doi:10.11835/j.issn.1000-582X.2021.07.006

基于哈希和 DNA 编码的彩色图像混沌加密算法

袁　立[1,2]，谢　俐[1]，龙　颖[3]，胡春强[2]，蒋淘金[4]

（1.重庆电力高等专科学校 信息工程学院，重庆 400053；2.重庆大学 大数据与软件学院，重庆 401331；
3.重庆应用技术职业学院 电子信息与财经商务系，重庆 410520；4.重庆市公安局交巡警总队，重庆 400054）

摘要：彩色图像的安全性一直受到学者的关注。针对彩色图像加密算法置乱效果不佳、扩散特性不强、抵御统计攻击能力较弱等问题，提出了一种基于哈希和 DNA 编码的彩色图像混沌加密算法。运用哈希函数生成 Arnold 混沌映射的参数，将 Arnold 混沌映射和 Logistic 混沌映射结合，对图像进行 R、G、B 3 个维度的置乱，再利用 DNA 编码对图像进行混乱处理。理论分析和计算机仿真表明：本文的算法具有良好的加密效果，且对统计、差分攻击具有很好的抵御效果。

关键词：混沌映射；DNA 编码；图像加密；加密算法

中图分类号：TP309　　**文献标志码**：A　　**文章编号**：1000-582X(2021)07-055-09

Hyper-chaotic color image encryption algorithm based on Hash and DNA coding

YUAN Li[1,2]，*XIE Li*[1]，*LONG Ying*[3]，*HU Chunqiang*[2]，*JIANG Taojin*[4]

(1. School of Information Engineering, Chongqing Electric Power College, Chongqing 400053, P. R. China;
2. School of Big Data and Software Engineering, Chongqing University, Chongqing 401331, P. R. China;
3. Department of Electronic Information and Financial Business, Chongqing Vocational College of Applied Technology, Chongqing 410520, P. R. China; 4.Traffic and Patrol Police Corps of Chongqing Public Security Bureau, Chongqing 400054, P. R. China)

Abstract: The security of color image has always been concerned by scholars. To deal with the defects of traditional color image encryption algorithm, such as poor scrambling effect, weak diffusion characteristics

收稿日期：2020-06-30

基金项目：国家自然科学基金资助项目（61702062）；重庆市技术创新及应用发展专项重点项目（cstc2019jscx-mbdxX0044）；重庆市基础科学与前沿技术研究专项（cstc2018jcyjAX0334）；重庆市留学人员回国创业创新计划（cx2018015）；中央高校基本科研前沿交叉专项（2019CDQYRJ006）；重庆市教育委员会科研基金资助（KJQN201802602）。

Supported by the National Natural Science Foundation of China (61702062), Key Project of Technology Innovation and Application Development of Chongqing (cstc2019jscx-mbdxX0044), the Chongqing Research Program of Basic Research and Frontier Technology with Grant (cstc2018jcyjAX0334), the Fundamental Research Funds for the Central Universities (2019CDQYRJ006), and Overseas Returnees Innovation and Entrepreneurship Support Program of Chongqing (cx2018015), and Research Fund of Chongqing Education Commission (KJQN201802602).

作者简介：袁立（1985—），男，主要从事图像加密方向研究，(E-mail)493642254@qq.com。

通讯作者：胡春强，研究员，博士生导师，(E-mail)chu@cqu.edu.cn。

and resistance to statistical attacks, this paper presents a Hyper-chaotic Color Image Encryption Algorithm based on Hash and DNA coding. In the proposed algorithm, the parameters of Arnold chaotic map are generated by hash algorithm first; then, combined with Arnold chaotic map and Logistic chaotic map, the image is scrambled in three dimensions of R, G, and B; Finally, the image is chaotically processed using DNA coding. The theoretical analysis and computer simulation show that the proposed algorithm has good encryption effect, and it has good resistance to statistical and differential attacks.

Keywords: chaotic mapping; DNA coding; image encryption; encryption algorithm

混沌系统对初始值非常敏感,且具有良好的非收敛性和类随机性,因此在图像加密处理中具有广泛的应用[1-3]。当前,混沌系统在图像加密中的应用主要包括混合迭代结构加密、置乱加密、灰度替换加密等技术。文献[4]提出了一种流密码算法,它结合了一次一密和强混沌映射,基于分段线性混沌序列生成相应的密钥流序列,综合了混沌算法和循环加密的优势。1994年,DNA计算被Adleman首次提出[5],为图像加密处理提供了新的思路和方向。文献[6]综合Chebyshev映射和DNA计算的优势,将图像进行扩散加密,结果显示加密效果良好。文献[7]将DNA计算用于进行图像加密,使得猫映射在图像安全处理效果上有极大提升。以上算法只是单纯处理数字图像加密的算法,没有与处理文本的加密算法结合,存在一定的局限性。在文献[8]中,Abbas提出了一种基于Hash的数字图像加密算法,结果显示加密效果良好。

文中将哈希函数、Arnold混沌映射和Logistic混沌映射结合,对图像进行R、G、B 3个维度的置乱;然后利用DNA编码对图像进行混乱处理。结合实验结果表明:文中图像加密算法具有很好的加密性。

1 算法基础

1.1 Logistic映射

Logistic映射模型比较经典,主要用于对动力系统、分形系统等复杂系统进行分析和研究。Logistic映射本质是一个在时间上离散的动力系统,其迭代公式为

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

式中,$\mu\in(0,4)$,$x_n\in(0,1)$。当$3.569\ 945\ 6<\mu\leqslant 4$时,Logistic映射处于混沌状态。

将Logistic映射[9]改为

$$x_{n+1}=\left[3.569\ 945\ 972+(4-3.569\ 945\ 972)*\sin\left(\frac{\pi}{2}\right)\right]x_n(1-x_n), \tag{2}$$

式中,x_n为映射变量,$0<x_n<1$。

1.2 Arnold映射

俄国数学家Vladimir Igorevich Arnold首次提出了Arnold映射,又称猫映射。本质来说,Arnold映射就是在有限的区域内进行反复折叠和伸缩变换。

其原始公式为

$$\begin{bmatrix}x_{n+1}\\y_{n+1}\end{bmatrix}=\begin{bmatrix}1&1\\1&2\end{bmatrix}\begin{bmatrix}x_n\\y_n\end{bmatrix}(\mathrm{mod}1), \tag{3}$$

对其进行数字化处理之后,得到映射关系为

$$\begin{bmatrix}x_{n+1}\\y_{n+1}\end{bmatrix}=\begin{bmatrix}1&a\\b&ab+1\end{bmatrix}\begin{bmatrix}x_n\\y_n\end{bmatrix}(\mathrm{mod}N), \tag{4}$$

式中,a、b、N均为正整数。

1.3 DNA序列编码

DNA序列由A、T、C、G 4个碱基组成,其中A和T、C和G存在互补关系。如果使用2 bit表示字节表示一个字母,那么DNA编码的方案共有4!种。但是满足碱基互补原则的只有8种,如表1所示。

表 1　DNA 序列的 8 种编码/解码规则

Table 1　Eight coding / decoding rules of DNA sequence

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

1.4　DNA 序列的加法、减法

一套基于 DNA 序列的基本代数运算被 King 等[10]提出,其基本思想起源于二进制的加减法运算。DNA 序列的基本代数运算与编码方案有很强的关系,不同编码方案对应的加减法规则也不同。以表 1 中第 1 种编码方案为例,其对应的加减运算规则如表 2 所示。

表 2　第 1 种编码方案的加减运算

Table 2　Addition and subtraction of the first coding scheme

+/−	A	G	C	T
A	A/A	G/T	C/C	T/G
G	G/G	C/A	T/T	A/C
C	C/C	T/G	A/A	G/T
T	T/T	A/C	G/G	C/A

1.5　SHA-256

哈希函数又叫散列函数,它能够将不同长度的信息转换成一个固定长度的信息。SHA-256 函数可以将图像信息转换成 256 位的哈希值。SHA-256 函数对初始值极其敏感,图像内容有任何细微的差别,计算出来的哈希值都会发生巨大的变化。

2　加密算法

2.1　加密算法

为了使加密效果更好,充分利用 SHA-256 函数、Arnold 混沌映射、改进 Logistic 混沌映射和 DNA 加密处理的优点,文中提出一种新型加密技术,其算法步骤如下:

步骤 1:假设明文图像的尺寸为 $M\times N$,将其按照红、绿、蓝 3 个维度进行转换,得到 3 个平面分别为 R、G、B。这 3 个平面尺寸均为 $M\times N$,每个像素的值均在(0,255)之间且为整数。若 M 和 N 值不相等,则可以通过补 0 的方式将其转换为$N_1\times N_1$的方阵。

步骤 2:分别求 R、G、B 3 个平面的像素值之和,然后运用 SHA-256 函数分别计算这 3 个和值的哈希值,得到 3 组 256 位哈希值。式(4)的 2 个参数 a、b 和加密轮数 N 就是由 SHA-256 函数产生的 3 个参数值,分别作为 R、G、B 3 个平面进行置乱处理的原始参数。

步骤 3:运用按照式(4)分别对 R、G、B 3 个平面进行置乱处理。

步骤 4:将置乱后的 R、G、B 3 个方阵进行二进制转换,每个平面转换后的大小均为$N_1\times 8\ N_1$,采用 DNA 编码规则对其进行编码处理,进而得到 3 个尺寸为$N_1\times 4\ N_1$的碱基方阵R_1、G_1、B_1。

步骤 5:按照式(2)进行混沌映射处理得到尺寸为$N_1\times N_1$的混沌序列 m,利用算子 mod(floor(m * power(10,5)),256)将序列 m 进行整数化处理,得到相应的序列,采用 DNA 编码规则对数化处理后的序列进行相应的编码处理得到对应的矩阵。

步骤 6:根据式(5)替换 R、G、B 3 个平面的碱基序列,从而得到相应的 3 个平面R_2、G_2、B_2。

$$\begin{cases} R_2(i,j)=R_1(i,j)+G_1(i,j) \\ G_2(i,j)=G_1(i,j)+B_1(i,j)。 \\ B_2(i,j)=R_2(i,j)+G_2(i,j) \end{cases} \tag{5}$$

步骤7:分别采用表1中的第4、2、7中的编码规则对置乱替换后的3个平面R_2、G_2、B_2进行解码处理,得到相应的3个平面R_3、G_3、B_3,尺寸为$N_1\times N_1$。

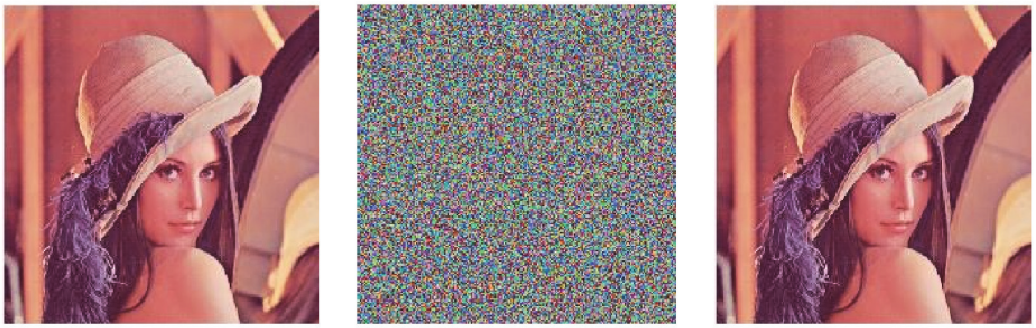
步骤6:合成R_3、G_3、B_3 3个平面得到相对应的密文图像,计算得到密文图像的和值,并将和值与密文图像进行异或运算,最终得到本文的加密图像。

2.2 解密算法

加密和解密互为逆过程。解密是对加密进行逆运算,将DNA加法运算替换为减法运算,并按照R、G、B的逆序对进行恢复,即可解密图像。

3 实验结果分析

文中选择明文图像为彩色的Lena图,尺寸为512×512,运行的环境为Intel Core i5 CPU@2.5GHz、8G内存、Win7 64位操作系统,仿真软件为MATLAB r2014a。对比图1中的3幅图分析可知,Lena图像经过文中加密算法处理后,已经看不到明文信息,说明文中提出的加密算法具有良好的效果。



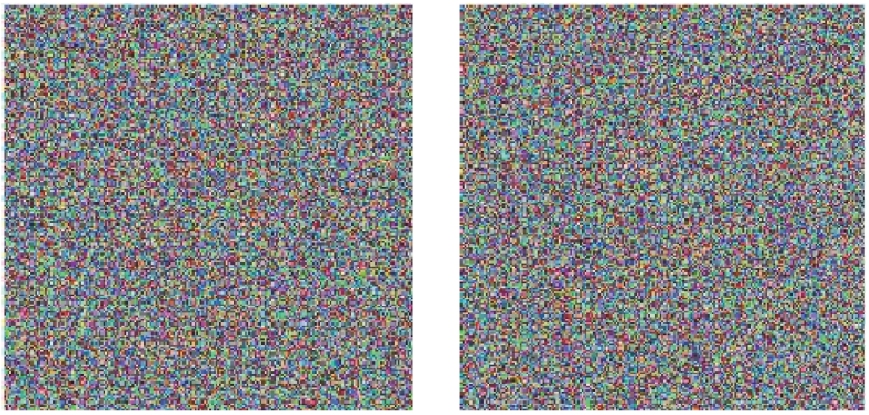
(a)加密前的图像 (b)加密后的图像 (c)解密后的图像

图1 Lena图加密前后对比

Fig. 1 Comparison of Lena before and after encryption

3.1 密钥敏感性分析

若式(2)的初始值和迭代次数发生细微改变,会导致加密后的图像不能恢复成原始图像。例如,若在解密过程中,将式(2)的初值增加1×10^{-15},则会导致图像解密失败,具体如图2所示。



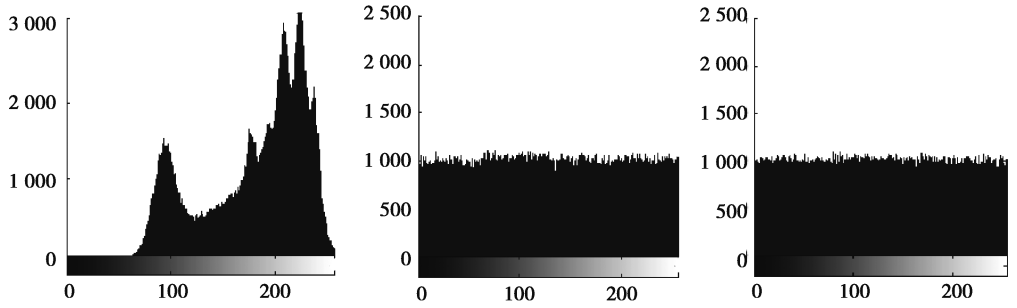
(a)初始值错误的解密图 (b)迭代次数错误的解密图

图2 错误密钥的解密图

Fig. 2 Decryption graph of wrong key

3.2　直方图分析

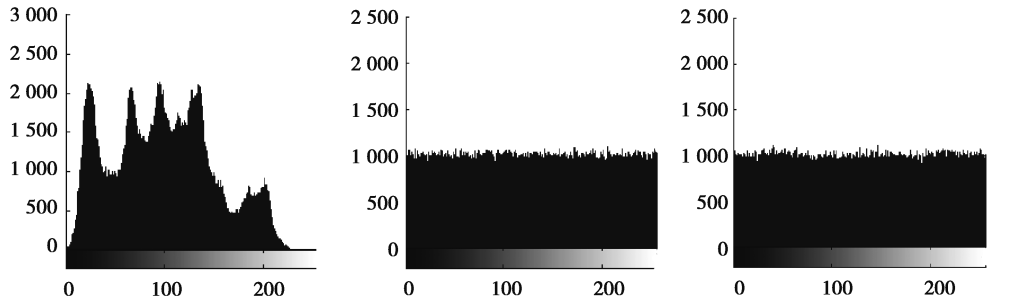
直方图能够体现出图像灰度值的分布情况。图像灰度值的分布情况能够体现出图像的抗攻击能力。若图像灰度值分布越平均,则其越能抵抗统计攻击[11-15]。从图 3、图 4、图 5 对比分析中可以看出:文中算法加密图像的直方图和文献[15]算法加密图像的 3 个分量直方图都是比较均匀的,说明都具有良好的统计攻击抵御能力。2 个算法加密的图像直方图差别很小,加密效果接近。



(a)原始图　　(b)本文算法加密后直方图　　(c)文献[15]算法加密后直方图

图 3　Lena 图的 *R* 图像

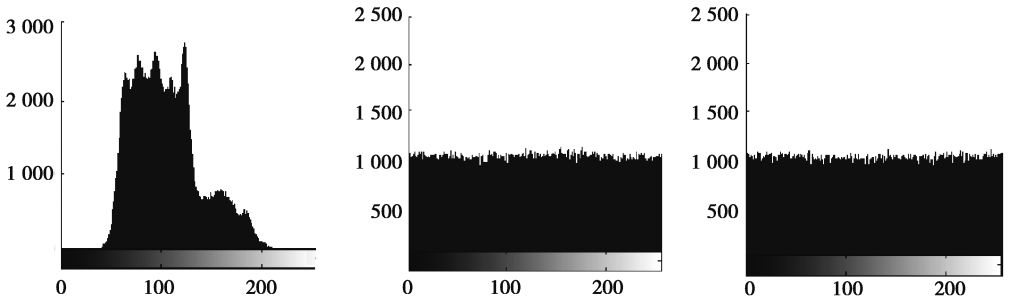
Fig. 3　*R* image of Lena graph



(a)原始图　　(b)本文算法加密后直方图　　(c)文献[15]算法加密后直方图

图 4　Lena 图的 *G* 图像

Fig. 4　*G* image of Lena graph



(a)原始图　　(b)本文算法加密后直方图　　(c)文献[15]算法加密后直方图

图 5　Lena 图的 *B* 图像

Fig. 5　*B* image of Lena graph

3.3　相邻像素相关性分析

为了验证文中算法的置乱效果,将基于水平、垂直和对角 3 个角度,从明文图像、加密图像中随机选取 4 000对相邻像素点,然后运用式 (6)～式(9)计算相邻像素间的相关性[15-20]。

$$E(x)=\frac{1}{N}\sum_{i=1}^{N}x_i, \tag{6}$$

$$D(x)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))2, \tag{7}$$

$$\mathrm{cov}(x,y)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))(y_i-E(y)), \tag{8}$$

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

式中：x 和 y 表示图像中两个相邻像素的灰度；N 表示图像像素个数；$E(x)$ 表示 x 的数学期望；$D(x)$ 表示 x 的方差；$\mathrm{cov}(x,y)$ 表示 x,y 的协方差；r_{xy} 表示相关系数。

若相关系数越接近0，则像素之间的相关程度越低，图像置乱效果越好，加密图像破译难度越大。从表3～表5可以看出，文中加密后的图像的相关系数更接近0，置乱效果更好。

表3 垂直像素相关性

Table 3 Vertical pixel correlation

算法算法	R	H	B
原始算法	0.970 9	0.969 5	0.945 2
文献[11]	−0.023 9	0.020 1	−0.016 1
文献[15]	0.008 6	0.008 2	−0.005 3
文中算法	0.004 1	0.004 3	−0.002 3

表4 水平像素相关性

Table 4 Horizontal pixel correlation

算法	R	H	B
原始算法	0.930 1	0.950 8	0.929 6
文献[11]	0.027 0	−0.016 8	0.015 2
文献[15]	0.016 3	−0.014 5	0.009 8
文中算法	0.001 6	−0.007 1	−0.003 1

表5 对角像素相关性

Table 5 Diagonal pixel correlation

算法	R	H	B
原始算法	0.939 9	0.948 1	0.900 1
文献[11]	−0.012 6	−0.018 5	−0.018 6
文献[15]	0.011 5	0.016 3	0.015 6
文中算法	−0.008 9	−0.007 1	−0.004 7

为了更加直观地展现像素之间的相关性，选择 B 平面，分别从水平、垂直、对角3个方面进行像素相关性图像的绘制。图6和图7分别表示的是加密前和文中加密的线性关系。对比分析可以看出原始图像 B 平面

3 个方向的图像像素值集中在主对角线上,相关性很强,而加密图像像素值均匀分布,相关性很弱,可破解性更小。

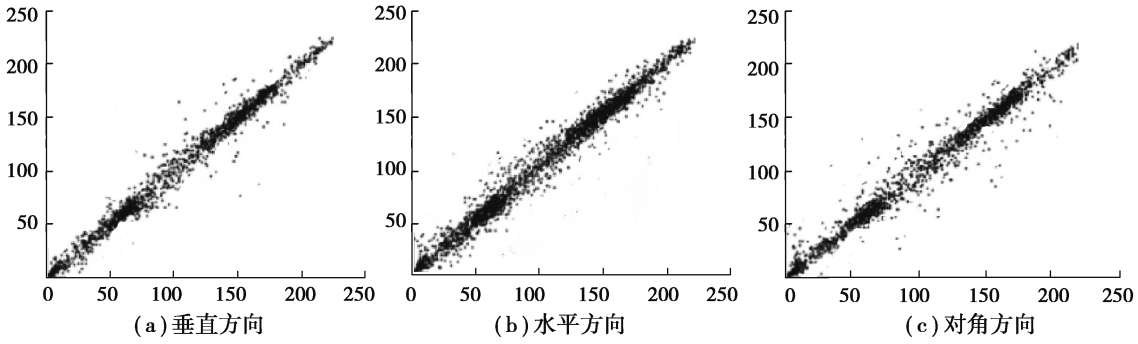


图 6　明文图像 *B* 平面相关性

Fig. 6　*B*-plane correlation of plaintext image

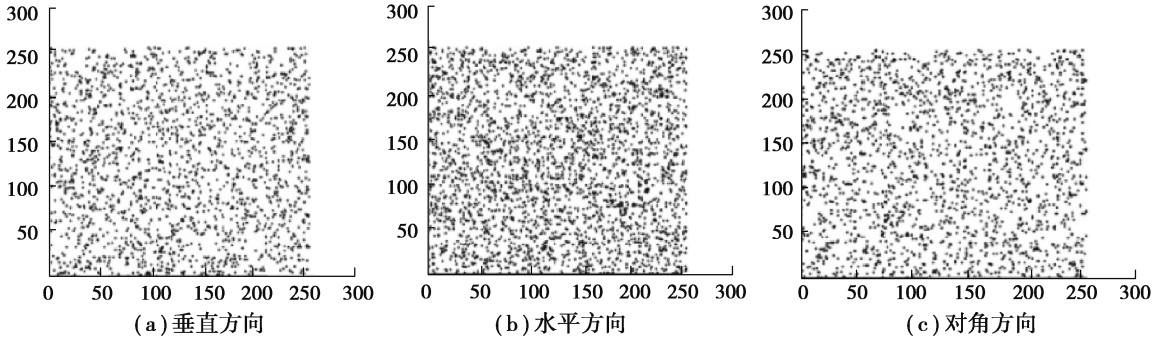


图 7　文中加密图像 *B* 平面相关性

Fig. 7　*B*-plane correlation of encrypted image

3.4　信息熵分析

信息熵体现了系统的随机性。图像直方图分布越均匀,则其随机性越强,信息熵就越大。式(10)所示的是信息熵的计算方式。对于灰度值范围为[0,255]的图像,其信息熵与 8 的逼近程度反映了抵御攻击的能力,信息熵越接近 8,抵御统计攻击的能力越强。根据式(10)计算所得结果如表 6 所示。

表 6　信息熵

Table 6　Information entropy

算法	H_R	H_G	H_B
原始	7.259 7	7.589 6	6.977 7
文献[11]	7.539 6	7.862 0	7.301 0
文献[15]	7.985 6	7.986 0	7.979 6
文中算法	7.992 8	7.993 8	7.990 6

可以看出,文中算法加密后的图像的信息熵更接近 8,抗统计攻击的能力更强。

$$H_m = -\sum_{i=0}^{255} p(m_i)\log p(m_i) \tag{10}$$

3.5　明文敏感性分析

式(11)～式(12)分别表示的是 NPCR(the number of pixels change rate)和 UACI(the unified average changing intensity)这 2 项指标,此 2 项指标表示了图像的差分攻击抵抗能力。改变原始图像的 R 平面中

(100,80)处的像素值,通过式(11)～式(12)计算出的 NPCR 和 UACI 的结果如表 7 所示。

$$\mathrm{NPCR}=\frac{\sum_{ij}D(i,j)}{m\times n}\times 100\%, \tag{11}$$

$$\mathrm{UACI}=\frac{1}{m\times n}\left[\sum_{ij}\frac{|D_1(i,j)-D_2(i,j)|}{255}\right]\times 100\%, \tag{12}$$

表 7 NPCR 和 UACI 分析

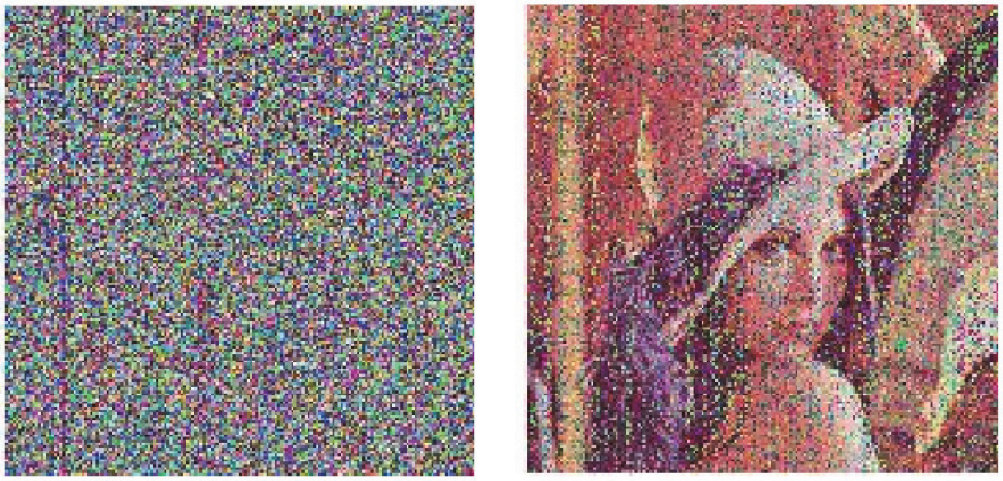
Table 7 NPCR and UACI analysis %

算法	NPCR	UACI
文献[11]	99.19	31.06
文献[15]	99.45	34.58
文中算法	99.68	37.01

通过对比 NPCR 值和 UACI 值,可以看出文中算法抗差分攻击能力更强。

3.6 抗干扰能力分析

将均值和方差分别为 0 和 0.05 的高斯噪声加入到加密后的图像中。图 8 中,图 8(a)表示的是加入高斯噪声后的加密图像,图 8(b)表示的是相应的解密图像。可以看出:文中的加密算法在图像混入少量噪声后,仍然能够将其解密出来,抗干扰能力较好。



(a)加噪后的密文图像 (b)解密后的含噪图像

图 8 抗干扰能力分析

Fig. 8 Analysis of anti-jamming capability

4 结束语

随着网络技术的高速发展,彩色图像的安全性越来越受到重视。图像加密是一种很好保护图像信息的方法。文中结合哈希函数、Arnold 混沌映射和 Logistic 混沌映射,使用 DNA 编码技术对图像进行混合加密。实验结果表明,本文的算法具有良好的加密效果,且对统计、差分攻击具有很好的抵御效果。

参考文献:

[1] 谢国波, 邓华军. 二次广义 cat 映射的混合混沌图像加密算法[J]. 计算机工程与应用, 2018, 54(15): 197-202.
Xie G B, Deng H J. Two hybrid chaotic image encryption algorithm based on generalized cat map[J]. Computer Engineering and Applications, 2018, 54(15): 197-202.(in Chinese)

[2] 朱淑芹, 李俊青. 一种混沌图像加密算法的选择明文攻击和改进[J]. 计算机工程与应用, 2017, 53(24): 113-121.

Zhu S Q, Li J Q. Chosen plain text attack and improvements of chaos image encryption algorithm[J]. Computer Engineering and Applications, 2017, 53(24): 113-121.(in Chinese)

[3] 文昌辞, 王沁, 黄付敏, 等. 基于仿射和复合混沌的图像自适应加密算法[J]. 通信学报, 2012, 33(11): 119-127.
Wen C C, Wang Q, Huang F M, et al. Self-adaptive encryption algorithm for image based on affine and composed chaos [J]. Journal on Communications, 2012, 33(11): 119-127.(in Chinese)

[4] 林敏, 龙飞. 基于分段线性混沌网络的序列密码算法[J]. 计算机应用与软件, 2016, 33(9): 306-309.
Lin M, Long F. Stream cipher algorithm based on piecewise linear chaotic networks[J]. Computer Applications and Software, 2016, 33(9): 306-309.(in Chinese)

[5] Adleman, L M. Molecular computation of solutions of combinational problems[J]. Science, 1994, 266(11): 1021-1024.

[6] 张健, 房东鑫. 应用混沌映射索引和 DNA 编码的图像加密技术[J]. 计算机工程与设计, 2015, 36(3): 613-618.
Zhang J, Fang D X. Image encryption technology applied chaotic maps index and DNA coding[J]. Computer Engineering and Design, 2015, 36(3): 613-618.(in Chinese)

[7] 李桂珍, 任晓芳. 基于 DNA 合成图像和混沌映射的图像加密算法[J]. 控制工程, 2018, 25(7): 1278-1284.
Li G Z, Ren X F. Research of image encryption algorithm based on DNA image synthesis and chaotic mapping[J]. Control Engineering of China, 2018, 25(7): 1278-1284.(in Chinese)

[8] Cheddad A, Condell J, Curran K, et al. A hash-based image encryption algorithm[J]. Optics Communications, 2010, 283(6): 879-893.

[9] 徐兵, 袁立. 基于改进 Logistic 混沌映射的数字图像加密算法研究[J]. 计算机测量与控制, 2014, 22(7): 2157-2159.
Xu B, Yuan L. Research on image encryption algorithm logistic chaotic based on an improved digital mapping[J]. Computer Measurement & Control, 2014, 22(7): 2157-2159.(in Chinese)

[10] King O D, Gaborit P. Binary templates for comma-free DNA codes[J]. Discrete Applied Mathematics, 2007, 155(5): 831-839.

[11] 黎娅, 徐江峰. 基于混沌的图像加密技术进展[J]. 河南师范大学学报(自然科学版), 2005, 33(3): 150-151.
Li Y, Xu J F. The new development of based-chaos image encryption technology[J]. Journal of Henan Normal University (Natural Science), 2005, 33(3): 150-151.(in Chinese)

[12] 黄方军. 基于数字化混沌理论的信息安全研究[D]. 武汉:华中科技大学, 2005.
Huang F J. Information security research based on discrete chaotic theory[D]. Wuhan: Huazhong University of Science and Technology, 2005. (in Chinese)

[13] 卢辉斌, 孙艳. 基于新的超混沌系统的图像加密方案[J]. 计算机科学, 2011, 38(6): 149-152.
Lu H B, Sun Y. Image encryption scheme based on novel hyperchaotic system[J]. Computer Science, 2011, 38(6): 149-152.(in Chinese)

[14] 朱和贵, 陆小军, 张祥德, 等. 基于二维 Logistic 映射和二次剩余的图像加密算法[J]. 东北大学学报(自然科学版), 2014, 35(1): 20-23.
Zhu H G, Lu X J, Zhang X D, et al. A novel image encryption scheme with 2D-logistic map and quadratic residue [J]. Journal of Northeastern University (Natural Science), 2014, 35(1): 20-23.(in Chinese)

[15] Hermassi H, Belazi A, Rhouma R, et al. Security analysis of an image encryption algorithm based on a DNA addition combining with chaotic maps[J]. Multimedia Tools and Applications, 2014, 72(3):2211-2224.

[16] 魏广政, 金鑫, 赵耿, 等. 一种改进的基于 DNA 编码和混沌映射的图像加密方法[J]. 计算机应用研究, 2015, 32(10): 3049-3051.
Wei G Z, Jin X, Zhao G, et al. Improved image encryption method based on DNA encoding and chaotic mapping[J]. Application Research of Computers, 2015, 32(10): 3049-3051,3069.(in Chinese)

[17] Enayatifar R, Sadaei H J, Abdullah A H, et al. A novel chaotic based image encryption using a hybrid model of deoxyribonucleic acid and cellular automata[J]. Optics and Lasers in Engineering, 2015, 71(8):33-41.

[18] Khan J S, Ahmad J, Khan M A. TD-ERCS map-based confusion and diffusion of autocorrelated data[J]. Nonlinear Dynamics, 2017, 87(1):93-107.

[19] Wang H D. A novel image encryption algorithm based on chaotic system[J]. Optical Technique, 2017, 43(3): 260-266.

[20] Wang X Y, Liu L T, Zhang Y Q. A novel chaotic block image encryption algorithm based on dynamic random growth technique[J]. Optics and Lasers in Engineering, 2015, 66: 10-18.

(编辑　詹燕平)