文章编号：1000-8608(2019)05-0543-08

基于密钥流缓冲区和DNA动态编码的图像加密算法

张丽君[1]，徐喜荣*[2]，耿　彧[1]，聂卫国[3]，张选平[3]

（1.锦州医科大学 公共基础学院，辽宁 锦州 121001；
2.大连理工大学 计算机科学与技术学院，辽宁 大连 116024；
3.西安交通大学 计算机科学与技术学院，陕西 西安 710049）

摘要：数字图像的安全性传输是研究热点问题.针对现有基于DNA序列的图像加密算法中密钥对明文敏感性不足的问题，提出了一种基于密钥流缓冲区和DNA动态编码的图像加密算法.首先，利用混沌系统产生伪随机序列对明文图像实现全局置乱；然后，通过PWLCM混沌系统初始化密钥流缓冲区，根据明文像素值选择密钥，对置乱图像进行DNA动态编码；最后，对编码后的密文序列再进行一轮扩散操作.仿真结果表明，该算法在置乱度、密钥空间、抵御差分攻击和统计攻击等方面均具有良好的效果.

关键词：图像加密；混沌系统；密钥流缓冲区；DNA动态编码

中图分类号：TP391　　**文献标识码：**A　　**doi：**10.7511/dllgxb201905014

0　引　言

数字图像是具有高保密要求的重要媒体形式，设计快速、高效、安全的图像加密算法已成为图像安全保护的研究热点[1].在图像加密中，图像数据具有数据量大且相邻像素点具有较强相关性的特点，所以采用传统的图像加密技术无法满足图像数据加密的实时性要求.混沌加密采用迭代的方式生成密钥序列，生成速度快，可以很好地满足图像加密的实时性要求，因此得到了广泛应用，其具有遍历性、初值敏感性和伪随机性等特点.现有的基于混沌系统加密算法主要分为置乱、替换和扩散3个过程[2].置乱是对图像像素位置的改变，如Arnold及其扩展变换、Baker变换、魔方变换、幻方变换等[3]，但单纯基于置乱变换的加密算法不能抵抗统计攻击，需要和其他加密理论结合使用.替换是对图像像素值的改变，替换图像的灰度值均匀分布效果越理想，抵御统计攻击的能力越强.由于像素值替换与混沌序列存在一定的映射关系，基于混沌的加密算法中常常引入扩散过程，以此提高抵抗差分攻击的能力.一些改进的混沌加密算法用于不断提高加密算法的安全性能，如充分利用DNA计算的高度并行性、超低能量消耗和海量存储能力等特点，实现对含有大数据量的图像信息进行存储和加密[4].饶妮妮提出了一种基于重组DNA技术的加密方案[5]，用到了数学变换和生物学技术，该方法不仅加密性好，而且安全性高.为了脱离复杂的生物学实验，Verma等[6]提出了一种伪DNA加密方法，利用分子生物学的中心法则实现文字加密.但是，现有的大多数基于DNA序列的图像加密算法仍存在一定的局限性，即密钥的选择并没有考虑与明文间的关系，导致加密算法明文敏感性不足，无法抵御穷举攻击和统计攻击等.

为了解决上述问题，本文引入密钥流缓冲区和DNA动态编码的图像加密算法来提高密钥对明文的依存度，并通过仿真实验验证算法是否满足数字图像的加密要求.

1　加密算法

1.1　混沌系统初始条件的产生

根据明文图像和SHA-512共同产生外部密

收稿日期：2018-12-09；　**修回日期：**2019-07-29.
基金项目：国家自然科学基金资助项目(61472465)；辽宁省自然科学基金资助项目(20180550161)；陕西省自然科学基金资助项目(2014JM8322).
作者简介：张丽君(1967-)，女，副教授，E-mail：zhanglijun@jzmu.edu.cn；徐喜荣*(1967-)，女，副教授，博士生导师，E-mail：xirongxu@dlut.edu.cn.

钥,然后由 512 位的外部密钥再产生混沌系统的初值.因此,明文图像的微小改变都会引起外部密钥的差异.将外部密钥 K 分成 16 块,每块长度为 32 bit,$K=\{k_0,\cdots,k_i,\cdots,k_{15}\}$.通过循环移位和异或运算更新块 $k_i(i=0,\cdots,15)$:

$$k_i=k_i\oplus((\bigoplus_{i=0}^{15}(k_i\gg 3i))\gg 5i) \tag{1}$$

由于 k_i 是一个 32 位二进制数,对应的十进制数整数范围为 0 到 $2^{32}-1$,将 k_i 转换为实数 $Q_i\in(0,1)$.

$$Q_i=(N+k_i+k_{(i+9)\%16})/(2N+2^{32}) \tag{2}$$

式中:N 表示明文图像的尺寸.

令 Chen 混沌系统的初始值为$(c_{x_0},c_{y_0},c_{z_0})$,PWLCM 混沌系统的初始值为$(p_{x_0},\mu_3)$,$(p_{x'_0},\mu_4)$和$(p_{x''_0},\mu_5)$,其中 $c_{x_0}=Q_0$,$c_{y_0}=Q_1$,$c_{z_0}=Q_2$,$p_{x_0}=Q_3$,$\mu_3=0.5Q_4$,$p_{x'_0}=Q_5$,$\mu_4=0.5Q_6$,$p_{x''_0}=Q_7$,$\mu_5=0.5Q_8$.

1.2 置乱过程

由于原始图像相邻像素之间有很强的相关性,在用 DNA 编码规则进行编码时,很可能编码都是一样的,特别是对于平滑图像来说更是如此.因此,对明文图像进行编码时首先要对图像进行置乱,打乱像素之间的位置,减小相邻像素之间的相关性.算法中实现全局置乱并采用基于四叉树压缩格式的三维 Chen 混沌系统[7]来增大密钥空间.三维 Chen 混沌映射为

$$\begin{aligned}\dot{x}&=a(y-x)\\ \dot{y}&=(c-a)x-xz+cy\\ \dot{z}&=xy-bz\end{aligned} \tag{3}$$

式中:x、y 和 z 是状态变量,当 $a=35$,$b=3$,$c\in[20,28.4]$时,Chen 混沌系统进入混沌状态.

对于给定图像 P 大小为 $H\times W$ 的置乱过程具体如下:

(1)设置 Chen 混沌系统的初始值$(c_{x_0},c_{y_0},c_{z_0})$,系统参数$(\mu_1,\mu_2)$,迭代 $N_0+H\times W$ 次,丢弃前 N_0 个数据,取$(c_{x_0},c_{x_1},c_{x_{m-1}})$、$(c_{y_0},c_{y_1},c_{y_{m-1}})$和$(c_{z_0},c_{z_1},c_{z_{m-1}})$.令 $N_0=1\ 000$,$m=H\times W$.

(2)根据 x_i 和 y_i 产生新的伪随机序列 y_i $(i\in[0,m-1])$,

$$z_i=\alpha c_{x_i}+\beta c_{y_i}+\gamma c_{z_i} \tag{4}$$

其中 $\alpha,\beta,\gamma\in(0,1)$且 $\alpha+\beta+\gamma=1$.

(3)将伪随机数$(z_0,z_1,\cdots,z_{m-1})$按升序重排,得到索引序列 $T=(T_0,T_1,\cdots,T_{m-1})$.

(4)利用 ZigZag 扫描算法对原始图像 P 进行扫描,得到初始置乱图像的一维数组 $P'=(P'_0,\cdots,P'_{m-1})$.ZigZag 扫描算法如图 1 所示.

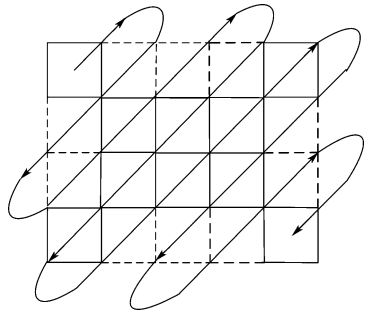


图 1 ZigZag 扫描算法

Fig. 1 ZigZag scanning algorithm

(5)因 x_i 与索引序列中的第 i 个位置相对应,将 P'_i 用对应的 P'_{T_i} 来替换,更新置乱后的一维数组 P'.

(6)将更新置乱后的一维数组 P'转换为二维矩阵 $\boldsymbol{P''}$,得到最终的置乱图像.

1.3 密钥流缓冲区

密钥流缓冲区是由混沌系统生成的随机数字池,可以根据当前像素值为前后相邻两个像素选择密钥.密钥流缓冲区包括两个操作:一个操作是初始化密钥流缓冲器,$init(x_0,y_0)$,首先将混沌系统的初始状态设置为(x_0,y_0),然后利用线性分段 PWLCM 混沌系统[8]生成混沌伪随机数序列,其表达式为

$$x_{n+1}=F(x_n,\mu)=\begin{cases}x_n/\mu; & 1\leqslant x_n<\mu\\ (x_n-\mu)/(0.5-\mu); & \mu\leqslant x_n<0.5\\ F(1-x_n,\mu); & x_n\geqslant 0.5\end{cases} \tag{5}$$

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

为了摆脱瞬态效应,对系统进行多次迭代.建立一个大小为 L_b 的存储空间(缓冲区)来存储伪随机序列的前 L_b 个数.为了根据图像像素容易地直接访问随机数,在此设置缓冲区大小 $L_b=256$.

另一个操作是从缓冲区中选取第 i 个随机数,$get(i)$.首先从缓冲区中将第 i 个随机数取出并返回该随机数,被选取的随机数取决于先前的替换像素值,其值为 0~255;然后用伪随机序列的首个随机数更新缓冲区中的第 i 个随机数.由

于密钥流缓冲区是根据明文像素值进行密钥选择，可以大幅度提高加密算法对明文的敏感性.

1.4　DNA 动态编码

在基于 DNA 序列的图像加密中，对原始图像进行 DNA 编码时，大多数方法采用统一编码方式，即图像中所有像素都使用同一种编码规则. 在本算法中，采用 DNA 动态编码，首先根据 $init(p_x,\mu)$ 方法实现密钥流缓冲区初始化，然后由置乱图像和密钥流缓冲区为每个像素选择相应的 DNA 编码规则进行编码，得到 DNA 编码序列. 具体方法如下：

(1)根据 $K_{b1\_}init(p_{x_0},\mu_3)$、$K_{b2\_}init(p_{x'_0},\mu_4)$ 和 $K_{b3\_}init(p_{x''_0},\mu_5)$ 初始化 3 个密钥流缓冲区 K_{b1}、K_{b2} 和 K_{b3}.

(2)将置乱图像 $\boldsymbol{P}''$ 转换为一维数组 $(P'_0,\cdots,P'_{m-1})$. 根据一维数组的第一个值 P'_0 和 $K_{b1\_}get(0)$，通过式(6)得到整数 S_0，依据整数 S_0 和 $K_{b2\_}get(0)$ 得到 P'_0 的密文 C_0：

$$\begin{aligned} S_0&=P'_0\oplus K_{b1\_}get(0)\\ C_0&=Code(S_0,\mathrm{mod}(K_{b2\_}get(0),7)) \end{aligned} \tag{6}$$

其中 $Code(S_0,\mathrm{mod}(K_{b2\_}get(0),7))$ 是指先将整数 S_0 转化为二进制序列，然后依据选择相应 $\mathrm{mod}(K_{b2\_}get(0),7)$ 的 DNA 编码方式对二进制序列进行编码，最后用 DNA 编码方式(7)进行解码得到 C_0.

(3)根据式(7)对一维数组 $P'=(P'_0,\cdots,P'_{m-1})$ 进行 DNA 动态编码，得到密文序列 $C=(C_1,\cdots,C_{m-1})$.

$$\begin{aligned} S_i&=P'_i\oplus K_{b1\_}get(i)\oplus C_{i-1}\\ C_i&=Code(S_i,\mathrm{mod}(K_{b2\_}get(i),7)) \end{aligned} \tag{7}$$

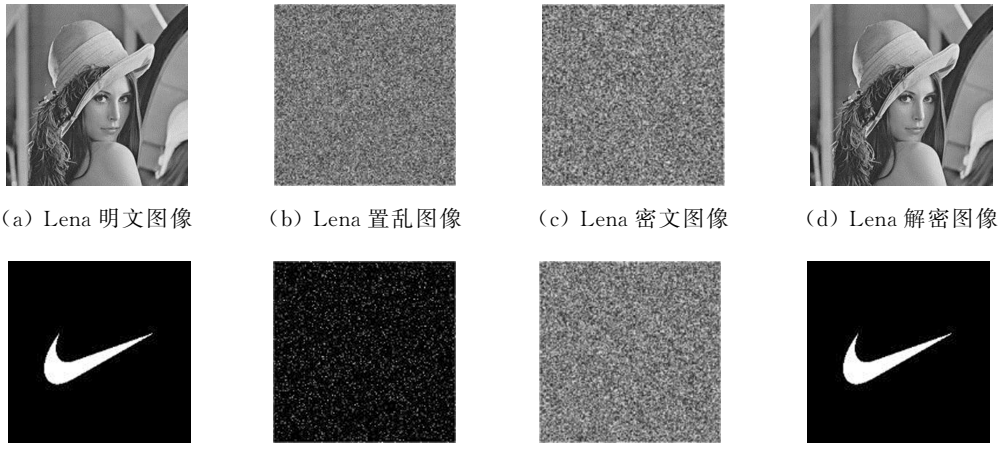
(4)通过式(8)进一步提高算法对明文图像的敏感性，得到最终的密文序列 $C'=(C'_0,\cdots,C'_{m-1})$.

$$\begin{aligned} C'_{m-1}&=C_{m-1}\oplus K_{b3\_}get(0)\\ C'_i&=C_i\oplus C'_{i+1}\oplus K_{b3\_}get(C'_{i+1}) \end{aligned} \tag{8}$$

2　实验分析

2.1　实验结果

选取两个灰度级为 256 的样本图像 Lena 和 Nike，图像 Lena 尺寸为 512×512，图像 Nike 尺寸为 256×256. 在 MATLAB 2013 环境下进行仿真实验，如图 2 所示. 从图可见，加密图像能够较好地隐藏原始图像特征并能够实现图像恢复.



(a) Lena 明文图像　(b) Lena 置乱图像　(c) Lena 密文图像　(d) Lena 解密图像

(e) Nike 明文图像　(f) Nike 置乱图像　(g) Nike 密文图像　(h) Nike 解密图像

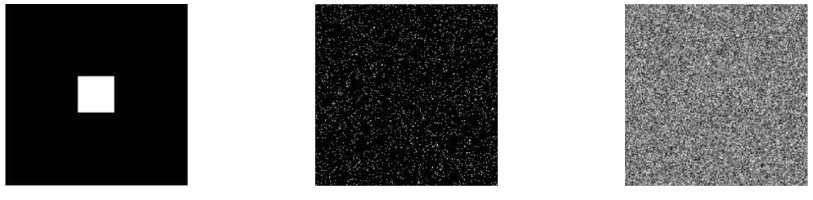
图 2　实验结果图

Fig. 2　Experimental result chart

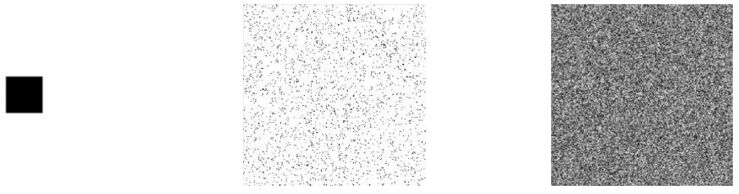
2.2　置乱度分析

(1)置乱度的定性分析

对算法的置乱度进行定性分析，将大小为 512×512 的大部分是黑色或白色，中间有一白块或黑块的图像作为测试图像，如图 3 所示. 从图 3(b)和 3(e)可以看出，明文图像 3(a)和 3(d)中的小白块和小黑块比较均匀地扩散到了整幅图像中；从图 3(c)和 3(f)可以看出，经过伪 DNA 动态编码后，已看不出中间小白块和小黑块的任何痕迹.



(a) 中间白块明文图像 (b) 中间白块置乱图像 (c) 中间白块密文图像



(d) 中间黑块明文图像 (e) 中间黑块置乱图像 (f) 中间黑块密文图像

图 3 置乱度定性测试

Fig. 3 Scrambling qualitative test

(2)置乱度的定量分析

采取 4 种置乱度评价方法来检验算法的置乱效果,实验结果如表 1 所示. 从中可以看出,不动点比均低于 0.4%;密文图像的信息熵都比较接近理论值,均在 7.996 以上,充分表明了密文图像灰度值分布的均匀性;此外,本算法产生的密文图像随机性较好,局部信息熵都在 7.9 以上. 综上分析,本算法具有比较理想的置乱效果.

表 1 置乱度的定量分析结果

Tab. 1 Quantitative analysis results of scrambling

图像	不动点比/%	灰度变化平均值	信息熵	局部信息熵
Boat	0.36	72.275 5	7.999 4	7.909 7
Plane	0.34	81.505 2	7.999 5	7.903 6
Lena	0.35	72.228 6	7.999 4	7.902 9
Elaine	0.38	72.103 1	7.999 4	7.902 7
Nike	0.33	127.250 9	7.999 3	7.907 0
Cameraman	0.37	79.485 6	7.999 5	7.904 3

2.3 安全性分析

为了能够抵御各种形式的攻击,一个理想的图像加密算法应该具有很好的鲁棒性. 从密钥空间、直方图、相邻像素的相关性和差分攻击分析、切割攻击和噪声攻击分析等方面对明密文图像进行安全性分析.

(1)密钥空间分析

一个安全的图像加密算法应该有较大的密钥空间用于抵抗穷举攻击,而且加密算法对密钥应具有较高敏感度. 所提算法使用的密钥为 512 位,其密钥空间是 $2^{512}\approx 1.341\times 10^{154}$,如此大的密钥空间足可以有效抵抗穷举攻击.

(2)直方图分析

直方图是图像的重要统计指标,可以较好地表示图像像素值分布情况. 为了抵御统计攻击,密文图像的直方图应该近似于均匀分布. 从图 4 可见,Plane 和 Nike 的密文图像直方图几乎呈均匀分布.

(3)相关性分析

明文图像相邻像素间的相关性较高,只有消除密文图像中的高相关性才能有效抵抗统计攻击. Lena 图像在水平、垂直、对角线 3 个方向的明密文图像相关性分析如图 5 所示. 从图可见,密文图像中相邻像素之间的强相关性大大降低.

(4)差分攻击分析

为了有效抵抗差分攻击,一个安全的加密系统对明文图像应该是非常敏感的. 也就是说,明文图像一个像素的细微变化都会使密文图像产生很大的变化. 实验中随机改变明文图像的一个像素点,再对原始图像和改变后的图像用同一密钥进行加密,计算两个密文图像的像素变化率和归一化平均变化强度,其定义参考文献[9]. 对每个样本的像素变化率和归一化平均变化强度的最大值、最小值和平均值测试 1 000 次,结果如表 2 所示. 结果表明采用相同密钥加密两幅仅一个比特位差异的明文图像,得到密文图像的像素变化率和归一化平均变化强度值非常接近理想值. 因此,

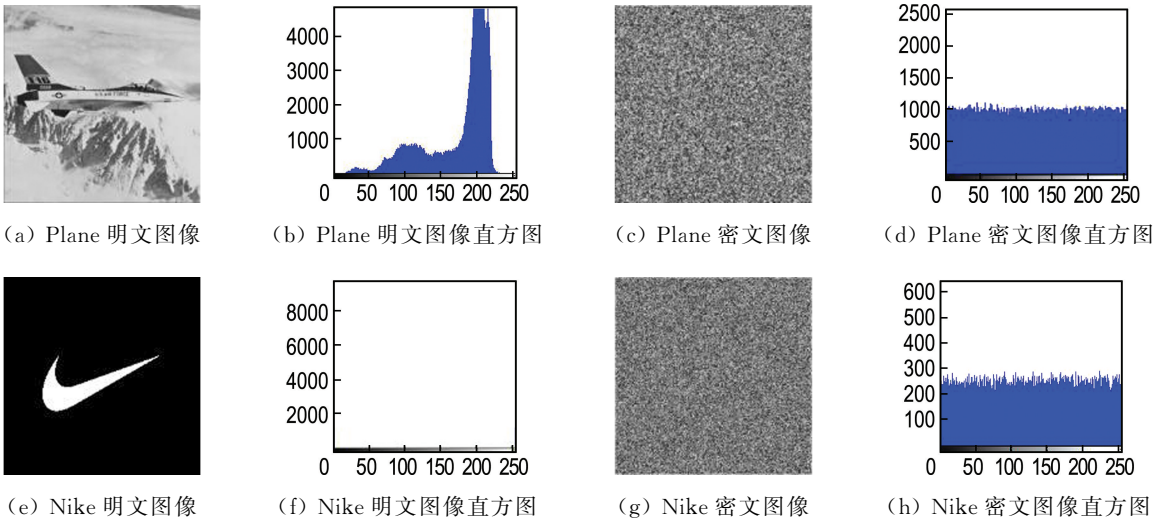


图 4　明密文直方图分析

Fig. 4　Histogram analysis of plaintext and ciphertext

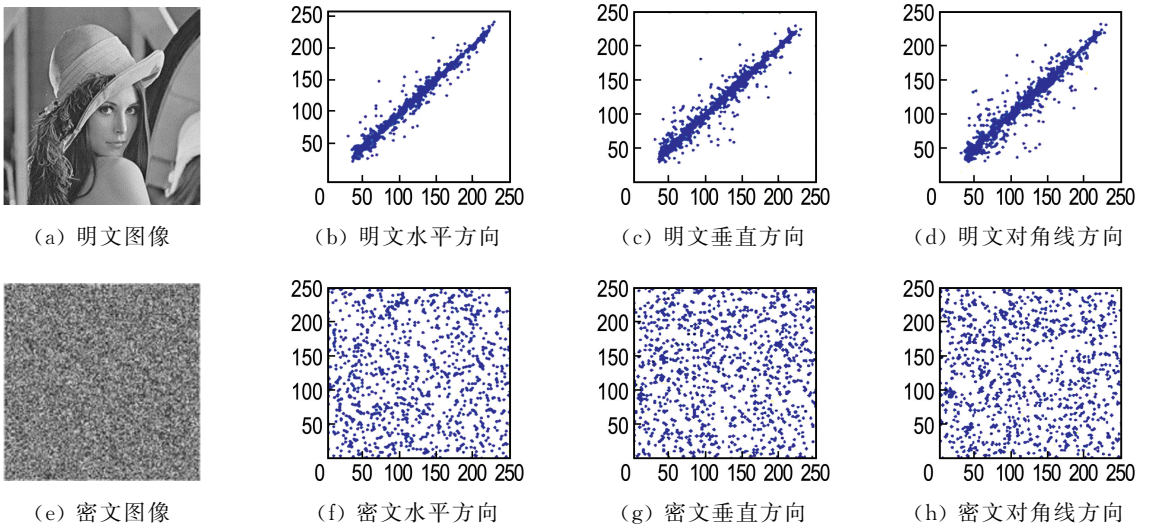


图 5　明密文图像相关性分析

Fig. 5　Image correlation analysis of plaintext and ciphertext

表 2　算法明文敏感性分析表

Tab. 2　Algorithmic plaintext sensitivity analysis table

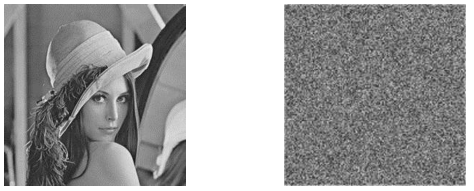
图像	平均值		最大值		最小值	
	像素变化率/%	归一化平均变化强度/%	像素变化率/%	归一化平均变化强度/%	像素变化率/%	归一化平均变化强度/%
Boat	99.605 1	33.492 7	99.783 4	33.893 3	99.543 4	33.378 0
Plane	99.628 9	33.462 3	99.821 9	33.710 6	99.535 3	33.358 2
Lena	99.634 7	33.455 9	99.693 0	33.752 1	99.492 9	33.376 3
Elaine	99.633 5	33.469 0	99.827 1	33.825 7	99.510 4	33.366 8
Nike	99.607 3	33.412 5	99.783 9	33.734 9	99.521 5	33.315 6
Cameramen	99.623 1	33.443 3	99.734 4	33.741 7	99.481 2	33.354 5

算法能有效抵抗差分攻击. 差分攻击仿真实验如图 6 所示.

(5)切割攻击与噪声攻击分析

在图像传输过程中,由于信道的复杂性,可能

会出现各种干扰攻击，常见的有切割攻击和噪声攻击. 为了测试此方法对于复杂干扰的抵抗性，对密文图像进行切割或加入椒盐噪声，如图 7 所示.



(a) 明文图像 (b) 密文图像

(c) 差分图像 (d) 差分密文图像

图 6 差分攻击仿真实验

Fig. 6 Differential attack simulation experiment

(a) 切割图像 (b) 切割后恢复图像

(c) 噪声图像 (d) 加噪声后恢复图像

图 7 切割攻击与噪声攻击仿真实验

Fig. 7 Cutting attack and noise attack simulation experiment

实验结果显示恢复出的明文图像仍可以显示出图像内容，因此本文的加密算法对于干扰具有很好的鲁棒性.

2.4 对比实验

为了对比改进算法的加密效果，挑选了文献[10-12]中 3 种比较有代表性的图像加密算法进行分析比较，主要侧重于统计分析、明文敏感性和加密速度的性能分析. 以尺寸为 512×512 的 Lena灰度图像作为测试图像.

(1)卡方值

卡方值可较好地分析灰度值分布情况，从表 3 结果可见，明文图像与密文图像的卡方值具有显著差异性. 通常当 $\chi^2(0.05,255)<293.5$ 时，认为直方图比较理想. 文献[12]和本文算法的密文卡方值比较理想，表示密文图像的直方图没有明显波峰，像素灰度值分布比较均衡.

表 3 卡方值分析比较实验

Tab. 3 Chi-square value analysis comparison experiment

加密算法	卡方值	
	明文图像	密文图像
文献[10]	160 835.04	413.48
文献[11]	160 835.04	734.14
文献[12]	160 835.04	255.26
本文	160 835.04	250.10

(2)相邻像素相关性分析

在明、密文图像的水平、垂直及对角线 3 个方向上各随机选择 1 000 对像素点，然后计算明、密文图像的相关系数，结果如表 4 所示. 从中可见，明文图像相邻像素之间的相关系数都比较大，经过加密以后相邻像素之间的相关性都接近于 0.

表 4 明文图像与密文图像相关性分析比较

Tab. 4 Comparison and analysis of correlation between plaintext and ciphertext image

算法	明文图像相关系数			密文图像相关系数		
	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
文献[10]	0.973 9	0.986 9	0.961 6	−0.002 8	−0.017 4	−0.003 2
文献[11]	0.973 9	0.986 9	0.961 6	0.003 7	−0.003 8	0.005 6
文献[12]	0.973 9	0.986 9	0.961 6	0.007 2	−0.004 4	−0.003 9
本文	0.973 9	0.986 9	0.961 6	0.003 6	0.000 3	0.004 4

(3)明文敏感性分析

为了比较算法的明文敏感性，随机改变一位 Lena 图像的像素值，然后用不同的加密算法加密明文图像和改变后的图像，计算像素变化率和归一化平均变化强度值. 进行 100 次测试，取平均值作为对比数据，具体实验结果见表 5. 从表可以看出，文献[10]和[11]的像素变化率和归一化平均变化强度值都是 0，说明不能抵御差分攻击. 文献[12]和本文算法的像素变化率和归一化平均变化强度比较大，表现出较强的抵御差分攻击能力. 本文算法的像素变化率和归一化平均变化强度更接近理论值，鲁棒性更好.

表 5　明文敏感性分析比较实验

Tab. 5　Comparison experiment of plaintext sensitivity analysis

图像	文献[10]算法		文献[11]算法		文献[12]算法		本文算法	
	像素变化率	归一化平均变化强度	像素变化率	归一化平均变化强度	像素变化率	归一化平均变化强度	像素变化率	归一化平均变化强度
Plane	0	0	0	0	0.799 4	0.206 7	0.996 3	0.334 6
Lena	0	0	0	0	0.874 2	0.266 4	0.996 3	0.334 6
Elaine	0	0	0	0	0.852 1	0.217 3	0.996 3	0.334 7
Cameraman	0	0	0	0	0.864 0	0.243 5	0.996 2	0.334 4

(4)加密速度分析

安全性与实时性是衡量加密算法好坏的两个重要指标. 仿真实验中，运行环境为 MATLAB 2013，硬件为主频 3.10 GHz，内存 8 GB 计算机. 对不同尺寸的灰度图像进行加密速度测试，每组测试 100 次，结果取加密时间的平均值. 从表 6 可见，本文算法的加密时间较少，说明其具有较好的加密实时性.

表 6　不同加密算法的加密速度分析

Tab. 6　Analysis of encryption speed of different encryption algorithms

加密算法	t/s					
	64 KB	256 KB	1 MB	4 MB	9 MB	54 MB
文献[10]	31.122 5	126.462 0	494.355 0	1 939.780 0	4 685.100 0	28 193.640 0
文献[11]	0.740 3	3.041 3	12.960 8	48.326 7	114.314 0	687.128 0
文献[12]	0.443 2	1.753 1	7.292 7	29.653 8	61.822 7	251.487 3
本文	0.460 5	1.791 1	7.321 8	30.907 3	61.843 4	252.162 4

3　结　语

针对现有基于 DNA 序列的图像加密算法对密钥的选择与明文无关，导致加密算法明文敏感性不足的问题，本文提出了一种基于密钥流缓冲区和 DNA 密码思想的图像加密算法. 为了增加密文图像安全性，算法将 DNA 加密思想与密钥流缓冲区相结合；为了有效抵抗差分攻击和统计攻击，对编码规则进行了改进，算法在编码过程中将静态变换为动态 DNA 编码方式，并结合明文图像信息和密钥流缓冲区来选择编码规则，同时，对编码后的密文序列再进行一轮扩散操作，大大地提高了密文图像安全性. 实验结果表明，所提算法不仅密钥空间大，而且安全性较高，适用于军事、医疗、司法等涉及机密图像的保密存储和网络传输.

参考文献：

[1] ZHOU Shihua, ZHANG Qiang, WEI Xiaopeng, *et al*. A summarization on image encryption [J]. **IETE Technical Review**, 2010, **27**(6): 503-510.

[2] WONG K W, KWOK B S H, YUEN C H, *et al*. An efficient diffusion approach chaos-based image encryption [J]. **Chaos, Solitons and Fractals**, 2009, **41**(5): 2652-2663.

[3] 林　青，王延江，王　珺. 基于超混沌系统的图像加密算法 [J]. 中国科学：技术科学，2016，**46**(9)：910-918.

LIN Qing, WANG Yanjiang, WANG Jun. The image encryption scheme with optional dynamic state variables based on hyperchaotic system [J]. **Scientia Sinica: Technologica**, 2016, **46**(9): 910-918. (in Chinese)

[4] 陈智华. 基于DNA计算自组装模型的若干密码问题研究 [D]. 武汉: 华中科技大学, 2009.
CHEN Zhihua. Researches on several cryptological problems based on DNA computing by self-assembly [D]. Wuhan: Huazhong University of Science & Technology, 2009. (in Chinese)

[5] 饶妮妮. 一种基于重组DNA技术的密码方案 [J]. 电子学报, 2004, **32**(7): 1216-1218.
RAO Nini. A cryptosystem based on recombinant DNA technique [J]. **Acta Electronica Sinica**, 2004, **32**(7): 1216-1218. (in Chinese)

[6] VERMA A K, DAVE M, JOSHI R C. DNA cryptography: a novel paradigm for secure routing in Mobile Ad hoc Networks [J]. **Journal of Discrete Mathematical Sciences and Cryptography**, 2008, **11**(4): 393-404.

[7] CHENG H. Partial encryption of compressed images and videos [J]. **IEEE Transactions on Signal Processing**, 2000, **48**(8): 2439-2451.

[8] 谭 琳. 基于DNA序列和混沌的图像加密算法 [J]. 信息系统工程, 2014(11): 90-92.
TAN Lin. Image encryption algorithm based on DNA sequence and chaos [J]. **CC News**, 2014(11): 90-92. (in Chinese)

[9] WU Yue, NOONAN J P, AGAIAN S. NPCR and UACI randomness tests for image encryption [J]. **Journal of Selected Areas in Telecommunications (JSAT)**, 2011, **1**(2): 31-38.

[10] KING O D, GABORIT P. Binary templates for comma-free DNA codes [J]. **Discrete Applied Mathematics**, 2007, **155**(6/7): 831-839.

[11] ZHANG Qiang, GUO Liang, WEI Xiaopeng. A novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system [J]. **Optik**, 2013, **124**(18): 3596-3600.

[12] ENAYATIFAR R, ABDULLAH A H, ISNIN I F. Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence [J]. **Optics and Lasers in Engineering**, 2014, **56**(5): 83-93.

Image encryption algorithm based on key-stream buffer and DNA dynamic encoding

ZHANG Lijun[1], XU Xirong[*2], GENG Yu[1], NIE Weiguo[3], ZHANG Xuanping[3]

(1. College of Public Basic Sciences, Jinzhou Medical University, Jinzhou 121001, China;
2. School of Computer Science and Technology, Dalian University of Technology, Dalian 116024, China;
3. School of Computer Science and Technology, Xi′an Jiaotong University, Xi′an 710049, China)

Abstract: The security of digital image information transfer is a research hotspot. To solve the problem that the key in the existing image encryption algorithm based on DNA sequence has nothing to do with plaintext, an image encryption algorithm based on key-stream buffer and DNA dynamic encoding is proposed. First, the plaintext is globally scrambled by pseudo random sequence generated by chaotic system. Then, key-stream buffers are initialized by PWLCM chaotic system, and the key is selected based on the pixel value of plaintext and DNA dynamic encoding is performed on scrambled images. Finally, a round of diffusion operation is executed on encoded ciphertext sequence. The simulation results show that the proposed algorithm has good performance in scrambling degree, key space, resisting differential attack and statistics attack.

Key words: image encryption; chaos system; key-stream buffer; DNA dynamic encoding