DOI：10.7652/xjtuxb201509016

伪 DNA 密码图像加密算法研究

毛彦斌，张选平，杨晓刚
（西安交通大学电子信息与工程学院，710049，西安）

摘要：针对现有基于 DNA 序列的图像加密算法实验环境要求苛刻、难于实现的不足，根据 DNA 加密的基本思想，提出了一种伪 DNA 密码图像加密算法。该算法首先利用二维 Logistic 混沌序列对原始图像进行位置置乱，打乱像素之间的分布规律；然后，将置乱图像转换为四进制序列，根据事先定义的编码规则采用动态 DNA 编码方法将四进制序列转换为 DNA 序列；利用三维 Chen 混沌系统产生与四进制序列相同大小的 DNA 序列，将四进制编码的 DNA 序列和三维 Chen 混沌系统生成的 DNA 序列按照 DNA 异或规则进行异或运算；最后，进行截取延长操作并进行 DNA 解码重组得到加密图像。实验结果表明，该算法不仅容易实现，而且加密速度快、安全性高，可用于军事、医疗、司法等涉及个人和单位隐私的数字图像的保密存储和网络传输。

关键词：DNA 序列；动态编码；混沌系统；图像加密
中图分类号：TP391 **文献标志码**：A **文章编号**：0253-987X(2015)09-0091-08

A Novel Image Encryption Algorithm Based on Pseudo DNA Coding

MAO Yanbin, ZHANG Xuanping, YANG Xiaogang
(School of Electronics and Information Engineering, Xi'an Jiaotong University, Xi'an 710049, China)

Abstract: Aiming at the fact that existing image encryption algorithms based on DNA sequence have strict experimental conditions and are difficult to implement, an image encryption algorithm based on pseudo DNA coding is proposed combining DNA coding and chaotic system. Firstly, the original image is scrambled by using two-dimensional chaotic system. Secondly, the scrambled matrix is transformed into quarternary sequence which is then converted to DNA sequence by using dynamic DNA coding method. Thirdly, generating a random DNA sequence by three-dimensional chaotic system, with the same size as the quarternary sequence. Then, implementing DNA XOR operation on the quarternary DNA sequence and the DNA sequence generated by three-dimensional chaotic system, the encrypted image is obtained by decoding and reorganization. The simulation results and analysis show that the algorithm has not only good encryption effect but also fast encryption speed and high safety, which can be applied to the storage and network transmission of military, medical, judicial and other digital images.

Keywords: DNA sequence; dynamic coding; chaos system; image encryption

随着计算机网络的快速发展，在日常生活中用网络进行数字图像传输已经变得非常普遍。然而，由于网络的开放性和自身协议中存在的某些缺陷，数字图像在网络上传输的安全问题已经成为人们研究的热点。在众多的数字图像安全保护中，图像加密是一种行之有效的方法。相对于文本数据，数字

收稿日期：2014-12-10。 作者简介：毛彦斌(1979—)，男，硕士生；张选平(通信作者)，男，副教授，硕士生导师。 基金项目：陕西省自然科学基金资助项目(2014JM8322)。

图像有数据量大、冗余度高、相关性强等特点。因此,传统的诸如 DES、IDEA 和 AES 等加密方法并不适合数字图像的加密[1-2]。近年来,学者们提出了很多关于图像加密的新算法。例如,基于混沌理论的图像加密方法[3-6]和基于 DNA 序列的图像加密方法[7]。基于混沌理论的图像加密算法主要分为像素位置置乱和像素值扰乱两个过程[8-10]。因简单置乱不能改变原始图像像素值的分布规律,所以不能有效抵抗统计攻击,而只进行扰乱,不进行像素位置置乱,则很难抵抗剪切攻击。所以,很多学者在加密过程中将两者结合起来使用,以达到更高的安全性。高维混沌系统由于具有密钥空间大、对初值敏感性高和混沌特性更加复杂等优点,因此被广泛应用于图像加密中。Wang 等提出了一种基于高维混沌系统的图像加密算法[11],仿真实验表明,该算法密钥空间大、对密钥敏感、安全性高。随着 NDA 计算的研究和发展,DNA 加密作为一个新的研究领域倍受学者们的青睐。Celland 等提出了一种新的加密方法[12],用 DNA 运算代替了传统的二进制加密;Shyam 等提出了一种新的基于 DNA 计算的加密算法[13],他们用自然的 DNA 序列对原始信息进行编码,然后进行异或操作,以此实现对文本的加密。以上加密都是基于 DNA 生物操作,对实验环境要求苛刻,实验设备昂贵,在一般实验室很难完成相应的实验。近年来,Kang 提出一种伪 DNA 加密方法[14],主要利用生物分子学中心法则的基本思想来实现信息的加密,但此方法只能对文字进行加密,不能对图像进行加密。为了克服以上基于混沌映射和 DNA 序列加密的缺点,本文采取伪 DNA 密码思想与高维混沌映射相结合的方法对图像进行加密。

1 混沌系统与 DNA 相关知识

1.1 混沌序列

本文研究的图像加密算法中涉及到二维 Logistic 混沌映射、Chen 混沌映射、PWLCM 混沌映射 3 个混沌映射,下面分别介绍这 3 个混沌映射。

二维 Logistic 映射形式为

$$\left.\begin{aligned} x_{n+1} &= 4\mu_1 x_n(1-x_n)+\gamma y_n \\ y_{n+1} &= 4\mu_2 y_n(1-y_n)+\gamma x_n \end{aligned}\right\} \tag{1}$$

式中:x 和 y 是状态变量,x、$y\in(0,1)$;μ_1、μ_2 和 γ 是控制参数,当 μ_1,$\mu_2\in[0.89,0.9]$、$\gamma\in(0,1)$时,系统处于混沌状态。

Chen 混沌映射是一种三维的混沌映射,其映射形式为

$$\left.\begin{aligned} \dot{x} &= a(y-x) \\ \dot{y} &= (c-a)x-xz+cy \\ \dot{z} &= xy-bz \end{aligned}\right\} \tag{2}$$

式中:x、y 和 z 是状态变量;a、b 和 c 是正实数。当 $a=35$、$b=3$、$c\in[20,28.4]$时,混沌系统便进入混沌状态。

PWLCM 混沌映射也是一种典型的混沌映射,其映射形式为

$$x_{n+1}=F(x_n,\mu)=\begin{cases} x_n/\mu \\ (x_n-\mu)/(0.5-\mu) \\ F(1-x_n,\mu) \end{cases} \tag{3}$$

式中:$\mu\in[0,1]$;$x_n\in(0,1)$,$n=0,1,2,\cdots$。当 $0\leqslant\mu<0.5$ 时,系统进入混沌状态;当 $0.5\leqslant\mu\leqslant1$ 时,系统逐渐进入分岔期,直至收敛为一点。

1.2 DNA 序列运算规则

1.2.1 DNA 编码 单链 DNA 序列由腺嘌呤 A、鸟嘌呤 G、胞嘧啶 C 和胸腺嘧啶 T 4 种碱基组成[15],其中 A 与 T、C 与 G 互补。算法中用 A、C、G、T 对四进制序列进行编码,共有 24 种编码组合。由于四进制 0 与 3 互补,1 与 2 互补,所以在 24 种编码中,只有 8 种编码满足碱基互补配对原则。编码方法如表 1 所示。

表 1 DNA 序列的 8 种编码方法

四进制	编码方法							
	I	II	III	IV	V	VI	VII	VIII
0	A	A	C	C	G	G	T	T
1	C	G	A	T	A	T	C	G
2	G	C	T	A	T	A	G	C
3	T	T	G	G	C	C	A	A

1.2.2 DNA 序列的截取与延长操作 P_1、P_2 均是一条完整的 DNA 序列,S_1、S_2 和 S_3、S_4 分别是 P_1 和 P_2 的子序列,P_3 是将 P_1 的子序列 S_2 截取后得到的新 DNA 序列,P_4 是将 P_1 的子序列 S_2 连接到 P_2 后得到的新 DNA 序列。

1.2.3 DNA 运算法则 随着 DNA 计算的发展,一些学者提出了 DNA 序列的生物和代数运算[16-17]。由于 DNA 序列有 8 种编码方法,因此在进行 DNA 异或运算时也有 8 种不同的结果。本文采用 0-A,1-C,2-G,3-T 的映射规则进行 DNA 编码,具体运算规则如表 2 所示。

表 2　DNA 序列异或运算法则

碱基	碱基	运算结果
A	A	A
A	C	C
A	G	G
A	T	T
C	A	C
C	C	G
C	G	T
C	T	A
G	A	G
G	C	T
G	G	A
G	T	C
T	A	T
T	C	A
T	G	C
T	T	G

2　伪 DNA 密码图像加密算法

本文算法的加密流程如图 1 所示，加密过程为：利用外部密钥和图像尺寸共同产生混沌系统的初始条件和控制参数；利用二维 Logistic 混沌系统产生的伪随机数对原始图像进行置乱；将置乱图像转换为四进制序列，利用 PWLCM 混沌系统产生的伪随机数和四进制序列值对四进制序列进行 DNA 动态编码；利用 Chen 混沌系统产生一个与四进制序列等长的随机 DNA 序列，并与编码后的 DNA 序列进行异或运算及截取延长操作；选择一种 DNA 解码方式进行解码得到加密图像。

2.1　混沌系统初始条件的产生

混沌系统的初始条件是根据 320 位的外部密钥和图像尺寸共同产生的，初始条件包括初始状态变量 x_0、y_0、p_0、q_0、r_0、k_0，控制参数包括 μ_1、μ_2、μ_3。外部密钥被分成 8 bit 长的块 $K_i(i=0,1,\cdots,40)$。设置 $C=0$，用 $C=K_i\oplus(C\gg1)$重复进行迭代操作，其中$\oplus$表示异或操作，$x\gg y$ 表示 x 向右移 y 个比特位；然后，通过 $K_i=K_i\oplus(C\gg3)$对块 $K_i(i=0,1,\cdots,40)$进行修正。

计算混沌系统的初始条件，需产生 9 个数 $Q_i(i=0,1,\cdots,8)$，计算公式为

$$Q_i=(n+\sum_{j=0}^{5}256^jK_{4i+j})/W \tag{4}$$

式中：$W=n+2^{48}$，n 表示原始图像的尺寸。

混沌系统的初始条件为：$x_0=Q_0$，$y_0=Q_1$，$\mu_1=0.89+0.01Q_2$，$\mu_2=0.89+0.01Q_3$，$p_0=Q_4$，$q_0=Q_5$，$r_0=Q_6$，$k_0=Q_7$，$\mu_3=0.5Q_8$。(x_0,y_0,μ_1,μ_2)为二维 Logistic 混沌映射的初始状态和控制参数；(p_0,q_0,r_0)为 Chen 混沌系统的初始状态；(k_0,μ_3)为 PWLCM 混沌映射的初始状态和参数。

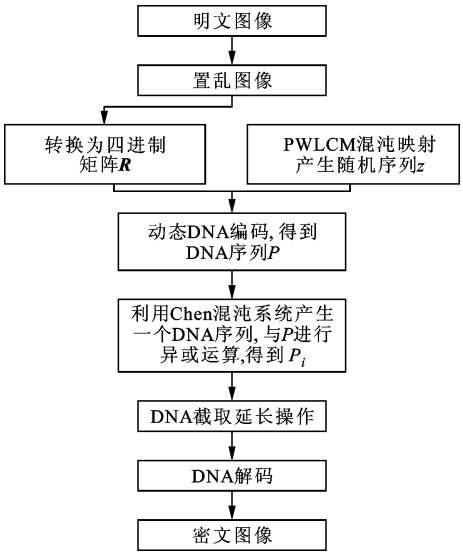


图 1　伪 DNA 密码图像加密算法流程图

2.2　置乱算法

置乱算法的具体步骤如下：

步骤 1　设置二维 Logistic 混沌映射初始状态(x_0,y_0)，系统参数(μ_1,μ_2)，从迭代的 M 步开始取$(x_0,x_1,\cdots,x_i)$、$(y_0,y_1,\cdots,y_i)$，$i=0,1,\cdots,mn-1$；

步骤 2　根据 $z_i=\alpha x_i+(1-\alpha)y_i$ 产生新的伪随机序列$(z_0,z_1,\cdots,z_i)$，$i=0,1,\cdots,mn-1$，参数 $\alpha\in(0,1)$；

步骤 3　将$(z_0,z_1,\cdots,z_{mn-1})$序列进行升序排序得到新序列$(z'_0,z'_1,\cdots,z'_{mn-1})$；

步骤 4　标记出原序列$(z_0,z_1,\cdots,z_{mn-1})$在排序后的新序列$(z'_0,z'_1,\cdots,z'_{mn-1})$的位置，得到位置序列$(w_0,w_1,\cdots,w_{mn-1})$，则每一个 z_i 对应一个位置序列 w_i；

步骤 5　将原始图像矩阵 $\boldsymbol{I}$ 转换为一维数组 $\boldsymbol{I}_i$，$i=0,1,\cdots,mn-1$，而 x_i 又对应位置 w_i，将原始图像一维数组 $\boldsymbol{I}(i)$用对应的 $\boldsymbol{I}(w_i)$来替换得到置乱后的一维数组 $\boldsymbol{I}'$。

2.3　DNA 动态编码

DNA 动态编码的具体步骤如下：

步骤 1　设置 PWLCM 混沌映射的初始状态(K_0,μ_3)，从迭代的第 M 步开始取$(k_0,k_1,\cdots,k_i)$，$i=0,1,\cdots,4mn-1$；

步骤 2 将 k_i 随机数按照 $V_i=\mathrm{mod}(\mathrm{floor}(k_i\times 10^{15}),M\times N)$ 进行计算得到整数序列 V_i，其中 mod()为取模函数，floor()为取下整函数；

步骤 3 将置乱后的图像转换为四进制序列 R_i，$i=0,1,\cdots,4mn-1$；

步骤 4 根据四进制序列第一个值 R_0 和整数 V_0 通过 $\left.\begin{aligned}S&=\mathrm{mod}(R_0+V_0,8)\\C_0&=\mathrm{bianma\_box}(R_0,S)\end{aligned}\right\}$ 计算出 S 值，依据 S 值选择相应的编码方式对四进制序列第一个值进行编码得到 C_0，其中 bianma_box()为编码函数；

步骤 5 根据 $\left.\begin{aligned}S&=\mathrm{mod}(S+C_{i-1}+V_i,8)\\C_i&=\mathrm{bianma\_box}(R_i,S)\end{aligned}\right\}$ 对四进制序列其他值进行 DNA 编码，得到动态编码后的 DNA 序列。

算法加密具体过程步骤如下：

步骤 1 输入待加密的 8 位灰度图像 $I(m,n)$，(m,n)为原始图像 I 的行数和列数；

步骤 2 设置二维 Logistic 混沌映射的初始状态 (x_0,y_0)，系统参数(μ_1,μ_2)，从迭代的第 M 步开始取 $(x_0,x_1,\cdots,x_i)$和$(y_0,y_1,\cdots,y_i)$，$i=0,1,\cdots,mn-1$；

步骤 3 根据式(7)产生新的伪随机序列$(z_0,z_1,\cdots,z_i)$，$i=0,1,\cdots,mn-1$；

步骤 4 将$(z_0,z_1,\cdots,z_{mn-1})$按照升序排序得到新序列$(z'_0,z'_1,\cdots,z'_{mn-1})$；

步骤 5 标记出原序列$(z_0,z_1,\cdots,z_{mn-1})$在排序后的新序列$(z'_0,z'_1,\cdots,z'_{mn-1})$的位置，得到位置序列$(w_0,w_1,\cdots,w_{mn-1})$，则每一个 z_i 对应一个位置序列 w_i；

步骤 6 将原始图像矩阵 $\boldsymbol{I}$ 转换为一维数组 $\boldsymbol{I}_i$，而 x_i 对应位置 w_i，故可以将原始图像一维数组 $\boldsymbol{I}(i)$用对应的 $\boldsymbol{I}(w_i)$来替代，得到置乱后的一维数组 $\boldsymbol{I}'$；

步骤 7 设置 PWLCM 混沌映射的初始状态(k_0,μ_3)，从迭代的第 M 步开始取$(k_0,k_1,\cdots,k_i)$，$i=0,1,\cdots,4mn-1$；

步骤 8 将 k_i 随机数进行计算得到整数序列 V_i；

步骤 9 将置乱后的图像转换为四进制序列 R_i，$i=0,1,\cdots,4mn-1$；

步骤 10 根据四进制序列第一个值 R_0 和整数 V_0 计算 S 值，依据 S 值选择相应的编码方式对四进制序列第一个值进行编码得到 C_0；

步骤 11 对四进制序列其他值进行 DNA 编码，得到动态编码后的 DNA 序列 G；

步骤 12 利用三维 Chen 混沌映射分别以初值(p_0,q_0,r_0)，从迭代的第 L 步开始取(p_i,q_i,r_i)序列$(i=0,1,\cdots,(4mn-1)/3)$，产生一维随机序列 $f_i(i=0,1,\cdots,4mn-1)$，利用 f_i 产生一个 DNA 序列 T，将 T 与 G 进行异或运算得到 G'

$$\left.\begin{aligned}f_{3i}&=p_i-\mathrm{floor}(p_i)\\f_{3i+1}&=q_i-\mathrm{floor}(q_i)\\f_{3i+2}&=r_i-\mathrm{floor}(r_i)\end{aligned}\right\}\tag{5}$$

步骤 13 选择一种解码方式对 G'进行 DNA 解码得到四进制序列 R'；

步骤 14 根据 R'值大小进行截取延长操作，并将截取延长后的四进制序列转换为十进制矩阵，得到最终加密图像。

3 实验结果与分析比较

3.1 实验结果

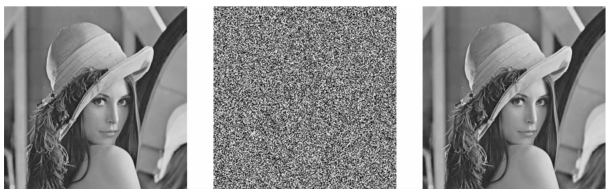
为了测试本文算法的性能，我们选取 6 个灰度级为 256，大小分别为 128×128、256×256、512×512、102 4×102 4 的样本图像，实验用图如图 2 所示。

(a)白图 (128×128)　(b)摄影者 (256×256)　(c)飞机 (512×512)

(d)莉娜 (512×512)　(e)辣椒 (512×512)　(f)黑图 (1 024×1 024)

图 2 实验用图

在 Matlab2012 环境下，对 512×512 的莉娜灰度图像进行加解密实验。加密和解密图像如图 3 所示。



(a)原始图像　(b)密文图像　(c)解密图像

图 3 加密和解密图像

3.2 置乱度定量分析

本文在对加密图像置乱度性能参数进行分析

时,采取不动点比、灰度变化平均值、信息熵以及局部信息熵等方法来检验算法的置乱效果,下面分别介绍 4 种置乱度评价参数。

(1)设 $P=(p_{ij})_{M\times N}$ 表示大小为 $M\times N$ 的原始图像,$C=(c_{ij})_{M\times N}$ 表示大小为 $M\times N$ 的加密图像,其中 p_{ij} 和 c_{ij} 是图像像素在位置(i,j)上的像素值。

若图像 P 中不动点占所有像素点的百分比用 $B(P,C)$表示,则不动点比表示式为

$$B(P,C)=\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}d(i,j)}{MN}\times 100\% \tag{6}$$

式中:$d(i,j)=\begin{cases}1,\text{if } p(i,j)=c(i,j)\\0,\text{if } p(i,j)\neq c(i,j)\end{cases}$。

(2)设 $P=(p_{ij})_{M\times N}$ 和 $C=(c_{ij})_{M\times N}$ 分别表示大小为 $M\times N$、灰度级为 V 的明文图像和密文图像,用 $G(P,C)$表示两幅图像的灰度变化平均值,计算公式为

$$G(P,C)=\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}\mid p_{ij}-c_{ij}\mid}{MN} \tag{7}$$

(3)信息熵是描述在一个给定的系统中不确定性或随机性的程度。计算公式为

$$H(m)=-\sum_{i=0}^{2^N-1}p(m_i)\log_2(p(m_i)) \tag{8}$$

式中:2^N 是总的样本数;$m_i\in m$;$p(m_i)$表示样本 m_i 的概率分布。

(4)加密图像的局部随机性可以通过局部信息熵来测试[16]。(k,T_B)局部信息熵定义为

$$\overline{H}_{k,T_B}(m)=\sum_{i=1}^{k}\frac{H(S_i)}{k} \tag{9}$$

式中:S_i 表示有 T_B 个像素随机选择的互不重叠的图像块。文献[16]建议取 $k=30$,$T_B=1\ 936$。

对于加密理想的图像,不动点比在 0.40% 以内,灰度变化平均值差值在 0.5 以内,信息熵在 7.996 以上,局部信息熵在 7.9 以上。

下面以标准的 512×512 莉娜图像为测试图像,分别选取 5 组不同的密钥对测试图像进加密,得到 5 幅加密图像然后进行分析评价,表 3 给出了分析结果。

从表 3 可以看出,不动点比、灰度变化平均值、信息熵和局部信息熵 4 个置乱度评价参数均取得了比较理想的值。在 5 组数据中,每幅加密图像的不动点比都比较小,均没有超过 0.4%;从明文图像与密文图像的差值变化情况来看,在不同密钥条件下,

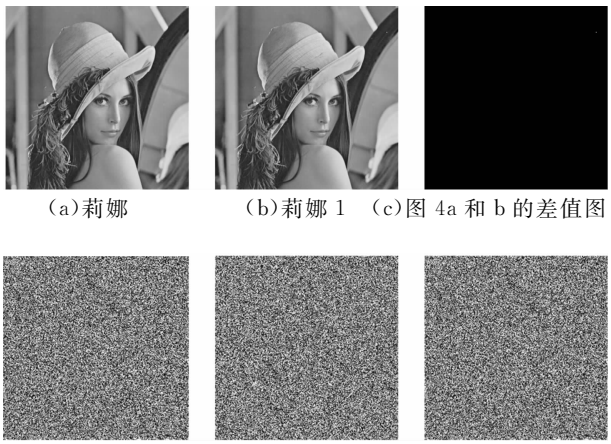
表 3　置乱度评价参数

明文图像	密文图像	不动点比/%	灰度变化平均值	信息熵	局部信息熵
莉娜	莉娜 1	0.399 4	72.958 7	7.999 2	7.900 6
	莉娜 2	0.383 4	72.776 5	7.999 3	7.899 8
	莉娜 3	0.390 6	72.970 9	7.999 3	7.902 8
	莉娜 4	0.389 1	73.001 0	7.999 3	7.904 0
	莉娜 5	0.380 7	73.060 9	7.999 2	7.901 7

5 幅密文图像与明文图像的灰度变化平均值变化非常均匀,灰度变化平均值在 72.7～73.1 之间,图像的最大灰度变化平均值与最小灰度变化平均值之差没有超过 0.5。从 5 组数据中可以看出:加密图像和原始图像的灰度差是均匀变化的;5 组密文信息熵均超过 7.996,非常接近 8 的理想值。由此可见:密文图像的灰度值分布非常均匀;图像的局部信息熵均在 7.9 左右,因此本算法加密的密文图像有很好的局部随机性。综上所述,本算法所得加密图像置乱效果较好,安全性较高。

3.3　安全性分析

3.3.1　*差分攻击分析*　差分攻击的手段主要是将原图像做细微改变,然后用相同的密钥分别对原图像和修改后的图像进行加密,通过比较和统计两幅加密图像之间的差别,找出明文图像和密文图像之间的规律和联系,以此来破解算法。因此,一个好的加密算法应该能够有效地抵抗差分攻击。本文算法中,明文图像像素即使发生 1 bit 的变化,所加密的图像也会与原始图像加密的密文图像截然不同。为了测试算法的明文敏感性,实验中将莉娜图像(75,480)坐标处的像素点设置为 0,其余像素点不变,得到改变后的图像莉娜 1 如图 4 所示。然后,用相同



(a)莉娜　(b)莉娜 1　(c)图 4a 和 b 的差值图

(d)莉娜加密图像　(e)莉娜 1 加密图像　(f)图 4d 和 e 的差值图

图 4　密文差值图

的密钥对莉娜和莉娜 1 进行加密，得到密文图像 C_1 和 C_2。

加密算法中明文的敏感性通常用像素变化率 T 和归一化平均变化强度 U 来计算。假设 C_1 和 C_2 仅是 1 bit 不同的明文图像加密得到的密文图像。$c_1(i,j)$和 $c_2(i,j)$分别代表密文图像 C_1 和 C_2 在第 i 行、第 j 列的灰度值，则 T 和 U 的计算公式为

$$T=\frac{\sum_{i}^{M}\sum_{j}^{N}D(i,j)}{MN}\times 100\% \tag{10}$$

$$U=\frac{\sum_{i}^{M}\sum_{j}^{N}\mathrm{abs}(c_1(i,j)-c_2(i,j))/255}{MN}\times 100\% \tag{11}$$

式中：abs()表示取绝对值。如果 $c_1=c_2$，$D(i,j)=0$；否则，$D(i,j)=1$。理想的加密算法，像素变化率值大约是 99.6%，归一化平均变化强度大约是 33.46%。

实验中，随机选择原始图像的一个像素进行改变得到改变后的图像，然后用相同的密钥对原始图像和改变后的图像进行加密，并计算两个密文图像的像素变化率和归一化平均强度。对于图 2 中的样本，每个样本测试 1 000 次。表 4 分别给出了每个样本的 T 和 U 的最大值、最小值和平均值。从表 6 中可以看出，用本文提出的加密算法加密的图像的 T 值均在 99.5%以上，U 值均在 33.2 以上，非常接近理想值。也就是说，在相同的密钥条件下，即使原始图像改变 1 bit，加密的图像与原始图像加密的图像也会截然不同。因此，本文算法有良好的雪崩效应，攻击者试图利用差分攻击的方法对算法或加密图像进行解密几乎是不可能的。

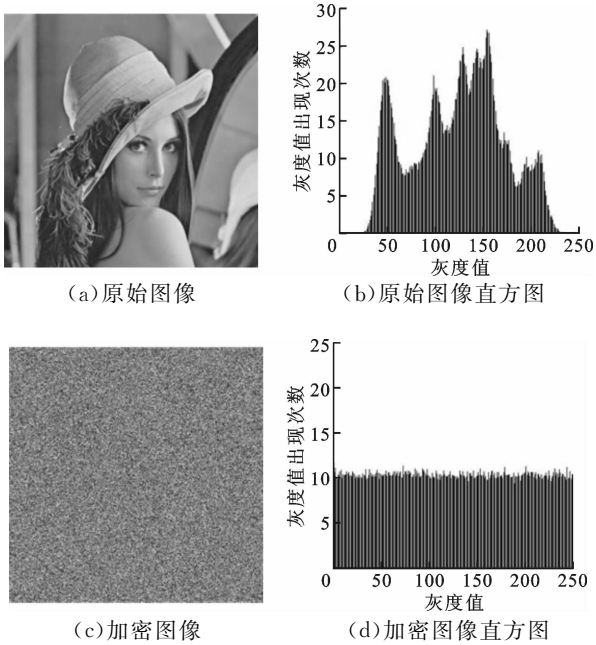
表 4 明文敏感性分析表 单位：%

图像	平均值		最大值		最小值	
	T	U	T	U	T	U
白图	99.643 4	33.378 5	99.737 5	33.781 7	99.530 0	33.054 3
摄影者	99.632 1	33.396 1	99.670 4	33.602 1	99.566 7	33.277 5
飞机	99.613 6	33.424 3	99.629 6	33.553 3	99.572 8	33.351 6
莉娜	99.609 0	33.459 5	99.645 6	33.620 1	99.553 4	33.330 9
辣椒	99.608 0	33.441 7	99.687 2	33.702 7	99.517 8	33.386 6
黑图	99.607 1	33.426 9	99.684 1	33.500 1	99.543 7	33.283 6

3.3.2 *密钥空间分析* 密钥空间的大小与能否抵抗穷举攻击有很大关系。因此，为了抵抗穷举攻击，一个好的图像加密算法应该有足够大的密钥空间，而且加密算法对密钥也要极其敏感。本文算法中，密钥空间为 320 bit，其密钥空间是 $2^{320}\approx 2.135\ 9\times 10^{96}$。根据目前计算机双精度浮点数的精度，我们取 8 B、15 bit 有效数字进行分析，设尝试一次破解所需时间的数量级为 1 ms，则分析密钥空间穷举破解所需时间约为 6.16×10^{85} a。因此，本文算法密钥空间是足够大的，能够有效抵抗穷举攻击。

3.3.3 *统计性分析* 一个理想的加密算法要能够抵抗统计攻击。为了更加科学地验证和分析算法的加密效果及安全性，我们从直方图、卡方值、密文图像相邻像素之间的相关性 3 个方面来分析加解密图像。

图像直方图表征图像像素的分布情况，它是图像的重要统计特性之一。作为评价图像加密效果的标准之一，加密后的图像直方图变化越大，与原始图像差别越大，原始图像的视觉特征就越不明显。通常情况下，认为直方图越均衡，加密效果越好。图 5



(a)原始图像 (b)原始图像直方图

(c)加密图像 (d)加密图像直方图

图 5 原始图像与加密图像直方图

显示了大小为 512×512 的莉娜原始图像和加密图像的直方图。从直方图来看,莉娜原始图像像素比较集中,(0,255)的两端像素分布比较少,而中间分布的较多,密文图像的灰度值分布相对比较均衡,基本接近理想的灰度值分布。因此,攻击者很难利用像素灰度值的统计特性得到有用的信息。图像像素值分布的均衡程度也可用卡方值χ^2测试来进行分析,一个灰度级为 256 的图像的χ^2计算公式为

$$\chi^2=\sum_{i=0}^{255}\frac{(n_i-n/256)^2}{n/256} \tag{12}$$

式中:n_i 表示灰度为 i 的像素出现的频率;$n/256$ 是每个灰度级出现的期望频率。对于灰度级为 256 的图像,理想的加密图像卡方值应小于$\chi^2(0.05,255)=293.5$。

不同图像的明文图像和密文图像卡方值如表 5 所示,从表中可以看出,明文图像的卡方值非常大,而每个密文图像的卡方值均小于 293.5,表明密文图像的直方图没有明显波峰,像素值分布比较均衡。原始图像像素间的相关性很高,为了抵抗统计攻击,必须降低加密图像的相关性。实验中,我们分别从原始图像和加密图像中随机选取在水平方向、垂直方向以及对角线方向上各 1 000 对像素点,然后计算各个方向的相关性,即

表 5　卡方值分析表

图像	卡方值	
	明文图像	密文图像
白图	4 177 920	276.31
摄影者	98 781.453	228.94
飞机	715 669.152	242.52
莉娜	158 063.623	261.15
辣椒	138 836.174	252.56
黑图	267 386 880	250.14

$$\left.\begin{aligned} r_{xy}&=\frac{\operatorname{cov}(x,y)}{(D(x)D(y))^{1/2}}\\ \operatorname{cov}(x,y)&=\frac{1}{Y}\sum_{i=1}^{N}(x_i-\bar{x})(y_i-\bar{y})\\ D(x)&=\frac{1}{Y}\sum_{i=1}^{N}(x_i-\bar{x})^2 \end{aligned}\right\} \tag{13}$$

式中:x_i 和 y_i 是两个相邻像素;Y 是相邻像素对的总数;$\bar{x}$ 和 $\bar{y}$ 代表 x 和 y 的平均值。

原始图像和加密图像相邻像素的关联度如表 8 所示。一幅自然图像相关性应在 0.9 以上,接近 1,效果理想的加密图像相关性应在 0.01 以下,接近 0。

从表 6 可以看出,明文图像无论水平、垂直、对角线方向的两个相邻像素的相关性都接近于 1,像白图和黑图两幅特殊单色图像,各方向相关性都等于 1,说明原始图像相关性非常强。密文图像无论水平、垂直还是对角线方向,两个相邻像素之间的相关性都接近于 0,表明原始图像经过加密以后,图像之间的相关性变得非常小,说明本文算法有很强的抵抗统计攻击的能力。

表 6　相关性分析表

图像	明文图像相关性			密文图像相关性		
	水平方向	垂直方向	对角线方向	水平方向	垂直方向	对角线方向
白图	1.000 0	1.000 0	1.000 0	−0.002 3	−0.005 8	−0.011 6
摄影者	0.931 3	0.962 2	0.908 3	−0.004 1	0.003 0	0.005 5
飞机	0.965 8	0.961 6	0.935 6	−0.006 2	0.007 4	0.011 8
莉娜	0.972 2	0.985 4	0.962 0	0.009 8	−0.003 3	0.008 1
辣椒	0.980 9	0.982 2	0.968 6	−0.001 4	−0.001 9	0.008 6
黑图	1.000 0	1.000 0	1.000 0	0.001 8	−0.005 8	−0.016 3

3.3.4　*加密速度分析*　一个好的加密算法不仅要有好的安全性,也要尽可能满足实时性的要求。仿真实验中,我们用 Matlab2012 在主频为 3.10 GHz、内存为 8 GB 的 win7 操作系统下,对不同尺寸的灰度图像进行加密速度测试,每组测试进行 100 次实验,然后取加密时间的平均值,实验结果如表 7 所示。

表 7　加密速度分析表　　单位:s

图像	加密速度			
	文献[8]	文献[17]	文献[18]	本文算法
白图(128×128)	0.312 7	0.373 6	0.507 9	0.249 3
摄影者(256×256)	0.922 3	1.209 2	1.613 6	0.696 6
飞机(512×512)	3.407 2	4.603 4	6.290 2	2.474 8
莉娜(512×512)	3.365 5	4.574 7	6.237 2	2.474 9
辣椒(512×512)	3.397 7	4.597 8	6.251 8	2.476 6
黑图(1 024×1 024)	12.893 3	17.912 2	24.705 3	9.346 3

4 结 论

本文针对现有基于 DNA 序列的图像加密算法对实验条件要求苛刻、实验难以实现的不足，结合高维混沌系统和伪 DNA 密码思想的特点，提出了一种基于伪 DNA 密码思想的图像加密算法。将 DNA 加密的一些基本思想与混沌系统结合使用，增加了密文图像的安全性。针对静态 DNA 编码对原始图像进行编码不能有效抵抗差分攻击和统计攻击的不足，本文算法在编码过程中采用动态 DNA 编码方式，结合原始图像信息和混沌系统产生的随机数来选择编码规则；同时，根据编码后的密文数值对 DNA 序列进行延长截取操作，使密文图像安全性进一步提高。仿真实验结果表明，本算法具有较好的安全性和较快的加密速度，能够抵抗枚举攻击和统计攻击，适用于军事、医疗、司法等机密图像的保密存储和网络传输。

参考文献：

[1] LI S, CHEN G, CHENG A, et al. On the design of perceptual MPEG-Video encryption algorithms [J]. IEEE Trans Circuits Syst Video Technol, 2007, 17(2): 214-223.

[2] ZHANG G, LIU Q. A novel image encryption method based on total shuffling scheme [J]. Optics Communications, 2011, 284(12): 2775-2780.

[3] WANG Z, HUANG X, LI Y, et al. A new image encryption algorithm based on the fractional order hyperchaotic Lorenz system [J]. Chinese Physics: B, 2013, 22(1): 010504.

[4] ZHU C. A novel image encryption scheme based on improved hyper-chaotic sequences [J]. Optics Communications, 2012, 285(1): 29-37.

[5] LIAN S G. A block cipher based on chaotic neural networks [J]. Neurocomputing, 2009, 72(4): 1296-1301.

[6] FU C, ZHU Z. Chaotic image encryption scheme based on circular bit shift method [C]// The 9th International Conference for Young Computer Scientists. Piscataway, NJ, USA: IEEE, 2008: 3057-3061.

[7] WEI X, GUO L, ZHANG Q, et al. A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system [J]. Journal of Systems and Software, 2012, 85(2): 290-299.

[8] ZHANG G, LIU Q. A novel image encryption method based on total shuffling scheme [J]. Optics Communications, 2011, 284(12): 2775-2780.

[9] LIAN S G, SUN J S, WANG Z Q. A block cipher based on a suitable use of the chaotic standard map [J]. Chaos, Solitons & Fractals, 2005, 26(1): 117-129.

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

[11] SHYAM M, KIRAN N, MAHESWARAN V. A novel encryption scheme based on DNA computing [J]. Nonlinear Dynamics, 2007, 23(1): 142-150.

[12] KANG N. A pseudo DNA cryptography method [EB/OL]. [2014-11-12]. http://arxiv.org/pdf/0903.2693v1.pdf.

[13] WATSON J D, CRICK F H. A structure for deoxyribose nuclei acid [J]. Nature, 1953, 171(4356): 737-738.

[14] GABORITP, KING O D. Linear constructions for DNA codes theory Compute [J]. Nonlinear Dynamics, 2005, 334(1): 99-113.

[15] KING O D, GABORIT P. Binary templates for comma-free DNA codes [J]. Discrete Appl Math, 2007, 155(1): 831-839.

[16] WU Y, ZHOU Y, SAVERIADES G, et al. Local Shannon entropy measure with statistical tests for image randomness [J]. Information Sciences, 2013, 222(2): 323-342.

[17] XUE X, ZHANG Q, WEI X, et al. An image fusion encryption algorithm based on DNA sequence and multi-chaotic maps [J]. Journal of Computational and Theoretical Nanoscience, 2010, 7(2): 397-403.

[18] ZHANG Q, GUO L, WEI X P. A novel image fusion encryption algorithm based on DNA sequence operation and hyperchaotic system [J]. Optik, 2013, 124(18): 3596-3600.

（编辑 赵炜）