论文题目

摘要

关键词：

# 介绍

随着互联网的迅速发展，人们将在网络上传递各种各样的信息，而随着传输速度的提高，图像与视频等具有直观视觉效果的多媒体数据逐渐成为当今信息流的主要载体[1], [2]。而在由于在网络中传输的数据易遭到第三方的窃取，若不对数据进行加密，则会存在信息泄露的风险。尤其是对于那些具有一定价值的图像数据，例如艺术家所创作的插画，云盘中存放的个人图片等，如果这些图像数据遭到泄露，所造成的损失是十分惨痛的。但是，随着图像数字高清化的快速发展[3]，图像的尺寸日渐增大，如今各大平台的图像分辨率动辄就是1080p，4k等，而这给图像加密所带来了较大的性能负担。当然，在许多应用场景中，不是所有的情况我们都需要加密解密完整尺寸的图像。比如，在视频网站内各个视频的封面，云盘内所保存的图片，以及某些需要付费购买版权使用的素材网站，在这些场景下，人们均需要进行图片预览操作来决定是否进行下一步，如下周原始图片，购买素材等。而图像预览的核心在于对图片的主要内容进行预览，而并不是图像的完整清晰度，因此我们可以对图像分为两部分，将图像的缩略图和原始图像分开加密，而当需要预览图像时，解密缩略图，而当需要完整图像时，再解密对应的完整图像。

自洛伦兹在1963年提出混沌系统这一概念[4]始，以及Chen和Lai提出了一种在非混沌离散时间系统中产生混沌的方法后[5]，各种各样复杂多变的混沌系统被相继提出[6]–[8]。由于混沌系统对初值的高度敏感以及混沌序列的为随机性，使得其非常适合用于图像加密[9]，因此近年来许多混沌系统图像加密算法被提出[10]–[17]。而DNA加密所具有高度并行和高信息密度的特点，基于混沌系统的DNA加密可以进一步提升像素间的混淆效果和加密算法的安全性[18]，越来越多基于混沌系统的DNA图像加密算法被提出[19]–[27]。但是，这些基于DNA的混沌系统加密方案也有一些缺点，耗时长且可能无法抵御选择明文攻击[28], [29]，并且不能很好的适应图像预览这已使用场景。

根据上文的分析，我们提出了一个新的图像压缩加密算法来适应那些需要图像预览的应用场景，且密钥生成的初值与明文图像高度相关，使得加密算法具有抵抗明文攻击的能力。

本文的主要贡献如下：

1. 本文提出了一个新的差值变换VDT，该变换不仅可以作为图像压缩编码的预处理，也可以提取出图像的缩略图和图像的重要信息，方便我们对总图像和缩略图进行加密。
2. 对原始图像和提取出的缩略图使用不同的加密方案，且在保障缩略图的加密性能的同时，完成对总图像的无损压缩。并且原始图像和缩略图能够分开解密，更好的契合那些需要图像预览的使用场景。
3. 在缩略图的加密方案中，利用VDT能够提取图像重要信息的特点，再与四维混沌系统相结合，将重要信息用高低位加密，而次要信息使用DNA加密，使得加密方案与图像本身高度契合，获得良好的安全性能。

# 预备知识

本节介绍了所提出的图像分块差值变换以及一些后续加密算法所需要的分数阶混沌系统和DNA编码。

## 差值变换

本文提出了一种图像分块差值变换(VDT)，它可以通过计算相邻像素的差值将一个图像分为一个携带重要信息的子带和三个次要子带，并且能够降低图像的总位数为后续的压缩做准备。

VDT的具体步骤如下：

1. 将一个大小为N×N的数字图像分成8×8的块
2. 每个块可等分作4个4×4的子块，选取4个子块中间部分的部分向四周做差值，如Fig.1所示，将得到的结果按图中颜色重排，黄色为左上，灰色为右上，红色为左下，绿色为右下。
3. 对黄色子块重复进行差值，一样选取中间的部分像四周做差值，并按图中颜色重新排列子块
4. 对最后的2×2黄色子块进行差值，用(2,2),(1,2)和(2,1)减去(1,1)，完成变换。

当8×8的图像块进行VDT变换后，四个子带中仅有LT保留了一个未改变的像素，其余三个子带内的值均全为差值。其中，进行VDT变换后留下的查值可类比为图像变化比较剧烈的部分，即高频分量，为图像中相对次要的部分，而LT子带中不仅含有差值，还存在一个未改变的像素，将图像所有8×8的块中所有该像素提取出来，即可得到尺寸为原图像八分之一的缩略图，因此，可以将LT看作四个子带中含有重要信息的子带，而RT, LB,RB三个子带则为次要子带。

同时，大多数图像相邻像素的值是较为接近的，因此图像在进行完VDT变换后，像素上值的位数得到了一定程度的减少，如Fig 2.1中所示。且VDT是一个完全可逆的变换，VDT的反变换INVDT如Fig 2.2所示。因此，可以利用DC编码来对图像进行无损压缩[30]，而通过不变像素提取出的缩略图可以通过额外的加密处理来保障图像预览的安全性。



Fig 2.1 VDT正变换



Fig. 2.2 VDT反变换

## Fractional-order hyperchaotic Chen system

在1999年，陈第一次提出了混沌陈系统[31]，之后又提出了超混沌陈系统[32]，而随着研究的深入，人们发现分数阶混沌系统可以比传统的整数阶混沌系统可以更好的描述自然现象[33]，且具有高非线性，非定域性等特点[34]，四维分数阶超混沌陈系统定义如下：

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。

## DNA编码

在生物学中，一个DNA学列有四种碱基：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，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Tab 2.1看出，可以由8种编码方式来实现DNA的编码[12]，例如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，XOR，XNOR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相结合，对三个次要子带进行DNA级别的扩散加密。

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 | 00 | 11 | 01 | 10 |
| C | 10 | 01 | 11 | 00 | 11 | 00 | 10 | 01 |

Tab 2.1 DNA编解码的八种方式

## 高低位加密

张在2021提出了一种基于高低位操作的混沌图像加密算法[35]，其通过将灰度图像分为高4位和低四位两部分，对两部分分别进行扩散和置换加密操作，该方案具有良好的加密安全性，因此将其作为重要子带LT的加密方案。

# 加密算法

本文提出的压缩加密算法包括两个部分，总体图像部分和缩略图部分，算法总体流程图如Fig 3.1。

1. 对总体图像进行VDT变换，得到变换后的图像和尺寸为原图百分之一的缩略图
2. 将变换后的图像展开成一维向量，用DC编码对其进行压缩，压缩后的数据再用四维超混沌系统的一维进行流密码加密。
3. 对缩略图进行更加完善的加密方案
   1. 对缩略图进行一次VDT变换，将每个子块的四个子带提取出来，分别合并成四个大的子带。对重要子带LT进行高低位加密，对三个次要子带进行DNA加密。再对四个加密后的子带进行INVDT，得到最终的缩略图加密图像



Fig 3.1 压缩加密流程图



Fig 3.2 解密解压缩流程图

## 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。本文提出的加密方案的密钥位数位有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。

密钥由两部分组成：

1. 代加密图像的sha-256的哈希值(2^256)
2. 循环移位值t(8^4)

通过密钥来生成混沌系统四个初值：

将256位数分为32份，每个8位，分别为到，公式中的为异或操作，为向左循环移位位，为模256运算。

利用待加密图像sha-256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，原始图像的微小变换都会导致密钥的变化，增强密钥的可靠性。

而密钥中的t值部分给加密方案使用者提供了密钥的一部分自主权的同时，不仅继续扩充了密钥空间，且使得sha-256的哈希值内各部分相互影响，使得算法可以更好的抵御选择明文攻击。

## 整张图像部分

具体步骤如下所示：

1. 对尺寸为N×N的图像I进行分割，分割成8×8的子块，对每个子块进行VDT变换，将每个子块的不变像素提取出来得到缩略图I\_S(尺寸为M×M，M=N/8)，对变换后的部分I1进行下一步处理。
2. 压缩
   1. 将图像I1从左至右，从上至下，从二维图像展开成一维向量I2。
   2. 利用Tab 3.1的编码规对该一维向量进行编码，得到压缩后的数据。例如图中的第一位5就编码为二进制100101，-2编码为01101。编码后的数据变为一串二进制数据I3。
3. 流密码加密
   1. 利用密钥生成的四个初值，迭代四维混沌系统，为了更好的随机性，迭代次数为(5000+图像像素个数)，迭代后舍去前5000个，得到四个长度为图像像素个数的混沌序列X, Y, Z, W。
   2. 将序列X通过公式转换为0~255的整数序列X1，并将X2转换成二进制序列X3，利用X3和I3进行异或操作，完成流密码加密，得到加密后数据I4。

## 缩略图部分

缩略图加密算法具体步骤如下：

1. VDT变换部分
   1. 对尺寸为M×M的缩略图I\_S进行VDT变换，将每个子块中的LT，RT，LB和RB分别提取出来，所有子块的LT凭借成一个LT1，所有RT，LB和RB也分别拼接成RT1，LB1和RB1（尺寸均为Q×Q，Q=M/2）。
   2. 按照公式对四个子带进行异或操作，使得四个子带之间彼此混淆，且使得LT额外携带了其余三个次要子带的信息。

公式

1. 对RT1，LB1和RB1进行DNA加密
   1. 将三个Q×Q的子带RT，LB和RB依次凭借成Q×3Q的新子带RSB
   2. 利用生成的四维混沌序列中的X，Y，Z和H生成DNA加密所需要的混沌矩阵R，DNA编码序列X\_D，DNA扩散序列Z\_D和DNA解码序列H\_D。
   3. 先利用X\_D对RSB进行DNA编码得到RSB\_1，再利用混沌矩阵R和扩散序列Z\_D对RSB\_1进行DNA级别扩散得到RSB\_2，最后使用H\_D对RSB\_2进行DNA的解码得到加密的RSB\_E
2. 对LT进行高低位加密，如Fig所示
   1. 将尺寸为Q×Q的LT1按高4比特和低4比特分成两个部分，分别记作高位图像LT\_h和低位图像LT\_l。
   2. 利用高位图像LT\_h扰乱低位图像LT\_l得到LT\_l1。

公式

* 1. 利用混沌序列X和Y生成置乱序列A，利用A置乱高位图像LT\_h得到LT\_h1。

公式

* 1. 利用混沌序列Z和H生成扩散序列B。将LT\_l1转换为4比特的二进制，再将相邻两位合并转成一个十进制数得到LT\_l2，利用序列B对LT\_l2进行扩散操作得到LT\_l3。

公式

* 1. 用LT\_l3扰乱LT\_h1, 异或得到LT\_h2

公式

* 1. 将LT\_h2, LT\_l3按索引分位奇, 偶序列, 将高位的奇和低位的偶互换，得到LT\_h3和LT\_l4，再将LT\_h3和LT\_l4合并成8位的LT\_E。

公式

1. 将经过DNA加密的结果RSB\_E重新拆分成三个子带RT\_E，LB\_E和RB\_E，将四个子带LT\_E，RT\_E，LB\_E和RB\_E按照步骤1)拆分的方式重新合并成一张图像，对这个图像做INVDT变换，得到最终的缩略图加密图像I\_S\_E

## 讨论

在本章提出的压缩加密算法中，为了适应图像预览这一使用场景，对尺寸较大的原始图像进行较为简便的加密以提升效率，而对尺寸较小的缩略图进行安全性能更高的加密。而算法中的压缩和加密步骤均依赖本文所提出的VDT，通过VDT，混沌系统，高低位加密等技术的结合，使得本文提出的算法具有以下的优点。

1. 在对图像进行压缩加密的同时生成一个可提供预览的缩略图。
2. VDT可以提取图像中的重要信息，变换会生成四个子带，其中一个子带具有图像主要信息，其余三个子带携带相对次要的信息。通过对重要子带和次要子带施加不同的加密方法，并且在加密后利用INVDT使得四个子带相互影响，扩散至整张图像，因此具有良好的安全性能。
3. 缩略图和总图像可以进行分开的解密与解压缩，使得用户可以预先看到尺寸较小的缩略图，再选择是否要解密/解压缩原始图像。

# 结果分析

本章节在MatlabR2021b上模拟了本文提出的压缩加密算法，并对压缩性能和安全能力进行了分析。

## 无损压缩率

对五张灰度图像的无损压缩率(CR)如Tab 4.1所示。在本文提出的算法中，利用VDT进行压缩预处理的核心是在自然图像中相邻像素的值会较为接近，因此压缩率与图片本身的性质关系较大，如表所示，纯黑的图像CR达到了4。

|  |  |  |  |
| --- | --- | --- | --- |
| Image Title | Raw bits | Compressed bits | CR |
| Lena | 2097152 | 1458383 | 1.4380 |
| Peppers | 2097152 | 1492021 | 1.4056 |
| Airplane(U-2) | 8388608 | 5888811 | 1.4245 |
| Boat | 2097152 | 1608209 | 1.3040 |
| Black | 2097152 | 524288 | 4 |

Tab 4.1

## 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。

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Fig 4.1 图中从左至右依次是代价密缩略图，原始直方图，加密后图像和加密的直方图。

从图中的实验结果可以看出，各个原始图像的之直方图携带图片的大量信息，而加密后的直方图类似随机分布，无法从加密后图像中获取与原始图像有关的统计信息，因此该加密算法能够抵抗统计攻击。

## 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成果，且无法用细微改动后的密钥却解密图像。

本文用Lena的缩略图进行这项测试，首先我们生成了Key1，对Key1进行了仅1比特的修改得到Key2和Key3，三者依次如下所示：

Key1=**25722568D126918052AB7B93683092B4043A5C2BB3110BC260627601EAE0FFA599AE6A9**

Key2=**15722568D126918052AB7B93683092B4043A5C2BB3110BC260627601EAE0FFA599AE6A9**

Key3=**25722568D126918052AB7B93683092B4043A5C2BB3110BC260627601EAE0FFA590AE6A9**

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
| 女人戴着帽子  描述已自动生成  (a) | (b) | (c) |

Fig 4.2 (a)从上至下是用Key1加密的C1和解密的Lean；(b)从上至下分别是用Key2加密的C2，|C2-C1|，以及用Key2去解密C1得到错误解密图像；(C)分别是用Key3加密的C3，|C3-C1|，以及用Key3去解密C1得到的错误解密图像。

如Fig 4.2所示，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，密钥的一点点变换也会导致完全不同的结果。同时，通常认为密钥空间的大于2^100时，可认为该密钥可以有效的抵抗穷举攻击[36]，本文的密钥长度为288位，足够有效的抵抗暴力攻击。因此，本文所提出的加密算法的密钥具有高度的敏感性和足够大的密钥空间，具有很好的安全特性来抵御明文攻击和穷举攻击。

## 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，证明加密算法的性能越好。相关性的定义如下：

其中, 和分别是数学上的期望，均值和标准差，同时X和Y是两个相邻的序列，可是沿水平，垂直或对角线方向的像素。如果X和Y表示出高相关性，则Corr接近1，否则接近0。

|  |  |  |
| --- | --- | --- |
|  |  |  |
| (a) | (b) | (c) |

Fig 4.3 (a)上下分别是原始图像和加密图像的水平相关性; (b)垂直相关性(c)对角相关性

Fig 4.3展示了Lena缩略图的原始相关性和加密后的相关性，其中原始图像在水平，垂直，对角三个方向均具有很强的相关性，而加密后图像在三个方向的相关性均接近于0，因此表明本文提出的算法可以有效的减少图像相邻像素相关性。

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Image Title | Directions/Origin | | | Directions/Cipher-images | | |
| Horizontal | Vertical | Diagonal | Horizontal | Vertical | Diagonal |
| Lena | 0.9709 | 0.9838 | 0.9568 | 0.0097 | 0.0088 | -0.0074 |
| Peppers | 0.9770 | 0.9783 | 0.9653 | 0.0049 | -0.0166 | -0.0017 |
| Airplane (U-2) | 0.9670 | 0.9418 | 0.9406 | 0.0156 | 0.0031 | 0.0014 |
| Boat | 0.9316 | 0.9765 | 0.9250 | 0.0055 | -0.0022 | -0.0205 |

Tab 4.2

Tab 4.2展示了4张不同图像的缩略图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。这表明我们的加密算法具有良好的加密性能。

## 信息熵

信息熵的公式如下，信息熵可以用来衡量信息的不确定性，因此在图像加领域中，

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位的灰度图像来说，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。

|  |  |  |
| --- | --- | --- |
| Image Title | Entropy/Origin | Entropy/ Cipher-images |
| Lean | 7.4028 | 7.9534 |
| Peppers | 7.5319 | 7.9496 |
| Airplane (U-2) | 5.6296 | 7.9887 |
| Boat | 7.1240 | 7.9493 |
| Black | 0 | 7.9532 |

Tab 4.3

由Tab 4.3得知，加密后的密文图像的信息熵均接近理想值8，这表明该图像加密算法具有预期的随机性和安全性。

## 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[37], [38]。NPCR和UACI的定义如下：

其中和是两张密文图像，他们各自的明文图像之间仅有1比特的差距。当不等于时，就等于1，否则等于0，且和是图像的高和宽。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Tab 4.4所示

|  |  |  |  |
| --- | --- | --- | --- |
| Image Title | NPCR | UACI | Test results |
| Lena | 0.9960 | 0.3331 | Pass |
| Peppers | 0.9955 | 0.3308 | Pass |
| Airplane (U-2) | 0.9960 | 0.3343 | Pass |
| Boat | 0.9965 | 0.3338 | Pass |

由表可知，测试图像均可以通过NPCR和UACI的测试，证明本文的加密算法可以有效的抵抗差分攻击。

# 总结

在本文中， 首先提出了一个新的差值变化(VDT)，该变换可以提取图像中的重要信息和次要信息，同时还可以获取到图像的缩略图和作为无损压缩编码的预处理。利用这个变换将图像加密分为两部分，原始图像采用速度较快的流密码加密，而对缩略图充分利用其内部信息，对其重要部分采用高低位加密，而次要部分采用DNA加密，对某些需要图像预览的使用场景提供了很好的安全性能和便利性。仿真结果也充分证明了我们的加密算法具有足够的安全性能，可以抵御不同的安全攻击。

参考文献

[1] L. Liu, Y. Zhang, and X. Wang, “A novel method for constructing the S-box based on spatiotemporal chaotic dynamics,” *applied sciences*, vol. 8, no. 12, p. 2650, 2018.

[2] M. Wan, M. Li, G. Yang, S. Gai, and Z. Jin, “Feature extraction using two-dimensional maximum embedding difference,” *Information sciences*, vol. 274, pp. 55–69, 2014.

[3] P. S. Minz, I. K. Sawhney, and C. S. Saini, “Algorithm for processing high definition images for food colourimetry,” *Measurement*, vol. 158, p. 107670, 2020.

[4] E. N. Lorenz, “The mechanics of vacillation,” *Journal of Atmospheric Sciences*, vol. 20, no. 5, pp. 448–465, 1963.

[5] G. Chen and D. Lai, “Feedback control of Lyapunov exponents for discrete-time dynamical systems,” *International Journal of Bifurcation and Chaos*, vol. 6, no. 07, pp. 1341–1349, 1996.

[6] Z. Wei, V.-T. Pham, A. J. M. Khalaf, J. Kengne, and S. Jafari, “A modified multistable chaotic oscillator,” *International Journal of Bifurcation and Chaos*, vol. 28, no. 07, p. 1850085, 2018.

[7] Q. Lai, Z. Wan, L. K. Kengne, P. D. K. Kuate, and C. Chen, “Two-memristor-based chaotic system with infinite coexisting attractors,” *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 68, no. 6, pp. 2197–2201, 2020.

[8] F. Meng, X. Zeng, Z. Wang, and X. Wang, “Anti-Synchronization of Fractional-Order Chaotic Circuit with Memristor via Periodic Intermittent Control,” *Advances in Mathematical Physics*, vol. 2020, p. e5158489, Jan. 2020, doi: 10.1155/2020/5158489.

[9] X. Wang and Y. Su, “Image encryption based on compressed sensing and DNA encoding,” *Signal Processing: Image Communication*, vol. 95, p. 116246, 2021.

[10] Ü. Çavuşoğlu, S. Kaçar, I. Pehlivan, and A. Zengin, “Secure image encryption algorithm design using a novel chaos based S-Box,” *Chaos, Solitons & Fractals*, vol. 95, pp. 92–101, Feb. 2017, doi: 10.1016/j.chaos.2016.12.018.

[11] M. Kaur and V. Kumar, “Beta chaotic map based image encryption using genetic algorithm,” *International Journal of Bifurcation and Chaos*, vol. 28, no. 11, p. 1850132, 2018.

[12] Y.-G. Yang, B.-W. Guan, J. Li, D. Li, Y.-H. Zhou, and W.-M. Shi, “Image compression-encryption scheme based on fractional order hyper-chaotic systems combined with 2D compressed sensing and DNA encoding,” *Optics & Laser Technology*, vol. 119, p. 105661, 2019.

[13] X. Wang, S. Chen, and Y. Zhang, “A chaotic image encryption algorithm based on random dynamic mixing,” *Optics & Laser Technology*, vol. 138, p. 106837, 2021.

[14] X. Yan, X. Wang, and Y. Xian, “Chaotic image encryption algorithm based on arithmetic sequence scrambling model and DNA encoding operation,” *Multimedia Tools and Applications*, vol. 80, no. 7, pp. 10949–10983, 2021.

[15] Z. Li, C. Peng, W. Tan, and L. Li, “An efficient plaintext-related chaotic image encryption scheme based on compressive sensing,” *Sensors*, vol. 21, no. 3, p. 758, 2021.

[16] X. Wang and Y. Li, “Chaotic image encryption algorithm based on hybrid multi-objective particle swarm optimization and DNA sequence,” *Optics and Lasers in Engineering*, vol. 137, p. 106393, 2021.

[17] Y. Xian and X. Wang, “Fractal sorting matrix and its application on chaotic image encryption,” *Information Sciences*, vol. 547, pp. 1154–1169, 2021.

[18] L. Liu, Q. Zhang, and X. Wei, “A RGB image encryption algorithm based on DNA encoding and chaos map,” *Computers & Electrical Engineering*, vol. 38, no. 5, pp. 1240–1248, Sep. 2012, doi: 10.1016/j.compeleceng.2012.02.007.

[19] X. Ouyang, Y. Luo, J. Liu, L. Cao, and Y. Liu, “A color image encryption method based on memristive hyperchaotic system and DNA encryption,” *International Journal of Modern Physics B*, vol. 34, no. 04, p. 2050014, 2020.

[20] S. Namasudra, R. Chakraborty, A. Majumder, and N. R. Moparthi, “Securing multimedia by using DNA-based encryption in the cloud computing environment,” *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM)*, vol. 16, no. 3s, pp. 1–19, 2020.

[21] J. Chen, L. Chen, and Y. Zhou, “Cryptanalysis of a DNA-based image encryption scheme,” *Information Sciences*, vol. 520, pp. 130–141, 2020.

[22] P. T. Akkasaligar and S. Biradar, “Selective medical image encryption using DNA cryptography,” *Information Security Journal: A Global Perspective*, vol. 29, no. 2, pp. 91–101, 2020.

[23] M. Roy *et al.*, “Data security techniques based on DNA encryption,” in *International Ethical Hacking Conference*, 2019, pp. 239–249.

[24] X. Chai, X. Fu, Z. Gan, Y. Lu, and Y. Chen, “A color image cryptosystem based on dynamic DNA encryption and chaos,” *Signal Processing*, vol. 155, pp. 44–62, 2019.

[25] D. A. Zebari, H. Haron, S. R. Zeebaree, and D. Q. Zeebaree, “Multi-level of DNA encryption technique based on DNA arithmetic and biological operations,” in *2018 International Conference on Advanced Science and Engineering (ICOASE)*, 2018, pp. 312–317.

[26] X. Wu, K. Wang, X. Wang, H. Kan, and J. Kurths, “Color image DNA encryption using NCA map-based CML and one-time keys,” *Signal Processing*, vol. 148, pp. 272–287, 2018.

[27] J. Wu, X. Liao, and B. Yang, “Image encryption using 2D Hénon-Sine map and DNA approach,” *Signal processing*, vol. 153, pp. 11–23, 2018.

[28] Y. Liu, J. Tang, and T. Xie, “Cryptanalyzing a RGB image encryption algorithm based on DNA encoding and chaos map,” *Optics & Laser Technology*, vol. 60, pp. 111–115, Aug. 2014, doi: 10.1016/j.optlastec.2014.01.015.

[29] Y. Dou, X. Liu, H. Fan, and M. Li, “Cryptanalysis of a DNA and chaos based image encryption algorithm,” *Optik*, vol. 145, pp. 456–464, Sep. 2017, doi: 10.1016/j.ijleo.2017.08.050.

[30] R. R. S. Tomar and K. Jain, “Lossless image compression using differential pulse code modulation and its application,” in *2015 International Conference on Computational Intelligence and Communication Networks (CICN)*, 2015, pp. 397–400.

[31] G. Chen and T. Ueta, “Yet another chaotic attractor,” *International Journal of Bifurcation and chaos*, vol. 9, no. 07, pp. 1465–1466, 1999.

[32] X. Ye, J. Mou, Z. Wang, P. Li, and C. Luo, “Dynamic Characteristic Analysis for Complexity of Continuous Chaotic Systems Based on the Algorithms of SE Complexity and C Complexity,” in *Machine Learning and Intelligent Communications*, 2018, pp. 647–657. doi: 10.1007/978-3-319-73447-7\_69.

[33] M. S. Tavazoei, “Fractional order chaotic systems: history, achievements, applications, and future challenges,” *The European Physical Journal Special Topics*, vol. 229, no. 6, pp. 887–904, 2020.

[34] F. Yang, J. Mou, K. Sun, Y. Cao, and J. Jin, “Color image compression-encryption algorithm based on fractional-order memristor chaotic circuit,” *IEEE Access*, vol. 7, pp. 58751–58763, 2019.

[35] K. Zhang, E. Bai, X. Jiang, and Y. Wu, “Chaotic image encryption algorithm based on higher and lower bit image operations,” in *International Conference on Signal Image Processing and Communication (ICSIPC 2021)*, 2021, vol. 11848, pp. 62–69.

[36] Y. Zhang, C. Li, Q. Li, D. Zhang, and S. Shu, “Breaking a chaotic image encryption algorithm based on perceptron model,” *Nonlinear Dynamics*, vol. 69, no. 3, pp. 1091–1096, 2012.

[37] Y. Wu, J. P. Noonan, and S. Agaian, “NPCR and UACI randomness tests for image encryption,” *Cyber journals: multidisciplinary journals in science and technology, Journal of Selected Areas in Telecommunications (JSAT)*, vol. 1, no. 2, pp. 31–38, 2011.

[38] A. Ullah, S. S. Jamal, and T. Shah, “A novel scheme for image encryption using substitution box and chaotic system,” *Nonlinear Dynamics*, vol. 91, no. 1, pp. 359–370, 2018.