

引用格式:王锬,张雪锋,姜文.一种基于 DNA 编码和比特置乱的彩色图像加密算法[J].微电子学与计算机,2021,38(3):33-38. [WANG K, ZHANG X F, JIANG W. A color image encryption algorithm based on DNA encoding and bit-level permutation [J]. Microelectronics & Computer,2021,38(3):33-38.]

一种基于 DNA 编码和比特置乱的彩色图像加密算法

王 锬¹,张雪锋¹,姜 文²

(1 西安邮电大学 网络空间安全,陕西 西安 710061;
2 国家计算机网络应急技术处理协调中心,北京 100029)

摘 要:针对目前彩色图像加密方案存在的效果差、安全性低等问题,提出了一种基于 DNA 编码和比特级置乱的彩色图像加密算法.该算法通过对选取 DNA 编码规则的均匀程度进行评价,使 DNA 的 8 种编码规则可以随机并且更加均匀的被选取.首先基于比特级置乱规则对彩色图像进行预处理;再使用 DNA 编码和循环移位的方式改变 RGB 平面本身的统计信息;最后使用 S 盒对 DNA 译码后的像素值进行非线性替换.理论分析和仿真结果表明,算法可以提供更大的密钥空间,密文图像也具有更高的信息熵,具有良好的安全性.

关键词:熵;比特置乱;DNA 编码;彩色图像加密

中图分类号: TP309.7 **文献标识码:** A **文章编号:** 1000—7180(2021)03—0033—06

A color image encryption algorithm based on DNA encoding and bit-level permutation

WANG Kun¹, ZHANG Xue-feng¹, JIANG Wen²

(1 School of Cyberspace Security, Xi'an University of Post & Telecommunications, Xi'an 710061, China;
2 National Internet Emergency Center, Beijing 100029, China)

Abstract: A color image encryption algorithm based on DNA coding and bit-level scrambling is proposed to solve the problems of poor effect and low security in the current color image encryption schemes. Firstly, the color image is preprocessed based on bite-level scrambling rules. Then the statistical information of the RGB plane itself was changed by means of DNA coding and cyclic shift. Finally, S-box is used for nonlinear replacement of pixel values after DNA decoding. Theoretical analysis and simulation results show that the algorithm can provide a larger key space, the cipher image also has higher information entropy, and has good security.

Key words: entropy; bit-level permutation; DNA encoding; color image encryption

1 引言

随着互联网和通信行业的快速发展,信息安全也越来越受关注,由此很多数据加密算法被提出,并被大量使用,例如 AES 算法,DES 算法等,由于人在生活中所获得的信息大部分来自于视觉,图像就成为了人类生活活动中最常见的信息载体.高辨

率的图像越来越受人们的欢迎,使得数字图像具有数据量大,冗余度高,像素之间相关性强等特征,传统的数据加密算法不适用于数字图像加密^[1-2],为防止图像信息泄露,人们提出了很多不同的加密算法文献[3-6],其目的是将有意义的原始图像转换为无法识别或类似噪声的密文图像,从而达到对原始图像进行保护的效果.例如,在图像加密算法中,人们

提出了很多位级的图像加密算法. 因为与像素级置乱相比, 比特置乱的优点是可以同时改变像素位置和像素值, 而且具有较好的加密效果. 文献[4]的置换过程中利用广义 Arnold 映射生成的随机序列对彩色图像的三维位矩阵进行置乱, 再用交叉方式对置乱后的三个平面分量进行扩散, 性能分析表明加密方案是安全有效的. 而近年来, 基于 DNA 的图像加密方案越来越受研究者的关注, 因为 DNA 技术具有并行性高、存储量大、功耗低的特点, 同时还可以在 DNA 碱基之间进行操作. 所以很多研究者将混沌系统和 DNA 编码结合. 文献[5]采用了一种跨信道操作的图像加密方案, 采用 DNA 减法和异或运算对普通图像的红、绿、蓝信道进行交叉操作, 提高普通图像的随机性. 在文献[6]中, 作者对产生的混沌序列进行 8 等分, 来产生 DNA 编码规则, 但是这样产生的编码序列存在缺点. 因为混沌序列分布不均匀的问题会导致选取 DNA 编码规则的次数相差较大的现象, 使得攻击者可以通过统计分析很容易获得一些与原始图像相关并且有用的信息.

本文将结合文献[7]提出的混沌系统提出了一种基于 DNA 编码和比特置乱的彩色图像加密算法. 本文对选取 DNA 编码规则不均的现象进行评价, 并且提出改进方案. 在加密过程中, 首先对原始图像进行预处理. 按照本文设计的比特置乱规则, 在彩色图像的 RGB 三个平面之间进行比特置乱操作, 可以增加密文图像的敏感性; 其次在 DAN 的编码和译码操作中设置不同的系统参数, 对图像进行加密操作; 再次, 在 DNA 编码后使用循环移位, 该操作可以把一个平面的 DNA 碱基置换到其他平面中, 从而改变每个平面中自身的统计信息(比特置乱也具有相同的作用); 最后使用 S 盒^[8]对像素值进行替换. 实验结果和仿真结果表明, 该方案可以有效的对彩色图像进行加密并且可以抵抗攻击.

2 理论基础

2.1 混沌系统

混沌映射对初始值非常敏感, 在这类函数中, 如果初始值发生轻微的变化, 也会使产生的混沌序列与之前的序列有完全不同的差异. 很多研究者构造出了很多不同类型的混沌映射.

(1)Logistic-Tent system^[7]是一个增强的一维混沌系统, 它结合了两个著名的种子映射, 即 logistic 映射和 tent 映射, 它的定义式为:

$$X_{n+1} =$$

$$\begin{cases} (rX_n(1-X_n)+(4-r)X_n/2)\bmod 1 & X_i < 0.5 \\ (rX_n(1-X_n)+(4-r)(1-X_n)/2)\bmod 1 & X_i \geq 0.5 \end{cases} \quad (1)$$

式中, 控制参数 $r \in (0, 4]$, 初始值 $x_n \in [0, 1]$, 在控制参数的范围内, Lyapunov 指数均大于零, 即在 $(0, 4]$ 范围内系统均为混沌.

(2)Logistic-Sine system^[7]是一个增强的一维混沌系统, 它结合了两个著名的种子映射, 即 logistic 映射和 Sine 映射, 它的定义式为:

$$X_{n+1} = (rX_n(1-X_n)+(4-r)\sin(\pi X_n)/4)\bmod 1 \quad (2)$$

式中, 控制参数 $r \in (0, 4]$, 初始值 $x_n \in [0, 1]$, 在控制参数的范围内, Lyapunov 指数均大于零, 即在 $(0, 4]$ 范围内系统均为混沌.

(3)Tent-Sine system^[7]是一个增强的一维混沌系统, 它结合了两个著名的种子映射, 即 Tent 映射和 Sine 映射, 它的定义式为:

$$X_{n+1} = \begin{cases} (rX_n/2+(4-r)\sin(\pi X_n)/4)\bmod 1 & X_i < 0.5 \\ (r(1-X_n)/2+(4-r)\sin(\pi X_n)/4)\bmod 1 & X_i \geq 0.5 \end{cases} \quad (3)$$

式中, 控制参数 $r \in (0, 4]$, 初始值 $x_n \in [0, 1]$, 在控制参数的范围内, Lyapunov 指数均大于零, 即在 $(0, 4]$ 范围内系统均为混沌.

2.2 DNA 编码和译码规则

一个 DNA 序列包含四种核酸碱基, 它们是 A (腺嘌呤), C(胞嘧啶), G(鸟嘌呤), T(胸腺嘧啶). 每种碱基分别与另一种碱基的化学性质完全互补. 依据碱基互补配对原则, A 总与 T 配对, G 总与 C 配对. 通常, 四个 DNA 碱基 ACGT 分别通过 00, 01, 10, 11 进行编码, 所以一共有 24 种编码方式. 但是满足沃森-克里克补充规则的只有 8 种编码方式, 如表 1 所示.

表 1 DNA 编码和译码规则

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

在 DNA 图像加密中, 像素的灰度值可以表示为相应的 8 位二进制序列, 通过编码规则可以将 8 位二进制序列编码成 DNA 序列. 相反, 通过编码规则也可以将 DNA 序列翻译成像素值, 选取不同的解码规则会将 DNA 序列翻译成不同的二进制序

列.例如:当图像的像素值为 180,其二进制序列是 10 110 100,在 DNA 编码过程中利用 DNA 编码规则 6 进行编码,得到的 DNA 碱基序列是 ACTG.在 DNA 译码过程中,DNA 译码规则是逆向的编码规则,利用规则 6 译码 DNA 序列就可以对原像素进行解密;使用规则 2 对其进行解码,则会获得另一个二进制序列 00 100 111,即可加密像素值.

3 彩色图像加密算法

3.1 信息熵评价

在使用混沌序列选取 8 种编码规则时,应尽可能地使编码规则能均匀的被选取.然而,文献[6]在选取 DNA 编码规则方面存在缺点,因为一些混沌系统会产生不均匀的混沌序列,如果将初始值

表 2 DNA 编码规则的数量和熵值

	1	2	3	4	5	6	7	8	熵
本文算法	131 072	131 072	131 072	131 072	131 072	131 072	131 072	131 072	3
文献[6]	244 031	109 381	90 534	84 539	84 078	90 083	107 576	238 354	2.846 605 82

3.2 图像的预处理

在图像加密之前对图像进行比特置乱,通过比特置乱可以改变像素值的大小.该过程将通过混沌系统产生的混沌序列选取比特置乱规则.RGB 平面中的像素的置换过程细节如下:首先,将 RGB 平面的每个像素值的 8 位二进制分成高 4 位和低 4 位.然后根据表 3,对彩色图像的 RGB 平面的像素进行比特级的交叉置乱,详细的操作步骤:先按照置乱规则将 RGB 的低 4 位交叉放在 RGB 的高 4 位,然后将 RGB 的高 4 位交叉放在 RGB 的低 4 位,最终完成 RGB 平面之间的比特置乱.例如,在 RGB 平面分别选取一个像素值,R 平面选取 10 010 100;G 平面选取 10 110 101;B 平面选取 10 100 110,使用规则 4 置换 RGB 的高 4 位,用规则 3 置换 RGB 的低 4 位.最终会使 R 平面的像素值转换为 01 101 001;G 平面的像素值转换为 01 000 110;B 平面的像素值转换为 01 010 101.

表 3 RGB 之间的比特置乱规则

规则	1	2	3	4	5	6
R	R	R	G	G	B	B
G	G	B	R	B	G	R
B	B	G	B	R	R	G

3.3 循环移位

在循环移位阶段输入大小为 $m \times 4n$ 的矩阵.对矩阵进行循环移位的步骤由两部分组成:行循环移

的取值范围直接进行 8 等分会使一些编码规则被选取的较多,一些编码规则将被选取的较少,也就是说,这种方式会使 DNA 编码规则不能近似均匀的被利用.为了对这种情况进行评价,本文将使用信息熵评价选取 DNA 编码规则的均匀程度.例如,编码的图像大小是 256×256 ,因此对原始图像编码后有 1 048 576 个 DNA 碱基,相应的选用 1 048 576 个 DNA 编码规则,理想情况下在均匀选取 DNA 编码规则后,每种选取的规则占总数的 12.5%,所以选取 DNA 编码规则的熵值的理想值为 3.当熵值越接近 3,选取的 DNA 编码规则分布的越均匀.表 2 将文献[6]和本文的方法进行了比较.从表中可以看出本方案在选取 DNA 编码规则时可以更加均匀.

位和列循环移位.具体步骤如下:

步骤 1:为减少加密步骤并充分利用混沌序列,使用 TSS 混沌系统产生序列.设定混沌系统 TSS 的初始值和控制参数 (x_0, r_0) 作为加密系统的密钥,并将混沌迭代 $1\,000 + 2 \times (m + 4n)$ 次,为了避免瞬态效应,舍去前 1 000 个数.即产生长度为 $2 \times (m + 4n)$ 的序列 $x, X = \{x_0, x_1, \dots, x_m\}, Y = \{x_{m+1}, x_{m+2}, \dots, x_{2m}\}, Z = \{x_{2m+1}, x_{2m+2}, \dots, x_{2m+4n}\}, W = \{x_{2m+4n+1}, x_{2m+4n+2}, \dots, x_{2m+8n}\}$.

步骤 2:根据等式(4)和(5)对序列进行修改:

$$\begin{cases} X' = \text{floor}(X \times 10^{-15}) \bmod 2 \\ Y' = \text{floor}(Y \times 10^{-15}) \bmod (\frac{n \times 4 \times 3}{2}) \end{cases} \quad (4)$$

$$\begin{cases} Z' = \text{floor}(Z \times 10^{-15}) \bmod 2 \\ W' = \text{floor}(W \times 10^{-15}) \bmod (\frac{3 \times m}{2}) \end{cases} \quad (5)$$

式中, x_i 是序列 x 中的元素,在完成步骤 2 之后,获得四个序列,分别是 X', Y', Z', W' .

步骤 3:对矩阵进行行置换.首先将 RGB 三个平面放成一行,即生成矩阵 $P_1 = [R \ G \ B]$,其大小为 $[m, 3 \times 4n]$,对矩阵 P_1 的第 $i (i = 1, 2, \dots, m)$ 行进行行置换.用 X' 中的数决定左循环还是右循环,用 Y' 中的数决定移动位置数.所有行都被置换后,获得新的矩阵 $P_2 = [R' \ G' \ B']$.

步骤 4:对矩阵进行列置换.首先将 R', G' 和 B'

三个平面放成一列,即生成矩阵 $\mathbf{P}_3 = \begin{bmatrix} R' \\ G' \\ B' \end{bmatrix}$,其大小

为 $[3m, 4n]$,对矩阵 $\mathbf{P}_3$ 的第 j ($j = 1, 2, \dots, 4n$) 列进行列置换. 用 Z' 中的数决定左循环还是右循环,用 W' 中的数决定移动位置数. 所有列都被置换后,获

得新的矩阵 $\mathbf{P}_4 = \begin{bmatrix} R'' \\ G'' \\ B'' \end{bmatrix}$,置换结束.

步骤 5:将矩阵 R'', G'' 和 B'' 进行合并,得到矩阵 $\mathbf{P}_5$.

3.4 DNA 编码和译码

DNA 编码阶段输入的图像被转换为 8 位二进制值,其中图像的大小是 $[m, n]$,并对每两个元素进行分组,得到矩阵 $\mathbf{P}_6$,其大小为 $[m, 4n]$. 对图像的 DNA 编码和译码的详细步骤如下.

(1)DNA 编码

将 LSS 混沌系统迭代 $1\,000 + m \times 4n$ 次,产生 $1\,000 + m \times 4n$ 个数,舍弃前 1 000 个数,获得混沌序列 $\mathbf{A}$. 然后将 $\mathbf{A}$ 转变成 $[m, 4n]$ 的矩阵 $\mathbf{M}$. 为了对矩阵 $\mathbf{P}_6$ 进行编码,需要将 $\mathbf{M}$ 矩阵转换成编码规则,编码规则生成步骤如下:

步骤 1:将序列 $\mathbf{A}$ 分别从小到大进行排列.

步骤 2:将排列后的序列等分成 8 段.

步骤 3:对每一段的最后一个值进行记录,得到 8 个值: $a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8$.

通过公式(6)得到编码矩阵 $\mathbf{CM}$ 为:

$$\mathbf{CM}(i, j) = \begin{cases} 1 & 0 < \mathbf{M}(i, j) \leq a_1; \\ 2 & a_1 < \mathbf{M}(i, j) \leq a_2; \\ 3 & a_2 < \mathbf{M}(i, j) \leq a_3; \\ 4 & a_3 < \mathbf{M}(i, j) \leq a_4; \\ 5 & a_4 < \mathbf{M}(i, j) \leq a_5; \\ 6 & a_5 < \mathbf{M}(i, j) \leq a_6; \\ 7 & a_6 < \mathbf{M}(i, j) \leq a_7; \\ 8 & a_7 < \mathbf{M}(i, j) \leq a_8; \end{cases} \quad (6)$$

式中, $\mathbf{M}(i, j)$ 和 $\mathbf{CM}(i, j)$ 分别表示位于矩阵 $\mathbf{M}$ 和 $\mathbf{CM}$ 的第 i 行,第 j 列元素,且 $1 \leq i \leq m, 1 \leq j \leq 4n$.

根据 DNA 编码规则表,用矩阵 $\mathbf{CM}$ 对平面进行编码,得到 DNA 碱基矩阵 $\mathbf{T}_1$.

(2)DNA 译码

和 DNA 编码类似,将 LSS 系统迭代 $1\,000 + m \times 4n$ 次,舍弃前 1 000 个数,将长度为 $m \times 4n$ 的序列转换成大小为 $m \times 4n$ 的矩阵 $\mathbf{T}_2$,按照公式(6)对混沌数进行处理,生成 DNA 编码规则矩阵,最后按照

DNA 编码表对矩阵 $\mathbf{T}_2$ 进行译码.

3.5 加密过程

加密算法的细节如下:

步骤 1:输入原始图像 $P[m, n]$, m 和 n 分别表示图像的高度和宽度. 将原始图像 P 分成 R, G 和 B 分量.

步骤 2:将 R, G 和 B 分别转换成 8 位二进制,并对每 4 个元素进行分组,得到矩阵 $\mathbf{R}_1[m, 2n], \mathbf{G}_1[m, 2n]$ 和 $\mathbf{B}_1[m, n]$.

步骤 3:产生比特置乱规则. 将 TLS 混沌系统迭代 $1\,000 + m \times 2n$ 次,舍弃前 1 000 个数. 将长度为 $m \times 2n$ 的序列转换成矩阵 $\mathbf{T}_1[m \times 2n]$,然后由公式(7)确定比特置乱规则.

$$\text{rule} = \text{mod}(\text{floor}(x \times 10^{15}), 6) + 1 \quad (7)$$

式中, rule 是比特置乱规则, x 是混沌系统 LTS 产生随机数.

步骤 4:通过比特置乱对图像进行预处理. 如第 3.2 节所述,使用比特置乱规则(表 3)对 $\mathbf{R}_1, \mathbf{G}_1$ 和 $\mathbf{B}_1$ 进行比特置乱,再将像素的高 4 位和低 4 位进行合并得到矩阵 $\mathbf{R}_2[m, 8n], \mathbf{G}_2[m, 8n]$ 和 $\mathbf{B}_2[m, 8n]$.

步骤 5:编码. 设定初始密钥 $(x_1, r_1), (x_2, r_2)$ 和 (x_3, r_3) ,如 2.4 节所述,分别对 $\mathbf{R}_2, \mathbf{G}_2$ 和 $\mathbf{B}_2$ 进行 DNA 编码,得到 DNA 编码矩阵 $\mathbf{R}_3[m, 4n], \mathbf{G}_3[m, 4n]$ 和 $\mathbf{B}_3[m, 4n]$.

步骤 6:循环移位. 设定初始密钥 (x_4, r_4) ,如 3.3 节所述,对 $\mathbf{R}_3, \mathbf{G}_3$ 和 $\mathbf{B}_3$ 进行循环移位,得到矩阵 $\mathbf{R}_4[m, 4n], \mathbf{G}_4[m, 4n]$ 和 $\mathbf{B}_4[m, 4n]$.

步骤 7:译码. 设定初始密钥 $(x_5, r_5), (x_6, r_6)$ 和 (x_7, r_7) . 如 2.4 节所述生成 DNA 译码规则,并且对 $\mathbf{R}_4, \mathbf{G}_4$ 和 $\mathbf{B}_4$ 进行译码,得到矩阵 $\mathbf{R}_5[m, n], \mathbf{G}_5[m, n]$ 和 $\mathbf{B}_5[m, n]$.

步骤 8:S 盒替换. 将使用文献[8]中建议的 S 盒对 $\mathbf{R}_5, \mathbf{G}_5$ 和 $\mathbf{B}_5$ 中的像素值进行替换,将获得三个新的矩阵 $\mathbf{R}_6, \mathbf{G}_6$ 和 $\mathbf{B}_6$.

步骤 9:最后合并 $\mathbf{R}_6, \mathbf{G}_6$ 和 $\mathbf{B}_6$,生成最终的密文图像. 并且再重复一次加密过程. 加密流程如图 1 所示. 解密过程即加密过程的逆过程.

4 性能分析

4.1 密钥空间分析

一个好的图像加密算法应该有大的密钥空间用来抵抗暴力破解. 密钥空间越大,可能出现的密钥数量就越多. 密钥空间的大小是由密钥的长度决定的,该加密系统的密钥精度为 10^{15} . 其中 x_1, x_2, x_3 ,

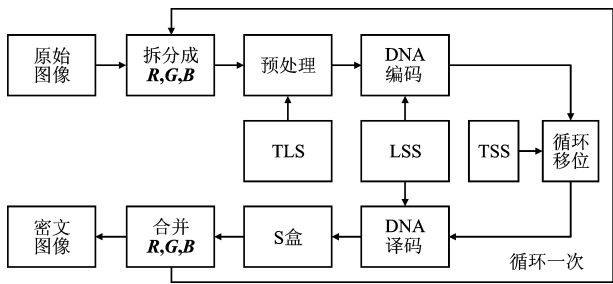


图 1 加密算法流程图

x_4, x_5, x_6 和 x_7 的取值范围是 $[0,1]$,其密钥空间是 10105 . $r_1, r_2, r_3, r_4, r_5, r_6$ 和 r_7 的取值范围是 $(0,4]$,其密钥空间是 $1.638\ 4\times10^{109}$,所以该加密系统的密钥空间是 $1.638\ 4\times10^{214}$,该系统足以抵抗蛮力攻击.

4.2 直方图分析

图像的直方图是图像的重要统计特性,它通过统计像素在图像中的分布方式,间接反映出图像的特点.所以使用一个好的加密系统对原始图像进行处理后,可以给出均匀分布的直方图,掩盖了原始图像中比较凸显的像素.为了分析密文图像的直方图,选取 Lena 彩色图像进行测试.图 2 可以看出,原始图像的 RGB 通道的直方图分布不均匀,而对原始图像加密后,直方图是几乎趋于水平,意味着密文图像的直方图几乎得不到关于原始图像像素分布的统计信息.因此,提出的图像加密方法对统计攻击具有较强的鲁棒性.

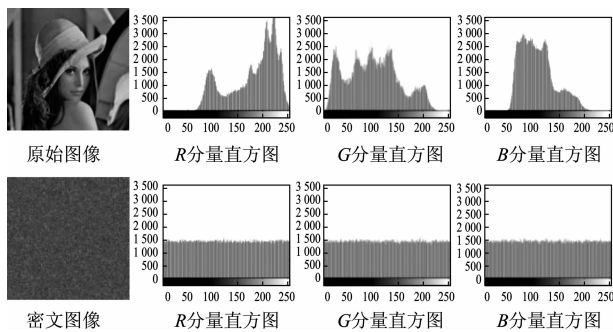


图 2 Lena 原始图像和密文图像的 RGB 直方图

4.3 相关性分析

另一种统计攻击是相关性分析,相关系数是图像加密领域的重要特征之一.通过对相邻像素之间的关系进行分析,可以发现其中所隐含的信息,从而对图片的内容进行预测.计算水平、垂直和对角方向上两个相邻像素的相关系数,其公式为:

$$r_{x,y} = \frac{E((x - E(x))(y - E(y)))}{\sqrt{D(x)D(y)}} \tag{8}$$

$$E(x) = \frac{1}{N} \sum_{i=1}^N x_i \tag{9}$$

$$D(x) = \frac{1}{N} \sum_{i=1}^N (x - E(x))^2 \tag{10}$$

式中, x 和 y 是两个相邻像素的像素值, N 表示选取的像素总数, r 表示两个相邻像素之间的相关系数.相关系数越大,表明像素之间的相关性越强;相关系数越小,表明像素之间的相关性越弱.

在原始图像中,相邻像素之间的相关性很高,由于像素之间高的相关性容易被攻击者利用,所以密文图像的相关性应尽可能地小.本文选用 Lena 彩色图像进行实验.在原始图像和密文图像中,分别在水平、垂直和对角线上随机抽取 5 000 对相邻像素,计算其相关系数.表 4 显示了原始图像和密文图像的 RGB 三个平面中相邻像素之间的相关系数.由表可知,原始图像中相邻像素之间相关系数趋近于 1,彼此之间存在很高的相关性;而密文图像的相关系数更趋近于 0,其相关性更低.表明本文算法具有更好的加密性能.

表 4 原始图像和密文图的相关系数

图像	方向	R	G	B
原始图像	水平	0.979 6	0.971 5	0.936 4
	垂直	0.989 6	0.982 9	0.961 6
	对角	0.969 9	0.958 5	0.919 0
密文图像	水平	0.001 9	0.000 6	0.000 9
	垂直	-0.000 1	-0.028 8	0.000 5
	对角	0.003 7	0.000 1	-0.000 6

4.4 信息熵分析

信息熵表示图像中灰度分布的聚集特征所包含的信息量,可以用来反应图像的随机性,衡量像素值的分布均匀程度.一般来说,如果平面图像的像素值分布越均匀,则图像抗攻击能力越强,反之,则越弱.信息熵 $H(m)$ 的计算公式为:

$$H(m) = \sum_{i=0}^{2^n-1} p(m_i) \log \frac{1}{p(m_i)} \tag{11}$$

式中, $p(m_i)$ 表示符号 m_i 的概率.信息的不确定度越小,信息熵越小.信息的不确定度越大,信息熵越大,所以对于一个 8 位灰度图像,信息熵的期望值是 8,当信息熵越接近 8,说明图像抵抗攻击的能力越强.

原始图像和密文图像的信息熵如表 5 所示.从表中可以看出,密文图像的信息熵值都非常接近 8,这意味着密文图像可以近似被看作是一个随机信号,该加密算法可以确保图像信息的安全性.本文的加密算法得到的信息熵与文献[9]相比更优,说明本文的加密算法具有很好的信息熵特征.

表 5 原始图像和密文图像的信息熵

	信息熵		
	R	G	B
原始图像	7.253 1	7.594 0	6.968 4
本文算法	7.999 4	7.999 3	7.999 4
文献[9]	7.989 2	7.989 8	7.989 9

4.5 差分攻击分析

通常使用像素变化率(NPCR) 和统一平均变化强度(UACI)来测试加密方法的抗差分攻击能力. NPCR 表示原始图像和密文图像之间不同像素数的百分比. UACI 表示原始图像和密文图像之间平均差异的强度. 将原始图像中任何一个像素进行改变,并对改变后的图像并进行加密,此密文图像将用于计算 NPCR 和 UACI. NPCR 和 UACI 的数学定义式为:

$$NPCR = \sum_{i=1}^m \sum_{j=1}^n D(i,j) / (m \times n) \times 100\% \quad (12)$$

$$D(i,j) = \begin{cases} 0, & C_1(i,j) = C_2(i,j) \\ 1, & C_1(i,j) \neq C_2(i,j) \end{cases} \quad (13)$$

$$UACI = \frac{1}{m \times n} \left[\sum_{i=1}^m \sum_{j=1}^n \frac{|C_1(i,j) - C_2(i,j)|}{255} \right] \times 100\% \quad (14)$$

式中, m 和 n 分别是密文图像的宽度和长度. C_1 和 C_2 代表两个密文图像,其对应的普通图像只有一个像素值不同. 对于一个 8 位的灰度图像, NPCR 和 UACI 的期望值分别是: NPCR = 99.609 4%, UACI = 33.463 5%.

为了测试 NPCR 和 UACI,该算法将使用相同的密钥对原始图像和修改一个像素的图像进行加密. 从表 6 中可以看出图像的 RGB 平面的 NPCR 和 UACI 都非常接近理想值,说明该算法对彩色图像的微小变化具有很强的敏感性,并且本文的加密算法与文献[10]的算法效果相比更优,说明本文加密算法更有效,且具有足够的安全性.

表 6 C_1 和 C_2 的 NPCR 和 UACI

	R/%	G/%	B/%
本文 NPCR	99.60	99.61	99.61
文献[10]NPCR	99.653 1	99.652 2	99.651 8
本文 UACI	33.59	33.49	33.44
文献[10]UACI	33.457 2	33.471 5	33.438 4

4.6 密钥敏感性分析

一个设计良好的图像加密方法对密钥非常敏感,细微的变化都会导致生成完全不同的密文图像. 为了了解本文算法如何应对密钥的细微变化,使用 NPCR 和 UACI 衡量密钥改变前后生成的密文图像之间的差异. 首先使用一组密钥对图像进行加密,

然后改变密钥对相同的图像进行加密,其中密钥只改变 10^{-15} . 使用正确的密钥可以将图像完全恢复,而使用错误的密钥将无法正确的恢复原始图像,说明本文的密钥具有很强的敏感性.

5 结束语

本文提供了一种彩色图像加密算法. 本文首先提出了一种对选取 DNA 编码规则的评价方法,并对选取 DNA 编码规则不均的现象提出了改进方案,使加密算法可以更加均匀的选取 DNA 编码规则;其次本文设计了一种基于 RGB 的比特置乱规则,可以使三个通道之间相互加密,改变一个平面内的像素可以使三个平面的密文图像发生巨大变化,增加密文图像的敏感程度;再次,利用 DNA 编码规则对图像进行编码和译码,在编码和译码之间对 DNA 碱基进行循环移位,提高图像的混淆和扩散的能力. 最后使用 S 盒对像素值进行替换, S 盒替换操作可以提高加密系统的非线性扩散能力. 本文通过仿真结果和安全性分析,证明本文的加密算法具有巨大的密钥空间,信息熵优于其他算法,且具有良好的加密效果,安全性更高.

参考文献:

[1] PAREEK N K, PATIDAR V, SUD K K. Image encryption using chaotic logistic map[J]. Image and Vision Computing, 2006, 24(9): 926-934. DOI: 10.1016/j.imavis.2006.02.021.

[2] ALVAREZ C, LI S J. Some basic cryptographic requirements for chaos-based cryptosystems[J]. International Journal of Bifurcation and Chaos, 2006, 16(8): 2129-2151. DOI: 10.1142/S0218127406015970.

[3] GAN Z H, CHAI X L, HAN D J, et al. A chaotic image encryption algorithm based on 3-D bit-plane permutation[J]. Neural Computing and Applications, 2019, 31(11): 7111-7130. DOI:10.1007/s00521-018-3541-y.

[4] YE R S, HUANG H Q, LI Y C, et al. A self-adaptive bit-level color image encryption algorithm based on generalized Arnold map[J]. ITM Web of Conferences, 2017, 11: 06002. DOI:10.1051/itmconf/20171106002.

[5] GIRDHAR A, KUMAR V. A RGB image encryption technique using Lorenz and Rossler chaotic system on DNA sequences[J]. Multimedia Tools and Applications, 2018, 77(20): 27017-27039. DOI: 10.1007/s11042-018-5902-z.

wild[J]. arXiv preprint arXiv:1212.0402, 2012.

[11] XUE T F, CHEN B A, WU J J, et al. Video enhancement with task-oriented flow[J]. International Journal of Computer Vision, 2019, 127(8): 1106-1125. DOI: 10.1007/s11263-018-01144-2.

[12] JADERBERG M, SIMONYAN K, ZISSERMAN A. Spatial transformer networks[C]//Advances in Neural Information Processing Systems. 2015: 2017-2025.

[13] HE K M, ZHANG X Y, REN S Q, et al. Deep residual learning for image recognition[C]//Proceedings of 2016 IEEE Conference on Computer Vision and Pattern Recognition. Las Vegas: IEEE, 2016: 770-778. DOI: 10.1109/CVPR.2016.90.

[14] DOSOVITSKIY A, FISCHER P, ILG E, et al. FlowNet: learning optical flow with convolutional networks [C]//Proceedings of 2015 IEEE International Conference on Computer Vision. Santiago, Chile: IEEE, 2015: 2758-2766. DOI: 10.1109/ICCV.2015.316.

[15] ILG E, MAYER N, SAIKIA T, et al. FlowNet 2.0: evolution of optical flow estimation with deep networks [C]//Proceedings of 2017 IEEE Conference on Computer Vision and Pattern Recognition. Honolulu: IEEE, 2017: 2462-2470. DOI: 10.1109/CVPR.2017.179.

[16] SU S C, DELBRACIO M, WANG J, et al. Deep video deblurring for hand-held cameras[C]//Proceedings of 2017 IEEE Conference on Computer Vision and Pattern Recognition. Honolulu: IEEE, 2017: 1279-1288. DOI: 10.1109/CVPR.2017.33.

[17] DENG J, DONG W, SOCHER R, et al. ImageNet: a large-scale hierarchical image database[C]//Proceedings of 2009 IEEE Conference on Computer Vision and Pattern Recognition. Miami, FL: IEEE, 2009: 248-255. DOI: 10.1109/CVPR.2009.5206848.

[18] SIMONYAN K, ZISSERMAN A. Very deep convolutional networks for large-scale image recognition[J]. arXiv preprint arXiv:1409.1556, 2014.

[19] BAO W B, LAI W S, MA C, et al. Depth-aware video frame interpolation[C]//Proceedings of 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition. Long Beach, CA: IEEE, 2019: 3703-3712.

作者简介:

张培健 男,(1995-),硕士研究生.研究方向为计算机视觉.

滕奇志(通讯作者) 女,(1961-),教授,博士生导师.研究方向为数字图像处理、模式识别.

E-mail: qzteng@scu.edu.cn.

何小海 男,(1964-),教授,博士生导师.研究方向为图像处理、模式识别和图像通信.

(上接第 38 页)

[6] CHAI X L, GAN Z H, YUAN K, et al. A novel image encryption scheme based on DNA sequence operations and chaotic systems[J]. Neural Computing and Applications, 2019, 31(1): 219-237. DOI: 10.1007/s00521-017-2993-9.

[7] ZHOU Y C, BAO L, CHEN C L P. A new 1D chaotic system for image encryption[J]. Signal Processing, 2014, 97: 172-182. DOI: 10.1016/j.sigpro.2013.10.034.

[8] BELAZI A, KHAN M, EL-LATIF A A, et al. Efficient cryptosystem approaches: S-boxes and permutation-substitution-based encryption[J]. Nonlinear Dynamics, 2017, 87(1): 337-361. DOI: 10.1007/s11071-016-3046-0.

[9] WU X J, WANG K S, WANG X Y, et al. Color image DNA encryption using NCA map-based CML and one-time keys[J]. Signal Processing, 2018(148): 272-287. DOI: 10.1016/j.sigpro.2018.02.028.

[10] KANG X J, GUO Z H. A new color image encryption scheme based on DNA encoding and spatiotemporal chaotic system[J]. Signal Processing: Image Communication, 2020(80): 115670. DOI: 10.1016/j.image.2019.115670.

作者简介:

王 钊 男,(1995-),硕士研究生.研究方向为网络信息安全技术及应用. E-mail: 2374805061@qq.com.

张雪锋 男,(1975-),博士,教授.研究方向为信息安全、信号与信息处理.

姜 文 男,(1983-),博士,高级工程师.研究方向为基础设施与工业互联安全.