文章编号:1671-6833(2019)04-0061-07

基于 Duffing 映射与遗传操作的图像加密方法

牛 莹[1], 张勋才[2]

(1.郑州轻工业学院 建筑环境工程学院,河南 郑州 450002; 2.郑州轻工业学院 电气信息工程学院,河南 郑州 450002)

摘 要: 提出了一种基于混沌系统和遗传操作的图像加密方案.首先,使用 SHA-3 算法计算明文图像的哈希值,作为混沌系统的初始值;其次,利用混沌映射对初始条件的敏感性与伪随机性,迭代 Logistic 映射得到伪随机序列并生成希尔矩阵,对图像进行置乱与置换;再次,结合 Duffing 映射与 DNA 编码技术,利用遗传操作在位水平上,实现像素的选择、交叉与变异来完成像素的扩散与置乱,显著增加算法的破译难度;最后,通过与混沌序列进行双向异或运算,进一步增强算法的混淆和扩散特性.实验和安全性分析结果表明,该算法对密钥的敏感性强,能有效抵抗统计攻击和差分攻击等,加密效果得到显著提升.

关键词: 图像加密; Duffing 映射; 遗传操作; DNA 编码; 核酸序列库

中图分类号: TP309.2 **文献标志码**: A **doi**:10.13705/j.issn.1671-6833.2019.04.014

0 引言

由于图像数据量大、冗余度高,并且图像中相邻像素之间具有很强的相关性,所以传统的数据加密方法诸如 AES、DES、IDEA 和 RSA 等加密效率不高.为此,研究人员致力于寻找新的满足混淆和扩散要求的图像加密方法.

混沌系统因其运动轨迹的非周期性以及对初始条件极度敏感性、非线性、各态遍历性、不可预测性等特性被许多学者和专家所重视[1].1998 年,Fridrich 首次将混沌系统应用于图像加密中,充分保证了算法的高效性[2].随后,基于混沌系统的图像加密方法取得了一系列的研究成果[3-5].但是,基于混沌系统的图像加密方法仍存在诸多不足,比如混沌退化、对基于明文的攻击方式防御能力低等.为此,将混沌系统与其他方法结合,成为目前的研究热点[6-9].

遗传算法是一种以自然选择为原则的随机搜索最优化算法[10-12].将遗传算法运用到信息加密中也是近几年加密领域中的研究前沿之一[13].2014 年,Wang 等引入基因重组和交叉两种操作来扰动密钥,提出了一种基于基因重组思想和超混沌系统的图像加密算法[14].同年,Enayatifar 等提出了基于遗传算法和 DNA 序列的图像加密算法[15].2018 年,Pujari 等结合 DNA 序列,给出一种基于混沌与遗传算法的图像加密算法[16].这些方法多采用遗传算法的优化策略来实现图像的加密.

基于此,笔者利用 Duffing、Logistic 映射的伪随机性、遍历性和遗传算法的交叉变异算子来解决图像加密所遇到的安全威胁和效率低下问题.增强算法的混淆和扩散特性.

1 理论基础

1.1 混沌映射

(1) Logistic 映射是研究动力系统、混沌、分形等复杂系统行为的一个经典模型,且具有良好的混沌特性,其数学描述如下:

$$x_{t+1}=\mu x_t(1-x_t), \tag{1}$$

式中:t 为迭代时间步;μ 为可调参数.当 $3.569\,945\,6<\mu\leqslant 4$ 时,Logistic 映射处于混沌状态.

(2) Duffing 映射(也称 Holmes 映射)是一个离散时间的动力系统,是 Duffing 方程的一个离散形式,其数学描述如下:

收稿日期:2019-02-15;**修订日期**:2019-04-07

基金项目:国家自然科学基金资助项目(61602424,61472371);河南省科技创新人才计划资助项目(174100510009);河南省高等学校重点科研计划资助项目(18A510020);河南省科技攻关计划资助项目(192102210134)

作者简介:牛莹(1982—),女,河南洛阳人,郑州轻工业学院副教授,主要从事智能信息处理研究,E-mail:niuying@zzuli.edu.cn.

$$\begin{cases} x_{t+1} = y_t; \\ y_{t+1} = -bx_t + ay_{t+1} - y_t^3. \end{cases} \tag{2}$$

Duffing 映射的两个常数 a 和 b 通常被设置为 $a=2.75$ 和 $b=0.2$,以产生混沌行为,如图 1 所示.它对初始值有极其敏感的依赖性.这里将其对初值的敏感性充分体现在加密算法对明文和密钥的扩散性与混乱性上.Duffing 映射还具有优良的伪随机性,其轨道的演化是非周期、不收敛的,具有很好的随机性及不可预测性.已从理论上证实了 Duffing 映射可以产生统计特性优良的伪随机序列.

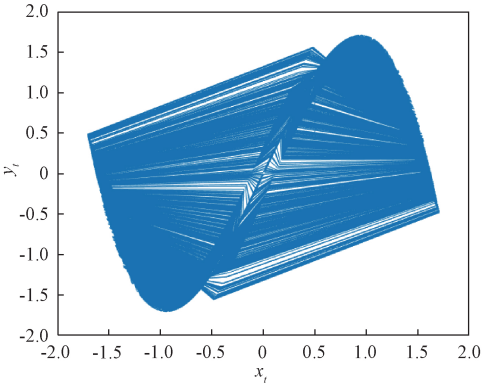


图 1 处于混沌状态的 Duffing 映射

Fig.1 The duffing map in chaotic state

1.2 DNA 编码

DNA 分子是遗传信息的载体,由 4 种脱氧核苷酸组成,分别是腺嘌呤(A)、胞嘧啶(C)、鸟嘌呤(G)、胸腺嘧啶(T).碱基的化学结构确定了碱基互补配对的原则,这一天然的四进制组合,正好与半导体通断所形成的二进制类似.因此,运用碱基的排列组合可以进行信息的存储和计算.

对于灰度图像来说,每个像素的灰度值可以用 8 位二进制数表示,如果采用 DNA 编码的话,则两位二进制编码一个碱基,只需 4 个碱基即可完成一个像素的编码.通过对每个像素进行 DNA 编码,将图像转换成 DNA 序列,可以将 DNA 序列的交叉变异操作用于图像加密.8 种编码规则如表 1 所示.

表 1 8 种编码规则

Tab.1 Eight types of encoding rules.

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

2 加密算法

2.1 密钥的产生

经典的数字图像加密中,密码仅受密钥控制,与明文无关,这种类型的图像密码系统易受选择明文攻击或已知明文攻击.如果相同的密钥,但不同的明文图像对应着不同的密码,将能有效抵抗选择明文攻击或已知明文攻击.

用给定密钥以及图像的哈希值作为混沌系统的初值和参数,实现加密的密码既与密钥有关,也与明文相关联.用 Keccak 算法生成明文图像的哈希值 K,其长度为 512 bit.将 K 分为 64 组,每组包含 8 个比特位,记 $K=\{k_1,k_2,k_3,\cdots,k_{64}\}$.按照如下公式计算混沌系统的初值 Key_1、Key_2、Key_3、Key_4:

$$h_i = \frac{(k_{j+1}k_{j+2}k_{j+3}k_{j+4}) + \sum_{q=1}^{q=64} k_q}{256}, \tag{3}$$

$$Key_i = Key'_i + abs(round(h_i) - h_i), \tag{4}$$

式中:Key'_i 为给定值;$j=4(i-1)$;$i=1$、2、3、4.

2.2 遗传操作

给定大小为 $M\times N$ 的灰度图像,将单个像素看作一个“个体”.使用混沌映射产生的序列值作为个体在图像中的位置来选择个体,用遗传算子对个体进行交叉、变异操作.

选择:给定 Duffing 映射初值,迭代 Duffing 映射 2 000 次,以消除暂态效应带来的不良影响,以此为起点,继续迭代 $M\times N$ 次,产生两个序列 $U=\{u_1,u_2,\cdots,u_{M\times N}\}$ 和 $V=\{v_1,v_2,\cdots,v_{M\times N}\}$,并根据公式(5)和(6)进行处理后得到序列 $U'=\{u'_1,u'_2,\cdots,u'_{M\times N}\}$ 和 $V'=\{v'_1,v'_2,\cdots,v'_{M\times N}\}$,确保 U 和 V 的每个元素取值大小在给定的范围内.

$$u'_i = floor(mod(10\hat{}14\cdot u_i,256)); \tag{5}$$

$$v'_i = floor(mod(10\hat{}14\cdot v_i,256)), \tag{6}$$

式中:$i=1,2,\cdots,M\times N$.

交叉:给定两个个体(像素)A 和 B,将其像素值用二进制表示.引入控制字 C 来控制两个个体的交叉操作.针对 8 位二进制的每一位,若控制字的当前位是 0 时,个体 A 和 B 的当前位保持不变,若控制字的当前位是 1 时,个体 A 和 B 互换当前位.最终得到新个体 A' 和 B'.比如给定个体 A、B 和控制字 C 分别为 10011001、00111100、01101001 时,交叉后得到的新个体 A' 和 B' 为 10111000 和 00011101,交叉过程如图 2 所示.

变异:变异是生成新个体的辅助手段.这里用

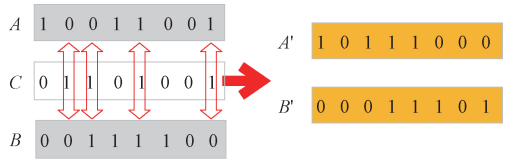


图 2　个体 10011001 和 00111100 进行交叉操作

Fig.2　Crossover between individuals 10011001 and 00111100

控制字来控制个体的变异.为增加密文的抗攻击特性,引入非线性扩散机制——DNA 编码技术,实现 DNA 分子级别上的变异,也符合基因变异的本质.为此,选取核酸数据库中的某一核酸序列作为控制字.通过选择表 1 中的某种编码规则(也可以进行动态编码)将待转换的图像矩阵转换为 DNA 序列,借助于核酸数据库中的某一序列来控制明文图像 DNA 序列的变异.引入一个变异函数 $\kappa(x)$,并进行如下约定:

$$\begin{cases} x \neq \kappa(x) \neq \kappa(L(x)) \neq \kappa(\kappa(\kappa(x))); \\ x = \kappa(\kappa(\kappa(\kappa(x)))), \end{cases} \tag{7}$$

式中:$x \in \{A,C,G,T\}$.按照这个约定,有 6 种碱基变异规则,如表 2 所示.

表 2　碱基变异规则

Tab.2　Base mutation rules

序号	规则
1	$A \xrightarrow{\kappa} C \xrightarrow{\kappa} G \xrightarrow{\kappa} T \xrightarrow{\kappa} A$
2	$A \xrightarrow{\kappa} C \xrightarrow{\kappa} T \xrightarrow{\kappa} G \xrightarrow{\kappa} A$
3	$A \xrightarrow{\kappa} T \xrightarrow{\kappa} C \xrightarrow{\kappa} G \xrightarrow{\kappa} A$
4	$A \xrightarrow{\kappa} T \xrightarrow{\kappa} G \xrightarrow{\kappa} C \xrightarrow{\kappa} A$
5	$A \xrightarrow{\kappa} G \xrightarrow{\kappa} T \xrightarrow{\kappa} C \xrightarrow{\kappa} A$
6	$A \xrightarrow{\kappa} G \xrightarrow{\kappa} C \xrightarrow{\kappa} T \xrightarrow{\kappa} A$

在进行个体变异时,可以随机选择一种变异规则进行碱基变异,从而达到像素值扰乱的目的.这里随机选取基因库中某一个 DNA 序列,从中截取长度为 $4\times M\times N$ 个碱基的序列,命名为序列 $Q=\{q_1,q_2,\cdots,q_{4\times M\times N}\}$,用于指导碱基的变异.控制变异的方法如下:

$$\begin{cases} x_i = x_i, & q_i = A; \\ x_i = \kappa(x_i), & q_i = C; \\ x_i = \kappa(\kappa(x_i)), & q_i = G; \\ x_i = \kappa(\kappa(\kappa(x_i))), & q_i = T. \end{cases} \tag{8}$$

2.3　希尔置换

希尔置换(也称希尔加密)是基于矩阵论的一种替换密码.它通过采用线性代数中的矩阵乘法运算和逆运算,能够较好地抵抗频率分析,很难被攻破.希尔密码的关键在于加密矩阵,如果加密矩阵不可逆,密文将无法还原成明文.为避免加密矩阵元素之间强相关性,笔者使用混沌序列构造自逆加密矩阵来降低矩阵之间的相关性,从而使密文难于破解.

将待加密的图像每 4 个像素为一组,组成 4×1 的矩阵 $\boldsymbol{I}_{4\times1}$.通过构造 4×4 自逆矩阵 $\boldsymbol{W}$,对每组图像矩阵进行局部的希尔置换加密.置换加密公式如下:

$$\boldsymbol{E} = (\boldsymbol{W} \times \boldsymbol{I}) \, mod 256, \tag{9}$$

$$\boldsymbol{W} = \begin{bmatrix} \boldsymbol{W}_{11} & \boldsymbol{W}_{12} \\ \boldsymbol{W}_{21} & \boldsymbol{W}_{22} \end{bmatrix} = \begin{bmatrix} w_{11} & w_{12} & w_{13} & w_{14} \\ w_{21} & w_{22} & w_{23} & w_{24} \\ w_{31} & w_{32} & w_{33} & w_{34} \\ w_{41} & w_{42} & w_{43} & w_{44} \end{bmatrix}, \tag{10}$$

式中:$\boldsymbol{W}_{11} = \begin{bmatrix} w_{11} & w_{12} \\ w_{21} & w_{22} \end{bmatrix}$;$\boldsymbol{W}_{12} = \begin{bmatrix} w_{13} & w_{14} \\ w_{23} & w_{24} \end{bmatrix}$;$\boldsymbol{W}_{21}$ 和 $\boldsymbol{W}_{22}$ 类似.

使用 $\boldsymbol{W}$ 的乘法逆矩阵 $\boldsymbol{W}^{-1}=\boldsymbol{W}$,对密文进行解密:$\boldsymbol{I}=(\boldsymbol{W}^{-1}\times\boldsymbol{E})\,mod256=(\boldsymbol{W}\times\boldsymbol{E})\,mod256$.

将自逆矩阵 $\boldsymbol{W}$ 分成 4 部分,其构造过程如下:

(1)Logistic 映射作为伪随机数发生器,给定初值和参数产生混沌序列,并对序列进行取模处理,然后依次选择混沌序列中的元素,填充 $\boldsymbol{W}_{11}$ 子矩阵.

(2)根据 $\boldsymbol{W}_{12}=n\times(\boldsymbol{I}-\boldsymbol{W}_{11})$ 计算生成子矩阵 $\boldsymbol{W}_{12}$,这里 n 取 2.

(3)令子矩阵 $\boldsymbol{W}_{22}=-\boldsymbol{W}_{11}$.

(4)根据 $\boldsymbol{W}_{21}=1/n\times(\boldsymbol{I}+\boldsymbol{W}_{11})$ 计算生成子矩阵 $\boldsymbol{W}_{21}$.最后将生成的 4 个子矩阵 $\boldsymbol{W}_{11}$、$\boldsymbol{W}_{12}$、$\boldsymbol{W}_{22}$、$\boldsymbol{W}_{21}$ 合并得到可逆加密矩阵 $\boldsymbol{W}$.

基于分块矩阵 $\boldsymbol{W}_{11}$,生成的置换矩阵更具有鲁棒性,免去求解逆矩阵.

2.4　像素扩散

密文扩散操作使明文的微小变化可以扩散到整个密文,从而打乱明文图像与密文图像的关系,可以有效抵抗选择明文等攻击手段,实现密文扩散.将图像矩阵按照行优先的顺序转换为长度为 $M\times N$ 的一维序列 $S=\{s_1,s_2,\cdots,s_{M\times N}\}$,给定的密码流 $C=\{c_1,c_2,\cdots,c_{M\times N}\}$,设密文扩散后的序列为 $E=\{e_1,e_2,\cdots,e_{M\times N}\}$,密文扩散的公式如下:

$$e_{i+1} = s_i \oplus e_i c_i. \tag{11}$$

初始化元素 $e(0)=127$,$i=1,2,\cdots,M\times N$.扩散过程包括正向扩散和反向扩散.根据上述公式对一维序列 S 从左到右进行一次如公式(11)所

示的运算,属于正向扩散,扩散效果是有限的,因此,需要将所得到的序列 E 赋值给 S,然后再按照式(11)进行一次从右到左的反向扩散.

2.5 加密过程

本算法的加密结构,主要包括:像素位置置乱、希尔矩阵置换、对图像像素进行遗传操作和密文扩散操作.加密流程如图3所示.具体步骤如下:

输入:灰度图像和密钥.

输出:加密图像.

(1) 将灰度图像转换成大小为 $M\times N$ 的二维矩阵 $\boldsymbol{P}_1$.

(2) 采用哈希函数计算图像矩阵 $\boldsymbol{P}_1$ 的哈希值 K,并根据式(3)和式(4)计算得到混沌初始化参数.

(3) 根据 Logistic 映射产生的序列 L,升序排列得到置换索引序列 L',将 L'按照每行 M 个值进行填充可得到置换矩阵,用其置乱图像矩阵 $\boldsymbol{P}_1$ 得到置乱后图像矩阵 $\boldsymbol{P}_2$.

(4) 采用 Logistic 映射产生的序列 L,构造 $T=(M\times N/4)$个希尔加密矩阵 $\boldsymbol{KM}_1,\boldsymbol{KM}_2,\cdots,\boldsymbol{KM}_T$.对加密图像 $\boldsymbol{P}_2$ 按照每4个像素一组,选择构造的希尔加密矩阵进行希尔置换,得到图像矩阵 $\boldsymbol{P}_3$.

(5) 从 GenBank 数据库中下载 ID 号为 NZ_LOZQ01000042 的 DNA 序列.从起始位置 r 处截取长度为 $4\times M\times N$ 个碱基的序列,作为序列 Q.

(6) 根据 Duffing 映射产生的序列 U 和 V,每次选择图像矩阵 $\boldsymbol{P}_3$ 中的两个个体,将序列 Q 中的碱基进行 DNA 解码,每4个碱基解码后组成一个控制字,依次控制个体的交叉操作,得到图像矩阵 $\boldsymbol{P}_4$.

(7) 将图像矩阵 $\boldsymbol{P}_4$ 变换为一维向量,并对其进行 DNA 编码,得到一维 DNA 序列,采用给定的 DNA 序列 Q,根据公式(8),选择表2中的一种变异规则,对图像 DNA 序列的每个碱基实现变异操作.随后对变异后的图像 DNA 序列进行 DNA 解码,恢复成二维矩阵形式,得到图像矩阵 $\boldsymbol{P}_5$.

(8) 根据前面描述的像素扩散技术,对每个像素实行正反扩散,Duffing 映射产生的序列 U 作为正向扩散密码流,序列 V 作为反向扩散的密码流.扩散后得到图像加密矩阵 $\boldsymbol{P}_6$,将其恢复成图像并输出,得到密文图像.

解密算法是上述过程的逆过程.这里不再阐述.本算法也适用于彩色图像的加密,只需将像素的值进行 RGB 分解处理即可.

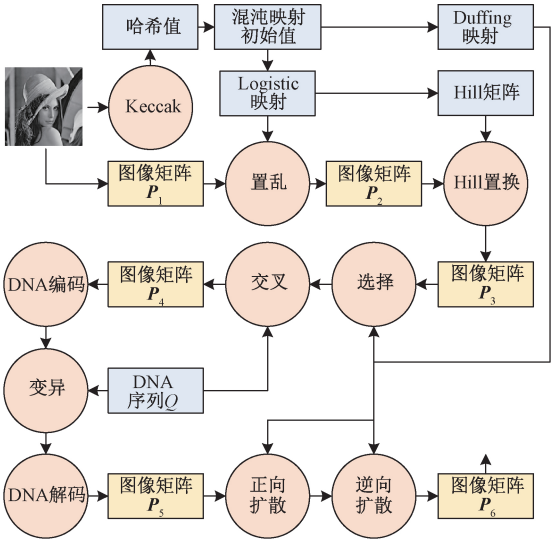
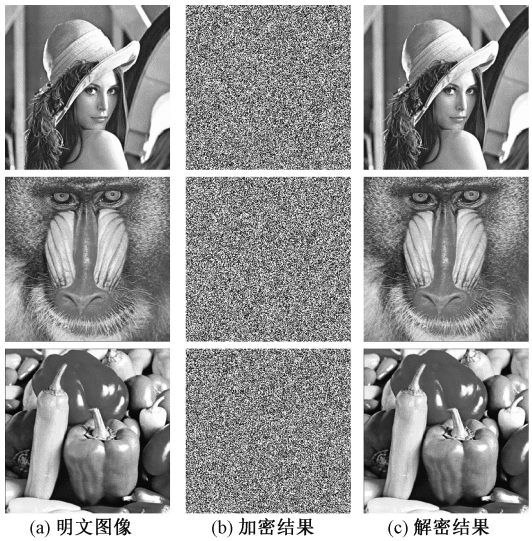


图3 加密流程图

Fig.3 Description of the encryption process

3 实验结果及安全性分析

采用3幅大小为256×256的灰度图像 Lena、Baboon 和 Pepper,使用 Matlab 软件来验证该算法的可行性和有效性.密钥给定值 $Key'_1 = Key'_3 = Key'_4 = 0.000\ 000\ 05$,$Key'_2 = 3.5$;核酸数据库的 DNA 序列 ID 号 NZ_LOZQ01000042,起始位置 $r=1$.初始值 Key_1 和 Key_2 作为 Logistic 映射的参数 μ 及初始状态值,初始值 Key_3 和 Key_4 作为 Duffing 映射的初始状态值.采用本算法对3幅图像进行加密.明文图像、加密图像和解密图像分别如图4(a)、4(b)和4(c)所示.



(a) 明文图像 (b) 加密结果 (c) 解密结果

图4 加密与解密图像

Fig.4 Cipher and decryption images of Lena

3.1 密钥空间

算法涉及的密钥有 Logistic 映射的参数 μ 及状态值,Duffing 映射的两个初值状态值,以及

DNA 序列 ID.如果计算精度为 10^{-15},密钥的空间总空间为 $10^{15}\times10^{15}\times10^{15}\times10^{15}\times10^{10}=10^{70}$.可见本算法具有足够的空间来抵抗穷举攻击.

3.2　统计分析

(1)灰度直方图分析.直方图在一定程度上可以反映出图像灰度值的分布规律,能否改变明文图像的统计分布也是图像加密中至关重要的指标.图 5 为明文和密文图像 Lena 的直方图,直观上密文图像具有平坦的直方图,而明文图像的直方图跌宕起伏.

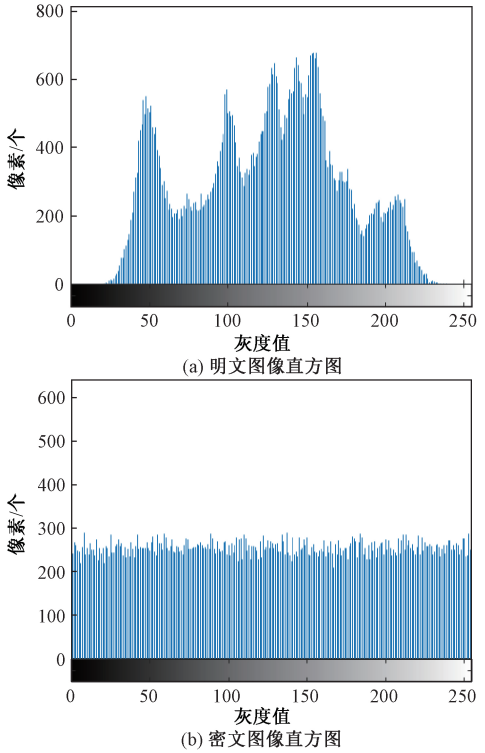


图 5　直方图分析

Fig.5　The histograms analysis

进一步,引入直方图的 χ^2 统计量在数量上衡量两者的差别[17].对于灰度等级为 256 的灰度图像,χ^2 统计量计算公式如下:

$$\chi^2=\sum_{i=1}^{256}\frac{(O_i-e_i)^2}{e_i},\tag{12}$$

式中:O_i 为观测到的频数分布;e_i 为理论频数分布.对于灰度等级为 256 的灰度图像而言,给定大小为 $M\times N$ 的图像,假设直方图中每个像素灰度值的像素点频数 O_i 服从均匀分布,即 $e_i=e=M/256$,则式(12)服从自由度为 255 的 χ^2 分布.当显著性水平 α 取 0.05 时,有 $\chi^2_{0.05}(255)=293.247\ 8$.表 3 列出了 χ^2 检验结果,3 个明文图像的 χ^2 检验结果明显大于 $\chi^2_{0.05}(255)=293.247\ 8$,而 3 个密文图像的 χ^2 检验结果均小于 $\chi^2_{0.05}(255)$,可以认为密文图像近似均匀分布.

表 3　χ^2 检验结果

Tab.3　Chi-square test results

	图像	Lena	Baboon	Pepper
本文算法	明文	39 851.328 1	79 056.906 3	31 629.656 3
	密文	240.296 9	265.765 6	270.742 2
文献[3]	密文	279.148 4	—	—

(2)相关性分析.明文图像在相邻像素之间一般具有较强的相关性,为抵御统计分析攻击,必须降低相邻像素之间的相关性.利用式(13),分别随机选取明文图像和密文图像各 2 000 对像素,测试其水平、垂直和对角方向的像素相关性,结果如表 4 所示.从表 4 中可以看出,密文图像像素之间相关性大大减少.这表明明文图像的统计特征已被扩散.图 6 给出了 Lena 图像的明文和密文在各个方向上的相关情况.

表 4　图像的相关性分析

Tab.4　Correlation coefficients of the images

图像		水平	垂直	对角
Lena	明文	0.966 829	0.936 229	0.915 573
	密文	0.030 221	−0.007 038	0.051 455
Baboon	明文	0.824 924	0.880 136	0.788 979
	密文	0.300 383 1	0.013 473	−0.024 117
Pepper	明文	0.973 794	0.965 969	0.944 112
	密文	0.009 228	0.010 356	−0.015 218

相关系数计算如下:

$$r_{xy}=\frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}},\tag{13}$$

式中:$cov(x,y)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))(y_i-E(y))$,$E(x)=\frac{1}{N}\sum_{i=1}^{N}x_i$;$D(x)=\frac{1}{N}\cdot\sum_{i=1}^{N}(x_i-E(x))^2$.

3.3　信息熵分析

信息熵反映了图像信息的不确定性.计算公式:

$$H=-\sum_{i=0}^{2^N-1}p(i)\log_2 p(i),\tag{14}$$

式中:$p(i)$ 表示信息 i 出现的概率.对于灰度图像来说,信息 i 有 256 种状态,最小值 0,最大值为 255.灰度图像信息熵的理论值为 8.密文信息熵越大,信息越安全.Lena、Baboon 和 Pepper 的密文图像的信息熵分别为 7.989 7、7.989 4 和 7.989 5,各个密文图像的信息熵接近理论值.

3.4　敏感性分析

度量敏感性通常使用 2 个标准:像素数目改

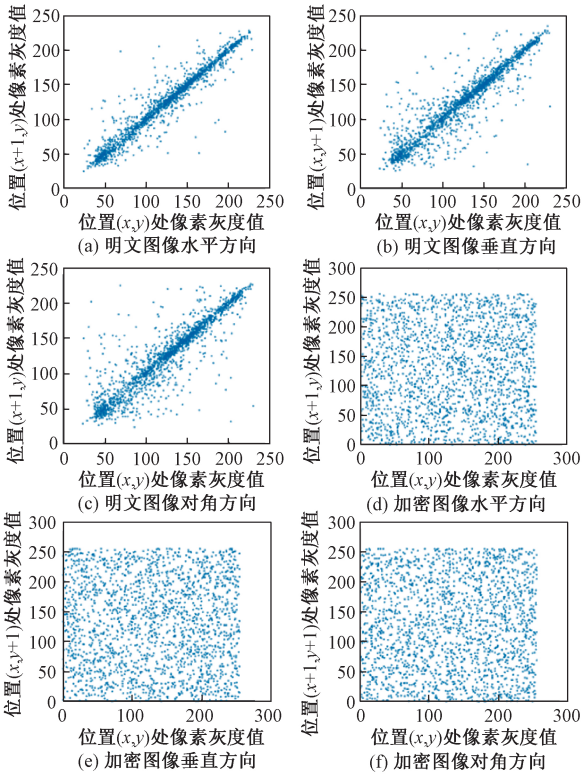


图 6 明密文图像的相关性

Fig.6 Correlations of plain and cipher images

变率(*NPCR*)和平均强度变化率(*UACI*).

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\%; \quad (15)$$

$$UACI = \frac{1}{W \times H}\left[\sum_{i,j} \frac{|C(i,j) - C'(i,j)|}{255}\right] \times 100\%, \quad (16)$$

式中:W 和 H 分别代表图像的长度和宽度;C 和 C' 表示两个密文图像.对于像素点(i,j)的像素值,如果 $C(i,j) \neq C'(i,j)$,则 $D(i,j)=1$,否则 $D(i,j)=0$.

(1)密钥敏感性.为测试密钥的灵敏度,将 Key'_3的值增加 0.000 000 01,在其他密钥不变的情况下,使用修改后的密钥解密被加密的 Lena 图像,无法解密出原图像.再者,利用修改后的密钥对图像重新加密,得到加密图像与图 4(b)中相应的加密图像进行对比可知,两个密文图像之间对应像素点的不同率在 99.65%以上,可见该算法具有较强的密钥灵敏性,且能抵抗暴力攻击,具有很好的密钥安全性.

(2)差分分析.差分分析是一种选择明文攻击即对明文图像做微小的改变后,再分别对原图像和改变后的图像进行加密.通过比较两幅被加密后的图像来获得原图像与加密图像之间的关系,从而破解加密系统.*NPCR* 和 *UACI* 两个标准常用来衡量加密方法抵御差分攻击的能力.

这里将明文图像位置(100,100)的像素点的像素值增加 50.针对 Lena 图像,算法的 *NPCR* 和 *UACI* 值如表 5 所示.明文微小的变化导致密文巨大的差异,因此算法具有很好的抗差分攻击能力.

表 5 差分分析的 *NPCR* 和 *UACI* 值

Tab.5 The *NPCR* and *UACI* values of the Lena image %

加密算法	*NPCR*	*UACI*
本算法	99.61	33.38
文献[3]	99.61	30.56
文献[4]	99.54	28.81
文献[7]	99.66	28.71
文献[8]	99.21	33.28

3.5 复杂度分析

采用 Matlab、Windows 10 操作系统、Intel Core 2.6 GHz CPU 和 4 GB RAM 计算机测试.测试为 256×256 的灰度 Lena 图像.本文算法的耗时主要集中在像素置换、置乱阶段,每一轮的置换、置乱均为 $M \times N$ 次,总共执行 5 轮的置换、置乱过程.因此整个算法的复杂度为 $O(M \times N)$.

4 结论

通过 Logistic 映射产生的混沌序列构造希尔矩阵,对图像进行置换与置乱,增强了混沌序列的随机性.希尔置换能实现局部的置乱,而无法满足全局置乱,这容易通过部分明文破解.进一步,结合 Duffing 映射与 DNA 编码技术,利用遗传操作实现像素的选择、交叉和变异来实现全局置乱与扩散.安全性分析表明该算法具有很好的安全性和抗攻击能力.

参考文献:

[1] DHALL S, PAL S K, SHARMA K. Cryptanalysis of image encryption scheme based on a new 1D chaotic system[J]. Signal processing, 2018, 146:22-32.

[2] FRIDRICH J. Symmetric ciphers based on two-dimensional chaotic maps[J]. International journal of bifurcation & chaos, 1998, 8(6): 1259-1284.

[3] ASKAR S S, KARAWIA A A, ALAMMAR F S. Cryptographic algorithm based on pixel shuffling and dynamical chaotic economic map[J]. IET image processing, 2018, 12(1): 158-167.

[4] SIVAKUMAR T, VENKATESAN R. Image encryption based on pixel shuffling and random key stream[J]. International journal of computer and information tech-

nology, 2014, 3(6): 1468-1476.
[5] OZKAYNAK F. Brief review on application of nonlinear dynamics in image encryption[J]. Nonlinear dynamics, 2018, 92(2): 305-313.
[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] ZHANG J, FANG D X, REN H G. Image encryption algorithm based on DNA encoding and chaotic maps [J]. Mathematical problems in engineering, 2014 (3):1-10.
[8] ZKAYNAK F, YAVUZ S. Analysis and improvement of a novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system[J]. Nonlinear dynamics, 2014, 78(2): 1311-1320.
[9] WEI X P, 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.
[10] 程适,王锐,伍国华,等.群体智能优化算法[J]. 郑州大学学报(工学版), 2018, 39(6): 1-2.
[11] 穆瑞杰. 基于遗传算法的地铁车站引导标识布点探析[J]. 郑州大学学报(工学版),2018,39(1): 73-77.
[12] TINÓS R, ZHAO L, CHICANO F, et al. Nk hybrid genetic algorithm for clustering[J]. IEEE transactions on evolutionary computation, 2018, 22(5): 748-761.
[13] RAJ R, SINGH P K, SINGH R S. Multi-image encryption using genetic computation [J]. CSI transactions on ICT, 2016, 4(2/4):95-101.
[14] WANG X Y, ZHANG H L. A novel image encryption algorithm based on genetic recombination and hyper-chaotic systems[J]. Nonlinear dynamics, 2016, 83 (1/2):333-346.
[15] ENAYATIFAR R, ABDULLAH A H, ISNIN I F. Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence[J]. Optics & lasers in engineering, 2014, 56:83-93.
[16] PUJARI S K, BHATTACHARJEE G, BHOI S. A hybridized model for image encryption through genetic algorithm and DNA sequence[J]. Procedia computer science, 2018, 125:165-171.
[17] KWOK H S, TANG W K S. A fast image encryption system based on chaotic maps with finite precision representation[J]. Chaos solitons & fractals, 2007, 32 (4): 1518-1529.

Image Encryption Algorithm Based on Duffing Map and Genetic Operators

NIU Ying[1], ZHANG Xuncai[2]

(1.School of Architecture Environment Engineering, Zhengzhou University of Light Industry, Zhengzhou 450002, China; 2.College of Electric Information Engineering, Zhengzhou University of Light Industry, Zhengzhou 450002, China)

Abstract: In this paper, an image encryption scheme based on chaotic systems and genetic operations was proposed. Firstly the SHA-3 algorithm was used to calculate the hash value of the plaintext image and input the key as the initial values of the chaotic system. Secondly the sensitivity of the chaotic map to initial conditions and pseudo-randomness were used to obtain pseudo-random sequence by iterative the Logistic map, and generate the Hill matrix to carry out image scrambling and permutation. Thirdly combining the Duffing map and DNA coding technology, the selection, crossover and mutation of pixels were realized at the level of genetic operations to achieve pixel diffusion and scrambling, which significantly increased the decoding difficulty of the algorithm. Finally, bidirectional exclusive OR operations with chaotic sequence was carried out to further enhance the confusion and diffusion characteristics of the algorithm. The experimental and security analysis results showed the algorithm was sensitive to the keys and could effectively resist statistical attacks and differential attacks, and the image encryption effect and performance could be significantly improved.

Key words: image encryption; duffing map; genetic operation; DNA code; nucleotide sequences database