Journal of Image and Signal Processing 图像与信号处理, 2023, 12(2), 116-127
Published Online April 2023 in Hans. https://www.hanspub.org/journal/jisp
https://doi.org/10.12677/jisp.2023.122012

Hans汉斯

基于中国剩余定理和混沌系统的高低位图像分治加密

曾皓炜，白恩健，吴　赟

东华大学信息科学与技术学院，上海

收稿日期：2023年3月24日；录用日期：2023年4月14日；发布日期：2023年4月26日

摘　要

提出了一种基于中国剩余定理(CRT)和分数阶混沌系统的高低位比特图像加密算法。通过CRT将相邻像素融合，利用高低位分割提取重要图像子带和次要图像子带，对重要子带进行DNA加密，再执行跨子带间的置乱扩散，最后再通过高低位的合并和CRT逆变换(INCRT)，将加密效果散布至全局。由于只对重要子带进行DNA加密，算法的效率得到提升。实验结果证明，算法具有良好的加密性能，能够抵御各种安全攻击。

关键词

中国剩余定理，高低位加密，分治加密，DNA加密，分数阶混沌系统

Divide-and-Conquer Encryption of High and Low Bit Images Based on Chinese Remainder Theorem and Chaotic System

Haowei Zeng, Enjian Bai, Yun Wu

School of Information Science & Technology, Donghua University, Shanghai

Received: Mar. 24th, 2023; accepted: Apr. 14th, 2023; published: Apr. 26th, 2023

Abstract

A high and low bit image encryption algorithm based on Chinese Remainder Theorem (CRT) and fractional order chaotic system is proposed. The adjacent pixels are fused by CRT, the important image sub-band and the secondary image sub-band are extracted by high and low bit segmenta-

文章引用: 曾皓炜, 白恩健, 吴赟. 基于中国剩余定理和混沌系统的高低位图像分治加密[J]. 图像与信号处理, 2023, 12(2): 116-127. DOI: 10.12677/jisp.2023.122012

tion, DNA encryption is performed on the important sub-band, and then scrambling and diffusion across sub-bands are performed, and finally the combination of high and low bits is performed and INCRT, to spread the encryption effect globally. Since DNA encryption is only performed on important sub-bands, the efficiency of the algorithm is improved. And the test results prove that the algorithm has good encryption performance and can resist various security attacks.

Keywords

Chinese Remainder Theorem, High and Low Encryption, Divide and Conquer Encryption, DNA Encryption, Fractional Chaos System

1. 引言

在移动互联网蓬勃发展的今天，各种多媒体充斥我们的生活，信息泄露的问题也愈发突出。图像作为多媒体信息的重要组成部分，具有生动直观，信息量大的特点，其一旦遭到窃取，会给人们的生活带来不小的困扰。因此，图像在网络中传输的安全性是移动多媒体时代的重点。

在众多图像安全技术中，如图像数字水印，图像信息和图像加密等，图像加密是最直观且有效的方法，其将明文图像加密成完全无序的密文图像，在没有正确密钥的前提下，即使窃取了图像也无法获取其中所蕴含的宝贵信息，因此图像加密领域一直是研究人员的研究重点。通常情况下，图像加密采用混沌理论作为基础，结合其他技术以提高安全性能，例如光场加密[1] [2]，DNA 加密[3] [4] [5] [6]以及基于离散余弦变换或离散小波变换的频域加密[7] [8] [9]等。其中，DNA 加密具有高度并行和高信息密度的特点，可以提高像素间扩散置乱的混淆效果，进一步提高图像加密的安全性，但其存在耗时间长的缺点。为了平衡加密性能与加密效率的问题，有选择性地加密图像重要信息就成为一种可能的方案。而图像压缩中的离散小波变换，或信息隐藏中的高低位分割[10]都可以作为图像重要信息的提取方法。

基于上述观点，本文提出了一种基于四维分数阶混沌系统和中国剩余定理的高低位图像分治加密。该加密算法首先利用中国剩余定理将相邻像素的信息融合，又通过高低比特位数的分割，提取出图像的重要和次要子带，对重要子带执行 DNA 加密，再通过跨子带间的置乱扩散将加密效果融合至所有子带，提高密文图像安全性能，且密钥与明文高度相关，能够抵抗已知明文攻击。实验结果表明，该加密系统具有良好的加密性能。

2. 理论知识

2.1. 中国剩余定理

中国剩余定理(Chinese Remainder Theorem, CRT)，是数论中的一个关于求解一元线性同余方程组的定理，其给出了以下的一元同余方程组

$$\begin{cases} x \equiv a_1 \left(\mathrm{mod}\, m_1\right) \\ x \equiv a_2 \left(\mathrm{mod}\, m_2\right) \\ \quad \vdots \\ x \equiv a_n \left(\mathrm{mod}\, m_n\right) \end{cases} \tag{1}$$

有解的判定条件：假设整数 $m_1, m_2, \cdots, m_n$ 其中任两数互质，则对任意的整数：$a_1, a_2, \cdots, a_n$ 方程组有解。具体解法如下所示

设 $M = \prod_{i=1}^{n} m_i$ ， $M_i = M / m_i$ ；

设 $t = M_i^{-1}$ 为 M_i 模 m_i 的数论倒数： $t_i M_i \equiv 1 \left(\mathrm{mod}\, m_i\right)$ 。

方程组的通解形式为：

$$\begin{aligned} x &= a_1 t_1 M_1 + a_2 t_2 M_2 + \cdots + a_n t_2 M_n + kM \\ &= \sum_{i=1}^{n} a_i t_i M_i + kM \quad \left(k \in Z\right) \end{aligned}$$

其在模 M 的前提下即只有唯一解 $\sum_{i=1}^{n} a_i t_i M_i$ 。

在图像处理领域，利用中国剩余定理，可以将多个像素的值计算为一个值，实现多个像素合一的过程，以此达到图像压缩的效果，2021 年，Vidhya 和 Brindha 就对此做了试验[11]，验证了该方案的可行性。其中，CRT 的计算结果减少了像素位数，在压缩的同时，也将两个像素的信息合并成一个更高位的像素，这一结果有助于后续的高低位分割，因此将 CRT 作为加密算法的预处理。

2.2. 四维分数阶混沌陈系统

将四维超混沌陈系统[12]结合微分算子，得到四维分数阶混沌陈系统，其定义如下：

$$\begin{cases} D_{t_0}^{q} x = a\left(y - x\right) + h \\ D_{t_0}^{q} y = bx - xz + cy \\ D_{t_0}^{q} z = xy - dz \\ D_{t_0}^{q} x = yz + rz \end{cases} \tag{2}$$

其中，当 $a = 35, b = 3, c = 12, d = 7, r = 0.5, q = 0.95$ 的时候，该系统进入混沌状态。

2.3. DNA 编码

在生物学中，一个 DNA 序列有四种碱基：C (胞嘧啶)、T (胸腺嘧啶)、A (腺嘌呤)和 G (鸟嘌呤)，其中 A 与 T 互补，C 与 G 互补。利用 DNA 的碱基互补配对原理，可以分别用二进制 00、01、10 和 11 来表示 A、T、C 和 G。因此，灰度图像的 8 位二进制数可以用长度为 4 的 DNA 序列来编码表示。

由表 1 看出，共有 8 种编码方式来实现 DNA 的编码[13]，选择表中的编码方式 1，八位二进制 11000101 就可以编码成 TAGG。在此基础上对 DNA 序列进行加，减，异或，同或运算后再进行 DNA 的解码即可实现数据的加密。

本文将混沌序列和 DNA 编码相结合，对重要子带进行扩散加密。

Table 1. Eight ways of DNA encoding and decoding
表 1. DNA 编解码的八种方式

Rules	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	11	11	01	10
C	10	01	11	00	00	00	10	01

3. 加密算法

本文提出的图像加密算法流程图如图 1 所示，采用 CRT 作前置处理，将相邻的两个 8 位像素计算为 1 个 16 位的像素，再将图像分为四个子带，其中两个是高 8 位的主要子带，两个是次要子带。之后对切割后的重要子带执行 DNA 加密，利用跨子带的置乱扩散将效果散布给剩余两个次要子带，提高整体密文的安全级别。最后将四个子带合并，并且进行 CRT 的逆运算，得到最终的加密图像。

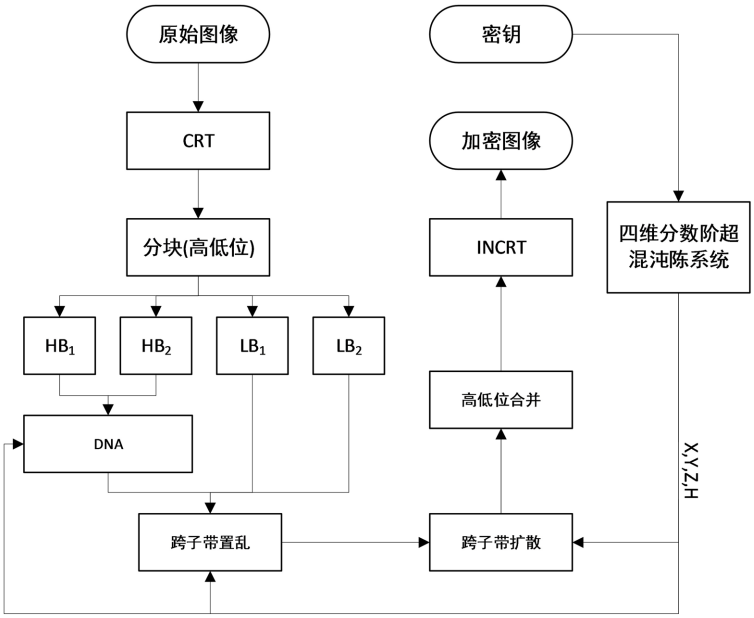


Figure 1. Algorithm encryption flow chart
图 1. 算法加密流程图

3.1. 加密方案的密钥

为了抵抗暴力攻击，一个图像加密算法必须拥有一个足够大的密钥空间，否则，攻击者可以通过枚举破解。本文加密算法的密钥位长度有 288 位，且分为两个部分，具有足够的密钥空间来抵抗暴力攻击。

第一部分密钥是原始图像的 SHA-256 哈希值，共 256 位，将其分成 32 部分，每部分 8 位，表示为 $k_1,k_2,\cdots,k_{32}$。第二部分密钥是循环移位值 t，共 32 位，将其分成 4 部分，每部分 8 位，表示为 t_1,t_2,t_3,t_4。这两部分 288 位密钥通过如下的公式来生成四维分数阶混沌系统的四个初值：

$$\begin{cases} h_1 = LC_{t_1}\left(k_1 \oplus k_2 \oplus \cdots \oplus k_8\right) \\ h_2 = LC_{t_2}\left(k_9 \oplus k_{10} \oplus \cdots \oplus k_{16}\right) \\ h_3 = LC_{t_3}\left(k_{17} \oplus k_{18} \oplus \cdots \oplus k_{24}\right) \\ h_4 = LC_{t_4}\left(k_{25} \oplus k_{26} \oplus \cdots \oplus k_{32}\right) \end{cases} \tag{3}$$

$$\begin{cases} x_0 = \mathrm{mod}\left(\left(h_1 + h_2\right) \times 10^{14}\right) / 255 \\ y_0 = \mathrm{mod}\left(\left(h_3 + h_2\right) \times 10^{14}\right) / 255 \\ z_0 = \mathrm{mod}\left(\left(h_3 + h_4\right) \times 10^{14}\right) / 255 \\ h_0 = \mathrm{mod}\left(\left(h_1 + h_2 + h_3 + h_4\right) \times 10^{14}\right) / 255 \end{cases} \tag{4}$$

其中，⊕为异或操作，LC_t 为向左循环移位 t 位，mod 为模 256 运算。

利用原始图像的哈希值作为密钥的一部分，可以使得密钥与原始图像强相关，原始图像的微小变化都会导致密钥的变化，增强密钥的可靠性。密钥中的 t 循环移位给加密方案使用者提供了密钥的一部分自主权，不仅继续扩充了密钥空间，且使得图像哈希值各部分相互影响，提高算法抵御选择明文攻击的能力。

3.2. 中国剩余定理预处理

通过 CRT 的计算，可以将相邻(从左至右)的两个 8 位像素融合成一个 16 位的像素。由于 CRT 计算过程中需要求取余数，在图像尺寸过大时可能耗费过多时间，便采取空间换时间的方法，对 CRT 的计算结果建表来加速算法的运行。同时，只对相邻像素的低 4 位做 CRT 计算，作为 16 位结果像素的低 8 位，将两个原像素的高 4 位合并，作为 16 位结果像素的高 8 位。具体步骤如下：

将待计算的像素分为高四位和低四位，将两个像素的高 4 位依次作为结果前 8 位。

对两个低 4 位的值进行计算，得到一个 8 位的 CRT 结果，即在预先建立好的表中查询对应结果。其中，由于 CRT 计算中的互质数需大于被计算数，因此有可能存在结果超过 8 位的情况，对此，将表中超过 8 位的部分结果替换为 0~255 中未在表中出现的数，以保证两个低 4 位的值计算结果为 8 位。

将步骤 1 和 2 的结果依次拼接在一起，即得到最终的 16 位像素值，具体示例如图 2。

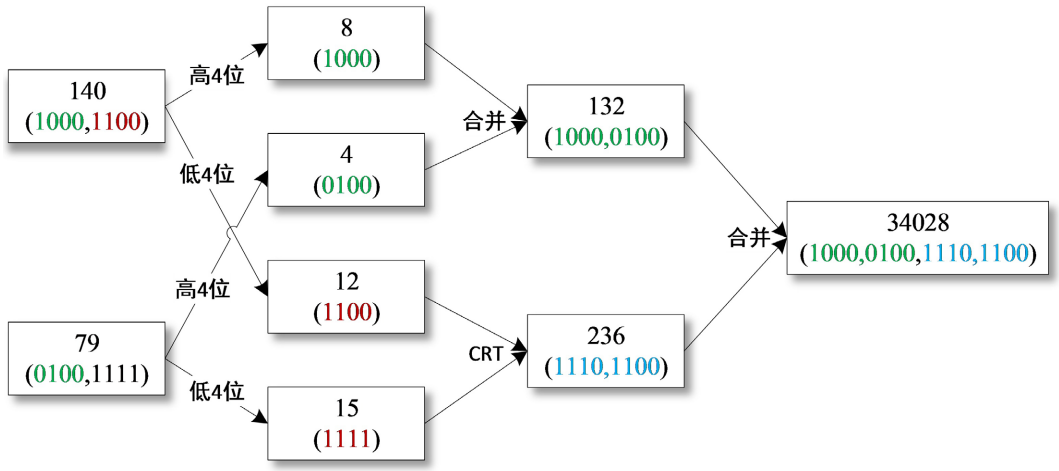


Figure 2. Schematic diagram of CRT calculation
图 2. CRT 计算示意图

对所有像素执行完上述步骤即得到 CRT 的结果矩阵 C。

3.3. 高低位分块加密

3.3.1. 高低位分块

将经过 CRT 计算的结果矩阵 C 进行高低位子带的分割，如图 3 所示。

首先从上至下进行对半的分割，再对每个像素进行二进制的分组，分为高 8 位和低 8 位，并按照原图矩阵的位置分别存放，得到 4 个 8 位子带图像。其中两个低 8 位的子带 LB_1, LB_2 为原始图像中相邻像素的低 4 位 CRT 计算结果，属于原始图像的次要信息，而两个高 8 位的子带 HB_1, HB_2 是原始图像中相邻像素的高 4 位合并结果，其携带了原始图像的主要信息，因此属于重要子带。

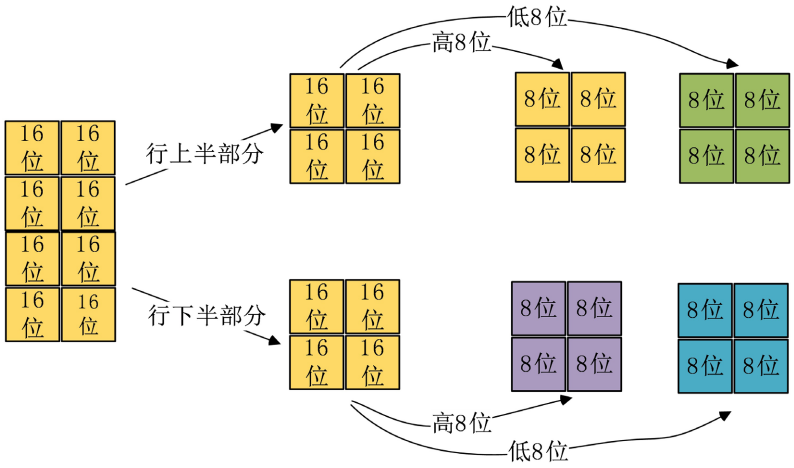


Figure 3. Schematic diagram of high and low blocks
图 3. 高低位分块示意图

3.3.2. 重要子带加密

用四维混沌序列中的 X 对分别对两个重要子带 HB_1, HB_2 进行 DNA 编码，再利用 X, Y, Z, H 生成 DNA 运算中所需要的混沌矩阵 R，对编码后的子带进行 DNA 级别的扩散，最后再使用 H 进行 DNA 的解码得到加密完成的子带 HB_1', HB_2'。

3.3.3. 跨子带置乱

跨子带置乱可以在四个子带间随机排列元素，可以显著降低子带内的元素相关性，并且将重要子带的 DNA 加密的效果散布给两个次要子带，以提高安全级别。置乱过程受混沌序列所控制，对于四个尺寸均为 $N \times M$ 的子带，具体步骤如下所示：

将四个子带合并成一个三维矩阵 P，其中 $P(i,j,1) = HB_1'$，$P(i,j,2) = HB_2'$，$P(i,j,3) = LB_1$，$P(i,j,4) = LB_2$。

利用混沌序列 X, Y, Z, H 计算出尺寸为 $N \times M \times 4$ 的随机矩阵 R，对 3 维矩阵R的第 3 维进行排序，得到 3 维索引矩阵 RR，然后利用 RR 置乱三维矩阵 P，得到结果矩阵 P'，其中 $P'(i,j,k) = P(i,j,RR(i,j,k)), (i \in [1,N], j \in [1,M], k \in [1,4])$，完成跨子带置乱。

重新将 3 维矩阵 P' 分割成四个子带，并展开成四个一维序列 W_1, W_2, W_3, W_4，再利用混沌系统生成四个混沌序列，并对其排序得到四个索引序列 I_1, I_2, I_3, I_4，，用 I_i 置乱 W_i 得到结果 W_i'，实现子带内置乱，其中 $W_j^i(j) = W_i(I_i(j)), (i \in [1,4], j \in [1, NM])$。

3.3.4. 跨子带扩散

四个子带间的相互扩散可以将任意像素值的微小变化传播到整个图像，使得重要子带的扰动扩散至次要子带，进一步将 DNA 加密的效果扩散至整张密文图像，以助于抵抗选择明文攻击。对于四个尺寸均为 $N \times M$ 的子带，将其依次重排为四个长度为 NM 一维序列 A_1, A_2, A_3 和 A_4，然后按如下步骤进行扩散：

用次要子带序列 A_4 和混沌序列 X 扰乱重要子带 A_1，得到 B_1

$$\begin{cases} B_1(1) = (A_1(1) + A_4(1) + X(1)) \bmod 256, i = 1 \\ B_1(i) = (A_1(i) + A_4(i) + X(i)) \bmod 256 \oplus B_1(i-1), i \in [2, N^2] \end{cases} \tag{5}$$

用次要子带序列 A_2 和混沌序列 Y 扰乱重要子带 A_3，得到 B_3

$$\begin{cases} B_3(1) = \left(A_3(1) + A_2(1) + Y(1)\right) \bmod 256, i = 1 \\ B_3(i) = \left(A_3(i) + A_2(i) + Y(i)\right) \bmod 256 \oplus B_3(i-1), i \in \left[2, N^2\right] \end{cases} \tag{6}$$

用序列 B_1 和混沌序列 Z 扰乱次要子带 A_2，得到 B_2

$$\begin{cases} B_2(1) = \left(A_2(1) + B_1(1) + Z(1)\right) \bmod 256, i = 1 \\ B_2(i) = \left(A_2(i) + B_1(i) + Z(i)\right) \bmod 256 \oplus B_2(i-1), i \in \left[2, N^2\right] \end{cases} \tag{7}$$

用序列 B_3 和混沌序列 H 扰乱次要子带 A_4，得到 B_4

$$\begin{cases} B_4(1) = \left(A_4(1) + B_3(1) + H(1)\right) \bmod 256, i = 1 \\ B_4(i) = \left(A_4(i) + B_3(i) + H(i)\right) \bmod 256 \oplus B_4(i-1), i \in \left[2, N^2\right] \end{cases} \tag{8}$$

将扩散完毕的四个序列重排为二维的子带，完成扩散。

4. 结果分析

本文使用 CPU 为 AMD 5800H 的硬件平台，在 Windosw11 操作系统上使用 MatlabR2021b 模拟仿真了本算法，并对其安全性能进行了测试和分析。

4.1. 加密效率分析

Table 2. Comparison of algorithm operation efficiency
表 2. 算法运行效率比较

图像尺寸	本文加密方案	DNA 加密
256 × 256	1.30s	1.43s
512 × 512	3.57s	4.98s
1024 × 1024	13.04s	19.46s

算法的运行效率是一个衡量算法优劣的重要指标，一个效率极低的加密系统是没有实际应用意义的。由表 2 可以看出，在不同尺寸下，本文加密方案的加密时间均小于对全图采用 DNA 加密的加密方案，且随着尺寸的增大，二者之间的差距越来越大。因此可以看出本算法的分治加密在加密速度上有着一定的优势。

4.2. 加密结果与直方图分析

一个有效的图像加密方案应该能够将普通图像加密为无法识别的密码图片，且在没有密钥的前提下无法从加密图像得到原始图像的任何信息。

图 4 给出了 Lena、Peppers、Airplane、Mandrill 四张图像的加密图像及加密前后的直方图。从图 4 的实验结果可以看到，原始图像(均为 512 × 512)的直方图携带有图片的大量信息，而加密后的直方图类似随机分布，无法从加密后的图像中获取与缩略图像有关的统计信息，因此该加密算法能够抵抗统计攻击。

4.3. 密钥敏感性与密钥空间

一个加密算法应该对密钥非常敏感，否则它的实际密钥空间可能远比理论值小，从而增加被暴力攻击破坏的风险。如果加密算法对密钥极其敏感的话，在对同一图像进行加密的过程中，对密钥的细微改动都会造成完全不同的加密效果，且无法用细微改动后的密钥去解密图像。

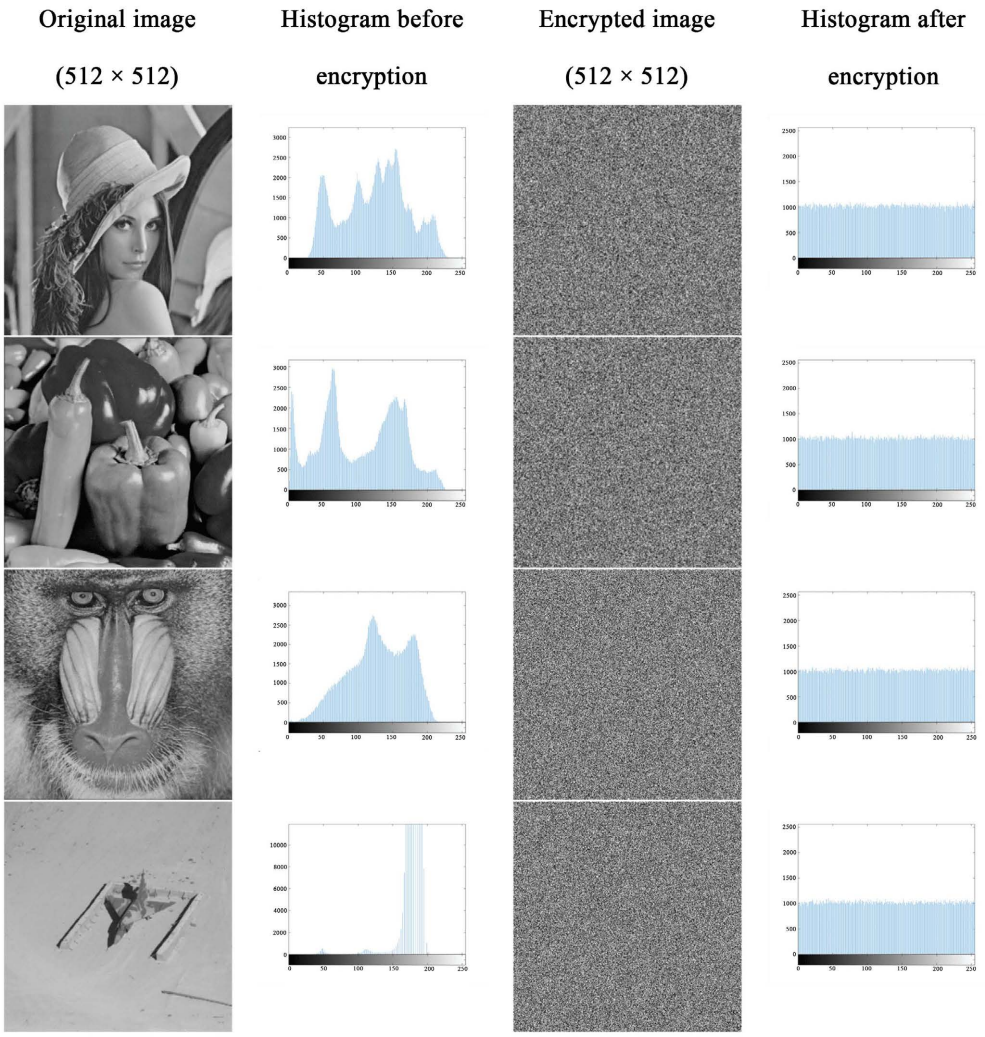


Figure 4. Results and histograms of different images before and after encryption
图 4. 不同图像加密前后的结果与直方图

对此我们采用 512 × 512 的 Lena 图像进行这项测试，首先生成 Key1，对 Key1 仅改动 1 比特得到 Key2 和 Key3，三个密钥分别为：

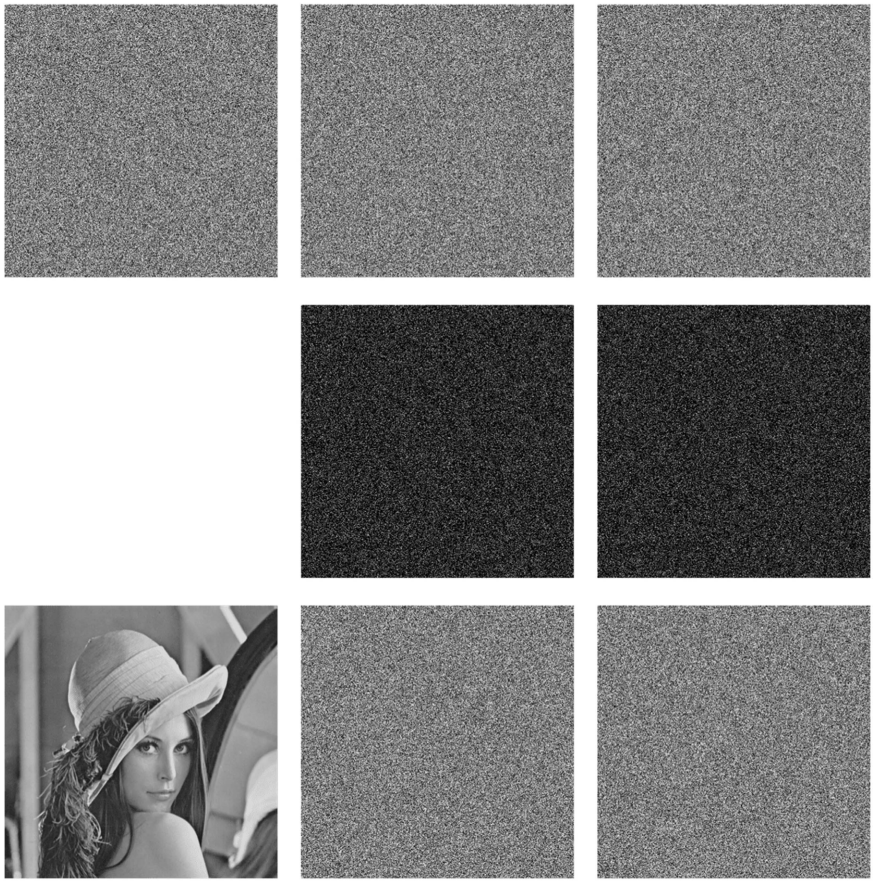
Key1 = 25728D126918052AB7B93683092B4043A5C2BB3110BC260627601EAE0FFA599AE6A9

Key2 = 25738D126918052AB7B93683092B4043A5C2BB3110BC260627601EAE0FFA599AE6A9

Key3 = 05728D126918052AB7B93683092B4043A5C2BB3110BC260627601EAE0FFA590AE6A9

图 5 中(a)从上至下是用 Key1 加密的 C1 和解密的 Lena，(b)从上至下是用 Key2 加密的 C2，|C2-C1|，以及用 Key3 去解密 C1 得到错误解密图像，(C)从上至下是用 Key3 加密的 C3，|C3-C1|，以及用 Key3 去解密 C1 得到的错误解密图像。可见用与 Key1 仅有一比特差距的 Key2 和 Key3 加密同一张图片，得到的密文图像与用 Key1 加密的密文图像完全不同，并且用图中的解密实验也验证了只有使用完全正确的密钥才可以获得正确的解密图像，密钥的极小变化也会导致完全不同的结果。

通常密钥空间大于 2^{100} 时，可认为该密钥能抵抗穷举攻击[14]，本文的密钥由 256 位的图像哈希值与 32 位的循环移位值组成，密钥空间为 2^{288}，足够抵抗暴力攻击。



(a) (b) (c)

Figure 5. Key sensitivity verification
图 5. 密钥敏感性验证

因此，本算法的密钥具有高度的敏感性和足够大的密钥空间，能抵御明文攻击和穷举攻击。

4.4. 相关性分析

在自然图像中，相邻像素的值存在很高的相关性。一个有效的图像加密算法应该具备降低相邻像素相关性的能力，相关性越小，表明加密算法的性能越好。相关性的定义为：

$$Corr(X,Y)=\left|\frac{E\left[(X-\mu_X)(Y-\mu_Y)\right]}{\sigma_X\sigma_Y}\right| \tag{9}$$

其中 E,μ 和 σ 分别表示数学期望，均值和标准差，同时 X 和 Y 是两个相邻的序列，可以是沿水平，垂直或对角线方向的像素。如果 X 和 Y 高相关，则 $Corr$ 接近 1，否则接近 0。

表 3 给出了 4 张不同图像的原始相关性和加密后相关性，所有图像的三个方向相关性均在加密后有了大幅度降低，远小于原始图像，且均接近于 0，因此表明本算法可以减少图像相邻像素相关性，具有良好的加密性能。

4.5. 信息熵

图像的信息熵定义为：

Table 3. Pixel correlation of images before and after encryption
表 3. 标准试验系统结果数据

图像	方向/原始图像			方向/加密图像		
	水平	垂直	对角	水平	垂直	对角
Lena	0.9723	0.9841	0.9587	0.0004	0.0011	0.0132
Peppers	0.9785	0.9821	0.9654	−0.0245	0.0049	−0.0013
Airplane	0.9528	0.9447	0.9130	0.0113	−0.0015	0.0006
Mandrill	0.8618	0.7620	0.7273	0.0007	0.0011	−0.0261

$$H=-\sum_{i=0}^{255}p(i)\log_2^{p(i)} \tag{10}$$

其中， $p(i)$ 表示 0~255 这 256 个像素值的概率。

信息熵可以用来衡量信息的不确定性，因此密文图像的信息熵越大，其不确定性也就越好，从密文图像中获取明文图像的信息就越难。对于 8 位的灰度图像，信息熵的理论最大值为 8。因此，密文图像的信息熵越接近 8 就越接近随机图像。

Table 4. Information entropy of image before and after encryption
表 4. 图像加密前后的信息熵

图像	原始图像信息熵	加密图像信息熵
Lena	7.4456	7.9992
Peppers	7.5715	7.9993
Airplane	4.0045	7.9994
Mandrill	7.3579	7.9993

表 4 对比了五张不同图像在加密前后的信息熵，加密后的密文图像信息熵均高于原始图像，且接近理想值 8，说明了本文算法具有预期的随机性和安全性。

4.6. 抗差分攻击

为了测试本文的加密算法是否能抵抗差分攻击，通常使用像素变化率(NPCR)和平均变化强度(UACI)来定量测试加密算法抵抗差分攻击的能力[15] [16]。NPCR 和 UACI 的定义如下：

$$\mathrm{NPCR}=\frac{\sum_{i,j}A(i,j)}{N\times M}\times 100\% \tag{11}$$

$$\mathrm{UACI}=\frac{1}{N\times M}\sum_{i,j}\left(\frac{C_1(i,j)-C_2(i,j)}{255}\right)\times 100\% \tag{12}$$

其中 C_1 和 C_2 是两张密文图像，他们各自的明文图像之间仅有 1 比特的差距。当 $C_1(i,j)$ 不等于 $C_2(i,j)$ 时，$A(i,j)$ 就等于 1，否则等于 0，且 M 和 N 是图像的高和宽。对于 512 × 512 的图像，NPCR 的期望值为 99.5893%，而 UACI 的期望区间为 33.3730%~33.5541%。当图像加密算法的 NPCR 高于对应的期望值，且 UACI 落入期望区间时，说明算法可以抵抗差分攻击。

Table 5. NPCR and UACI of the image
表 5. 图像的 NPCR 和 UACI

图像	NPCR	UACI	差分攻击测试结果
Lena	99.6075%	33.4514%	通过
Peppers	99.6103%	33.4473%	通过
Airplane	99.6028%	33.4481%	通过
Mandrill	99.6131%	33.4605%	通过

本实验对每张测试图像选取了 100 个不同的位置来计算 NPCR 和 UACI，并对此取平均值。实验结果如表 5 所示，四张测试图像的 NPCR 均高于理论期望值，且 UACI 落入期望区间，说明本文的图像加密算法可以抵抗差分攻击。

5. 总结

算法中的中国剩余定理预处理，可以融合相邻像素的信息，在完成轻加密同时为后续的高低位加密做基础。

本文算法中的高低位分治加密部分，采取对重要子带执行 DNA 加密，再通过子带间置乱扩散的策略，将加密效果散布至整张密文图像。因此在保证加密性能的同时，提高了加密效率，而实验仿真的结果验证了这一结论。

在中国剩余定理的预处理部分，还可以通过优化编码规则，在加密的同时，实现无损压缩，进一步提升该加密系统的可行性。今后也可以继续对高低位的分治加密作进一步的研究，进一步提升加密效率。

参考文献

[1] Li, X., Mou, J., Cao, Y. and Banerjee, S. (2022) An Optical Image Encryption Algorithm Based on a Fractional Order Laser Hyperchaotic System. *International Journal of Bifurcation and Chaos*, **32**, Article ID: 2250035. https://doi.org/10.1142/S0218127422500353

[2] Faragallah, O.S., *et al.* (2021) Efficient Optical Double Image Cryptosystem Using Chaotic Mapping-Based Fresnel Transform. *Optical and Quantum Electronics*, **53**, 305. https://doi.org/10.1007/s11082-021-02864-5

[3] Tang, Z., Yin, Z., Wang, R., Wang, X., Yang, J. and Cui, J. (2022) A Double-Layer Image Encryption Scheme Based on Chaotic Maps and DNA Strand Displacement. *Journal of Chemistry*, **2022**, Article ID: 3906392. https://doi.org/10.1155/2022/3906392

[4] Huang, Z.-W. and Zhou, N.-R. (2022) Image Encryption Scheme Based on Discrete Cosine Stockwell Transform and DNA-Level Modulus Diffusion. *Optics & Laser Technology*, **149**, Article ID: 107879. https://doi.org/10.1016/j.optlastec.2022.107879

[5] Chen, L., Li, C. and Li, C. (2022) Security Measurement of a Medical Communication Scheme Based on Chaos and DNA Coding. *Journal of Visual Communication and Image Representation*, **83**, Article ID: 103424. https://doi.org/10.1016/j.jvcir.2021.103424

[6] Elsaid, S.A., Alotaibi, E.R. and Alsaleh, S. (2023) A Robust Hybrid Cryptosystem Based on DNA and Hyperchaoticfor Images Encryption. *Multimedia Tools and Applications*, **82**, 1995-2019.

[7] Gupta, M., Singh, V.P., Gupta, K.K. and Shukla, P.K. (2023) An Efficient Image Encryption Technique Based on Two-Level Security for Internet of Things. *Multimedia Tools and Applications*, **82**, 5091-5111. https://doi.org/10.1007/s11042-022-12169-8

[8] Wen, H., *et al.* (2022) Design and Embedded Implementation of Secure Image Encryption Scheme Using DWT and2D-LASM. *Entropy*, **24**, 1332. https://doi.org/10.3390/e24101332

[9] Dong, Y., Huang, X. and Ye, G. (2021) Visually Meaningful Image Encryption Scheme Based on DWT and Schur Decomposition. *Security and Communication Networks*, **2021**, Article ID: 6677325. https://doi.org/10.1155/2021/6677325

[10] Tütüncü, K. and Çataltaş, Ö. (2021) Compensation of Degradation, Security, and Capacity of LSB Substitution Methods by a New Proposed Hybrid n-LSB Approach. *Computer Science and Information Systems*, **18**, 1311-1332.

[11] Vidhya, R. and Brindha, M. (2021) Evaluation and Performance Analysis of Chinese Remainder Theorem and Its Application to Lossless Image Compression. *Journal of Ambient Intelligence and Humanized Computing*. https://doi.org/10.1007/s12652-021-03532-y

[12] Ye, X., Mou, J., Wang, Z., Li, P. and Luo, C. (2018) Dynamic Characteristic Analysis for Complexity of Continuous Chaotic Systems Based on the Algorithms of SE Complexity and C Complexity. In: Gu, X.M., Liu, G.L. and Li, B., Eds., *Machine Learning and Intelligent Communications*, Springer, Berlin, 647-657. https://doi.org/10.1007/978-3-319-73447-7_69

[13] Yang, Y.-G., Guan, B.-W., Li, J., Li, D., Zhou, Y.-H. and Shi, W.-M. (2019) Image Compression-Encryption Scheme Based on Fractional Order Hyper-Chaotic Systems Combined with 2D Compressed Sensing and DNA Encoding. *Optics & Laser Technology*, **119**, Article ID: 105661. https://doi.org/10.1016/j.optlastec.2019.105661

[14] Zhang, Y., Li, C., Li, Q., Zhang, D. and Shu, S. (2012) Breaking a Chaotic Image Encryption Algorithm Based on Perceptron Model. *Nonlinear Dynamics*, **69**, 1091-1096. https://doi.org/10.1007/s11071-012-0329-y

[15] Wu, Y., Noonan, J.P. and Agaian, S. (2011) NPCR and UACI Randomness Tests for Image Encryption. *Cyber Journals*: *Multidisciplinary Journals in Science and Technology*, *Journal of Selected Areas in Telecommunications* (*JSAT*), **1**, 31-38.

[16] Ullah, A., Jamal, S.S. and Shah, T. (2018) A Novel Scheme for Image Encryption Using Substitution Box and Chaotic System. *Nonlinear Dynamics*, **91**, 359-370. https://doi.org/10.1007/s11071-017-3874-6