

基于混沌系统和动态 DNA 编码与运算的彩色图像加密算法

杨吉云, 吴 昊

(重庆大学 计算机学院, 重庆 400044)

摘 要: 现有结合混沌系统和 DNA 计算的图像加密算法因 DNA 编码规则和运算规则单一、加密结构安全性低, 导致算法易被破解。为此, 提出一种结合 Intertwining Logistic 映射和动态 DNA 编码与运算的彩色图像加密算法。该算法包括置乱阶段和扩散阶段, 在置乱阶段, 利用模拟退火算法构造的置乱序列分别对彩色图像信道进行行和列置乱, 得到置乱信道。在扩散阶段, 先根据随机序列值动态选择各置乱信道每个像素点的 DNA 编码规则及运算规则, 然后结合密文反馈机制进行 DNA 加密计算。实验结果表明, 该算法具有良好的抗攻击能力及加密效果。

关键词: Intertwining Logistic 映射; DNA 编码; DNA 计算; 图像加密; 安全性分析

中文引用格式: 杨吉云, 吴 昊. 基于混沌系统和动态 DNA 编码与运算的彩色图像加密算法[J]. 计算机工程, 2018, 44(2): 151-157.

英文引用格式: YANG Jiyun, WU Hao. Color Image Encryption Algorithm Based on Chaotic System and Dynamic DNA Coding and Operation[J]. Computer Engineering, 2018, 44(2): 151-157.

Color Image Encryption Algorithm Based on Chaotic System and Dynamic DNA Coding and Operation

YANG Jiyun, WU Hao

(College of Computer Science, Chongqing University, Chongqing 400044, China)

[Abstract] Aiming at the problem that the chaos based image encryption algorithm combined with DNA coding can be broken caused by incorrect use of DNA coding rules and calculation methods, a new image encryption algorithm combined Intertwining Logistic mapping and dynamic DNA coding is proposed in this paper. This algorithm includes a scrambling phase and a diffusion phase. In the scrambling phase, the rows and columns of each channel of the color image are scrambled via scrambling sequences constructed by the simulated annealing algorithm. In the diffusion phase, the DNA coding rules and calculation rules of each pixel are determined according to the random sequence values, and then the DNA encryption is carried out. Experimental results show that this algorithm can resist against common attacks and have an excellent performance.

[Key words] Intertwining Logistic mapping; DNA coding; DNA calculation; image encryption; safety analysis

DOI: 10.3969/j.issn.1000-3428.2018.02.027

0 概述

随着数字技术和通信网络的发展,越来越多的数字信息需要通过网络传输。由于数字图像具有直观、生动等特点,已成为应用最广泛的一种数字信息,但其也面临着日益严重的安全威胁。数字图像加密技术是一种有效保护数字图像安全的方法,由于混沌加密技术具有实现简单、鲁棒性好、加密速度快、安全性高等特点,经过多年的发展,已被应用于图像加密技术研究中^[1-3]。文献[1]提出一种

基于置乱扩散结构的采用时空混沌系统的图像加密算法。文献[2]提出了一种提出了基于多维混沌系统同时对图像像素位置置乱和像素值加密的新算法。但安全性分析表明,混沌加密技术保护图像安全性的能力还需进一步提高^[4-5]。文献[4]指出加密算法对于明文改变的低敏感性使得攻击者易于采用选择明文攻击破解加密算法的置乱过程。文献[5]研究发现当密钥与明文无关及加密过程中各像素相互独立,算法无法有效抵抗已知明文和选择明文攻击。

基金项目: 中央高校基本科研业务费专项资金(106112015CDJXY180006)。

作者简介: 杨吉云(1975—),男,副教授、博士,主研方向为信息安全;吴 昊,硕士研究生。

收稿日期: 2017-02-17 **修回日期:** 2017-03-21 **E-mail:** yangjy@cqu.edu.cn

文献[6]中首次提出了DNA计算,其具有超大规模并行性、超低的能量消耗和超高的存储密度等优点。DNA计算作为提高混沌图像加密技术安全性的有效途径,已被一些学者应用于混沌图像加密方案。文献[7]将DNA序列操作应用到了加密算法的置乱和扩散过程,有效提高了算法抵抗明文攻击的能力。文献[8]在置乱和扩散阶段有效结合混沌序列的随机性和DNA编码的特性,扩大了算法的密钥空间并且提高了抵抗统计攻击的能力。

然而,当前结合混沌系统和DNA计算的图像加密算法也存在不足之处。文献[9]通过对加密算法数学模型的分析,找到了加密系统中存在的线性关系,通过对加密算法进行等价代换,一方面减小了算法密钥空间,削弱了算法抵抗穷举攻击的能力,另一方面针对算法采用单一的编码规则和运算规则的缺陷,运用选择明文攻击获取了算法的等价密钥。文献[10]指出了采用固定编码和单一运算规则的DNA混沌图像加密算法容易通过选择明文攻击进行破解。

针对上述DNA混沌图像加密算法中存在的不足,本文结合混沌系统和DNA计算,通过用Intertwining Logistic映射产生的随机序列值动态选择彩色图像R、G、B信道每个像素在进行DNA加密计算时所采用的编码规则和运算规则,避免算法因采用固定编码规则和单一运算规则而导致易被破解的缺陷。采用模拟退火算法构造置乱序列分别对R、G、B信道行和列进行充分置乱,再结合混沌映射通过动态DNA计算对图像进行扩散,消除加密系统中存在的线性关系,并解决算法抵御穷举攻击及明文攻击能力弱的问题。

1 混沌系统及DNA编码

1.1 Intertwining Logistic映射

Intertwining Logistic映射可被描述为以下形式:

$$\begin{cases} x_{n+1} = [\mu \times k_1 \times y_n \times (1 - x_n) + z_n] \bmod 1 \\ y_{n+1} = [\mu \times k_2 \times y_n + z_n \times 1 / (1 + x_{n+1}^2)] \bmod 1 \\ z_{n+1} = [\mu \times (x_{n+1} + y_{n+1} + k_3) \times \sin(z_n)] \bmod 1 \end{cases} \quad (1)$$

其中, $0 < \mu \leq 3.999$, $|k_1| > 33.5$, $|k_2| > 37.9$, $|k_3| > 35.7$ 。Intertwining Logistic映射比Logistic映射具有更优秀的混沌特性,且因其没有空白窗口而具有更好的特性^[11],如图1所示。

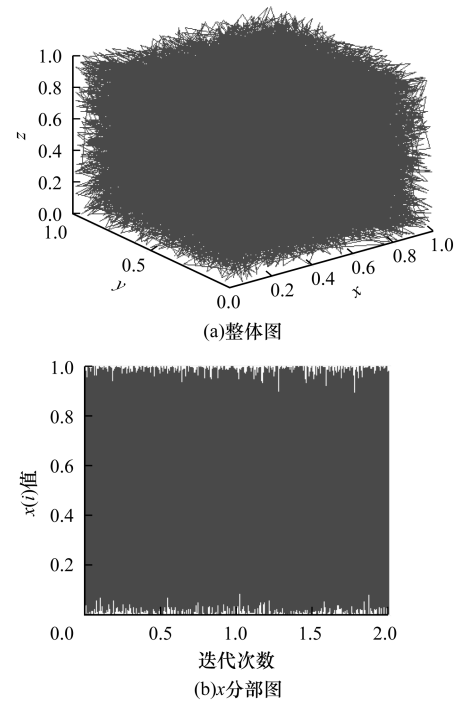


图1 Intertwining Logistic映射

1.2 DNA编码

一个DNA序列由A、T、C、G4种核酸碱基组成,其中,A与T,C与G互补配对。二进制序列中0与1互补,因此可以使用A、C、G、T编码00、01、10、11,根据Watson.Crick互补规则^[12]有8中编码规则符合要求,如表1所示。另外,根据编码规则0定义的DNA加法、减法和异或操作,分别如表2~表4所示。

表1 DNA编码规则

规则0	规则1	规则2	规则3	规则4	规则5	规则6	规则7
A-00	A-00	A-01	A-01	A-10	A-10	A-11	A-11
T-11	T-11	T-10	T-10	T-01	T-01	T-00	T-00
C-01	C-10	C-00	C-11	C-00	C-11	C-01	C-10
G-10	G-01	G-11	G-00	G-11	G-00	G-10	G-01

表2 DNA加法运算规则

+	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减法运算规则

-	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 异或运算规则

\oplus	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 算法描述

2.1 图像加密算法概述

本文算法由 2 个阶段组成: 行列置乱阶段和 DNA 加密扩散阶段。第 1 阶段利用 Intertwining Logistic 映射产生随机序列, 将其与模拟退火算法相结合构造出置乱序列, 然后对图像进行置乱。第 2 阶段通过 Intertwining Logistic 映射产生随机序列, 先根据随机序列值对图像进行 DNA 编码并选择运算规则, 再进行 DNA 加密计算。算法加密流程如图 2 所示。

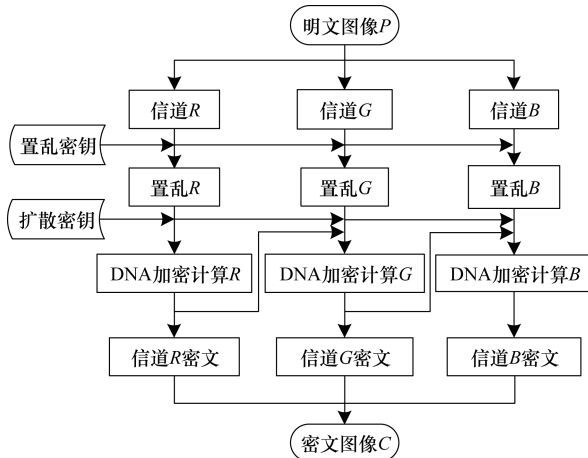


图 2 本文算法加密流程

2.2 图像加密过程

算法的具体执行过程如下所示。

步骤 1 提取大小为 $M \times N$ 的彩色图像 P 的 R 、 G 、 B 信道。针对信道 R , 用置乱密钥 $key_1(x_0, y_0, z_0, k_1, k_2, k_3, \mu, t)$, 其中 t 为混沌映射初值和参数的增量, 根据式(2)生成 $key_1'(x'_0, y'_0, z'_0, k_1, k_2, k_3, \mu)$, 将 key_1' 作为 Intertwining Logistic 映射的初值与参数, 获得 2 个长 $3M$ 的随机序列 r_1, r_2 和长 $3N$ 的随机序列 c_1, c_2 , 利用式(3)分别使其值 $r(i) \in [1, M]$ ($i = 1, 2, \dots, 3M$)、 $c(j) \in [1, N]$ ($j = 1, 2, \dots, 3N$)。同理分别将 $key_1' + t, key_1' + 2t$ 作为混沌初值和参数, 为信道 G, B 产生随机序列。

$$\begin{cases} x'_0 = abs(x_0 - \text{mod}(sumr, 100)) / 1000 \\ y'_0 = abs(y_0 - \text{mod}(sumg, 100)) / 1000 \\ z'_0 = abs(z_0 - \text{mod}(sumb, 100)) / 1000 \end{cases} \quad (2)$$

$$\begin{cases} r(i) = \text{round}(\text{mod}(r(i) \times 1014, M - 1)) + 1 \\ c(j) = \text{round}(\text{mod}(c(j) \times 1014, N - 1)) + 1 \end{cases} \quad (3)$$

式(2)中 $sumr, sumg, sumb$ 分别为各信道像素和。

步骤 2 对于信道 R , 借鉴文献[13]采用模拟退火算法(SA)构造无序序列的方法, 将 r_1, r_2 和 $1, 2, \dots, M$ 作为 SA 输入值, 构造行置乱序列 u_1, u_2, \dots, u_M , 其中 $u_i \in [1, M]$ 。同样用 c_1, c_2 和 $1, 2, \dots, N$ 构造列置乱序列 v_1, v_2, \dots, v_N , 其中 $v_i \in [1, N]$ 。采用相同方法为信道 G 和 B 构造置乱序列。

步骤 3 R 信道中先把第 $1, 2, \dots, M$ 行重新置于第 u_1, u_2, \dots, u_M 行, 再将第 $1, 2, \dots, N$ 列重新置于第 v_1, v_2, \dots, v_N 列, 获取置乱信道 R' 。同理获取信道 G, B 的置乱信道 G', B' 。

步骤 4 由扩散密钥 $key_2(x_0, y_0, z_0, k_1, k_2, k_3, \mu)$ 通过式(2)获取 Intertwining Logistic 映射的初值与参数 $(x'_0, y'_0, z'_0, k_1, k_2, k_3, \mu)$, 然后产生 3 个长 $M \times N$ 的随机序列 LR, LG, LB , 利用式(4)使其值 $l(i) \in [0, 255]$ ($i = 1, 2, \dots, MN$)。将置乱信道 R', G', B' 自左向右、由上而下转化为长 $M \times N$ 的置乱信道序列 PR, PG, PB 。

$$l(i) = \text{floor}(\text{mod}(l(i) \times 1014, 256)) \quad (4)$$

在 DNA 加密计算过程中随机序列与信道序列的 DNA 编码方式和计算规则选取如下所示。

1) DNA 编码。由表 1 可知, DNA 编码有 8 种不同规则, 在 DNA 加密计算中, 由随机序列值 $l(i)$ 根据式(5)确定每个信道序列和随机序列第 i 个值的编码规则 $rule$ 。编码时将随机序列值和信道序列值分别转换为 8 位二进制序列, 再将二进制序列转换为由 4 个碱基组成的 DNA 序列。

$$rule = \text{mod}(l(i), 8) \quad (5)$$

2) 计算规则的选取。本文算法中 DNA 计算公式如式(6)所示, 其中 $P(i)$ 为信道序列第 i 个值的 DNA 序列, $C(i)$ 为 $P(i)$ 的密文 DNA 序列, $C(i-1)$ 为密文对应的前一个密文 DNA 序列, $L(i)$ 为随机序列第 i 个值的 DNA 序列。运算规则 $frule(*, \cdot)$ 定义如表 5 所示, 其中 DNA 运算规则 $frule$ 由 $l(i)$ 根据式(7)确定。

$$C(i) = P(i) \times C(i-1) \cdot L(i) \quad (6)$$

$$frule = \text{mod}(l(i), 9) \quad (7)$$

表 5 DNA 计算规则

$frule$	0	1	2	3	4	5	6	7	8
*	+	\oplus	+	-	+	-	\oplus	-	\oplus
\cdot	\oplus	-	+	+	-	-	+	\oplus	\oplus

步骤 5 由式(8)获得 $sumc_0$, 根据其值利用式(5)将其编码为初始 DNA 密文 C_0 。将 C_0 作为 PR 初始密文 $CR(0)$, 依次先根据 LR 的元素 $LR(i)$ 把 $PR(i)$ 和 $LR(i)$ 编码成长为 4 的 DNA 序列并选取运算规则, 再利用式(6)进行 DNA 加密计算获取 $CR(i)$, 最后获得长 $M \times N \times 4$ 的 PR 密文 DNA 序列 CR , 其中, $i = 1, 2, \dots, MN$ 。将 $CR(MN)$ 作为 PG 初始密文, 进而获得 CG ; 然后将 $CG(MN)$ 作为 PB 初

始密文,计算 CB 。

$$\text{sum}c_0 = \text{mod}((\text{sum}r + \text{sum}g + \text{sum}b), 256) \quad (8)$$

步骤 6 将 3 个密文序列根据对应随机序列值利用式(5)选择编码规则进行解码,然后转换为 3 个 $M \times N$ 的密文矩阵,合并 3 个矩阵得到密文图像 C 。

2.3 图像解密过程

解密算法为加密算法的逆,具体过程如下:

步骤 1 使用扩散密钥获取随机序列 LR 、 LG 、 LB ,利用式(4)使其值 $l(i) \in [0, 255]$ ($i = 1, 2, \dots, MN$)。再将密文图像 C 各信道转化为长 $M \times N$ 的一维密文信道序列。

步骤 2 每个密文信道序列和随机序列的每个值依次根据 $l(i)$ 编码为 DNA 序列,再用 $l(i)$ 选取的计算规则利用式(6)的逆运算获取每个密文信道中每个密文的明文 DNA 序列。各密文信道序列计算完成后分别得到长度为 $M \times N \times 4$ 的明文 DNA 序列。

步骤 3 根据 $l(i)$ 选取编码规则将 3 个明文 DNA 序列解码为长 $M \times N$ 的一维置乱信道序列 PR 、 PG 、 PB ,再将其转化为 $M \times N$ 的二维置乱信道 R' 、 G' 、 B' 。

步骤 4 运用置乱密钥获取随机序列,然后采用 SA 构造行列置乱序列,将 R' 、 G' 、 B' 行和列的位置根据置乱序列反向重排列,从而得到恢复像素 R 、 G 、 B 。最后合并 R 、 G 、 B 信道得到解密后的原始图像 P 。

3 仿真实验

在 Windows7 64 位系统环境下使用 MATLAB 软件,运用本文算法对标准 512 像素 \times 512 像素的 Lena. bmp 和 Baboon. bmp 彩色图像进行加密和解密。选用的密钥如表 6 所示,实验结果如图 3 所示。

表 6 加密和解密密钥

密钥	x_0	y_0	z_0	k_1	k_2	k_3	μ	t
key_1	0.23	0.35	0.85	33.8	38.1	36.5	2.33	$1e-5$
key_2	0.47	0.29	0.12	34.7	45.1	46.8	0.13	—

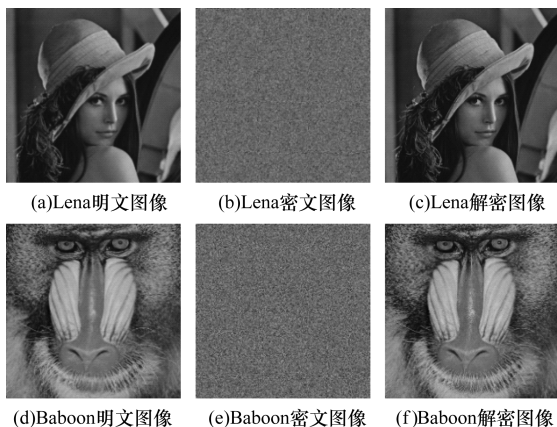


图 3 加密解密效果

通过观察图 3 可以看出加密后的图像没有显示任何明文信息。通过比较原始图像图 3(a)、图 3(d)和解密图像图 3(c)、图 3(f)的所有像素点可知,2 个图像像素点的值完全相同,说明本文提出的算法在加密和解密过程中没有丢失图像的任何信息。

4 安全性分析

4.1 密钥空间

本文算法的密钥由 Intertwining Logistic 映射在 2 个加密阶段的初始值及参数和 t 组成,即表 6 所示的置乱密钥 key_1 和扩散密钥 key_2 。根据文献[14]和 IEEE Standard 754-2008 存储密钥采用的类型为双精度浮点型,其使用 8 Byte 对数据进行存储,密钥精度为 10^{-15} ,因此,本文算法密钥长度为 960 bit,密钥空间可达 $2^{960} \approx 9.75 \times 10^{288}$ 。由文献[15]可知本文的密钥空间可以很好地抵抗各种类型的穷举攻击并且提高加密系统的安全性。

4.2 密钥敏感性

对表 6 所示的密钥 key_1 、 key_2 ,在此仅仅将 key_2 中的 μ 做一个微小的改变,即 $\mu = \mu + 10^{-15}$,其余密钥保持不变得到一个改变后的密钥 key_2' ,然后用 key_1 、 key_2' 对 key_1 、 key_2 加密的图像进行解密。图 4 给出了 key_1 、 key_2 和 key_1 、 key_2' 的解密结果,从图中可以看出 key_1 、 key_2' 无法正确解密密文图像,说明本文算法对密钥具有极强的敏感性。

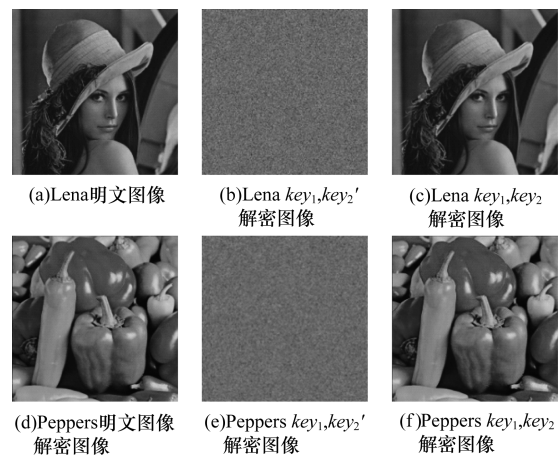


图 4 密钥敏感性分析

4.3 相邻像素相关性分析

随机选取 Lena 和 Baboon 的 R 、 G 、 B 信道明文和密文图像中 5 000 对相邻像素点,分别进行水平、垂直、对角 3 个方向的相关性统计测试,测试结果如表 7 所示。

表 7 明文、密文图像 R、G、B 信道的相关性系数

图像类型	信道	水平方向	垂直方向	对角方向
Lena 明文图像	R	0.979 7	0.977 4	0.963 2
	G	0.971 6	0.961 7	0.945 1
	B	0.949 6	0.938 9	0.921 6
Lena 密文图像	R	-0.013 1	0.014 2	-0.004 4
	G	-0.000 7	-0.016 7	-0.014 5
	B	-0.003 6	-0.008 3	0.021 4
Baboon 明文图像	R	0.864 7	0.922 9	0.850 7
	G	0.754 4	0.864 2	0.732 4
	B	0.881 1	0.906 7	0.840 6
Baboon 密文图像	R	-0.006 4	-0.004 9	0.014 6
	G	-0.008 8	-0.002 5	0.020 5
	B	-0.009 6	-0.013 5	0.000 2

相关性计算公式如下:

$$r_{xy} = \frac{\text{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad (9)$$

$$\text{cov}(x,y) = \frac{1}{N} \sum_{i=1}^N E(x - E(x))(y - E(y)) \quad (10)$$

$$D(x) = \frac{1}{N} \sum_{i=1}^N (x_i - E(x))^2 \quad (11)$$

$$E(x) = \frac{1}{N} \sum_{i=1}^N x_i \quad (12)$$

从表 7 可以看出, Lena 和 Baboon 的明文图像相关系数均接近于 1, 密文图像相关性系数均接近于 0。其中 Lena 图像中选取的水平方向上 5 000 对相邻像素点分布情况如图 5 所示。

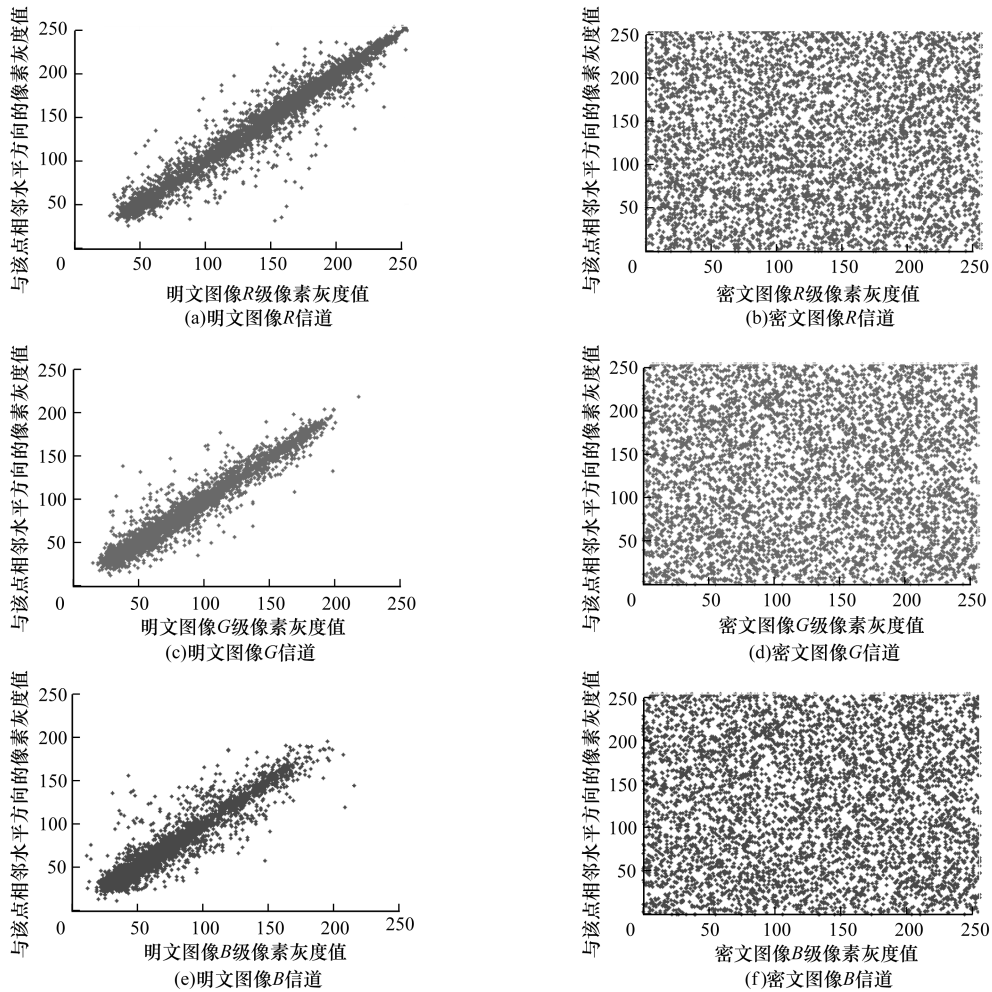


图 5 Lena 水平方向相邻像素相关性分析

可以看出, 明文图像相邻像素点连续分布, 密文图像相邻像素点值随机分布且布满整个二维空间。由以上可知, 密文图像已基本消除了相邻像素的相关性且掩盖了原始图像的数据特征。

4.4 直方图分析

图 6 为 Lena 图像 R、G、B 信道的明文和密文频

率直方图, 其中图 6(a)、图 6(c)、图 6(e) 分别是明文图像直方图, 图 6(b)、图 6(d)、图 6(f) 分别是密文图像直方图。通过比较直方图能够发现, 明文图像的像素值都集中在一些值上, 而密文图像的像素值是均匀分布的, 这些均匀分布的密文像素值能够较好的抵抗统计攻击。

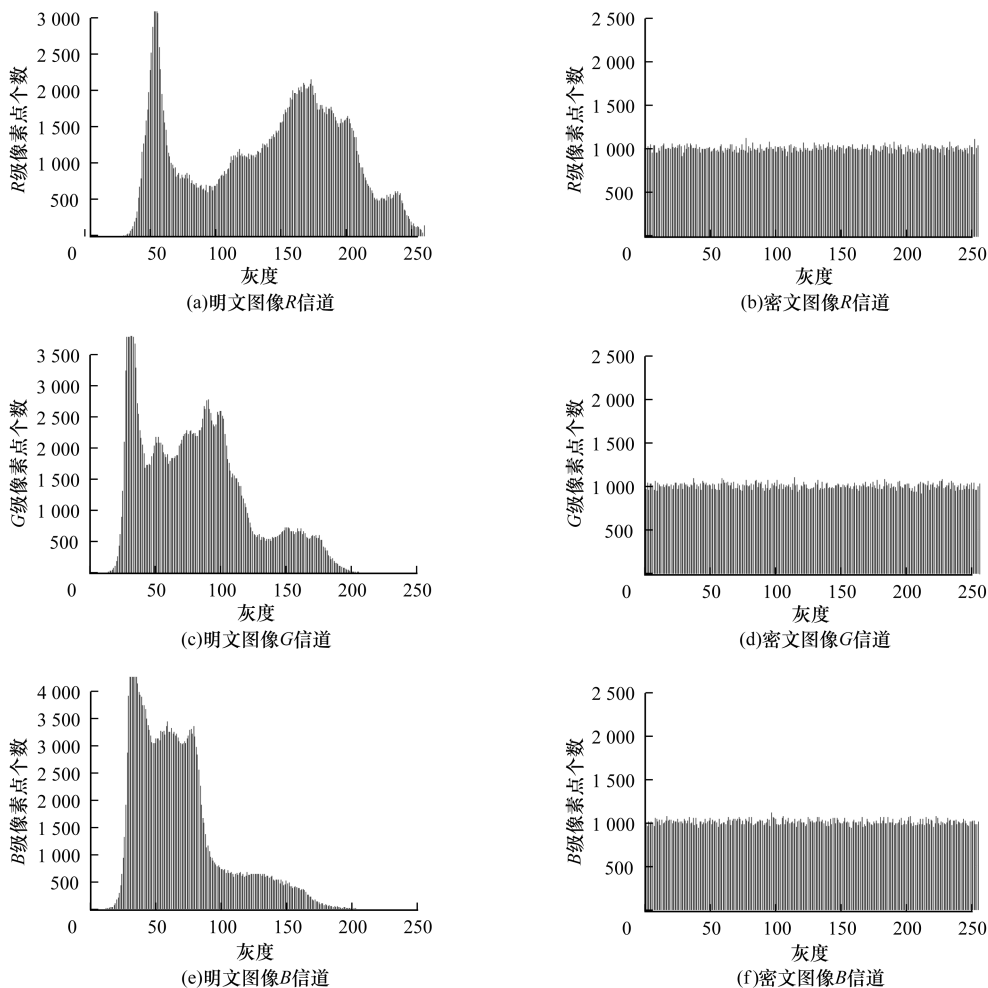


图6 Lena 图像直方图

4.5 信息熵分析

信息熵可以判断元素的随机性,图像信源的熵值越接近8,图像信息的随机性就越强。对 Lena 密文图像的每个信道计算信息熵结果见表8,计算公式如下:

$$H(s) = \sum_{i=0}^{2^L-1} p(s_i) \text{lb} \frac{1}{p(s_i)} \quad (13)$$

表8 Lena 密文 R、G、B 信道图像信息熵

算法	Red	Green	Blue
本文算法	7.991 7	7.991 6	7.991 7
文献[16]	7.988 1	7.989 8	7.985 4
文献[17]	7.991 3	7.991 4	7.991 6

由表8可以看出,本文算法加密后图像的信息熵均接近8,与文献[16-17]相比本文具有更大的熵值,因此,证明本文算法加密后密文中各像素点值具有更强的随机性,能有效地抵御熵攻击。

4.6 抗差分攻击能力分析

加密算法抗差分攻击的能力可以用像素数改变率 NPCR(Number of Pixels Change Rate)和归一化像素值平均改变强度 UACI(Unified Average Changing Intensity)

来度量,计算公式如下:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\% \quad (14)$$

$$D(i,j) = \begin{cases} 0, & C(i,j) = C'(i,j) \\ 1, & C(i,j) \neq C'(i,j) \end{cases} \quad (15)$$

$$UACI = \frac{\sum_{i=1}^M \sum_{j=1}^N \frac{|c(i,j) - c'(i,j)|}{255}}{M \times N} \times 100\% \quad (16)$$

在 Lena 明文图像中随机选择一个像素,改变其像素值,根据式(14)~式(16)进行100组的实验后,计算得到 NPCR 和 UACI 的平均值如表9所示,表中也展示了其他彩色图像加密算法的实验结果。

表9 NPCR 与 UACI 度量数据

度量项目	信道	本文算法	文献[17]算法	文献[18]算法
NPCR	R	0.996 3	0.996 0	0.996 6
	G	0.996 3	0.995 9	0.995 9
	B	0.995 6	0.995 9	0.995 6
UACI	R	0.334 3	0.334 4	0.333 1
	G	0.336 4	0.334 6	0.334 7
	B	0.335 8	0.334 7	0.334 2

由表9可以看出,本文算法各分量的NPCR均超过0.99,UACI均超过0.33,且与文献[17-18]对比可以看出,本文总体上具有更大的NPCR和UACI,可知本文算法具有良好的抗差分攻击能力。

4.7 已知明文和选择明文攻击

在已知明文和选择明文攻击中,攻击者通常会 对明文图像做一些微小的改变并观察相应的密文图像或者选择特殊的明文图像(比如各像素点都相同的明文图像)进行加密来获取密钥信息。通过实验可以看出本文算法对明文极其敏感,任意改变明文图像一个像素将获得几乎完全不同的密文图像。在加密过程中,步骤1和步骤4采用式(2)利用初始密钥和明文图像重新计算了混沌映射的初值,因此攻击者使用特殊明文获取的密钥对于其他已加密的明文图像来说是无效的。另外,在步骤5中初始密文DNA序列也由明文图像确定,不同的明文图像生成不同的初始序列。

本文算法在步骤5中运用式(6)计算密文 $C(i)$ 时 $P(i)$ 和 $L(i)$ 的DNA编码及采用的计算规则都是动态变化的,当明文发生变化时加密过程中所采用的编码规则和计算规则也相应发生变化。在DNA加密计算过程中还采用了密文反馈机制,一方面计算每个像素点密文时会受到前面所有密文的影响,另一方面使得明文图像各信道在加密过程中互相影响。

因此,通过采取以上措施,本文算法抵抗已知明文和选择明文攻击的能力得到了有效提高。

5 结束语

本文提出一种结合Intertwining Logistic映射和动态DNA编码与运算的图像加密算法。首先在对明文图像置乱和扩散过程中使密文与密钥、明文的关系复杂化,并且2个阶段的密钥都依赖于明文,增强算法对明文的敏感性。其次在DNA计算中编码规则和运算规则的动态变化提高了算法抵抗已知明文和选择明文及穷举攻击的能力。在加密过程中,2个阶段都融合了混沌系统的随机性,并且扩散阶段在彩色图像 R 、 G 、 B 各信道内及信道间还采用了密文反馈机制,有效增强了算法的安全性和可靠性。通过安全性分析可以看出,该算法密钥空间大,对图像置乱扩散效果良好,能够抵抗常见的攻击。下一步将在实际应用中进一步优化时间复杂度,提高运行速度。

参考文献

- [1] ZHANG Xuanping, ZHAO Zhongmeng. Chaos-based Image Encryption with Total Shuffling and Bidirectional Diffusion[J]. Nonlinear Dynamics, 2014, 75(1/2): 319-330.
- [2] 朱从旭, 李力, 陈志刚. 基于多维混沌系统组合的图像加密新算法[J]. 计算机工程, 2007, 33(2): 142-144.
- [3] MOLLAEFAR M, SHARIF A, NAZAR M. A Novel Encryption Scheme for Colored Image Based on High Level Chaotic Maps[J]. Multimedia Tools & Applications, 2017, 76: 1-23.
- [4] JENG Fuhgwo, HUANG Weilun, CHEN Tzungheer. Cryptanalysis and Improvement of Two Hyper-chaos-based Image Encryption Schemes[J]. Signal Processing: Image Communication, 2015, 34: 45-51.
- [5] XIAO Di, LIAO Xiaofeng, WEI Pengcheng. Analysis and Improvement of a Chaos-based Image Encryption Algorithm[J]. Chaos Solitons & Fractals, 2009, 40(5): 2191-2199.
- [6] ADLEMAN L. Molecular Computation of Solutions to Combinatorial Problems[J]. Science, 1994, 266(5187): 1020-1024.
- [7] HUANG Xiaoling, YE Guodong. An Image Encryption Algorithm Based on Hyper-chaos and DNA Sequence[J]. Multimedia Tools & Applications, 2014, 72(1): 57-70.
- [8] SONI A, KUMAR A A. A Novel Image Encryption Approach Using an Index Based Chaos and DNA Encoding and Its Performance Analysis[J]. International Journal of Computer Applications, 2012, 47(23): 1-6.
- [9] BELAZI A, HERMASSI H, RHOUMA R, et al. Algebraic Analysis of a RGB Image Encryption Algorithm Based on DNA Encoding and Chaotic Map[J]. Nonlinear Dynamics, 2014, 76(4): 1989-2004.
- [10] OZKAYNAK 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.
- [11] SHATHEESH S I, DEVARAJ P, BHUVANESWARAN R S. An Intertwining Chaotic Maps Based Image Encryption Scheme[J]. Nonlinear Dynamics, 2012, 69(4): 1995-2007.
- [12] WATSON J D, CRICK F H. Molecular Structure of Nucleic Acids[J]. Nature, 1953, 171(25): 737-738.
- [13] WANG Xingyuan, LIU Chuanming, Xu Dahai, et al. Image Encryption Scheme Using Chaos and Simulated Annealing Algorithm [J]. Nonlinear Dynamics, 2016, 84(3): 1417-1429.
- [14] BORIGA R, DASCALESCU A C, DIACONU A. A New One-dimensional Chaotic Map and Its Use in a Novel Real-time Image Encryption Scheme [J]. Advances in Multimedia, 2014(7): 1-15.
- [15] NOROUZ B, SEYEDZADEH S M, MIRZAKUCHAKI S, et al. A Novel Image Encryption Based on Row-column, Masking and Main Diffusion Processes with Hyper Chaos[J]. Multimedia Tools and Applications, 2015, 74(3): 781-811.
- [16] LIU Shubo, SUN Jing, XU Zhengquan. An Improved Image Encryption Algorithm Based on Chaotic System [J]. Journal of Computers, 2009, 4(11): 1091-1100.
- [17] KADIR A, AILI M, SATTAR M. Color Image Encryption Scheme Using Coupled Hyper Chaotic System with Multiple Impulse Injections [J]. Optik International Journal for Light and Electron Optics, 2017, 129: 231-238.
- [18] TONG Xiaojun, CUI Minggen. Image Encryption Scheme Based on 3D Baker with Dynamical Compound Chaotic Sequence Cipher Generator [J]. Signal Processing, 2009, 89(4): 480-491.