基于混沌加密和 DNA 编码的“一图一密”图像加密算法*

方洁[1)2)] 姜明浩[1)] 安小宇[1)] 孙军伟[1)2)†]

1) (郑州轻工业大学电气信息工程学院, 郑州 450002)

2) (河南省信息化电器重点实验室, 郑州 450002)

(2020 年 10 月 6 日收到; 2020 年 11 月 30 日收到修改稿)

提出了一种基于混沌加密和 DNA 编码的“一图一密”图像加密算法. 首先将明文图像按 R, G, B 通道分为 3 个二维矩阵, 并和 Logistic 序列生成的矩阵分块进行 DNA 编码, 然后将 3 个二维矩阵分别和 Logistic 矩阵对应位置的子块进行 DNA 运算和解码, 最后对 DNA 解码后的图像进行置乱, 得到密文图像. 其中, 每一子块的 DNA 编解码方式以及子块与子块之间的 DNA 运算规则的选取均由超混沌系统生成的混沌序列决定, 解决了 DNA 编解码和运算规则单一的问题. 由于算法的密钥与原始图像相关联, 不同的图像对应着不同的密钥, 因此保证了“一图一密”的效果. 仿真结果和安全性能分析表明, 该算法密钥容量大、对密钥的敏感性极高, 具有较高的复杂度和安全性, 对提高保密通信的安全性具有重要意义.

关键词: 图像加密, 混沌系统, DNA 编码, 一图一密

PACS: 05.45.Gg, 05.45.Jn **DOI:** 10.7498/aps.70.20201642

1 引 言

随着互联网技术的飞速发展, 信息传输和储存的安全性越来越重要, 图像作为一类重要的信息载体, 广泛应用于军事、商业、医疗等行业. 图像信息安全往往与个人隐私、商业机密、军事情报甚至与国家安全密切相关, 但是大量图片在网络传输过程中的安全性并不能得到保证, 因此如何对图像内容有效加密越来越受到人们的重视. 图像加密技术通常是将原始图像转化为类噪声图像进行传输, 与文本内容不同的是, 图片信息具有数据量大、相邻像素相关性强及冗余度高等特点, 传统的数据加密方式并不适合图像加密[1–3]. 随着人们对图像安全性需求的日益提高, 寻找高效安全的图像加密方法已成为热门研究课题.

由于混沌系统具有伪随机性、遍历性、对初值极度敏感等特点, 非常适用于图像加密, 基于混沌系统的图像加密技术受到越来越多人的关注. 已有的混沌图像加密大多是基于低维混沌系统, 如 Logistic 映射[4–6]、Kent 映射[7]、Henon 映射[8]、Lorenz 系统[9] 等. 然而低维混沌系统产生的混沌序列往往随机性差、密钥空间小、安全性低、易于破解. 相比于低维混沌系统, 超混沌系统具有更复杂的动力学行为, 基于超混沌系统的图像加密算法密钥容量大、混沌序列随机性高, 在图像加密方面具有先天的优势[10,11]. Yang 等[12] 将 Liu 混沌系统和 SHA-算法相结合, 构造了一个新的四维超混沌系统, 提出了一种新的图像加密算法. Gong 等[13] 基于超混沌系统、离散余弦变换和离散分数随机变

* 国家自然科学基金 (批准号: 61775198)、河南省重点研发与推广专项 (批准号: 202102210317, 192102210083) 和河南省高等学校重点科研项目 (批准号: 20A413012) 资助的课题.

† 通信作者. E-mail: junweisun@yeah.net

换, 设计了一种能够同时压缩和加密多幅图像的加密方案. Zhou 和 Wang[14] 构造了一个五维的超混沌系统, 用两个不同的初值得到两个不同的混沌序列, 分别用于图像加密的置乱和扩散阶段. 彭再平等 [15] 提出了一种新型的四维多翼超混沌系统, 并将其应用于物理混沌加密和高级加密标准加密的混合图像加密算法. 尽管基于混沌系统的图像加密研究已经取得了一定成果, 但已有的加密算法大都是基于单一的混沌系统, 能否在图像加密算法中引入多个混沌系统, 并将混沌理论与其他理论相结合来提高算法安全性是一个值得思考的问题.

随着基因工程的发展, 研究人员发现含有大量生物遗传信息的 DNA 链与图像加密系统的密码序列具有相似性, 为图像加密提供了新的思路. 由于 DNA 计算拥有巨大的并行处理能力、很高的能量效率和存贮容量, 基于 DNA 计算的加密算法具有传统加密算法所没有的独特优势 [16–20]. 随着计算机数据处理能力的不断提高, 对保密通信系统安全性的要求也越来越高, 近年来一些学者将 DNA 编码技术与混沌系统相结合, 设计出更高效、安全的加密算法. Wu 等 [21] 提出一种基于 DNA 编码和二维混沌映射的图像加密算法, 通过实验仿真验证了方案的安全性. Som 等 [22] 利用广义 Arnold cat 映射对图像像素位置进行置乱, 提出了一种基于 DNA 编码和混沌系统的彩色图像加密算法. Chai 等 [23] 设计了一种基于四维超混沌系统和 DNA 编码的新型彩色图像加密算法. Wu 等 [24] 提出了一种基于 DNA 编码和两个改进的混沌系统的图像加密算法, 利用密钥对密文图像进行交叉扩散, 提高了算法的安全性和加密速度.

本文在上述研究基础上提出了一种新的将超混沌系统、Logistic 映射和 DNA 编码三者相结合的彩色图像加密算法, 通过对直方图分布、相邻像素相关性、信息熵、密钥敏感性、密钥空间、抗噪声、抗剪切等性能的分析, 表明该加密系统具有密钥容量大、抗噪声能力强、抗攻击能力强等特点. 本文的主要贡献有: 第一, 基于单一混沌系统安全性较差的问题, 将两个混沌系统同时引入图像加密算法, 产生多个不同的混沌序列对明文图像进行交替加密, 在一定程度上提高了加密算法的复杂度和安全性; 第二, 采用了明文关联的图像密码系统, 使得加密明文图像的密钥的生成与明文图像有关, 保证了“一图一密”的效果, 即不同的明文图像对应着不同的密钥, 从而可以有效抵抗选择明文攻击或已知明文攻击; 第三, 对图像进行分块处理, 每个子块的编码解码方式和子块与子块间的 DNA 运算规则均由混沌序列决定, 提高了算法的复杂度和安全性.

2 混沌系统与 DNA 编码

2.1 Logistic 映射

密码体系中最常用的一个混沌系统是 Logistic 映射, 它是一种典型的一维混沌映射, 其定义式为

$$x_{n+1} = f(x_n, \mu) = \mu x_n(1 - x_n), \tag{1}$$

其中, 状态变量 $x_n \in (0,1)$, Logistic 参数 $\mu \in (0,4)$, 当 $\mu < 3$ 时, 迭代的结果趋于定值, 当 $3.569 \leqslant \mu \leqslant 4$ 时, Logistic 映射处于混沌状态, 给定初始值 x_0, 生成的序列是非周期性的、非收敛的、以及对初值敏感的. 本文中 Logistic 映射有 3 个不同的初值, 生成 3 个不同的序列, 第一个序列转化为与原始图像相同大小的矩阵, 并与原始图像做 DNA 运算, 第二和第三个序列分别用于对 DNA 解码后的矩阵做行置换和列置换.

2.2 超混沌系统

本加密算法所采用的超混沌系统模型如下:

$$\begin{aligned} \dot{x} &= a(y - x) + yz, \\ \dot{y} &= dx - cy - xz + ew, \\ \dot{z} &= -bz + xy, \\ \dot{w} &= rw - yz, \end{aligned} \tag{2}$$

式中, a, b, c, d, e 为超混沌系统的参数, x, y, z, w 为状态变量, 当参数 $a = 27$, $b = 1.5$, $c = 5$, $d = 43$, $r = 0.5$, $e = 3.5$ 时, 上述系统处于超混沌状态. 设定好 4 个初值后, 利用 Runge-Kutta 法对方程组求解, 可以得到 4 个混沌序列 $\{X_i\}$, $\{Y_i\}$, $\{Z_i\}$, $\{W_i\}$, 其中序列 $\{X_i\}$ 决定原始图像矩阵 $\boldsymbol{I}_1$, $\boldsymbol{I}_2$ 和 $\boldsymbol{I}_3$ 相同子块的编码方式, 序列 $\{Y_i\}$ 决定 Logistic 生成的矩阵 $\boldsymbol{H}$ 的编码方式, 序列 $\{Z_i\}$ 决定矩阵 $\boldsymbol{I}_1$, $\boldsymbol{I}_2$, $\boldsymbol{I}_3$ 和矩阵 $\boldsymbol{H}$ 对应子块间的 DNA 运算法则, 序列 $\{W_i\}$ 决定经过 DNA 运算后的子块的解码方式.

2.3 DNA 编码与运算

DNA 序列由 4 种脱氧核苷酸组成, 分别为腺嘌呤 (A)、胸腺嘧啶 (T)、胞嘧啶 (C)、鸟嘌呤 (G),

其中 A 与 T 配对, C 与 G 配对. 同样, 在二进制中 0 和 1 互补, 因此对于两位二进制数来说, 00 和 11, 01 和 10 也为互补关系. 如果用 A, T, C, G 分别表示二进制数 00, 11, 01, 10, 灰度图像中每一个像素值可以用 8 位二进制数表示, 因此每一个像素值就可以用长度为 4 的 DNA 序列表示. 例如图像的像素值为 189, 用二进制数表示为 10111101, 用 DNA 序列表示为 GTTC.

3 加密算法

3.1 加密算法思想

该加密算法将彩色图像根据 R, G, B 通道分为 3 个二维矩阵, 将每一个二维矩阵按规定分块, 每个分块的 DNA 编码方式和运算规则都是伪随机的, 由超混沌系统产生的混沌序列决定, 而混沌序列的初值又由原始图像的灰度值决定, 因此, 待加密图像就有多种 DNA 编码方式和运算操作, 大大增加了加密系统的复杂度, 提高了安全性. Logistic 映射产生的 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. 加密算法流程图如图 1 所示.

DNA 计算是指 DNA 编码间的“加”、“减”、“异或”、“同或”运算. 一般地, 有如表 1 所列的 8 种 DNA 编码方式, 因此, 这里的 DNA 计算本质上仍然是二进制数的算术运算.

当采用规则 1 进行编码时, 运算规则如表 2—表 5 所列.

3.2 加密算法具体步骤

1) 读入样本图像 $\boldsymbol{I}(M, N, 3)$, M 和 N 分别为像素矩阵的行数和列数, 将 $\boldsymbol{I}$ 根据 R, G, B 通道分为 3 个二维灰度矩阵, 记为 $\boldsymbol{I}_1$, $\boldsymbol{I}_2$, $\boldsymbol{I}_3$.

$$\begin{aligned}\boldsymbol{I}_1 &= \boldsymbol{I}(:,:,1),\\ \boldsymbol{I}_2 &= \boldsymbol{I}(:,:,2),\\ \boldsymbol{I}_3 &= \boldsymbol{I}(:,:,3).\end{aligned} \tag{3}$$

2) 填充 3 个矩阵使其满足 (4) 式, 填充的数据值取为 0

$$\begin{aligned}&\mathrm{mod}\,(M,t)=0,\\ &\mathrm{mod}\,(N,t)=0,\end{aligned} \tag{4}$$

其中 t 为分块大小, 将填充后的新图像尺寸重新赋予 M 和 N 值. mod 为求余运算, 表示两个数值做除法运算后的余数. 由 (4) 式可知, 矩阵 $\boldsymbol{I}_1$, $\boldsymbol{I}_2$, $\boldsymbol{I}_3$ 都能分为 $(M\times N)/t^2$ 个图像块.

3)Logistic 映射产生混沌序列 $\{\boldsymbol{k}_i\}$. 设定参数 μ 为 3.9999, 迭代序列长度为 $M\times N$, 初值 x_0 由 (5) 式产生

$$x_0=\frac{\mathrm{sum}(\boldsymbol{I}_1(:))+\mathrm{sum}(\boldsymbol{I}_2(:))}{255\times M\times N\times 2}, \tag{5}$$

其中 $\mathrm{sum}(\boldsymbol{I}_1(:))$ 和 $\mathrm{sum}(\boldsymbol{I}_2(:))$ 分别为矩阵 $\boldsymbol{I}_1$ 和 $\boldsymbol{I}_2$ 的数据总和, x_0 即为 $\boldsymbol{I}_1$ 和 $\boldsymbol{I}_2$ 的灰度平均值, 其为密钥之一. 将序列 $\{\boldsymbol{k}_i\}$ 按照 (6) 式转化为大小为 $M\times N$ 的矩阵 $\boldsymbol{H}$, 并将矩阵中的每个元素变换为 0—255 之间, 用于与 $\boldsymbol{I}_1$, $\boldsymbol{I}_2$, $\boldsymbol{I}_3$ 进行 DNA 运算.

$$\begin{aligned}\boldsymbol{k} &= \mathrm{mod}(\mathrm{round}(k\times 10^4),256),\\ \boldsymbol{H} &= \mathrm{reshape}(\boldsymbol{k},M,N),\end{aligned} \tag{6}$$

round 函数表示四舍五入到最接近的整数, reshape $(\boldsymbol{k},M,N)$ 表示将序列 $\{\boldsymbol{k}_i\}$ 转化为 M 行 N 列的矩阵.

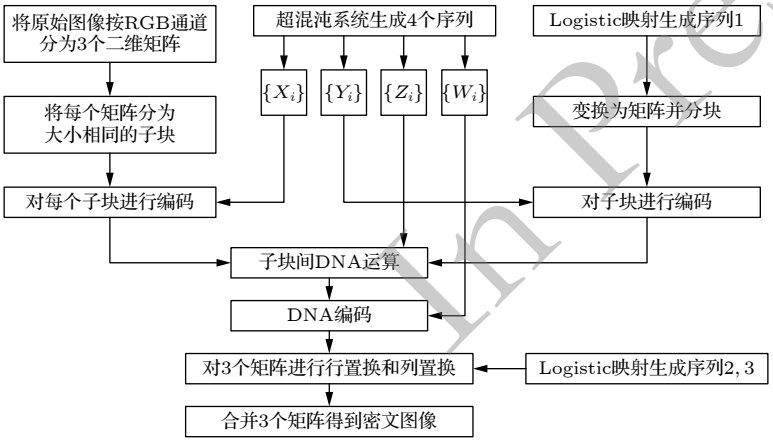


图 1 加密算法流程图

Fig. 1. Flow chart of encryption algorithm.

表 1 DNA 编码规则
Table 1. DNA encoding rules.

	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
C	01	10	00	11	00	11	01	10
G	10	01	11	00	11	00	10	01

表 2 加法运算法则
Table 2. Add operation.

+	A	T	C	G
A	A	T	C	G
T	T	G	A	C
C	C	A	G	T
G	G	C	T	A

表 3 减法运算法则
Table 3. Subtraction operation.

–	A	T	C	G
A	A	C	T	G
T	T	A	G	C
C	C	G	A	T
G	G	T	C	A

表 4 异或运算法则
Table 4. XOR operation.

$\oplus$	A	T	C	G
A	A	T	C	G
T	T	A	G	C
C	C	G	A	T
G	G	C	T	A

表 5 同或运算法则
Table 5. XNOR operation.

$\odot$	A	T	C	G
A	T	A	G	C
T	A	T	C	G
C	G	C	T	A
G	C	G	A	T

4) 对超混沌系统用 4 阶 Runge-Kutta 法进行求解, 产生 4 个随机序列, 分别为$\{\boldsymbol{X_i}\}$, $\{\boldsymbol{Y_i}\}$, $\{\boldsymbol{Z_i}\}$, $\{\boldsymbol{W_i}\}$, 长度均为$(M\times N)/t^2$. 由于 $\boldsymbol{I_1}$ 中的每个像素值都在 0—255 之间, 因此每个像素值都可以用一个 8 位二进制数来表示, $\boldsymbol{I_1}$ 可以看作是由 8 个比特面组成. 将 $\boldsymbol{I_1}$ 的值和 00010001 做“与”运算, 即与 17 做“与”运算, 就可以得到 $\boldsymbol{I_1}$ 的第一个和第五个比特面的值. 同理, 将 $\boldsymbol{I_2}$ 的值和 00100010 做“与”运算, 即与 34 做“与”运算, 就可以得到 $\boldsymbol{I_2}$ 的第二个和第六个比特面的值. 超混沌系统的 4 个初值$X(0)$, $Y(0)$, $Z(0)$, $W(0)$由 (7) 式给出:

$$\begin{aligned} X(0) &= \text{sum}(\text{sum}(\text{bitand}(\boldsymbol{I}_1,17)))/(M\times N),\\ Y(0) &= \text{sum}(\text{sum}(\text{bitand}(\boldsymbol{I}_2,34)))/(M\times N),\\ Z(0) &= \text{sum}(\text{sum}(\text{bitand}(\boldsymbol{I}_3,68)))/(M\times N),\\ W(0) &= \text{sum}(\text{sum}(\text{bitand}(\boldsymbol{I}_1,136)))/(M\times N). \end{aligned} \tag{7}$$

即四个初值分别由 $\boldsymbol{I_1}$ 的第一和第五比特面, $\boldsymbol{I_2}$ 的第二和第六比特面, $\boldsymbol{I_3}$ 的第三和第七比特面, $\boldsymbol{I_1}$ 的第四和第八比特面的像素平均值决定, 对于不同的待加密图像, 就会有不同的初值, 这 4 个初值作为密钥使用.

5) 将 $\boldsymbol{I_1}$, $\boldsymbol{I_2}$, $\boldsymbol{I_3}$ 相同位置的分块使用同一种编码方式, 编码方式由序列$\{\boldsymbol{X_i}\}$决定, 矩阵 $\boldsymbol{H}$ 各个子块之间的编码方式由序列$\{\boldsymbol{Y_i}\}$决定, 因为 DNA 编码一共有 8 种编码方式, 因此将序列$\{\boldsymbol{X_i}\}$和$\{\boldsymbol{Y_i}\}$的值转化为 1—8 之间的整数, 将序列$\{\boldsymbol{X_i}\}$和$\{\boldsymbol{Y_i}\}$按 (8) 式进行转化:

$$\begin{aligned} X &= \text{mod}(\text{round}(X\times 10^4),8)+1,\\ Y &= \text{mod}(\text{round}(Y\times 10^4),8)+1. \end{aligned} \tag{8}$$

此时, 序列$\{\boldsymbol{X_i}\}$和$\{\boldsymbol{Y_i}\}$的值为 1—8 之间的随机整数, $\boldsymbol{I_1}$, $\boldsymbol{I_2}$, $\boldsymbol{I_3}$ 矩阵中第 i 个分块的编码方式为 X_i, 混沌矩阵 $\boldsymbol{H}$ 第 i 个分块的编码方式为Y_i.

6) 将 $\boldsymbol{I_1}$, $\boldsymbol{I_2}$, $\boldsymbol{I_3}$ 和混沌矩阵 $\boldsymbol{H}$ 对应分块之间采用同一种运算方法, 由超混沌系统产生的混沌序列$\{\boldsymbol{Z_i}\}$决定. 由于 DNA 编码有 4 种运算方法, 因此将序列$\{\boldsymbol{Z_i}\}$中的值转化为 1—4 之间的整数, 将序列$\{\boldsymbol{Z_i}\}$按 (9) 式进行转化:

$$Z = \text{mod}(\text{round}(Z\times 10^4),4)+1. \tag{9}$$

规定: 若 $Z_i=1$, 采用加法运算; 若 $Z_i=2$, 采用减法运算; 若 $Z_i=3$, 采用异或运算; 若 $Z_i=4$, 采用同或运算. 为获得更好的扩散效果, 除第一分块外, 将当前分块的加密结果与上一个分块再进行一次 DNA 运算, 运算规则仍然由序列$\{\boldsymbol{Z_i}\}$决定.

7) 对经过 DNA 运算的分块进行 DNA 解码, 解码规则由混沌序列$\{\boldsymbol{W}_i\}$决定, DNA 解码是编码的逆过程, 即把 A, T, C, G 输出为对应的数值.

8)Logistic 映射产生混沌序列$\{\boldsymbol{k_x}\}$和$\{\boldsymbol{k_y}\}$, 长度分别为 M 和 N, 设定参数μ为 3.9999, 两个初值

x_{01}和x_{02}由 (10) 式产生:

$$x_{01}=\frac{\mathrm{sum}(\boldsymbol{I}_1(:))+\mathrm{sum}(\boldsymbol{I}_3(:))}{255\times M\times N\times 2},$$
$$x_{02}=\frac{\mathrm{sum}(\boldsymbol{I}_2(:))+\mathrm{sum}(\boldsymbol{I}_3(:))}{255\times M\times N\times 2}. \tag{10}$$

x_{01}即为 $\boldsymbol{I}_1$ 和 $\boldsymbol{I}_3$ 的灰度平均值, x_{02}即为 $\boldsymbol{I}_2$ 和 $\boldsymbol{I}_3$ 的灰度平均值, 这两个初值也作为密钥使用, 将序列 $\{\boldsymbol{k}_x\}$和 $\{\boldsymbol{k}_y\}$从大到小排列, 并用索引序列 $\{\boldsymbol{U}_x\}$和 $\{\boldsymbol{U}_y\}$记录排序后对应点在原序列 $\{\boldsymbol{k}_x\}$和 $\{\boldsymbol{k}_y\}$中的位置. 通过 DNA 解码后的三个通道的矩阵, 按照序列 $\{\boldsymbol{U}_x\}$进行行置换, 并按照序列 $\{\boldsymbol{U}_y\}$进行列置换.

9) 将经过行列置换的 3 个二维矩阵合并为一个三维矩阵, 得到密文图像.

解密过程是加密过程的逆操作, 通过密钥可以得到混沌序列以及 DNA 编码和运算方式, 只有使用与加密时完全相同的密钥, 才能由密文图像恢复出原始明文图像.

4 仿真结果与分析

基于 Matlab R2014a 仿真平台对大小为 512 × 512 × 3 的彩色 lena 图像进行模拟测试. 仿真中图像的分块大小取为 4 × 4, Logistic 映射参数 μ取 3.9999, 超混沌系统参数 $a=27$, $b=1.5$, $c=43$, $r=0.5$, $e=3.5$, 密钥由 x_0, x_{01}, x_{02}, $X(0)$, $Y(0)$, $Z(0)$, $W(0)$组成. 图 2(a)—图 2(c) 分别为原始图像、密文图像、解密后的图像, 可看出, 密文图像呈雪花状, 与原始图像无任何关联, 可见该算法成功地将原始图像信息完全掩盖.

4.1 直方图分析

直方图反映了一幅图像中各个灰度值出现的频率与灰度值的关系, 图 3(a)—图 3(f) 分别为图像 R, G, B 三个通道加密前后的直方图. 由仿真结果可以看出, 加密后的图像三个通道的直方图分布均匀, 隐藏了原始图像的统计特性, 攻击者很难从分析密文图像的直方图获取任何有用的信息.

4.2 相邻像素的相关性分析

在一般图像中, 每个像素点跟其相邻像素点之间都会呈现很高的相关性, 密文图像相邻像素间的相关性越低, 加密算法抵抗攻击的能力就越强. 为了测试图像的抗攻击能力, 分别随机选取密文图像水平方向、垂直方向和对角线方向相邻的 5000 对像素点, 计算其相关性, 相关系数计算公式如下:

$$r_{xy}=\frac{\mathrm{cov}(x,y)}{\sqrt{D(x)D(y)}}, \tag{11}$$

其中

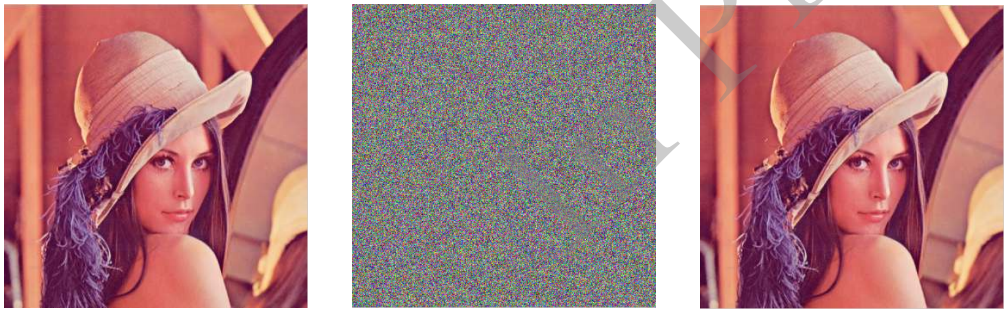
$$\mathrm{cov}(x,y)=\frac{1}{N}\sum_{i=1}^{N}[x_i-E(x)]\,[y_i-E(y)], \tag{12}$$

$$E(x)=\frac{1}{N}\sum_{i=1}^{N}x_i, \tag{13}$$

$$D(x)=\frac{1}{N}\sum_{i=1}^{N}[x_i-E(x)]^2, \tag{14}$$

x, y 为相邻像素的灰度值, r_{xy}为相邻像素的相关系数, 其绝对值越大, 表示相关性越强, N为所取像素点对数 5000, $\mathrm{cov}(x,y)$表示相关函数, $E(x)$表示所取像素平均值, $D(x)$表示方差. 图 5 为原始图像与密文图像 R, G, B 三个通道在水平、垂直、对角线 3 个方向上相邻像素相关性分布.

表 6 为原始图像和密文图像 3 个通道相邻像素的相关性的数据对比, 可以看出原始图像像素间



(a) (b) (c)

图 2 加密效果图 (a) 原始图像; (b) 密文图像; (c) 解密后的图像

Fig. 2. Encryption effect: (a) Original image; (b) encrypted Image; (c) decrypted image.

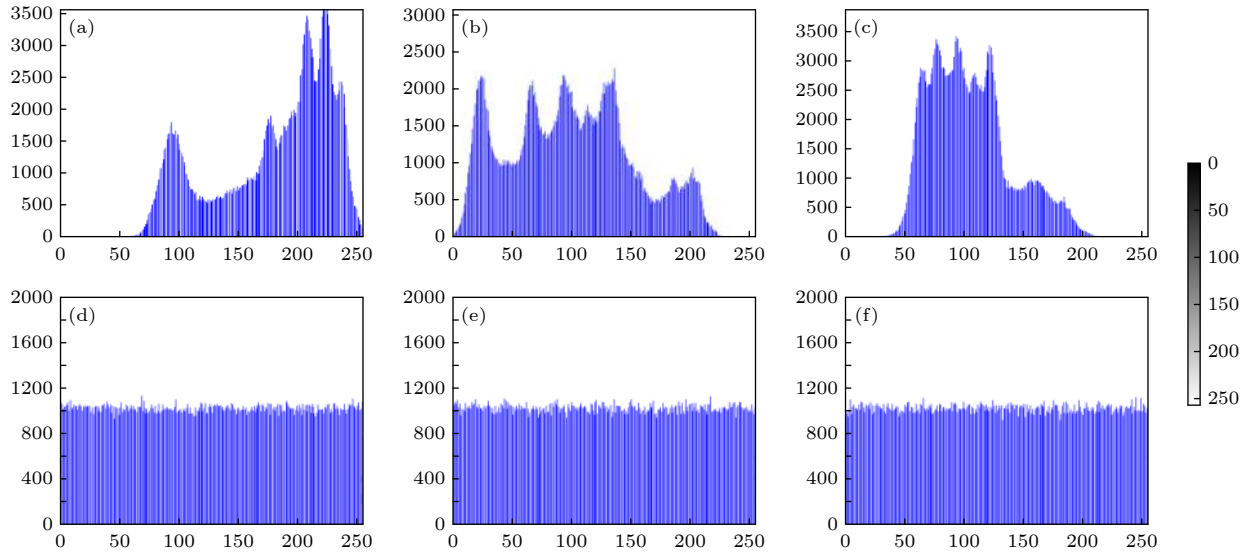


图 3 直方图比较 (a) R 通道加密前直方图; (b) G 通道加密前直方图; (c) B 通道加密前直方图; (d) R 通道加密后直方图; (e) G 通道加密后直方图; (f) B 通道加密后直方图

Fig. 3. Histogram comparison: (a) Histogram of R channel before encryption; (b) histogram of G channel before encryption; (c) histogram of B channel before encryption; (d) histogram of R channel after encryption; (e) histogram of G channel after encryption; (f) histogram of B channel after encryption.

具有更高的相关性, 而密文图像的相关性趋近于 0, 说明密文图像 3 个通道在水平、垂直、对角线 3 个方向上相邻像素的数据值基本无关联性, 说明此算法加密后图像的混乱程度很高.

4.3 信息熵分析

信息熵作为一个系统复杂程度的度量, 可以用来表示图像信息的不确定性, 在图像中, 图像像素的灰度值分布越均匀, 信息熵就越大, 反之就越小. 信息熵的数学定义式如下:

$$H(x) = -\sum_{i=0}^{2^N-1} p(x_i)\log_2 p(x_i), \tag{15}$$

其中, 2^N 表示图像的灰度级, $p(x_i)$表示灰度级 x_i 在这幅图像中出现的概率, $\sum_{i=0}^{2^N-1} p(x_i) = 1$. 对于灰度级为 256 的图像来说, 最大的信息熵为 8. 表 7 为原始图像和密文图像的信息熵数据对比.

由表 7 可以看出, 加密后 R, G, B 三通道的信息熵非常接近最大值 8, 说明该加密算法保密效果好, 能够抵御基于图像信息熵的攻击.

4.4 密钥敏感性分析

密钥的微小变化, 会导致完全不同的解密结果, 密钥敏感性越高, 加密算法的安全性越高, 可以通过在解密时稍微改变一个密钥的值来测试算法对密钥的敏感程度. 密钥之一的 Logistic 初值 x_0 加密时的取值为 0.5475, 在解密时对其做出微小改变取为 0.5475000000000001, 即 $\Delta x_0 = 10^{-16}$. 初值 $X(0)$加密时的取值为 0.4953, 解密时变为 0.4953000000000001, 即 $\Delta X(0) = 10^{-16}$, 图 5 为两种不同情况的错误解密图像. 由以上两例可以看出, 密钥的改变仅仅是 10^{-16}, 解密图像却完全不同, 说明此算法的密钥敏感性较强.

4.5 密钥空间分析

该算法的密钥一共有 8 个, 分别为 Logistic 系统的参数 μ 和 3 个不同初值 x_0, x_{01}, x_{02}, 超混沌系统的 4 个初值 $X(0)$, $Y(0)$, $Z(0)$, $W(0)$, 8 个密钥的敏感度均为 10^{-16}, 则此加密算法的密钥容量为 $10^{16}\times10^{16}\times10^{16}\times10^{16}\times10^{16}\times10^{16}\times10^{16}\times10^{16} = 10^{128} \approx 2^{425}$, 本算法的密钥空间足够大, 可以很好地抵御穷举攻击.

4.6 抗噪声性能分析

图像噪声是指存在于图像数据中的不必要的或多余的干扰信息, 在图像获取和传输过程中, 由于图像传感器材料、工作环境、传输信道等影响, 图像会受到多种噪声的污染. 为测试该算法的抗噪声性能, 对密文图像加入不同强度的椒盐噪声. 图 6 为密文图像分别加入噪声密度为 0.05, 0.1, 0.15,

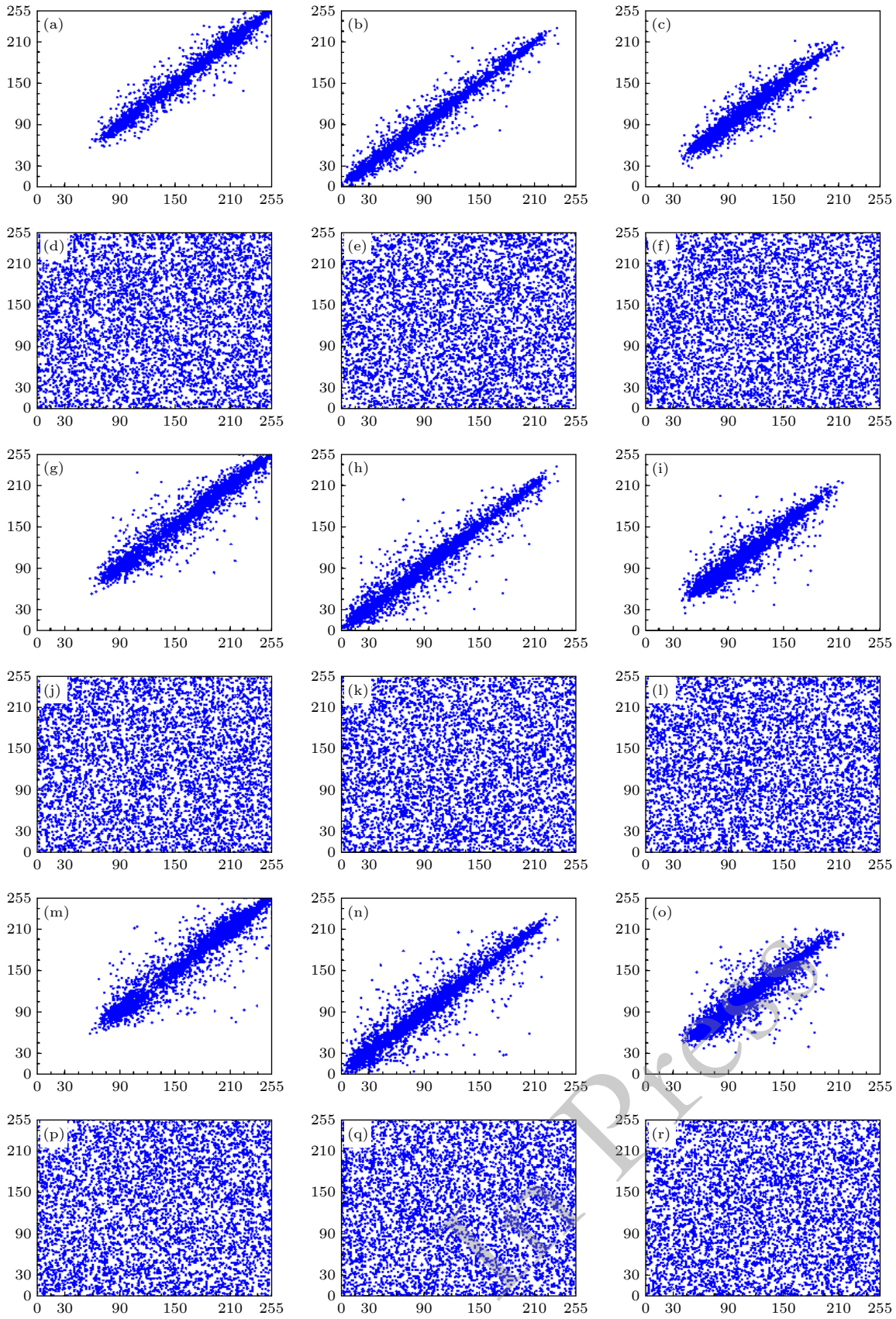
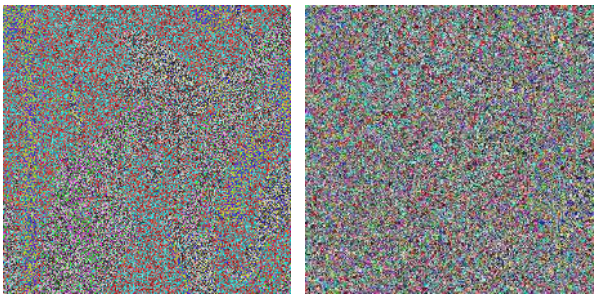


图 4 R, G, B 三通道加密前后水平、垂直、对角线方向上相邻像素相关性分布 (a)—(c) 原始图像 R, G, B 通道水平方向; (d)—(f) 加密图像 R, G, B 通道水平方向; (g)—(i) 原始图像 R, G, B 通道垂直方向; (j)—(l) 加密图像 R, G, B 通道垂直方向; (m)—(o) 原始图像 R, G, B 通道对角线方向; (p)—(r) 加密图像 R, G, B 通道对角线方向

Fig. 4. Correlation distribution of adjacent pixels in horizontal, vertical and diagonal directions before and after encryption of R, G, B channels: (a)–(c) Horizontal direction of R, G, B channels of original image; (d)–(f) horizontal direction of R, G, B channels of encrypted image; (g)–(i) vertical direction of R, G, B channels of original image; (j)–(l) vertical direction of R, G, B channels of encrypted image; (m)–(o) diagonal direction of R, G, B channels of original image; (p)–(r) diagonal direction of R, G, B channels of encrypted image.



(a) (b)

图 5 错误解密图像 (a) $\Delta x_0 = 10^{-16}$时的解密图像; (b) $\Delta X(0) = 10^{-16}$时的解密图像

Fig. 5. Incorrect decrypted image: (a) Decrypted image when $\Delta x_0 = 10^{-16}$; (b) decrypted image when $\Delta X(0) = 10^{-16}$.

表 6 原始图像与密文图像相邻像素相关系数

Table 6. Correlation coefficient of adjacent pixels of original image and encrypted image.

	水平		垂直		对角线	
	原始图像	密文图像	原始图像	密文图像	原始图像	密文图像
R	0.9772	–0.0174	0.9877	0.0012	0.9641	0.0123
G	0.9773	–0.0004	0.9883	0.0054	0.9643	–0.0079
B	0.9556	–0.0174	0.9743	–0.0025	0.9320	0.0029

表 7 原始图像与密文图像信息熵对比

Table 7. Information entropy of original image and encrypted image.

	R	G	B
原始图片	7.2682	7.5901	6.9951
密文图片	7.9994	7.9992	7.9992

0.2 的椒盐噪声后的解密图像, 可以看出, 该解密算法基本能恢复出原始图像. 噪声的强度越大, 解密图像的质量越差, 但从整体的视觉效果来看, 仍然能分辨出原图的主要信息, 说明该加密算法能够容忍一定程度的噪声, 抗干扰能力较强.

4.7 抗剪切性能分析

图像在加密传输过程中, 可能会受到恶意剪切攻击, 对于一些存在细节信息的图像, 应最大程度保留其细节信息. 图 7 为经过剪切攻击后的密文图像, 剪切位置的像素均为 0. 图 8 为解密经过剪切后的密文图像得到的结果, 可以看出, 即使图像受到部分剪切, 经过解密后仍能恢复出大致的图像信息, 说明该加密系统可以有效抵抗剪切攻击.

(a) (b) (c) (d)

图 6 加入不同椒盐噪声后的解密图像 (a) 椒盐噪声为 0.05; (b) 椒盐噪声为 0.1; (c) 椒盐噪声为 0.15; (d) 椒盐噪声为 0.2

Fig. 6. Decryption image after adding different salt and pepper noise: (a) The salt and pepper noise is 0.05; (b) the salt and pepper noise is 0.1; (c) the salt and pepper noise is 0.15; (d) the salt and pepper noise is 0.2.

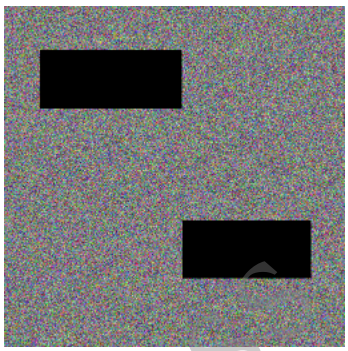


图 7 剪切后的密文图像

Fig. 7. Encrypted image after cutting.

图 8 解密被剪切的图像

Fig. 8. Decrypt the cut image.

5 结 论

本文提出了一种超混沌系统、Logistic 映射和 DNA 计算相结合的图像加密算法, 此算法将待加密图像和 Logistic 混沌矩阵分块进行 DNA 编码, 之后对二者相同位置的图像块之间进行 DNA 运算和解码, 最后得到加密后的图像. 其中, 超混沌系统产生的混沌序列决定了该图像加密算法中的 DNA 编解码方式和运算规则. 加密系统的密钥与明文图像相关联, 保证了“一图一密”的效果. 理论分析和仿真结果表明, 本文图像加密算法密钥容量大、敏感性高, 具有很强的安全性, 十分适用于数字图像的加密.

参考文献

[1] Özkaynak F 2018 *Nonlinear Dyn.* **92** 305

[2] Silva-García V M, Flores-Carapia R, Rentería-Márquez C, Luna-Benoso B, Aldape-Pérez M 2018 *Appl. Math. Comput.* **332** 123

[3] Tang H Q, Sun Q F, Yang X L, Long K P 2018 *IEEE Access* **6** 26059

[4] Zhou Y C, Hua Z Y, Pun C M, Chen C L 2015 *IEEE Trans. Cybern.* **45** 2001

[5] Pak C, Huang L L 2017 *Signal Process.* **138** 129

[6] Brahim A H, Pacha A A, Said N H 2020 *Opt. Laser Technol.* **132** 106489

[7] Guo Y, Jing S W, Zhou Y Y 2020 *Comput. Eng. Des.* **41** 1829 (in Chinese) [郭媛, 敬世伟, 周艳艳 2020 计算机工程与设计 **41** 1829]

[8] Anandkumar R, Kalpana R 2019 *J. Inf. Secur. Appl.* **49** 102390

[9] Malik D S, Shah T 2020 *Math. Comput. Simul.* **178** 646

[10] Tong X J, Cui M G 2010 *Sci. China Inf. Sci.* **53** 191

[11] Huang X, Sun T T, Li Y X, Liang J L 2014 *Entropy* **17** 28

[12] Yang Y, Wang L D, Duan S K, Luo L 2021 *Opt. Laser Technol.* **133** 106553

[13] Gong L H, Deng C Z, Pan S M, Zhou N R 2018 *Opt. Laser Technol.* **103** 48

[14] Zhou M J, Wang C H 2020 *Signal Process.* **171** 107484

[15] Peng Z P, Wang C H, Lin Y, Luo X W 2014 *Acta Phys. Sin.* **63** 240506 (in Chinese) [彭再平, 王春华, 林愿, 骆小文 2014 物理学报 **63** 240506]

[16] Head T, Rozenberg G, Bladergroen R S, Breek C K D, Lommerse P H M, Spaink H P 2000 *Biosystems* **57** 87

[17] Adleman L 1994 *Science* **266** 1020

[18] Wang Q, Zhang Q, Wei X P 2010 *IEEE Fifth International Conference on Bio-Inspired Computing: Theories and Applications (BIC-TA)* Changsha, China, September 23–26, 2010 p132

[19] Akhavan A, Samsudin A, Akhshani A 2017 *Opt. Laser Technol.* **95** 94

[20] Enayatifar R, Guimarães F G, Siarry P 2019 *Opt. Lasers Eng.* **115** 131

[21] Wu J H, Liao X F, Yang B 2018 *Signal Process.* **153** 11

[22] Som S, Kotal A, Chatterjee A, Dey S, Palit S 2013 *1 st International Conference on Emerging Trends and Applications in Computer Science* Shillong, India, September 1314, 2013 p108

[23] Chai X L, Fu X L, Gan Z H, Lu Y, Chen Y R 2019 *Signal Process.* **115** 44

[24] Wu X J, Wang K S, Wang X Y, Kan H B 2017 *Nonlinear Dyn.* **90** 855

"One image corresponding to one key" image encryption algorithm based on chaotic encryption and DNA encoding*

Fang Jie [1)2)] Jiang Ming-Hao [1)] An Xiao-Yu [1)] Sun Jun-Wei [1)2)†]

1) (*College of Electrical and Information Engineering, Zhengzhou University of Light Industry, Zhengzhou* 450002, *China*)

2) (*Henan Key Laboratory of Information-based Electrical Appliances, Zhengzhou* 450002, *China*)

(Received 6 October 2020; revised manuscript received 30 November 2020)

Abstract

Chaotic system is extraordinarily suitable for image encryption because of its characteristics of pseudo randomness, ergodicity and extreme sensitivity to initial values. Combining the chaos theory with other theories to design more secure and efficient encryption algorithms has become a hot research topic. With the rapid advance of genetic engineering, researchers have found that DNA containing a lot of biological genetic information is similar to the code sequence of image encryption system, which provides a new idea for image encryption. The DNA computing has huge parallel processing ability, high energy efficiency and storage capacity. The encryption algorithm based on DNA computing has unique advantages that the traditional encryption algorithm does not have. To improve the security of image transmission, this paper presents a "one image corresponding to one key" image encryption algorithm based on the chaotic encryption and DNA encoding. Firstly, the original image is divided into three two-dimensional pixel matrices with M rows and N columns according to R, G and B channel. At the same time, a matrix of the same size is generated by Logistic map. The above four matrices are divided into blocks for DNA encoding. Then, the three two-dimensional matrices and the sub-blocks corresponding to the Logistic matrix are respectively used for DNA operation and decoding. Among them, the DNA operation rules between the blocks and the DNA encoding and decoding rules of each block are determined by the chaotic sequences generated by the hyperchaotic system, which solves the problem of monotonicity of the DNA codec and operation rules. Finally, the images of three channels after DNA decoding are scrambled and integrated into one image to obtain the ciphertext image. Because the keys of the algorithm are generated by the original image and different original images correspond to different keys, which ensures the effect of "one image corresponding to one key", so it can effectively resist chosen-plain text attack or known-plain text attack. The simulation analyses of histogram distribution, adjacent pixel correlation, information entropy, key sensitivity and other performance analysis show that the encryption algorithm has a large key capacity, high sensitivity to keys, high complexity and security, which is of great significance in improving the security of secure communication.

Keywords: image encryption, chaotic system, DNA encoding, one image corresponds to one key

PACS: 05.45.Gg, 05.45.Jn **DOI:** 10.7498/aps.70.20201642

* National Natural Science Foundation of China (Grant No. 61775198), the Key R&D and Promotion Projects in Henan Province, China (Grant No. 202102210317, 192102210083), and the Scientific Research Foundation of the Higher Education Institutions of Henan Province, China (Grant No. 20A413012).

† Corresponding author. E-mail: junweisun@yeah.net