

抗明文攻击的动态 DNA 编码数字图像加密算法

黄湧[†], 雷通

(中国能源建设集团 广东省电力设计研究院有限公司, 广东 广州 510000)

摘 要: 针对传统图像加密算法易受明文攻击的问题, 提出了结合 DNA 动态编码和离散混沌系统的数字图像加密算法。首先, 选取动力学特性复杂且计算复杂度低的离散混沌系统, 为图像密码系统提供优质熵源。接着, 设计明文相关机制生成混沌加密序列以抵御选择明文攻击。然后, 利用混沌序列对图像比特平面置乱, 并依次进行 DNA 编码、混淆和解码的操作。最后, 执行比特平面混淆以获得最终的密文。理论分析和实验结果表明, 本文的图像加密算法具有密钥空间大、相邻像素相关性强、直方图统计特性优良等特性, 该算法在抵抗明文攻击时的鲁棒性。

关键词: DNA 编码; 图像加密; 混沌系统

中图分类号: TP393.08

文献标识码: A

Dynamic DNA-encoded Digital Image Encryption Algorithm Against Plaintext Attacks

HUANG Yong, LEI Tong

(China Energy Engineering Group Guangdong Electric Power Design
Institute Co., Ltd., Guangzhou, Guangdong 510000, China)

Abstract: Aiming at the problem that traditional image encryption algorithms are susceptible to plaintext attacks, this paper proposes a digital image encryption algorithm that combines DNA dynamic coding and discrete chaotic system. Firstly, a discrete chaotic system with complex dynamics and low computational complexity is selected to provide a high-quality entropy source for the image cryptosystem. Next, a plaintext correlation mechanism is designed to generate chaotic encryption sequences to defend against selected plaintext attacks. Then, the chaotic sequence is used to disrupt the image bit plane and perform the operations of DNA encoding, obfuscation and decoding sequentially. Finally, bit-plane obfuscation is performed to obtain the final ciphertext. Theoretical analyses and experimental results show that the image encryption algorithm in this paper has the properties of large key space, strong correlation between adjacent pixels, and excellent statistical properties of histogram, the algorithm has the ability of robustly resisting plaintext attacks.

Key words: DNA coding; image encryption; chaos system

当今, 计算机网络与信息技术蓬勃发展, 人们已进入了数字化信息时代。而在网络大数据环境下, 多媒体信息的安全逐渐得到重视。数字图像是重要的多媒体介质, 它的隐私保护问题尤为引人关

注^[1]。混沌具有确定性系统的固有随机性、密集的周期点、遍历性以及初始值和控制参数的高度敏感性, 与香农密码学的扩散与混淆有许多相似之处^[2]。因此, 问世以来, 受到了众多专家学者的广

泛关注,被视为是信息安全领域极具应用前景的隐私保护技术^[3~4]。然而,由于缺乏权威的安全检测标准,当前许多此类算法不具有可证明的安全性^[5],这也是应用中必须解决的重要问题。因此,如何解决混沌加密算法具有实际安全性的问题,从而更安全地保护数字图像的安全性和保密性,成为当前的技术前沿和学术研究热点之一^[6]。

近几年,研究者在利用混沌系统进行数字图像加密方面取得了一系列重要的理论和应用成果^[7~10]。其中,结合 DNA 计算的混沌图像加密算法具有并行性好、效率高的特点,成为数字图像混沌加密的新研究方向^[11]。2021 年,文献[12]报道了基于多目标粒子群优化、DNA 编码序列和一维 Logistic 图谱的图像加密算法。仿真结果表明,该方法具有较好的加密效果。为了增强图像的安全性,Jiang 等^[13]提出了一种基于压缩感知(CS)和双随机相位编码(DRPE)的光学混沌技术的非对称双色图像密码系统。仿真结果和安全性分析证实,该密码系统具有多层保护,高效且能够保证图像的安全性,可为图像安全和隐私保护提供替代解决方案。2022 年,文献[14]的作者提出了一种采用分数傅里叶变换、超混沌系统、改进的逻辑图谱和 DNA 的创新图像块加密算法。实验结果表明了密码系统的有效性和安全性。同年,Zang 等^[15]提出了一种构建一维离散混沌系统的方法,并设计了一种基于均匀分布的离散混沌系统和 DNA 编码的图像加密方案。实验结果表明,所提出的加密算法具有密钥灵敏度高、加密速度快的特点,能够抵抗差分和统计攻击。

随着大量的结合 DNA 计算和数字图像混沌加密算法的设计和分析方面的研究被提出,密码设计和分析这对矛盾相互促进,推动着混沌密码技术向前发展。然而,目前结合 DNA 计算的混沌图像加密方案普遍仍然以下几点不足:(1)DNA 编码和运算规则单一,容易被攻击者破解。(2)加密算法结构不合理;没有采取明文关联或者密文反馈的方式,容易受到已知明文或者选择明文的攻击;此外,现有图像加密中像素级置乱,存在安全隐患。(3)现有混沌密码学的混沌系统或混沌图的安全性不足。现有低维混沌系统产生的混沌序列很难通过美国国家标准与技术研究院(NIST)的测试。混沌序列有被估计或识别的风险。其中,最为显著的问题是难以抵御已知明文攻击或选择明文攻击^[16]。

因此,本文提出了一种结合 DNA 动态编码和离散混沌系统的安全增强数字图像加密算法。首

先,使用了具有更复杂的动力学特性的混沌系统作为密码系统的熵源。接着,设计了明文相关机制生成用于加密的混沌伪随机序列,实现了动态密钥的效果,从而抵御选择明文攻击。然后,选取其中的一个混沌伪随机序列对图像执行二进制位平面排列,并基于混沌序列依次进行 DNA 编码、DNA 混淆和 DNA 解码的加密操作。最后,执行二进制位平面混淆以获得最终的密文。与现有研究相比,本论文创新性地开展了以下工作:(1)与以往的静态 DNA 编码不同,采用动态 DNA 编码来提高加密效果。(2)使用了离散混沌系统,所产生的序列随机性好,可通过严格的 TESTU01 测试,另外,该混沌系统还具有密钥参数多、结构设计灵活等优点。(3)引入明文关联的加密算法结构,可以在较高的运算效率前提下,提高算法抵御密码学分析和攻击的能力。(4)基于密码学,从密码分析视角对所提出的算法进行了差分分析,定量分析了其抵御明文攻击的能力,从而提升其安全性。

1 相关原理

1.1 DNA 编码和操作规则

编码及操作规则^[17]介绍:DNA 有四种组成成分,即腺嘌呤(A)、胸腺嘧啶(T)、胞嘧啶(C)、鸟嘌呤(G)。根据排列组合原理,有 24 种排列方式。但是,DNA 计算还应满足互补规则的需要,即 A 与 T 互补;因此,满足互补规则需要的 DNA 序列编码规则有八种,如表 1 所示。此外,在 DNA 计算中有三种运算,即加法、减法和异或运算,运算规则如表 2 所示。

表 1 DNA 编码规则

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

表 2 DNA 运算规则

AGCT												
	加法				减法				异或			
A	A	G	C	T	A	T	C	G	A	T	C	G
G	G	C	T	A	G	A	T	C	G	C	T	A
C	C	T	A	G	C	G	A	T	C	G	A	T
T	T	A	G	C	T	C	G	A	T	A	G	C

根据表 1,同样的信息被不同的 DNA 编码规则编码后,会有不同的 DNA 序列。例如,十进制数 54 的 8 位二进制“00110110”采用第一个 DNA 编码规则“ATGC”,第六个编码规则“CGTA”。同样,不同的解码规则导致不同的恢复信息。例如,“ATCG”采用的第一个解码规则为“00111001”,对应十进制数 57。如果采用第四个解码规则,为“01100011”,对应十进制数 99。显然,解码结果是不同的。DNA 结构域的加、减、异或操作与二元系统类似。加法和减法是互为逆运算,而异或运算本身则是互为对立的运算。

1.2 所使用的混沌系统

本文所采用的 2D-LSM 混沌系统是由 Hua 等^[18]提出的二维混沌系统,该模型的方程表达式为:

$$\begin{cases} h(i+1) = \cos\{4\alpha h(i)[1-h(i)]\} + \beta \sin[\pi w(i) + 1] \\ w(i+1) = \cos\{4\alpha w(i)[1-w(i)]\} + \beta \sin[\pi h(i) + 1] \end{cases} \quad (1)$$

其中 $h(i)$ 和 $w(i)$ 为序列初始值, α 和 β 为密钥参数。当 $\alpha, \beta \in [1, 100]$ 时,该系统处于混沌状态。

2 所提出的加密方案

该算法包括初始值生成、明文图像比特级置乱、DNA 动态编码、DNA 域混淆加密和 DNA 解码。该加密算法的总体框图如图 1 所示。

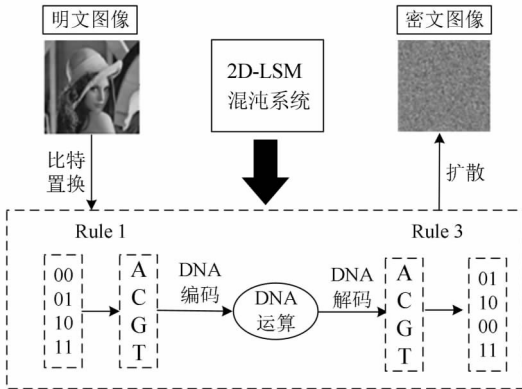


图 1 加密方案流程图

2.1 加密部分

步骤 1: 密钥参数选取与序列生成

本文算法选取明文 MD5 值和混沌系统参数作为密钥。为使得混沌密码序列对明文和密钥更加敏感,将所有的密钥参数进行如下处理后生成总密钥参数,处理方法为

$$\text{sum}K = \text{mod}(\alpha + \beta, 1) \quad (2)$$

同时对明文取 128 位散列值,切分为 8 个 16 比特的 $h_i, i = 1, 2, \dots, 16$, 进而处理为 4 个扰动参数 $n_j = \text{hex2dec}(h_{2j-1} + h_{2j}) / (3 \times 2^{16}), j = 1, 2, 3, 4$ 。最后,利用两个扰动参数 $\text{sum}K$ 和 n_j 按照如下方法分别对混沌系统的初始值进行微小的扰动:

$$\begin{cases} x_1(0) = x + \text{sum}K + n_1 \\ x_2(0) = x + \text{sum}K + n_2 \\ x_3(0) = x + \text{sum}K + n_3 \\ x_4(0) = x + \text{sum}K + n_4 \end{cases} \quad (3)$$

步骤 2: 序列预处理

利用已扰动的初始值,通过混沌系统生成加密所需的序列 x_1, x_2, x_3 , 并通过如下公式进行预处理:

$$\begin{cases} x_1 = \text{mod}[(\lfloor x_1 \rfloor \times 10^{14} - \lfloor x_1 \rfloor \times 10^{14}) \times 10^3, 256] \\ x_2 = \text{mod}[(\lfloor x_2 \rfloor \times 10^{14} - \lfloor x_2 \rfloor \times 10^{14}) \times 10^3, 256] \\ x_3 = \text{mod}[(\lfloor x_3 \rfloor \times 10^{14} - \lfloor x_3 \rfloor \times 10^{14}) \times 10^3, 256] \\ x_4 = \text{mod}[(\lfloor x_4 \rfloor \times 10^{14} - \lfloor x_4 \rfloor \times 10^{14}) \times 10^3, 256] \end{cases} \quad (4)$$

其中 $\lfloor \cdot \rfloor$ 为向下取整符号, $\text{mod}(\cdot)$ 为求余函数。

步骤 3: 比特级置换

对尺寸为 $M \times N$ 的明文图像 P 进行比特行列置乱。首先对序列 x_1 进行排序,得到两条排序序列 $\text{row}K, \text{col}K$ 。接着,将图像按照比特级展开,调整图像尺寸为 $M \times 8N$,最后使用排序序列对分层图像进行操作。具体操作如下:

$$\begin{cases} [w_1, \text{row}K] = \text{sort}(x_1(1:M)) \\ [w_2, \text{col}K] = \text{sort}[x_1(M+1, 9M)] \\ C_1(i, j) = P[\text{row}K(i), \text{row}K(j)] \end{cases} \quad (5)$$

其中 $\text{sort}(\cdot)$ 函数表示将输入序列中的每一位由低到高排序。 C_1 为置换后的图像。 w_1, w_2 表示将序列重新排序后的结果。 i, j 表示排序索引, $i = 1, 2, 3, \dots, M, j = 1, 2, 3, \dots, 8N$ 。

步骤 4: DNA 动态编码

使用混沌产生的 2 个序列 x_2, x_3 用于控制图像的 DNA 编码和解码方式,在加密前需对序列进行如下的数学公式处理:

$$\begin{cases} E = \text{mod}(\lfloor x_2 \rfloor \times 10^{14} - \lfloor x_2 \rfloor \times 10^{14}, 8) + 1 \\ D = \text{mod}(\lfloor x_3 \rfloor \times 10^{14} - \lfloor x_3 \rfloor \times 10^{14}, 8) + 1 \end{cases} \quad (6)$$

其中, E 和 D 的长度为 $M \times N$, 每一个序列值对应一种编码或解码方式。接着,对图像比特矩阵的 DNA 编码采用从左到右、从上到下的顺序进行,每 8 个比特即 4 个 DNA 字符动态更新一种编码规则,通过增强编码的复杂度以提高算法的安全性。第 3 条混沌序列 x_3 所构成的密钥图像 K 采用同样的方式调整为 $M \times N \times 8$ 的图像比特矩阵 K_1 , 进

而通过同样的编码方式生成尺寸为 $M \times N \times 4$ 的 DNA 矩阵。置乱比特矩阵 C_1 和密钥比特矩阵 K_1 经过 DNA 编码后分别表示为 C_2 和 K_2 。DNA 动态编码的具体过程如下:

$$\begin{cases} C_2\{[4(i-1)+1]:[4(i-1)+4]\} = \\ \quad \text{Encode}\{C_1[(8(i-1)+1):(8(i-1)+8)], E(i)\} \\ K_2\{[4(i-1)+1]:[4(i-1)+4]\} = \\ \quad \text{Encode}\{K_1[(8(i-1)+1):(8(i-1)+8)], E(i)\} \end{cases} \quad (7)$$

步骤 5: DNA 扩散

为了使得加密算法具有更强的抵御差分攻击能力,在 DNA 域上采用密文反馈的扩散方式使得明文、密钥和密文的关系变得更加复杂。DNA 域扩散过程表示为:

$$\begin{cases} C_3(i) = [C_2(i) + K_2(i)] \oplus K_2(i), i = 1 \\ C_3(i) = [C_2(i) + K_2(i)] \oplus K_2(i) + C_3(i-1), \\ \quad i = 2, 3, \dots, 4MN \end{cases} \quad (8)$$

步骤 6: DNA 动态解码

DNA 解码过程与编码过程类似。但值得指出的是,解码所用序列是对序列 x_3 进行处理,与编码序列不同,因此不是简单的逆过程,而是相当于双重加密变换。DNA 解码过程表示为:

$$\begin{aligned} C_4\{[8(i-1)+1]:[8(i-1)+8]\} = \\ \text{Decode}\{C_3[(4(i-1)+1):(12(i-1)+4)], \\ D(i)\} \end{aligned} \quad (9)$$

其中, C_4 为 DNA 解码后的图像。

最后,图像 C_4 经过进制转换为 $M \times N$ 的密文图像。

步骤 7: 扩散

加密算法必须具有扩散性质。大多数图像加密算法通过根据某些固定顺序使用先前像素来改变当前像素来实现扩散。本文采用链式密文反馈机制,并利用混沌序列的良好的伪随机性来增强加密性能,提高对图像的保护,降低密码分析的可能性。具体方程如下:

$$\begin{cases} C_5(i) = \text{mod}[C_4(i) + C_4(M \times N) + S(i), 256], \\ \quad i = 1 \\ C_5(i) = \text{mod}[C_4(i) + C_5(i-1) + S(i), 256], \\ \quad i = 2, 3, \dots, MN-1 \\ C_5(i) = \text{mod}[C_5(i-1) + S(i), 256], i = MN \end{cases} \quad (10)$$

其中 S 是由混沌序列 x_4 构成的密钥矩阵, C_5 是扩散后的密文矩阵,至此,完成整个加密过程。

2.2 解密部分

解密是加密的逆过程,与加密过程对应,首先对密文图像逆扩散,并进行反向 DNA 编码;接着,

在 DNA 域中进行逆扩散;然后解码并进行逆置换,最终恢复后的图像即为原文。

3 实验结果与讨论

3.1 实验环境

实验平台在 Windows 10 64bit 操作系统的 PC 上进行,环境为 MATLAB r2016a,处理器为 Intel(R) Core(TM) i5-3470 CPU @ 3.20 GHz 3.60 GHz,安装内存为 8 GB。针对多张不同的彩色图像进行实验,为便于与其他算法比较,采用尺寸为 256×256 的经典 Lena 彩色图像作为主要的实验对象。其中,加密 Lena 彩色图像的加密时间约为 2.5338 s。加密前后的图像如图 2 所示。加密后的图像呈现为彩色的雪花状,具有较好的加密效果。

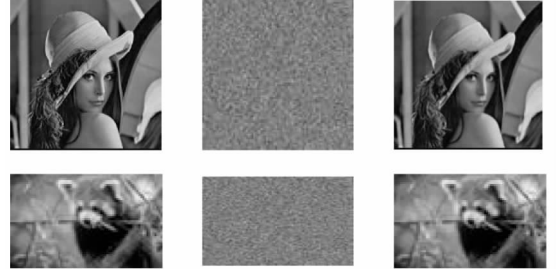


图 2 加密和解密前后的图像

3.2 数值统计与分析

3.2.1 直方图分析

直方图分析是一种统计分析方法,用于对数据的分布情况进行可视化和描述。本算法加密前后的图像如图 3 所示。加密后的图像均呈现为彩色的雪花状,具有较好的加密效果。

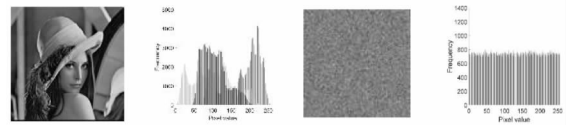


图 3 加密前后图像及对应直方图

3.2.2 相邻像素相关性分析

普通图像包含具有高邻域相关性的像素,而在通过良好加密算法加密的图像中,任何像素与其相邻像素之间都没有相关性。因此,安全加密方案应该将普通图像转换为相邻像素之间具有低相关性的加密图像。

通常采用相关系数来比较明文图像与密文图像的相关特性。 x, y 为两幅不同的图像,它们之间的相关系数定义如下:

$$r_{xy} = \frac{\sum_{i=1}^M (x_i - \frac{1}{M} \sum_{j=1}^M x_j)(y_i - \frac{1}{M} \sum_{j=1}^M y_j)}{\sqrt{\sum_{i=1}^M (x_i - \frac{1}{M} \sum_{j=1}^M x_j)^2} \sqrt{\sum_{i=1}^M (y_i - \frac{1}{M} \sum_{j=1}^M y_j)^2}}$$

(11)

其中, x_i 和 y_i 构成第 i 对水平/垂直/对角相邻像素, M 是水平/垂直/对角相邻像素的总数。明文图像在水平、垂直、对角线方向上的相邻像素点间均具有较强的相关性,而密文图像中的相邻像素点

间应没有相关性。彩色图像的 RGB 三个分量都具有类似的统计特性,具体的实验结果如图 4 和表 3 所示。

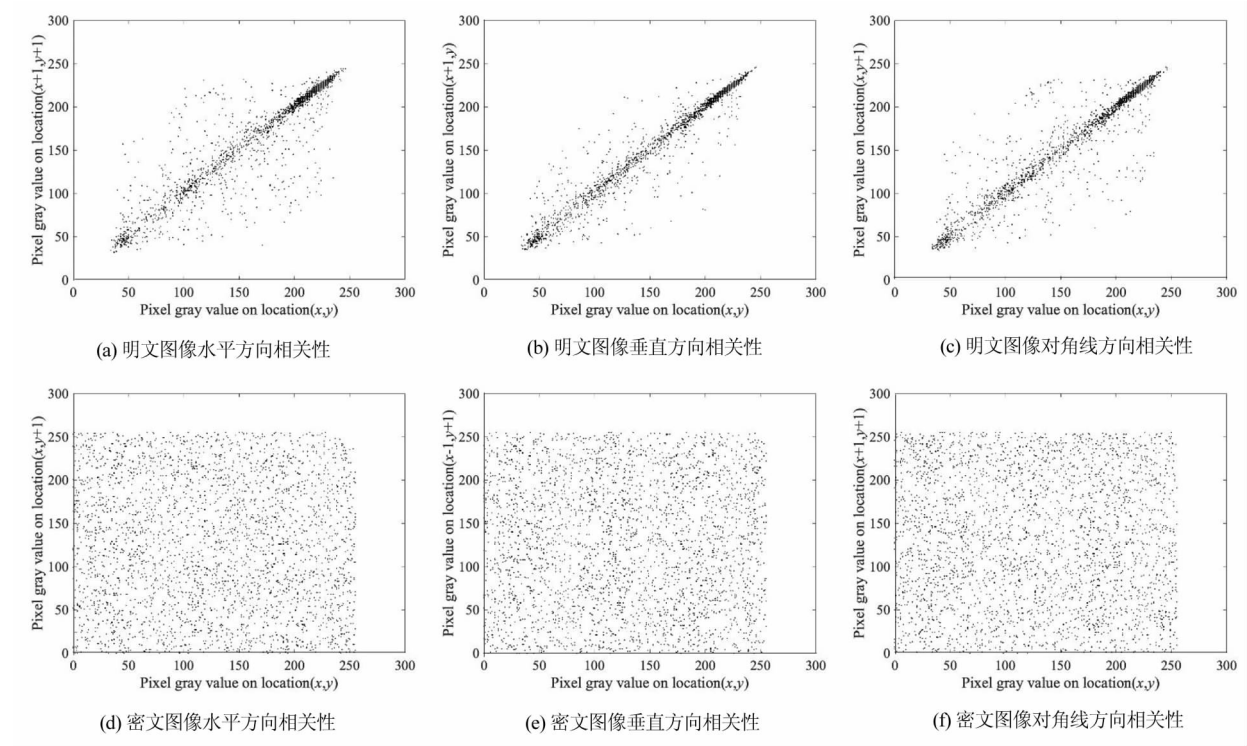


图 4 明文和密文图像相邻像素相关性

表 3 明文和密文 RGB 图像相邻像素的相关性			
分量	方向	原图	本文算法
R	水平	0.9712	-0.0253
	垂直	0.9616	-0.0053
	对角线	0.9388	0.0132
G	水平	0.9599	-0.0219
	垂直	0.9449	0.0069
	对角线	0.9279	-0.0401
B	水平	0.9512	0.0095
	垂直	0.9167	0.0425
	对角线	0.9030	0.0185

3.2.3 信息熵

信息熵是衡量图像内容复杂度和不确定性的度量指标。信息熵值越大,则图像信息的不确定性越大,信息的可见性越小,表明算法的加密性能越好。因此,本文比较了加密前后图像的信息熵。对于信息源 m , 信息熵 $H(m)$ 由下式给出:

$$H(m) = - \sum_{i=1}^L p(m_i) \log_2 [p(m_i)]$$

(12)

其中, L 是符号 $m(i) \in m$ 的总数, $p(m_i)$ 表示符号的概率。

假设信息源发送 256 个符号,并且我们可以通过式(12)获得理论值 $H(m) = 8$ 。信息熵越接近 8,攻击者解码加密图像的可能性就越小。表 4 显示了图像和密前后信息熵的比较。从表 4 可知,实

验结果接近 8,因此本文所提出的算法具有良好的信息熵特性。

表 4 图像信息熵				
图像	R	G	B	平均值
原图	7.5549	7.0167	6.7347	7.1021
本文	7.9995	7.9992	7.9999	7.9994

3.2.4 密钥空间分析

密钥空间是决定密码系统强度的重要指标之一,密钥空间的大小取决于安全密钥的长度。因此,需要大的密钥空间来有效抵御穷举攻击。在本文构建的密钥空间中,选择了两个精度为 10^{-16} 的密钥参数,并引入了明文关联和密文关联的 MD5 哈希值,以进一步增大密钥空间,形成 128 位的哈希值。因此,可以推断出密钥空间大小约为 $10^{16 \times 2} \times 2^{128} \approx 2^{234}$,远大于 2^{100} 的理论要求,如表 5 所示,不难看出该算法比其他文献具有更大的密钥空间。总之,该算法的关键空间足够大,可以抵御各种穷举攻击。

表 5 密钥空间大小对比			
算法	本文	文献[19]	文献[20]
密钥空间	2^{234}	2^{186}	2^{200}

3.2.5 差分统计分析

原始图像和加密图像之间的区别可以通过两个标准来衡量,即 NPCR 和 UACI 指标。图像加密算法对明文敏感性度量通常采用像素改变率 NPCR(Number of Pixels Change Rate)和归一化平均改变强度 UACI(Unified Average Changing Intensity)。计算公式为:

$$\left\{ \begin{aligned} \text{NPCR} &= \frac{1}{M \times N} \times \sum_{i=1}^M \sum_{j=1}^N D(i,j) \times 100\% \\ \text{UACI} &= \frac{1}{M \times N} \times \sum_{i=1}^M \sum_{j=1}^N \frac{|v_1(i,j) - v_2(i,j)|}{255} \times 100\% \end{aligned} \right.$$

(13)

其中, $M \times N$ 为图像的尺寸大小; v_1, v_2 分别为明文图像改变一个像素前后的密文图像。 D 可以由下式定义:

$$D = \begin{cases} 0 & \text{if } v_1(i,j) = v_2(i,j) \\ 1 & \text{if } v_1(i,j) \neq v_2(i,j) \end{cases}$$

(14)

表 6 和表 7 显示了根据公式所计算出的算法

结果。得到 NPCR 和 UACI 的平均值分别为 99.6112%和 33.7745%,非常接近理论值,表明加密算法具有强的抗明文攻击能力。

表 6 NPCR 测试值				
图像	R	G	B	平均值
Lena	99.6098	99.6173	99.6024	99.6098
All black	99.5712	99.6491	99.6323	99.6175
Worldcup	99.5952	99.6066	99.6082	99.6033
Vision	99.6113	99.5794	99.6048	99.5985
Animal	99.6210	99.6106	99.6490	99.6268

表 7 UACI 测试值				
图像	R	G	B	平均值
Lena	33.4816	33.4860	33.4546	33.4740
All black	34.8173	34.8528	34.7957	34.8219
Worldcup	33.6099	33.6037	33.4850	33.5662
Vision	33.3815	33.4313	33.5851	33.4659
Animal	33.5533	33.5331	33.5470	33.5444

3.3 鲁棒性分析

鲁棒性是图像加密算法评估中的一个重要指标,它衡量了加密算法在面对各种干扰噪声时,能否有效地保护图像的内容不受损坏或泄露。在现实世界中,图像可能受到多种干扰的影响。因此,对图像加密算法的鲁棒性进行分析和评估是至关重要的。本节选取椒盐噪声和遮挡噪声进行分析。

3.3.1 椒盐噪声攻击分析

分别在密文图像上加入 5%、10%和 20%的椒盐噪声,由图 5 可以看出,加噪的图像解密后仍然可以有效辨认图像信息。

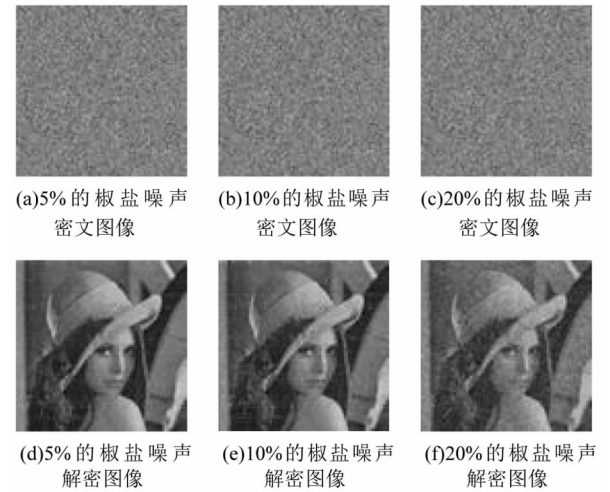


图 5 加入椒盐噪声后的密文及解密图像

3.3.2 遮挡噪声攻击分析

分别在密文图像上加入 64×64 、 80×80 和

96×96 的遮挡噪声,由图 6 可以看出,加噪的图像解密后仍然可以有效辨认图像信息。

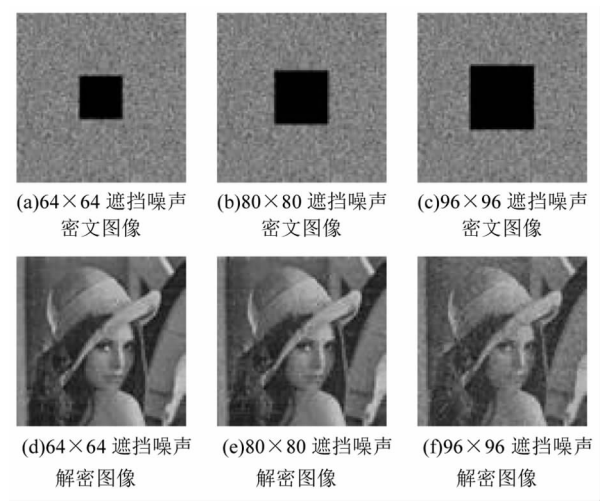


图 6 加入遮挡噪声后的密文及解密图像

4 结 论

本文提出了一种将 DNA 动态编码和 2D-LSM 离散混沌相结合的安全增强型数字图像加密方案。以离散混沌为加密算法的核心,采用二进制比特平面加扰,DNA 动态编解码以及 DNA 域密文扩散等方法对数字图像进行加密。实验结果和理论分析表明,加密算法可以抵抗椒盐噪声攻击及遮挡噪声攻击。理论分析和数值仿真表明,所提出的图像加密算法具有密钥空间大、相邻像素相关性强、直方图等统计结果优良的性能,差分分析实验结果有效佐证了该算法具有抵抗明文攻击的鲁棒性。因此,本文所提出的结合 DNA 动态编码和离散混沌的数字图像加密算法是一个优良的隐私保护技术方案。在未来的工作中,将进一步对加密方案的安全性以及效率性能开展研究,结合实际应用场景,设计更为优选的图像加密技术方案,为网络大数据环境下的多媒体信息安全赋能。

参考文献

[1] HUA Z Y, ZHOU Y C, HUANG H J. Cosine-transform-based chaotic system for image encryption[J]. Information Sciences, 2019, 480: 403—419.

[2] PISARCHIK A N, ZANIN M. Chaotic map cryptography and security[J]. Encryption: Methods, Software and Security, 2010: 1—28.

[3] XU L, GOU X, LI Z, et al. A novel chaotic image encryption algorithm using block scrambling and dynamic index based diffusion[J]. Optics and Lasers in Engineering, 2017, 91: 41—52.

[4] 温贺平. 正弦驱动的 Chen 超混沌系统动力学特性及其电路仿真[J]. 合肥工业大学学报(自然科学版), 2018, 41(8): 1046—1051.

[5] WEN H P, CHEN R T, YANG J Y, et al. Security analysis of a color image encryption based on bit-level and chaotic map [J]. Multimedia Tools and Applications, 2023, 82:1—17.

[6] XIAN Y J, WANG X Y, YAN X P, et al. Image encryption based on chaotic sub-block scrambling and chaotic digit selection diffusion[J]. Optics and Lasers in Engineering, 2020, 134: 106202.

[7] YU F, GONG X H, LI H P, et al. Differential cryptanalysis of image cipher using block-based scrambling and image filtering[J]. Information Sciences, 2021, 554: 145—156.

[8] WANG Y H, ZHAO Q Y, ZHANG H R, et al. Optical single-channel color image encryption based on chaotic fingerprint phase mask and diffractive imaging[J]. Applied Optics, 2023, 62: 1009—1018.

[9] ZHANG Y S, ZHOU W T, ZHAO R Y, et al. F-TPE: Flexible thumbnail-preserving encryption based on multi-pixel sum-preserving encryption [J]. IEEE Transactions on Multimedia, 2022, 41: 1—15.

[10] CAO Z J, MARKOWITCH O. Comment on circuit cipher-text policy attribute-based hybrid encryption with verifiable delegation in cloud computing [J]. IEEE Transactions on Parallel and Distributed Systems, 2021, 32(2): 392—393.

[11] ZEFREH E Z. An image encryption scheme based on a hybrid model of DNA computing, chaotic systems and hash functions[J]. Multimedia Tools and Applications, 2020, 79 (33—34): 24993—25022.

[12] WANG X Y, LI Y P. Chaotic image encryption algorithm based on hybrid multi-objective particle swarm optimization and DNA sequence[J]. Optics and Lasers in Engineering, 2021, 137: 106393.

[13] JIANG X, XIAO Y, XIE Y Y, et al. Exploiting optical chaos for double images encryption with compressive sensing and double random phase encoding[J]. Optics Communications, 2021, 484: 126683.

[14] QOBBY Y, JARJAR A, ESSAID M, et al. Image encryption algorithm based on genetic operations and chaotic DNA encoding[J]. Soft Computing, 2022,26: 5823—5832.

[15] ZANG H Y, TAI M D, WEI X Y. Image encryption schemes based on a class of uniformly distributed chaotic systems[J]. mathematics, 2022, 10(7): 1027.

[16] Dou Y, Li M. Cryptanalysis of a new color image encryption using combination of the 1d chaotic map[J], Applied Sciences, 2020, 10(6): 2187.

[17] 牛莹, 张勋才. 基于变步长约瑟夫遍历和 DNA 动态编码的图像加密算法[J]. 电子与信息学报, 2020, 42(6): 1383—1391.

[18] HUA Z, ZHU Z, CHEN Y, et al. Color image encryption using orthogonal Latin squares and a new 2D chaotic system [J]. Nonlinear Dynamics, 2021, 104: 4505—4522.

[19] YE G, PAN C, DONG Y X, et al. Image encryption and hiding algorithm based on compressive sensing and random numbers insertion [J]. Signal Processing, 2020, 172: 107563.

[20] GUESMI R, FARAH M A B. A new efficient medical image cipher based on hybrid chaotic map and DNA code[J]. Multimedia Tools and Applications, 2021, 80: 1925—1944.