基于模运算 – 中心折叠 RDH–EI 的加密域图像可逆数据隐藏方法研究

张永杰[1]
ZHANG Yongjie

摘 要 互联网所存储信息主要以数字流的形式存在，而如何在传输过程中保障这些信息的安全性，则成为了保护网络隐私的主要研究方向。基于此，文章提出基于模运算 - 中心折叠 RDH-EI 的加密域图像可逆数据隐藏方法。针对目标像素点进行取模运算，并联合中心折叠策略，对原始图像进行加密处理，在此基础上根据图像插值，将目标信息嵌入加密域图像中，从而实现信息提取与图像恢复，完成对加密域图像可逆数据的隐藏。实验结果表明，所提方法不但保障了加密图像的安全，还解决了彩色图像跨通道空间利用率低的问题，缓解了灰度图像冗余空间被浪费的情况，在网络信息安全方面具有更好的保障效果。

关键词 模运算；中心折叠；RDH-EI 算法；加密域图像；可逆数据隐藏；图像加密；图像插值

doi：10.3969/j.issn.1672-9528.2025.11.037

0 引言

信息隐藏演化出了可逆信息隐藏技术的分支研究方向[1]，针对该方向的研究，李季瑀等人提出了基于跨域对抗适应的隐藏算法，利用超分辨率网络将秘密信息藏入图像内容中，再加入注意力机制，抑制目标数据的冗余特征，从而在对抗训练编码信息的同时，避免载体图像与载密图像出现明显的跨域差异[2]。对抗冗余特征时，超分辨率网络以牺牲一部分密文信息模板的方式，保障原图像的完整性，所以基于该方法隐藏数据容易造成关键信息缺失的问题。高光勇等人提出了基于颜色通道关联性和熵编码的隐藏方法，分离原始彩色图像的 RGB（Red（红）、Green（绿）、Blue（蓝） 的缩写）通道，再结合自适应熵编码和预测误差直方图生成完整的嵌入空间，利用颜色通道相关性扩展已生成的嵌入空间，从而在完成载密图像可逆置乱处理的同时，将秘密信息嵌入加密图像目标位置[3]。

为解决上述问题，针对基于模运算 - 中心折叠 RDH-EI（在加密图像中实现可逆数据隐藏的技术）的加密域图像可逆数据隐藏方法展开研究。模运算是整数除法运算思想，主要用于计算一个数除以另一个数所得余数[4]。中心折叠是指将目标对象围绕中心轴或中心点进行对称处理。在加密域图像信息隐藏中，结合模运算与中心折叠，就是利用前者生成周期性数据，再利用后者处理所生成数据的对称性。模运算定义了具体的加密算法，而中心折叠对所生成密钥进行了二次对称加密操作，在图像加密中，这种连续的处理方式不但调整了像素值，也能够实现对区域性数据的对称加密与隐藏处理。

1 加密域图像可逆数据隐藏

1.1 像素点取模运算

取模运算是一种数学运算原则，其求解结果表示为两个自然数相除后所得的余数。在加密域图像可逆数据隐藏中，通过对像素点的取模运算，可以改变目标数据的像素值，并为数据加密及后续嵌入提供良好的图像环境[5]。对插值图像进行分块处理，通过取模式（1）对加密域图像中的非基准像素点进行取模，并得到其余数定义式。

$$\begin{cases} M_1 = N_\alpha\left(\tilde{b}+\delta_1\right)\bmod\beta \\ M_2 = N_\alpha\left(\tilde{b}+\delta_2\right)\bmod\beta \\ \vdots \\ M_n = N_\alpha\left(\tilde{b}+\delta_n\right)\bmod\beta \end{cases} \tag{1}$$

式中：M_1、M_2、…、M_n 表示 n 个不同的余数；α 表示分块数量；N_α 表示插值图像 N 在 α 分块条件下的表示；$\tilde{b}$ 表示原始图像的像素值；δ_1、δ_2、…、δ_n 表示 n 个不同的随机数；β 表示合适的模数。

通过对像素点的取模运算可以确定目标加密信息在原图像中的分布情况[6]。

1.2 中心折叠策略

中心折叠策略是实现 RDH（可逆数据隐藏）的有效方法。

1. 中国石油天然气管道通信电力工程有限公司
河北廊坊 065000

该方法将非十进制的秘密信息转化为十进制表达形式，再通过减去图像区域内所有数据的中间值来折叠秘密信息，达到减小像素值修改的目的[7]。对于该方法实现原理的描述如图1所示。

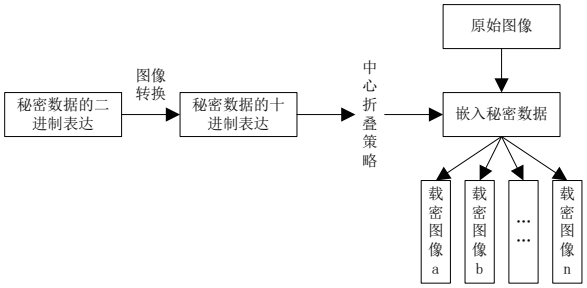

图1 中心折叠策略的实现原理

在加密域图像中，中心折叠策略通过对原始图像像素的位平面划分，得到两个位平面，再将折叠后的秘密数据分别嵌入到两个位平面的最高有效位中，生成两个隐秘像素[8]。设置一个常数χ用于转换十进制数据$\dot{v}$，$\dot{v}$经过中心折叠后可以得到$\dot{v}'$，二者之间数值关系用公式表示为：

$$\dot{v}' = \dot{v} - 2^{\chi-1} \tag{2}$$

中心折叠策略将秘密数据分成了两部分，在实际处理过程中，这两部分被分别嵌入至不同的加密域图像中，具体用公式表示为：

$$\begin{cases} \dot{v}_1' = \left[\dfrac{\dot{v}}{2}\right], \dot{v}_2' = \left[\dfrac{\dot{v}}{2}\right] \\ B_1' = B + \dot{v}_1', B_2' = B + \dot{v}_2' \end{cases} \tag{3}$$

式中：B表示原始像素值；$\dot{v}_1'$、$\dot{v}_2'$表示两个秘密数据；B_1'、B_2'表示两个加密域图像。

1.3 原始图像加密

出于对原始图像隐私的保护，发送方在开始传输图像之前需要对其进行加密处理。如果通过模运算 - 中心折叠的方式进行加密，则具体处理流程包括如下几个步骤：

步骤1：设原始图像像素的平均值为$\overline{X}$，在(0,1)的实数范围内选择一个参数γ作为混沌运算的初始值，利用公式计算新值X'。

$$X' = \gamma + \left(\dot{v}_1' + \dot{v}_2'\right)\overline{X} \Big/ \left(B_1' + B_2'\right)^2 \tag{4}$$

步骤2：利用取模运算生成二维混沌加密矩阵，利用步骤一所得新值X'，经过多次迭代循环后，使原图像中的像素达到充分混沌状态，其运算式为：

$$Z = \varphi \times X' \times \left(1 - X'\right) \tag{5}$$

式中：φ表示混沌参数，其取值满足$0 \le \varphi \le 4$。

步骤3：生成一个与原始图像等大数值矩阵，参考像素点取模运算条件，再基于像素点的混沌表达Z，可将原始图像加密原则表示为：

$$C = \left(\varepsilon - 1\right) \times \sqrt{\frac{Z \cdot F\left(X'\right)}{M_1^{\,2} + M_2^{\,2} + \cdots + M_n^{\,2}}} \tag{6}$$

式中：ε表示像素点位数；$F(X')$表示新值X'的加密函数。通过模运算 - 中心折叠与原始图像最低有效位的结合，可以保证加密函数的准确性，从而在RDH-EI中提高数据嵌入容量[9]。

1.4 图像插值

图像插值的定义对加密域图像的视觉质量和嵌入率具有较大影响。基于模运算 - 中心折叠对原始图像进行加密后，其中只包含基准像素，若直接通过RDH-EI算法隐藏数据，可能导致密码信息过于局限的问题[10]。对于图像插值原则的描述如图2所示。

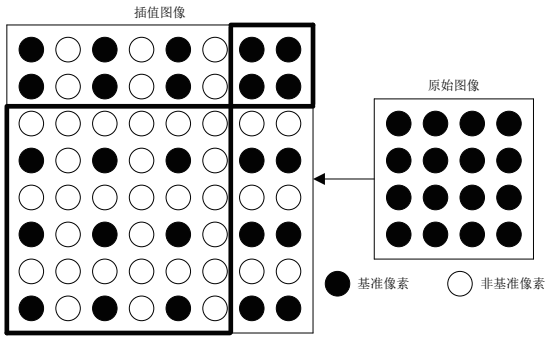

图2 图像插值原则

在基准像素位置上嵌入像素点时，目标信息不可以被更改；而在非基准像素位置上嵌入像素点时，像素值会随着秘密数据的取值而发生变化，即目标信息可以被更改[11]。推导RDH-EI算法下的图像插值运算式为：

$$A = \sum_{\iota=1}^{+\infty} s_\iota \cdot C + f\vec{D} + \left(a_t - a_0\right)^2 \tag{7}$$

式中：ι表示基准像素；s_ι表示基准像素位置上的信息插入值；f表示像素点嵌入项；$\vec{D}$表示秘密数据取值；a_t表示基准像素位置上的隐秘密钥；a_0表示非基准像素位置上的隐秘密钥。

1.5 信息嵌入

由插值信息经过折叠运算后可能会表现出取值为负的情况，因此在实施嵌入处理时，可以设置Sign标志位，以用来标记目标信息所对应的嵌入位置，从而保障RDH-EI技术在加密域图像可逆数据隐藏中的有效性[12]。对于图像插值Sign标志位定义为：

$$\text{Sign} = \begin{cases} 1, A < 0 \\ 0, A \ge 0 \end{cases} \tag{8}$$

由于加密域图像中像素点的分布通常保持直方图特征，所以在嵌入目标信息时，可以将秘密数据直接加入到直方图峰值（Sign标志位所对应的像素点）所对应的像素点中[13]。基于Sign标志位可将信息嵌入计算式表示为：

$$G=\frac{\phi A}{\mathrm{Sign}}\cdot\frac{\kappa^2-1}{|\Delta H|}\cdot\left(g_1+g_2\right)^2 \tag{9}$$

式中：g_1、g_2 分别表示私钥信息与公钥信息；ΔH 表示加密域图像的单位面积；κ 表示秘密数据添加项；ϕ 表示信息合并。信息嵌入可以在不损害加密域图像像素质量的前提下，实施 RDH-EI 技术，从而实现对目标数据的可逆隐藏。

1.6 信息提取与图像恢复

对于拥有数据隐藏密钥的终端而言，其在提取被嵌入的秘密信息时需要将当前数据转换为二进制表达形式，再进行分块提取 [14]。对于信息提取表达式的定义为：

$$L=\boldsymbol{j}^{\nu_1+\nu_2}\cdot G^i \bmod \dot{q}^2 \tag{10}$$

式中：$\boldsymbol{j}$ 表示隐藏密钥中的数据加密向量；ν_1、ν_2分别表示行向与列向加密参数；i 表示二进制转换系数；$\dot{q}$表示像素误差。

对于拥有图像加密密钥的终端而言，其中恢复原始图像时必须一并将被折叠的秘密数据还原，才能够准确分析密文信息与原文信息之间的对应关系 [15]。对于图像恢复表达式的定义为：

$$E=\lambda\cdot\log_G\left(\frac{r_o u_o}{\tilde{\boldsymbol{W}}}\right) \tag{11}$$

式中：λ 表示秘密数据折叠度；$\tilde{\boldsymbol{W}}$表示被折叠部分的数据还原向量；o 表示目标信息；r_o、u_o 分别表示目标信息 o 所对应的原文与密文数据。通过合理的模运算与中心折叠操作，可以在实现 RDH-EI 的过程中减小对原始图像的视觉影响，从而保持较好的图像质量。

2 实验分析

实验部分将针对基于模运算 - 中心折叠 RDH-EI 的加密域图像可逆数据隐藏方法与经典的密文域图像可逆信息隐藏算法设计对比实验，通过对不同实验结果的分析，验证所研究算法的有效性。本次研究硬件环境为 CUP：Core i7 最高主频 2.8 GHz，内存 16 GB，硬盘 512 GB。出于对图像质量的保障，应选择较为适宜的像素阈值。图 3 反映了像素阈取值为 4、6、8、10 时像素量与 PSNR 指标之间的数值关系。

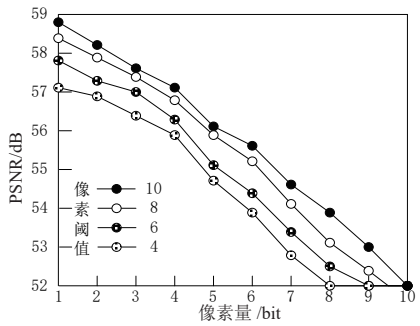

图 3 像素阈值对 PSNR 的影响

根据图 3 可知，在数据嵌入率相同的情况下，像素阈的取值越大，其在原图像中的调整范围就越宽，虽然所需执行时间较长，但 PSNR 指标的数值水平相对较高，表示图像质量也较高。因此，后续实验研究中将像素阈值设定为 10。分别应用基于模运算 - 中心折叠 RDH-EI 的加密域图像可逆数据隐藏方法（实验组）、经典的密文域图像可逆信息隐藏算法（对照组）对原图像中的目标数据进行加密处理。将原图像中的像素信息拆分为 USC-SIPI 数据集、UCID 数据集两种表达形式，分别应用实验组方法、对照组方法对这两类数据集进行加密，并对比加密后图像中 R、G、B 三通道直方图 χ^2 检验的平均取值情况。实验详情如表 1 所示。

表 1 R、G、B 三通道直方图的 χ^2 检验

数据集	通道	实验组	对照组
USC-SIPI 数据集	R 通道	300.34	342.27
	G 通道	306.50	375.45
	B 通道	291.67	352.56
UCID 数据集	R 通道	431.05	463.65
	G 通道	440.23	500.43
	B 通道	432.78	494.58

分析表 1 可知，实验组方法在 USC-SIPI 数据集和 UCID 数据集实验中，所得到的 R、G、B 三通道直方图 χ^2 检验值均小于对照组方法，说明该方法加密图像中直方图的分布更加均匀，在传输过程中，接收终端难以通过数字统计的方式破解密文模板。如果原图像为灰度图像，在加密过程中，可以通过其对比加密前、后冗余空间被占据的情况，分析所研究方法的有效性。通常情况下，灰度图像的像素水平相对较低，原图像中一部分像素点保持空白状态，而加密处理可以填补这些空白的像素点，从而在将明文信息转换为密文信息的同时，控制冗余空间的浪费情况，从而保障信息安全性。图 4 为原图像、实验组以及对照组加密后灰度图像冗余空间的具体实验情况。

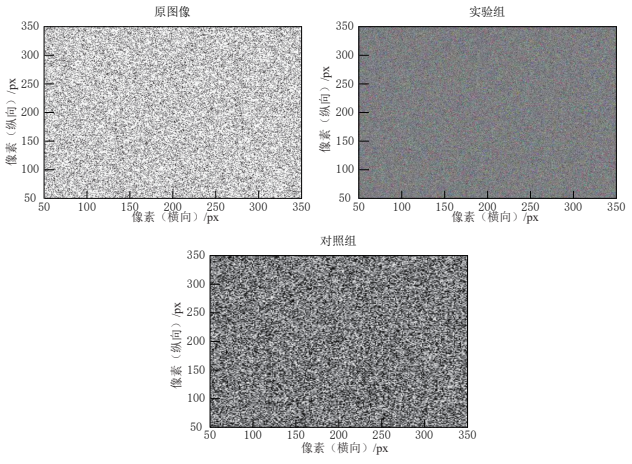

图 4 灰度图像冗余空间分析

分析图 4 可知，对照组方法加密后，原图像中的冗余空间虽然得到了有效占据，但整个图像空间中依然存在较多的空白像素点，表示该方法的加密能力相对有限，不足以保障信息安全性。

3 结语

文中所提出的基于模运算与中心折叠策略的加密域图像可逆数据隐藏（RDH-EI）方法，意在平衡图像质量与安全性以及信息嵌入容量之间的关系，通过理论研究结合实验论证的方式，突出说明了该方法在保障数据嵌入高效性、实现图像无损恢复方面的应用价值。模运算与中心折叠策略的结合，提供了一种全新的像素值调整思想，既利用了加密图像的统计学特性，也大幅提升了原图像中的信息嵌入容量，且在处理过程中，图像视觉质量并不会出现明显下降。相较于其他方法，所研究方法为加密域图像可逆数据隐藏提供了更有效的实施方案。尽管该方法仍然存在许多需要改进的问题，但其实用性与创新性依然在网络信息安全方面带来了巨大进步。

参考文献：

[1] 李喜艳，周清雷，刘征．信息预处理的加密域大容量可逆图像信息隐藏 [J]. 计算机应用与软件，2023, 40(3):343-349.

[2] 李季瑶，付章杰，张玉斌．一种基于跨域对抗适应的图像信息隐藏算法 [J]. 信息网络安全，2023, 23(1):93-102.

[3] 高光勇，季驰，夏志华．基于颜色通道关联性和熵编码的彩色密文图像可逆信息隐藏 [J]. 计算机研究与发展，2025, 62(4):1050-1064.

[4] 李冰，刘怀骏，张伟功．魔方派：面向全同态加密的存算模运算加速器设计 [J]. 电子与信息学报，2023, 45(9):3302-3310.

[5] 韩娟，周思琪，平萍．基于四叉树加密与自适应块编码的密文图像可逆数据隐藏 [J]. 计算机工程，2025, 51(2):202-212.

[6] 周艺腾，唐鑫，金路超．基于自适应 MSB 可逆信息隐藏的图像云数据密文安全去重机制 [J]. 计算机科学，2024, 51(12):352-360.

[7] 项聪，朱毅，陶永鹏，等．基于预测误差绝对值标记的加密图像可逆信息隐藏方法 [J]. 南京师大学报 (自然科学版), 2024, 47(4):126-134.

[8] 陈振宇，殷赵霞，占鸿渐，等．隐含异位联合编码的密文图像可逆信息隐藏 [J]. 中国图象图形学报，2025, 30(3):769-783.

[9] 项聪，陶永鹏，朱毅，等．基于图像块高位平面无损压缩的可逆信息隐藏方法 [J]. 东北师大学报 (自然科学版), 2023, 55(3):101-108.

[10] 蒋宗宝，张敏情，董炜娜，等．基于自适应中值预测和霍夫曼编码的密文域可逆信息隐藏算法 [J]. 科学技术与工程，2024, 24(27):11752-11762.

[11] 张翔宇，栗风永，秦川．基于块分类的密文域多重嵌入可逆信息隐藏算法 [J]. 应用科学学报，2023, 41(2): 272-283.

[12] 郦姝伊，郭玳豆，孔平，等．基于轮廓绘制及填色的构造式信息隐藏算法 [J]. 上海理工大学学报，2024, 46(3): 259-270.

[13] 苏海，余松森，杨珊．基于分离训练与图像去噪的频率域彩色图像隐写方法 [J]. 微电子学与计算机，2024, 41(2): 28-36.

[14] 胡润文，项世军，李晓龙，等．基于 CNN 计算局部复杂度的可逆信息隐藏算法 [J]. 计算机学报，2024, 47(4):776-789.

[15] 苏童，和红杰，原长琦，等．降低文件增长和失真的零系数 JPEG 图像可逆信息隐藏 [J]. 铁道学报，2023, 45(1): 51-62.

【作者简介】

张永杰（1983—），男，河北邢台人，本科，中级，研究方向：卫星技术、网络安全。

（收稿日期：2025-06-16　修回日期：2025-11-07）