制在 $[1,1]\times[1,1]$ 内。

与一维 Logistic 混沌系统相同,离散 Arnold 映射因参数太少无法生成复杂混沌系统,无法有效保证加密过程的安全性。因此在文中使用广义 Arnold 变换参与加密流程。

1.4.2 广义 Arnold 变换

当然,Arnold 映射同 Logistic 映射一样,也是一种混沌映射[14]。其数学式为

$$\begin{bmatrix}x_{n+1}\\ y_{n+1}\end{bmatrix}=\begin{bmatrix}1 & p\\ q & pq+1\end{bmatrix}\begin{bmatrix}x_{n+1}\\ y_{n+1}\end{bmatrix}\mathrm{mod}(N)$$

其中,x_n 和 y_n 是大小为 $N\times N$ 的图像置乱前所处的像素位置,x_{n+1}和 y_{n+1}为置乱后所处的像素位置,p, q, N 均为正整数且 p、q 的值小于 N。由于二维 Arnold 映射数字化是具有周期性现象[15],所以基于 Arnold 映射的图像在加密时如果知道加密算法,通过在某一个密文空间以任意状态进行迭代,都能够在有限步骤中内被恢复为明文。例如:当 $p=40$,$q=8$, $N=124$ 且 iter=5(迭代轮数)时,此时加密图像可恢复原样,因而将 Arnold 映射和 Logistic 映射结合起来,能够达到更好的加密效果。

1.5 DNA 编码规则和 DNA 基础算法

1.5.1 DNA 编码规则

生物研究表明:DNA 是由 4 种脱氧核苷酸通过碱基互补配对组成的双螺旋链式结构。4 种脱氧核苷酸分别为腺嘌呤(A)、鸟嘌呤(G)、胸腺嘧啶(T)和胞嘧啶(C),碱基互补配对规则为 A 与 T 配对、G 与 C 配对。根据电脑二进制中 1 和 0 互补的特性可以利用 DNA 的碱基互补原则,用两位二进制数值来表示 4 种脱氧核苷酸,且由于不同规则的核苷酸的二进制数值指定是不同的,所以满足碱基互补配对的规则组合有 8 种[16],如表 1 所示。由于图像在计算机中是由像素组成,且每个像素值都可以通过编制 DNA 单链来加密,然后通过互补单链来解密。以灰度值来举例:设一个像素的灰度值为 8bit,其二进制表示为“11000101”,用表 1 的规则 1 来编码,可得编码为“TACC”。

表 1　DNA 编码规则

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

1.5.2 DNA 基础运算

整个加密过程中可能使用到的 DNA 编码运算方法分为 DNA 的加法、DNA 的减法和 DNA 的异或。DNA 的加法、减法和异或运算类似于传统的代数运算[17],运算规则如表 2 ~ 4 所示。

表 2 DNA 加法

加法	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 DNA 减法

减法	A	G	C	T
A	A	T	C	G
G	G	A	T	C
C	C	G	A	T
T	T	C	G	A

表 4 DNA 异或

异或	A	G	C	T
A	A	G	C	T
G	G	A	T	C
C	C	T	A	G
T	T	C	G	A

2 加密过程与加密算法

本次加密算法使用真彩图像进行实验,先利用 RGB 转 CIE L * a * b * 色彩空间原理将原图转换至该色彩空间,然后在 Matlab 中使用函数使其变为灰度图像,再做进一步操作。加密过程如图 2 所示。

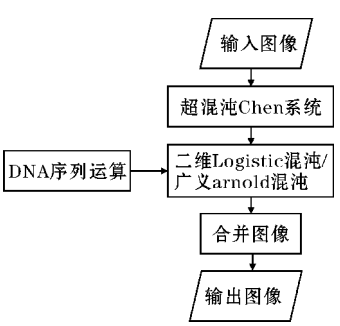


图 2 加密算法简略流程图

文中对图像加密分为 4 部分:

步骤 1 根据 RGB 图像至 CIE L * a * b * 色彩空间的原理和两步转换规则,转换输入的 RGB 图像 $\boldsymbol{I}_0$ 的色彩空间,并将图像降至二维,分别得到 CIE L * a * b * 色彩空间下的图像 $\boldsymbol{I}_1$ 和降维后图像 $\boldsymbol{I}_2$。

步骤 2 根据超混沌 Chen 系统生成 4 个混沌(8bit)序列,应用于后续 DNA 编码置换的过程。

步骤 3 根据二维 Logistic 混沌映射规则,对 $\boldsymbol{I}_2$ 图像进行扩散置乱,得到图像 $\boldsymbol{E}_1$,再根据广义 Arnold 混沌映射规则,对 $\boldsymbol{E}_1$ 图像进行操作得到图像 $\boldsymbol{E}_2$。

步骤 4 利用步骤 2 获得的 X', Y, Z, H 4 个混沌序列,结合 DNA 编码规则将图像的每个像素点进行对应转换,对图像 $\boldsymbol{E}_2$ 进行置乱操作,得到最终加密图像 $\boldsymbol{E}_3$。详细加密流程图如图 3 所示。

加密流程具体步骤如下:

输入 真彩图像 $\boldsymbol{I}_0$,参数初值

输出 加密图像 $\boldsymbol{E}_3$

步骤 1 将真彩图像 $\boldsymbol{I}_0$ 进行色彩空间的转换,得到 CIE L * a * b * 色彩空间的图像 $\boldsymbol{I}_1$。

步骤 2 将步骤 1 得到的图像 $\boldsymbol{I}_1$ 通过降维函数将其改变为灰度图像 $\boldsymbol{I}$,并将图像矩阵 $\boldsymbol{I}$ 转换成大小为 $M \times N$的二维矩阵 $\boldsymbol{I}_2$。

步骤 3 将图像 $\boldsymbol{I}_2$ 分解为 4 个相等大小子块,编号依次为 $T_i(i \in [1,4])$,并将图像的行列数都补成可以被 4 整除的数。由于 4 块的加密方法均相同,加密方法中混沌序列加密过程仅根据其中 1 块进行说明,另外 3 块加密方式类似。

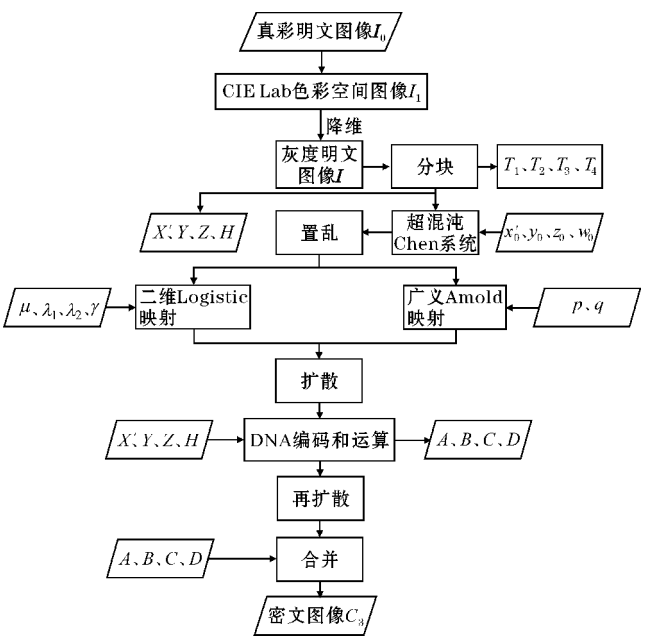


图 3 加密算法流程图

步骤 4 根据 Chen 系统所需的 4 个初值参数,采用 ody45 的方法和微分方程进行求解,输入超混沌 Chen 系统的初始值 x, y, z, ω,生成 4 个混沌(8bit)序列 X',Y,Z,H,将应用于后续 DNA 编码置换的过程。

$$\begin{cases} X' = \mathrm{mod}(\mathrm{floor}(X'_1 \times 10^{13}), 2^8 \\ Y = \mathrm{mod}(\mathrm{floor}(Y_1 \times 10^{13}), 2^8 \\ Z = \mathrm{mod}(\mathrm{floor}(Z_1 \times 10^{13}), 2^8 \\ H = \mathrm{mod}(\mathrm{floor}(H_1 \times 10^{13}), 2^8 \end{cases}$$

步骤 5　初始化 Logistic 映射控制参数:$\mu=4$,$\lambda_1=0.9$、$\lambda_2=0.9$、$\gamma=0.1$,根据二维 Logistic 公式进行迭代映射,得到图像序列 $\boldsymbol{I}_3$ 和加密图像 $\boldsymbol{E}_1$。

步骤 6　广义 Arnold 变换矩阵的形式为 $\boldsymbol{A}=[1,p;q,1+p\cdot q]$;按照输入的密钥 p, q 构建广义 Arnold 变换矩阵 $\boldsymbol{A}$,将输入的图像 $\boldsymbol{E}_1$ 在 $\boldsymbol{A}$ 的作用下进行迭代置乱加密得到密文图像 $\boldsymbol{E}_2$,并得到图像序列 $\boldsymbol{I}_4$。

步骤 7　根据步骤 4 获得的 X',Y,Z,H,取其前 $8MN$ 项,并不重复地对 T_1,T_2,T_3,T_4 依次将连续 8 个比特数进行比特合并,得到 4 个长度为 MN 的随机序列,分别记为 K_1,K_2,K_3,K_4。接着,令 $Q=K_1\oplus K_2\oplus K_3\oplus K_4$。对于 $\boldsymbol{I}_4$ 中的第 $i(i=1,2,\cdots,MN)$ 个像素点,构建公式:

$$\begin{cases}A=(K_1(i)\bmod 8)+1\\B=(K_2(i)\bmod 8)+1\\C=(K_3(i)\bmod 8)+1\\D=(K_4(i)\bmod 8)+1\end{cases}$$

可以得出,A、B、C、$D\in(1,2,3,\cdots,8)$,又根据 DNA 序列编码和其运算规则,按照规则 A,将密文图像 $\boldsymbol{E}_2$ 中的 T_1 部分图像块进行 DNA 编码,按照规则 B,将 T_2 部分图像块进行编码,按规则 C,将 T_3 部分图像块进行编码,按规则 D,将 T_4 部分图像块进行编码;然后对对应的图像块根据编码规则进行 DNA 运算操作;将运算结果再进行上一步骤的运算,成为扩散过程。最后将分别加密的图像块按照原始的分块方式进行拼接,合并成完整的最终加密图像 $\boldsymbol{E}_3$。

解密为加密的逆向流程。在文中不做详细说明。

3　仿真测试

3.1　测试环境

本次使用 Windows10,内存 16G,CPU 为 Inter i5 的电脑配置进行实验,测试平台为 Matlab 2018a。作为对比,选用 Lena 图(256×256 像素)进行测试。该算法的仿真测试从密钥空间、灰度直方图、相关系数、差分攻击、信息熵等 5 个方面来进行,从而得出本文算法是否具有足够高的安全性。图 4 为本文算法测试的真彩 Lena 明文图像和加密后的密文图像。图 5 为本文加密图像的解密结果。无法简单用肉眼分辨解密后图像和加密前原图的差异,基本判定该算法能够将图像信息进行加密传递,并让接收者也能够顺利解密获得该图像信息。

(a)加密前Lena图　　(b)加密后Lena图

图 4　加密前后 Lena 图

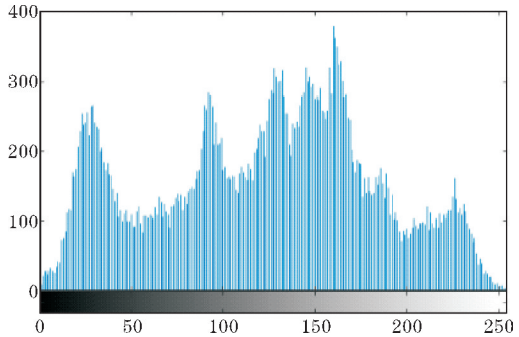
图 5　解密后 Lena 图(且恢复 RGB 颜色空间)

3.2　密钥空间分析

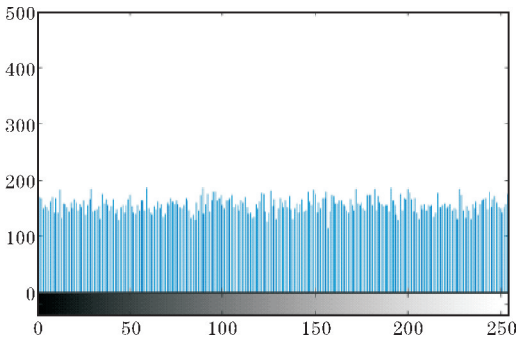
如果要让加密的效果达到最好,也就是能够接受多种密钥的攻击,需要足够大的密钥空间。研究数据显示:当整个算法的密钥空间达到 2^{100} 时才能够说加密图像的安全性达到了可以保障的程度[18]。本次使用了 64 位的 CPU,假设计算机浮点数的计算精度可以达到 10^{-14},则整个加密算法的密钥空间可以达到 $(10^{14})^5=10^{70}$。经过计算,所要求的 $2^{100}\approx1.27\times10^{30}$,$10^{70}$ 远大于 2^{100},故满足要求。因此,可以得出初步结论:这种加密方式有足够大的密钥空间,能够有效地抵御绝大部分的物理攻击。

3.3　灰度直方图分析

灰度直方图是将数字图像中的所有像素,按照灰度值的大小,统计其出现的频率。灰度直方图是灰度级的函数,表示图像中具有某种灰度级的像素的个数,反映图像中某种灰度出现的频率[19]。一个理想的加密算法应该使任何灰度图像在加密之后得到的密文图像中尽可能少地呈现出明显的特征,即灰度直方图在加密后呈现均匀分布。密文直方图的分布越均匀,说明该加密算法就越安全[20]。图 6 是该算法应用到 Lena 图前后灰度直方图的对比,可以看出:加密之后的灰度直方图分布均匀,说明加密后的图像不具有任何对解密有用的明显信息,证明加密系统有效且安全性高。



(a)明文图像 Lena 直方图



(b)密文图像 Lena 直方图

图 6 加密前后 Lena 图灰度直方图分析

3.4 相关系数分析

一般情况下,一张未加密的、完整的图像相邻像素之间的相关性较高,可以达到 90% 及以上。为防止攻击者对图像进行统计分析,需要降低图片相邻像素的相关性。本次实验随机选取原始图像和加密图像上 5000 对相邻像素点(水平、垂直、对角方向),并计算像素间的相关性。

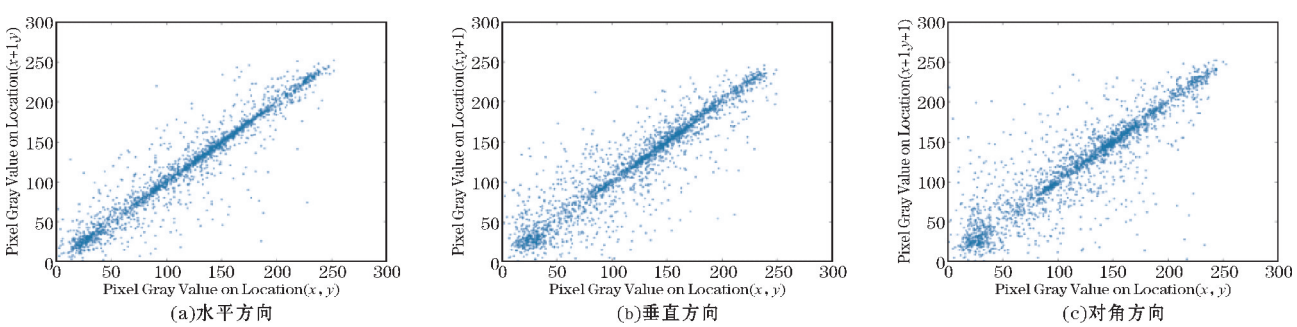
$$\left.\begin{aligned} E(x)&=\frac{1}{N}\sum_{i=1}^{N}x_i\\ D(x)&=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))^2\\ \operatorname{cov}(x,y)&=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))(y_i-E(x))\\ r_{xy}&=\frac{\operatorname{cov}(x,y)}{\sqrt{D(x)}\times\sqrt{D(y)}} \end{aligned}\right\}$$

其中:x,y 分别代表图像中相邻像素的横、纵方向灰度值;$\operatorname{cov}(x,y)$ 代表协方差;$D(x)$ 和 $E(x)$ 分别代表方差和平均值。表 5 给出了原始图像和加密后图像在水平方向、垂直方向、对角方向相邻像素的相关性。并与文献[21-22]比较,以表现本文算法的安全性之高。

表 5 相关系数测试结果

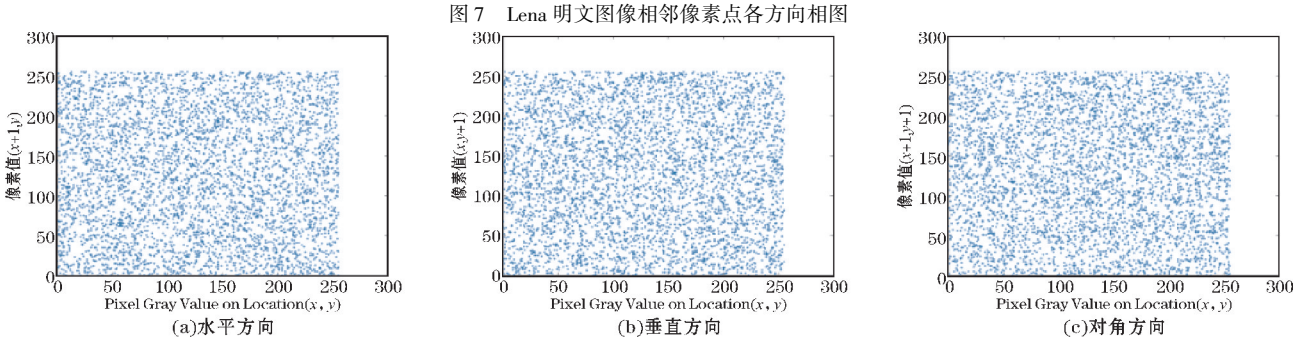
算法	方向	明文图像	密文图像
文献[21]	水平方向	0.9487	-0.0131
	垂直方向	0.9701	-0.0165
	对角方向	0.9354	0.0204
文献[22]	水平方向	0.9642	-0.0381
	垂直方向	0.9824	-0.0291
	对角方向	0.9656	0.0027
本文	水平方向	0.9363	-0.0033
	垂直方向	0.9698	-0.0103
	对角方向	0.9172	-0.0024

由表 5 可知,当明文图像的相关系数均非常接近于 1,同时加密图像的相关系数均非常接近于 0 时,就表明明文图像的相邻像素点之间具有较强的相关性,而加密图像的相邻像素点之间基本不具备相关性[23]。图 7 和图 8 分别为 Lena 灰度图加密前后的相邻像素点在水平方向、垂直方向和对角方向的相关性散点相图。



(a)水平方向 (b)垂直方向 (c)对角方向

图 7 Lena 明文图像相邻像素点各方向相图



(a)水平方向 (b)垂直方向 (c)对角方向

图 8 Lena 密文图像相邻像素点各方向相图

3.5　差分攻击分析

本文的加密算法,使用的密钥和明文图像相关,使得明文图像对密文图像非常敏感,故只要稍微修改一点明文图像的像素值就会使密文图像大相径庭,从而保证加密算法的安全性。这里,假设明文图像为 $\boldsymbol{I}$,则 H,W 分别为明文图像的长与宽,C_1 为加密图像,通过将 $\boldsymbol{I}$ 中某一个像素值进行微调(将像素值加 1bit 或减 1bit),得到调整后的加密图像 C_2。引入两个相关概念,分别是像素改变率(number of pixels change rate, NPCR)和归一化平均变化强度(unified average changing, UACI)。

$$\mathrm{NPCR}=\frac{\sum_{i=1}^{H}\sum_{j=1}^{W}D(i,j)}{H\times W}\times 100\%$$

$$\mathrm{UACI}=\frac{1}{H\times W}\sum_{i=1}^{H}\sum_{j=1}^{W}D(i,j)\frac{|C_1(i,j)-C_2(i,j)|}{255}$$

$$D(i,j)=\begin{cases}1, C_1(i,j)\neq C_2(i,j)\\ 0, C_1(i,j)=C_2(i,j)\end{cases}$$

其中,$C_1(i,j)$ 和 $C_2(i,j)$ 分别代表明文图像像素值被微调之前后所对应的密文像素值。NPCR 的值越接近 100%,或 UACI 的值越接近 33%,此时的加密算法处理后的加密图像敏感性越高,抵抗差分攻击的能力越强。表 6 是本文算法与文献[8,21,25]的算法比较,可以看出,本文算法处理图像能够有效抵御差分攻击。

表 6　NPCR/UACI 测试结果　　单位:%

算法	NPCR	UACI
文献[8]	99.60	33.52
文献[21]	99.19	33.47
文献[25]	99.54	33.31
本文	99.60	33.46

3.6　信息熵

1948 年,香农提出了“信息熵”的概念,为解决信息量化的问题。信息熵被定义为描述系统的不确定性的程度,可以用来表示图像信息的不确定性。计算公式如下:

$$H(m)=-\sum_{k=0}^{2^N-1}p(m_i)lbp(m_i)$$

其中,$p(m_i)$ 表示某信息 m_i 出现的概率。根据实验数据知,信息熵越大,越接近完全随机的图像信息熵 8,则该加密图像的灰度值分布越均匀、随机性越大、信息传递越安全。表 7 为本文算法和文献[8,25,27]的算法加密图像后的信息熵测试结果。

表 7　加密图像信息熵

算法	文献[8]	文献[25]	文献[27]	本文
信息熵	7.9944	7.9873	7.9913	7.9947

与其他算法比较,可以看出本文算法得到一个较大的信息熵值,非常接近理想值。这表明该加密图像发生信息泄露的可能性极小,也间接证明了加密算法的安全性。

4　结束语

提出了一种将 DNA 编码规则和超混沌系统相结合的图像加密算法。通过转化图像色彩空间、降低图像维度;利用 Chen 超混沌系统、二维 Logistic 系统、广义 Arnold 系统和 DNA 编码序列的多重运算来达到安全高效加密明文图像,实现图像置乱和像素值扩散过程。先转换图像颜色空间,再分别通过 Chen 超混沌系统、二维 Logistic 映射和广义 Arnold 映射组成的超混沌系统对图像像素值进行扩散、置乱操作,最后结合 DNA 编码规则对处理后的图像再次置乱加密,得到最终的密文图像。本文经过密文图像密钥空间、灰度直方图、相关系数、差分攻击和信息熵值等测试方法,从多方面专业化地验证了该算法处理后的加密图像的安全性。下一步将研究深度学习和基于 DNA 序列卷积神经网络的图像加密算法。计划针对深度学习中的 LSTM 神经网络,通过预测时间序列,生成预测新混沌信号,并使用 Pytorch 等工具进行混沌序列的训练,得到新混沌信号,再结合多维混沌系统和 DNA 编码,能够更进一步提升图像加密的安全性。

致谢:感谢大学生创新创业训练计划项目(202010621260)对本文的资助。

参考文献:

[1] DELOSIÈRES L, GARCÍA D. Infrastructure for Detecting Android Malware[C]. Proceedings of the 28th International Symposium on Computer and Information Sciences, 2013:389-398.

[2] 许莉,王敏,温月. 基于 Lab 颜色空间的运动目标检测[J]. 华中科技大学学报(自然科学版),2013,41(s1):219-222.

[3] 金汉均,曾婷. 小波变换在 HSV 颜色空间上的图

像检索应用研究[J]. 电子测量技术,2016,39(7):106-109.

[4] Zhou S H, Wang B, Zheng X D, et al. An image encryption scheme based on DNA computing and cellular automata [J]. Discrete Dynamics in Nature and Society,2016(2):1-9.

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

[6] 田海江,雷鹏,王永. 基于混沌和 DNA 动态编码的图像加密算法[J]. 吉林大学学报(工学版),2014,44(3):801-806.

[7] Bonny B R, Vijay J F, Mahalakshmi T. Secure data transfer through DNA cryptography using symmetric algorithm[J]. International Journal of Computer Applications,2016,133(2):19-23.

[8] 陈炜,郭媛,敬世伟. 基于深度学习压缩感知与复合混沌系统的通用图像加密算法[J]. 物理学报,2020,69(24):99-111.

[9] 牛莹,张勋才. 基于比特置换与核酸序列库的混沌图像加密算法[J]. 计算机工程与应用,2017,53(17):130-136.

[10] Alvarez G, Montoya F, Romera M, et al. Cryptanalysis of an ergodic chaotic cipher[J]. Physics Letters A,2003,311(2):172-179.

[11] 胡苏阳,黄水源,陈智毅. 基于 CIELAB 颜色模型的数字照片背景色替换[J]. 计算机应用与软件,2016,33(7):229-233.

[12] Imageship. RGB 和 CIEXYZ 颜色空间的转换及相关优化[DB]. 2013.

[13] Tipping M E. Bishop CM Probabilistic Principal Component Analysis[J]. Journal of the Royal Statistical Society: Series B (Statistical Methodology),1999,61(3):611-622.

[14] Chen G R, Mao Y B, Charles K C. A symmetric image encryption scheme based on 3D chaotic cat maps[J]. Chaos, Solitons & Fractals, 2004, 21(3):749-761.

[15] 杨凤霞. 基于二维 Arnold 映射的彩色图像加密算法[J]. 小型微型计算机系统,2014,35(8):1922-1925.

[16] Yuen C H, Wong K. Cryptanalysis on secure fractal image coding based on fractal parameter encryption [J]. Fractals-complex Geometry Patterns and Scaling in Nature and Society, 2012,20(1):41-51.

[17] 张勋才,刘奕杉,崔光照. 基于 DNA 编码和超混沌系统的图像加密算法[J]. 计算机应用研究,2019,36(4):1139-1143.

[18] Alvarez G, Li S J. Some Basic Cryptographic Requirements for Chaosbased Cryptosystems[J]. International Journal of Bifurcation and Chaos, 2006,16(8):2129-2151.

[19] 吴锐,黄剑华,唐降龙,等. 基于灰度直方图和谱聚类的文本图像二值化方法[J]. 电子与信息学报,2009,31(10):2460-2464.

[20] 黄林荃,刘会,张牧. 改进 Arnold 变换与量子混沌的图像加密系统[J]. 小型微型计算机系统,2019,40(9):1897-1902.

[21] 刘为超,刘义沛. 基于 Logistic 混沌置乱的图像加密算法[J]. 科技信息,2020(36):125-126.

[22] Zhou M J. A novel image encryption scheme based on conservative hyperchaotic system and closed-loop diffusion between blocks[J]. Signal Processing,2020,171.

[23] 徐扬,黄迎久,李海荣. 基于量子 Logistic 映射的图像加密算法研究[J]. 包装工程,2018,39(7):180-186.

[24] Zhu Z L, Zhang W, Wong K W, et al. A chaos-based symmetric image encryption scheme using a bit-level permutation [J]. Information Sciences, 2011,181(6):1171-1186.

[25] 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.

[26] El-Khamy, Said. An efficient DNA-inspired image encryption algorithm based on hyper-chaotic maps and wavelet fusion [J]. MULTIMEDIA TOOLS AND APPLICATIONS, 2021, 80 (15): 23319-23335.

[27] Liu Q, Liu L. Color Image Encryption Algorithm Based on DNA Coding and Double Chaos System [J]. IEEE Access,2020(99):83596-83610.

Image Encryption Algorithm based on DNA Coding and Two-dimensional Chaotic System

TANG Haozhe[1], HUANG Yuanyuan[1], REN Zhenyu[1], CHENG Jiangyu[1], LI Chaorong[2]

(1. College of Cybersecurity, Chengdu University of Information Technology, Chengdu 610225, China; 2. Yibin University, Faculty of Artificial Intelligence and Big Data, Yibin 644000, China)

Abstract: In order to solve the problem that the information of images may be decoded after being intercepted by hackers in the information transmission nowadays, this paper proposes an image encryption algorithm based on DNA coding and two-dimensional chaotic system group. It can effectively solve the problem of protecting image information while during the transmission process. The algorithm first converts the input the image into CIE L * a * b * image color space and reduces the image to a two-dimensional one, then it generates chaotic mapping through Chen chaotic system, so that the positions of image pixels are scrambled. Then we realize further scrambling by combining with two-dimensional Logistic chaos and generalized Arnold chaos. Finally, DNA sequence operation was performed to obtain the encrypted image. According to a variety of test results for the security of the image, they show that the algorithm can not only improve the security in the transmission process, but it also has sufficient key space, small enough image adjacent pixel value correlation and large enough information entropy.

Keywords: image encryption; CIE L * a * b * color space; Chen chaos; two-dimensional chaotic system group; DNA encoding