基于动态提升小波优化算法的数字图像加密研究

周卉芬 [1]
ZHOU Huifen

摘 要 一旦数字图像被加密，任何对像素的篡改都会破坏其加密结构。因此，加密有助于确保图像的安全性。为有效避免图像中的像素被篡改，针对基于动态提升小波优化算法的数字图像加密算法展开研究。根据动态提升标准，优化小波基函数，从而定义关于像素对象的加密索引关系，实现基于动态提升小波优化算法的图像加密索引构建。利用所生成的密钥流，堆叠图像哈希值，进而在加密过程中完成与像素样点相关的动态二元扩散与置乱，实现数字图像加密算法的设计。实验结果表明，在相邻像素区域内，明文图像呈现较为集中的分布状态，而密文图像则呈现明显散乱的分布状态，表示经过该方法的加密后密文图像在相邻像素区域的相关性明显降低，篡改像素对象的难度大幅提升，能够较好保证数字图像的安全性。

关键词 动态提升；小波优化算法；数字图像；图像加密；加密索引；密钥流

doi：10.3969/j.issn.1672-9528.2025.09.024

0 引言

数字图像是一种特殊的二维图像，可以利用有限的数字来代替像素对象。在互联网应用中，数字化模拟图像可以直接获得数字图像。如果将像素作为基本图像元素，则可以利用数字计算机或数字电路完成对图像信息的存储 [1]。在单幅数字图像中，一个像素样点只对应一个整数行和一个整数列坐标，但由于灰度值和颜色值的不同，所以位置坐标相同的像素并不一定对应同一个图像节点。像元组合可以用来描述数字图像中的物体形状，且在二维矩阵中，这些像元所对应的行列号决定了其所处的像素区域。在数字图像中，物体的大小可以表示为像元的集聚状态，聚集个数越多，就表示描述物体越大。

对于数字图像加密算法的研究不但有助于保障图像的真实性，还能够避免像素对象被篡改。赵芃等人 [2] 提出了基于分形谢尔宾斯基三角形模型的加密算法，根据明文图像的尺寸确定像素样点的分形维度，再建立四维耗散混沌序列，以用于定义图像编码规则，最后通过三角形旋转子图对象的方式，生成完整的密文模板。然而，四维耗散混沌序列中所包含的像素样点数量相对有限，所以基于该方法进行加密，有可能出现编码原则与像素样点不完全对称的情况，从而影响加密准确性。王淑梅等人 [3] 提出了基于交替量子随机行走的加密算法，根据离散余弦原则，对明文图像进行 DCT 域变换，再基于交替量子随机行走机制构造概率分布矩阵，从而在计算概率分布矩阵奇异值的同时，给出相应的十六进制表达式，以作为数字图像的加密密钥。概率分布矩阵在单次行为过程中只能输出一个奇异值对象，而完整加密数字图像所需的奇异值样本相对较多，所以该方法必须通过多次迭代才能获得最终的加密结果，这就使得其执行准确性难以得到保障。

为解决上述问题，充分保障数字图像的真实性，设计基于动态提升小波优化算法的数字图像加密算法。在图形压缩与识别领域中，小波算法可以在时间和频率层面上对信号或数据进行分析 [4]。通过伸缩平移运算对信号进行多尺度细化，当其到达高频处实施时间细分、达到低频处实施频率细分。基于动态提升优化小波算法就是通过动态调整小波变换中的参数，以适应不同的信号或数据特征。同时，利用动态提升优化技术对小波算法的性能进行进一步优化，从而提高算法的处理速度和精度。

1 基于动态提升小波优化算法的图像加密索引构建

构建加密索引是实现数字图像加密的基础，本章节内容基于动态提升标准优化原始的小波函数，并联合大量的像素样点，定义相关性的加密索引关系。

1.1 动态提升小波优化算法

1.1.1 小波基函数

小波基函数是小波变换的基础，决定了小波变换的特性和效果。在数字图像处理中，最常应用 DbN 小波函数。DbN 小波基函数具有较高的消失矩和较好的正则性，能够较好保留图像中的细节信息 [5]。由于数字图像中包含大量的像素样

1. 闽西职业技术学院 福建龙岩 364021

点，且这些样点对象之间不存在相互覆盖关系，所以应确保 N 参数取值保持在中间位置处，才能够避免出现像素样点的相位畸变问题。

规定 δ 表示 N 参数，对于数字图像而言，其赋值涉及整个正实数区间，即：

$$\delta \in (0, n) \tag{1}$$

式中：n 表示一个无限大的自然数。

满足小波变换需求的 N 参数定义式应为：

$$\delta \to \frac{n}{2} \neq 1 \tag{2}$$

式中：δ=1 表示变换前、后样点对象的取值相同，在加密数字图像时，表示明文、密文图像相同，故这种赋值情况没有意义。

在式（2）的基础上，推导 DbN 小波基函数为：

$$F = \frac{1}{\sqrt{2\delta \boldsymbol{A}_0}} \dot{d}^{-(a-s)^2 / 2\chi^2} \tag{3}$$

式中：$\dot{d}$表示像素样点的细节信息；a 表示行向的相位畸变系数；s 表示列向的相位畸变系数；χ 表示正则运算参数；$\boldsymbol{A}_0$ 表示 DbN 小波基向量。

1.1.2 动态提升标准下的小波函数优化

在动态提升标准下的数字图像加密中，优化小波函数就是根据基函数将图像分解为不同频率的子带，再对每个子带进行独立处理，从而提取图像的局部特征并实现数据压缩。动态提升标准体现在小波基函数尺度参数宽度的控制方面 [6-7]。设$\tilde{g}$表示频率子带中的像素分辨率特征；α 表示频率子带分解系数；$\bar{g}$表示当前图像中的像素分辨率均值；β 表示像素尺度的动态提升参数，联立上述物理量，可将基于动态提升标准的频率分辨率定义式表示为：

$$D = \tilde{g} + \sqrt{\frac{\beta \bar{g}}{\alpha}} \tag{4}$$

联立式（3~4），推导小波函数优化表达式为：

$$H = \frac{\boldsymbol{h}}{F} f\left(\frac{j_{\max} - j_{\min}}{D}\right)^2 \tag{5}$$

式中：$j_{\max}$ 表示小波函数局部尺度特征的最大取值；$j_{\min}$ 表示局部尺度特征的最小取值；f 表示像素压缩参数；$\boldsymbol{h}$ 表示基于小波基函数的图像局部特征动态压缩向量。

基于动态提升小波优化算法确定数字图像的频率分辨率能够最大化提升压缩处理后像素样点的清晰度，从而使数字图像的加密效果与安全性能得到保障。

1.2 加密索引关系定义

在数字图像加密中，索引关系通常指的是加密前后像素值之间的对应关系。基于提升小波算法的数字图像加密，索引关系涉及小波系数的分解以及加密过程中的像素置换 [8]。使用动态提升小波算法对原始图像进行多尺度分解，分解过程中，可以根据图像的特点和需求动态调整小波系数和分解层数。对于小波系数（γ）和分解层数（k）的计算参考为：

$$\begin{cases} \gamma = \varphi \sqrt{\ln(J \times L)} \\ k = (\varepsilon - 1) \cdot \left| \dfrac{J}{L} \right|^2 \end{cases} \tag{6}$$

式中：J 表示原始图像像素；L 表示加密图像像素；φ 表示像素需求；ε 表示数字图像的动态分解系数。

加密后图像与原始图像之间的索引关系可以通过加密过程中的变换规则来定义。具体来说，就是记录每个像素在加密前后的位置变化，从而建立加密索引关系 [9]。设 ι 表示随机像素对象，其在加密前的位置信息为 z_ι，加密后的位置信息为 x_ι，联立式（5~6），可将数字图像的加密索引关系定义式表示为：

$$C = \left[\mathrm{H}(x_\iota - z_\iota)^2 \, k / \gamma \right] \times \frac{1}{\Delta X} \tag{7}$$

式中：ΔX 表示加密过程中所涉及的像素样点总量。

通过动态调整小波系数和分解层数，以及采用灵活的加密方法和索引构建策略，可以保护数字图像信息的安全，这也使得数字图像的有效加密成为可能。

2 数字图像加密算法设计

2.1 密钥流生成

密钥流是由一系列伪随机数组成的码元序列，这些伪随机数通过某种算法生成，并用于加密或解密过程中的每一步操作。在数字图像加密中，密钥流通常用于控制图像的像素错乱、扩散及其他变换操作。通过动态提升小波优化算法定义适当的混沌映射表达式，并设置初始条件，可以生成具有复杂动态行为的混沌码元信号 [10-11]。规定 Z 表示基于动态提升小波优化算法所选择的混沌码元，其定义式为：

$$Z = -\sum_{\kappa=1}^{+\infty} C\iota(X_z) \log \lambda \left| \frac{x_z}{\tilde{\boldsymbol{C}}} \right| \tag{8}$$

式中：ι 表示伪随机数；z 表示像素信号；X_z 表示像素 z 的混沌序列项；x_z 表示像素 z 的码元序列；λ 表示映射参数；$\tilde{\boldsymbol{C}}$表示像素信号的动态行为向量。

在式（8）的基础上，推导数字图像的密钥流定义为：

$$V = \liminf \left| \eta \dot{b} - \frac{\hat{\boldsymbol{B}}}{Z} \right|^o \tag{9}$$

式中：η 表示像素信号的离散程度；$\dot{b}$表示像素样点的离散序列特征；$\hat{\boldsymbol{B}}$ 表示密钥索引向量；O 表示混沌码元赋值参数。密钥流的微小变化都会导致加密图像完全不同，确保了即使

攻击者获得了部分密钥信息，也难以还原出原始数字图像。

2.2 图像哈希值堆叠

哈希函数是将任意长度的数据转换为固定长度无规律数值的函数。在数字图像加密中，哈希函数可以用于生成像素样点的哈希值，这个哈希值可以作为图像的唯一标识或用于验证原图像的完整性[12]。哈希值堆叠则是指将多个哈希值按照某种方式进行组合或叠加，以进一步增强加密效果。对明文图像进行哈希运算，从而生成图像的哈希值。这个哈希值既可以是图像整个内容的哈希，也可以是图像部分内容的哈希[13]。将生成的哈希值与密钥流按照动态提升小波优化算法进行堆叠，其目的在于将哈希值与密钥流紧密结合，从而增强加密效果。利用式（9），可将数字图像的哈希值堆叠运算式表示为：

$$N=\lim_{m\leftarrow\infty}\frac{1}{q}\left|V\left(\mu\boldsymbol{W}\right)\right|^{2}+\left(\ln\tilde{Q}\right)^{2} \tag{10}$$

式中：m 表示数字图像原像素的长度值；q 表示标准哈希值；μ 表示像素标识参数；$\boldsymbol{W}$ 表示基于密钥流所定义的图像内容哈希向量；$\tilde{Q}$表示目标像素的堆叠特征。

利用堆叠后的哈希值对明文图像进行加密处理[14-15]。这个加密过程完全是基于异或运算的，由于图像中不再具有与原像素格式相同的像素样点，所以加密后的图像将变得难以识别和理解，也就达到了保护图像数据的目的。

3 实验分析与研究

对于数字图像的加密有助于保障图像真实性，从而避免像素对象被篡改。本次实验以图 1 所示数字图像作为研究对象，在其中随机选择 10 个像素样点作为参考，以 RGB 色彩空间为标准，分析这些样点处的色域值情况。在 RGB 色彩空间中，R 表示红色、G 表示绿色、B 表示蓝色，最大色域值为 255。若将 RGB 色彩描述为坐标形式，则第一位对应红色，第二位对应绿色，第三位对应蓝色。例如一个像素点的色域值为（200, 12, 0），表示该位置的颜色组成为红色和绿色，且红色成分相对较多。

表 1 记录了图 1 中目标像素样点的色域组成情况。

表 1 数字图像中的标准色域值

编号	数值	编号	数值
1	（198,15,6）	6	（209,58,8）
2	（203,26,2）	7	（255,0,0）
3	（185,21,0）	8	（179,3,1）
4	（196,100,13）	9	（196,18,4）
5	（201,42,9）	10	（241,102,17）

分析表 1 可知，7 号像素样点只由红色组成，其他各样点处红色的色域值也明显最高，绿色的色域值低于红色但高于蓝色，故整幅图像中红色占比最高、绿色次之、蓝色最低。

利用 Worktile 软件分析加密前数字图像的色彩组成情况，如图 1 所示。

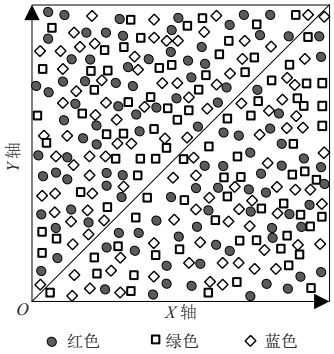

图 1 加密前数字图像色彩组成

图 1 中，对角线用来区分图像的相邻像素区域。结合红色、绿色、蓝色像素的分布情况来看，红色所占比值最大、绿色次之、蓝色最小，与表 1 所对应的标准色域情况相同。左、右两分区中色彩样点的分布情况较为相似，且相同像素样点所占比值也基本相同。本次实验选择基于动态提升小波优化算法的数字图像加密算法（A 组）、基于分形谢尔宾斯基三角形模型的加密算法（B 组）、基于交替量子随机行走的加密算法（C 组）对图 1 所示图像进行加密，根据相邻像素区域内像素样点的分布情况，总结实验规律。图 2 反映了不同方法加密后，像素样点的实际分布情况。

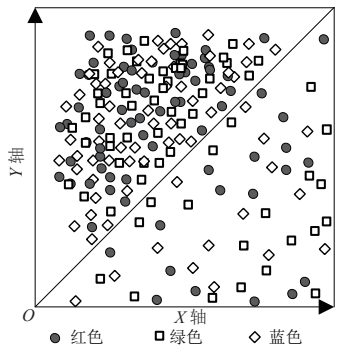

图 2 A 组数字图像加密

分析图 2 可知，左侧区域内所分布的像素样点较多，且中间部分的密度较大、边缘区域的密度较小；右侧区域内只分布极少数的像素样点，且无明显规律。与图 2 相比，加密前后的色彩组成差异极大。

相较于图 2，图 3 的色彩组成情况也发生了明显变化；左侧区域内像素样点集中分布在左上端，右上端及下部无任何像素样点；右侧区域内像素样点主要分布在右下端，右上端仅分布个别样点，但与左侧区域相比，集中分布部分像素样点的相似度较高。

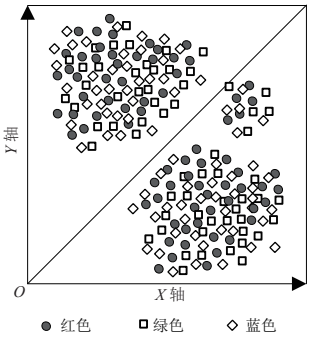

图 3 *B* 组数字图像加密

图 4 左右两侧的像素样点组成虽然明显不同，但其右侧区域与图 3 右侧区域在色彩组成方面的相似性较高，无论是像素样点个数还是分布密度上都没有明显的差异；左侧区域则明显异于图 2 左侧区域。综上所述，*B* 组、*C* 组方法对于数字图像的加密都具有一定的局限性，并不足以保证数字图像的安全性；*A* 组方法的加密能力相对较强，大幅提升了攻击对象篡改像素样点的难度，在保障数字图像安全性方面的应用能力更强。

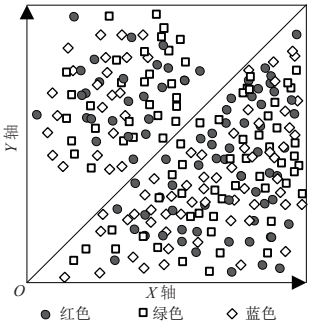

图 4 *C* 组数字图像加密

4 结语

随着信息技术的飞速发展，数字图像加密技术已经成为信息安全领域的重要研究方向。上述研究深入探讨了基于动态提升小波优化算法的数字图像加密技术，旨在通过引入动态提升小波变换和优化算法，提高图像加密的效率和安全性。在研究中，首先对小波变换进行了详细地介绍，并分析了其在图像加密中的潜在应用。随后，结合动态提升思想，提出了一种新颖的图像加密方案。该方案通过动态调整小波变换的参数，实现了对图像数据的灵活加密，同时利用优化算法提高了加密过程的稳定性和效率。

参考文献：

[1] 樊爽 , 郭玉荣 . 基于逐点移动最小二乘拟合的数字图像相关测量 [J]. 激光与光电子学进展 , 2023, 60(6):240-250.

[2] 赵芃 , 王金婵 , 彭欢庆 , 等 . 基于分形谢尔宾斯基三角形模型的图像加密算法 [J]. 计算机工程与设计 , 2024, 45(11): 3216-3224.

[3] 王淑梅 , 宋佳宝 , 刘广哲 , 等 . 基于交替量子随机行走的改进 AES 和离散余弦变换的图像加密算法 [J]. 北京工业大学学报 , 2023, 49(6):647-655.

[4] 应鑫迪 , 厉晓华 . 结合改进算术优化算法与小波神经网络的网络流量预测模型 [J]. 传感技术学报 , 2024, 37(8): 1350-1361.

[5] 郭昕刚 , 许连杰 , 程超 , 等 . 加权核范数最小化和改进小波阈值函数的图像去噪算法 [J]. 国防科技大学学报 , 2024, 46(2): 238-246.

[6] 肖定汉 , 禹思敏 , 王倩雪 . 椭圆曲线与自适应 DNA 编码的混沌图像加密算法 [J]. 中国图象图形学报 , 2023, 28(11): 3428-3439.

[7] 牛士铭 , 薛茹 , 丁聪 . 基于改进型 3D-Henon 混沌映射的彩色图像加密方法 [J]. 计算机工程与科学 ,2024,46(4):657-666.

[8] 傅彬 . 基于松鼠搜索算法优化 Logistic-Ushiki 混沌融合的数字图像加密研究 [J]. 科技通报 , 2024, 40(7):26-33.

[9] 黄佳鑫 , 赵凯悦 , 李佳文 , 等 . 基于 Logistic-Sine-Cosine 映射的图像加密算法 [J]. 科学技术与工程 ,2023,23(27):11713-11721.

[10] 杨宇光 , 王嘉伟 . 基于 SHA-256 和 Arnold 映射的量子 Logistic 映射图像加密算法 [J]. 安徽大学学报 (自然科学版), 2024, 48(1):35-42.

[11] 郭现峰 , 李浩华 , 魏金玉 . 基于 Fibonacci 变换和改进 Logistic-Tent 混沌映射的图像加密方案 [J]. 吉林大学学报 (工学版), 2023, 53(7):2115-2120.

[12] 王伟杰 , 姜美美 , 王淑梅 , 等 . 基于量子长短期记忆网络的量子图像混沌加密方案 [J]. 物理学报 ,2023, 72(12):21-32.

[13] 高献伟 , 郭维凯 , 程逸煊 , 等 . 基于孪生物理不可克隆函数和压缩感知的视觉有意义图像加密 [J]. 图学学报 , 2024, 45(5): 998-1007.

[14] 陈善学 , 杜文正 , 任丽丹 . 一种动态密钥与 DNA 交错编码的多图像加密算法 [J]. 电讯技术 ,2023, 63(4):529-535.

[15] 庄裕富 , 许志平 , 彭侠夫 , 等 . 基于预定时间混沌同步系统的图像加密算法 [J]. 厦门大学学报 (自然科学版), 2023, 62(4): 647-653.

【作者简介】

周卉芬（1995—），女，福建平和人，硕士，助教，研究方向：信息与通信工程技术应用研究。

（收稿日期：2025-02-11 修回日期：2025-07-18）