



## 基于预测误差编码的加密域可逆数据隐藏算法

马广瑶, 黄德璐, 王建军

(复旦大学 信息科学与工程学院, 上海 200433)

**摘要:** 为提高加密图像可逆数据隐藏的嵌入容量与安全性, 提出一种改进的加密域可逆数据隐藏算法。以分块加密方式保留图像块内相邻像素间的相关性, 利用多元线性回归模型对图像块内特定像素进行预测, 同时以位替换方式将预测误差码元和秘密信息同时嵌入目标像素中, 通过差分对称编码提升编码效率并扩展嵌入空间, 使得接收者在仅拥有加密密钥和嵌入密钥的情况下可无失真地恢复原始图像和提取秘密信息。实验结果表明, 该算法在BOWS-2和UCID数据集上的平均嵌入率分别达到1.717和1.310 bit/pixel, 在提高嵌入容量和安全性的同时实现了信息提取操作和图像恢复操作的完全分离。

**关键词:** 多元线性回归; 加密域; 可逆数据隐藏; 差分对称编码; 嵌入容量

开放科学(资源服务)标志码(OSID):



**中文引用格式:** 马广瑶, 黄德璐, 王建军. 基于预测误差编码的加密域可逆数据隐藏算法[J]. 计算机工程, 2021, 47(5): 138-143, 153.

**英文引用格式:** MA Guangyao, HUANG Delu, WANG Jianjun. Reversible data hiding algorithm in encrypted domain based on prediction error coding[J]. Computer Engineering, 2021, 47(5): 138-143, 153.

## Reversible Data Hiding Algorithm in Encrypted Domain Based on Prediction Error Coding

MA Guangyao, HUANG Delu, WANG Jianjun

(School of Information Science and Technology, Fudan University, Shanghai 200433, China)

**[Abstract]** To improve the embedding capacity and security of the Reversible Data Hiding in Encrypted Images (RDH-EI), this paper proposes an improved Reversible Data Hiding (RDH) algorithm in encrypted domain. In the algorithm, block-level encryption is used to keep the correlation between adjacent pixels in the image block. Then, the specific pixels in the image block are predicted by using the multivariable linear regression model. At the same time, the encoded prediction error and secret information are embedded into the target pixels in the way of bit replacement, and the method of differential symmetric coding is used to improve the coding efficiency and the embedding capacity. Thus the receiver can restore the original image without distortion in the case of having only the encryption key, or extract the secret information in the case of having only the embedded key. Experimental results show that the proposed algorithm effectively improves the average embedding rate, which reaches 1.717 bit/pixel on BOWS-2 and 1.310 bit/pixel on UCID, demonstrating its high embedding capacity and security. Also, it enables information extract operations to be fully separable from the image restoration operations.

**[Key words]** multiple linear regression; encrypted domain; Reversible Data Hiding (RDH); differential symmetric coding; embedding capacity

DOI: 10.19678/j.issn.1000-3428.0057500

### 0 概述

数字图像的可逆数据隐藏(Reversible Data Hiding, RDH)技术可将秘密数据隐秘地嵌入到载体图像中, 并在接收端无失真地恢复载体图像和秘密

数据。随着人们对数据安全及个人隐私重视程度的逐渐提高, 数字图像在传输前通常需要加密。因此, 加密图像可逆数据隐藏(Reversible Data Hiding in Encrypted Images, RDH-EI)技术应运而生, 并受到国内外学者的广泛关注, 成为数据隐藏技术的重要分

基金项目: 国家自然科学基金(61170207)。

作者简介: 马广瑶(1995—), 女, 硕士研究生, 主研方向为可逆信息隐藏; 黄德璐, 硕士研究生; 王建军, 副教授。

收稿日期: 2020-02-25 修回日期: 2020-05-11 E-mail: maguangyaomgy@163.com

支。现有的RDH-EI算法主要可分为加密前预留空间(Vacating Room Before Encryption, VRBE)和加密后腾出空间(Vacating Room After Encryption, VRAE)两类。

VRBE方法通过图像加密前的预处理预留嵌入空间。文献[1]使用传统RDH算法,将图像中部分像素的最低有效位(Lowest Significant Bit, LSB)嵌入其余像素以获取嵌入空间。文献[2]通过预测误差直方图平移方法预留嵌入空间。文献[3]使用稀疏编码方法对图像进行压缩获得隐藏空间。但是,此类方法均要求图像所有者对原始图像进行除加密以外的所有操作,实用性较差。VRAE方法更具实际操作性,获得了研究人员的广泛关注。文献[4]使用流加密方法加密图像,通过翻转图像块内一半像素的3个最低有效位并将其嵌入秘密信息。文献[5]引入边匹配机制,提高了信息提取操作的精确度。文献[6]优化了波动评估函数。文献[7-8]调整最低有效位的翻转方式。由于无法做到无失真恢复原始图像,因此以上方法并不是完全可逆的,并且算法必须在明文域内进行信息提取操作。为解决上述问题,文献[9]提出一种可分离的RDH-EI算法,即可在加密域内完成信息提取操作。文献[10]改进了加密像素的压缩方法。文献[11]提出将加密图像像素分为三组并分别嵌入秘密信息,接收端采用迭代方法恢复原始图像。文献[12]提出基于预测误差的信息嵌入方法,提高了嵌入率。为更好地利用像素间的相关性,文献[13]设计一种新型加密框架。基于该框架,一些明文域RDH算法可被应用于加密域。文献[14]将直方图平移随机化,增强了算法安全性,并通过多层级嵌入增加嵌入容量。文献[15]将图像分块并使块内像素分组,建立差值直方图,通过直方图平移方法嵌入秘密信息。文献[16]采用不同的加密方法加密原始图像的高低位平面,利用同态加法和差值扩展方法分别在高低位平面嵌入秘密信息。上述算法虽然实现了在明文域进行信息提取,但只能在同时拥有加密密钥和嵌入密钥的情况下进行图像恢复操作。针对该问题,文献[17]提出基于矩阵编码的RDH-EI算法,实现信息提取操作和图像恢复操作的完全分离,但由于该算法采用Arnold变换加密方法,因此安全性不高。文献[18]提出基于最高有效位预测的RDH-EI算法,在提高嵌入率的同时实现了信息提取操作和图像恢复操作的完全分离。

针对现有加密图像可逆数据隐藏算法的嵌入容量较低与安全性较差的问题,本文提出一种基于预测误差编码的加密域可逆数据隐藏算法。该算法利用基于图像块的多元线性回归模型进行目标像素预测并对预测误差编码预留嵌入空间。通过差分对称编码提升编码效率,扩展嵌入空间,并且接收者在仅拥有加密密钥的情况下可无失真地恢复原始图像,在仅拥有嵌入密钥的情况下可无误地提取秘密信息。

## 1 多元线性回归预测与差分对称编码

### 1.1 多元线性回归模型

多元线性回归分析常被用来探究多个因变量与一个自变量之间的相关关系。多元线性回归模型在多次观测下的一般形式为:

$$y_i = b_0 + b_1 x_{1i} + b_2 x_{2i} + \cdots + b_k x_{ki} + \varepsilon_i \quad (1)$$

其中,  $y_i (1 \leq i \leq n)$  为第  $n$  组观测值中因变量的值,  $x_{1i}, x_{2i}, \dots, x_{ki}$  为自变量,  $b_0, b_1, \dots, b_k$  为  $(k+1)$  个回归系数,  $\varepsilon_i$  为误差项。式(1)的矩阵形式为:

$$Y = X \cdot B + \varepsilon \quad (2)$$

在确保误差平方和最小的前提下寻找回归系数的估计值(如式(3)所示),采用最小二乘法进行求解(如式(4)所示),并将求解结果通过矩阵形式进行表示(如式(5)所示)。

$$Q = \sum_{i=1}^n \varepsilon_i^2 = (Y - XB)^T (Y - XB) \quad (3)$$

$$\frac{\partial (Y - XB)^T (Y - XB)}{\partial B} = 0 \quad (4)$$

$$B = (X^T X)^{-1} X^T Y \quad (5)$$

对于最小二乘法得到的残差,即训练误差表示为:

$$\varepsilon = Y - XB = \{I_n - X(X^T X)^{-1} X^T\} Y \quad (6)$$

其中,  $I_n$  为  $n$  阶单位阵。假设最小二乘法得到的残差服从  $N(0, \sigma^2)$  分布,则平均预测误差表示为:

$$\zeta = \frac{1}{n} E(Y - XB)^T (Y - XB) = \frac{n-k}{n} \sigma^2 \quad (7)$$

可以看出,样本越多,模型的拟合效果越好。当在新样本集上进行预测时,实际预测误差如式(8)所示,实际预测误差除了固定项  $\sigma^2$ ,还包括用样本估计真实值所产生的误差。

$$\varepsilon_0 = E(Y_0 - X_0 B)^T (Y_0 - X_0 B) = \sigma^2 + \sigma^2 X_0 (X^T X)^{-1} X_0 \quad (8)$$

在得到参数的最小二乘估计值后,还需进行统计检验并判断模型的拟合优度  $R^2$ ,  $R^2$  计算公式如下:

$$R^2 = 1 - \frac{E_{ESS}}{T_{TSS}} \quad (9)$$

其中:  $E_{ESS} = \sum_{i=1}^n (y_i - \hat{y}_i)^2$ ;  $T_{TSS} = \sum_{i=1}^n (y_i - \bar{y})^2$ ;  $R^2$  值越大,表明拟合效果越好。一般而言,在多元线性回归模型的拟合和预测过程中,自变量与因变量之间的相关关系越强,拟合和预测效果越好,并且图像相邻像素之间的强相关关系有助于多元线性回归模型的拟合和预测。

### 1.2 基于图像块的多元线性回归预测

在对一幅大小为  $M \times M$  的灰度图像进行预测时,首先将图像划分为  $3 \times 3$  的图像块,然后逐图像块进行像素预测。如图1所示,将块内4个角上的像素  $v_1, v_2, v_3, v_4$  作为参考像素,图像块中心的像素  $u_1$  既可以被预测,又可以作为参考像素对其余像素

$x_1, x_2, x_3, x_4$  进行预测。

$v_1$	$x_1$	$v_2$
$x_2$	$u_1$	$x_3$
$v_3$	$x_4$	$v_4$

图1 基于图像块的多元线性回归预测

Fig.1 Multiple linear regression prediction based on image block

在一个图像块内共进行5组预测,5组预测模型如式(10)所示:

$$\begin{aligned} u_1 &= b_{10} + b_{11}v_1 + b_{12}v_2 + b_{13}v_3 + b_{14}v_4 \\ x_1 &= b_{20} + b_{21}v_1 + b_{22}u_1 + b_{23}v_2 \\ x_2 &= b_{30} + b_{31}v_1 + b_{32}u_1 + b_{33}v_3 \\ x_3 &= b_{40} + b_{41}v_2 + b_{42}u_1 + b_{43}v_4 \\ x_4 &= b_{50} + b_{51}v_3 + b_{52}u_1 + b_{53}v_4 \end{aligned} \quad (10)$$

其中,  $b_{ij}$  为第  $i$  组模型的第  $j$  个回归系数。

### 1.3 差分对称编码

在差分对称编码方法中,码元与误差值( $d$ )的对应关系为:当码元长度( $n$ )为1时,以二进制码‘0’表示十进制意义上的误差值0,以二进制码‘1’表示误差值1;当码元长度大于1时,以码元的第一位表示误差的正负,其余位为误差绝对值或者误差值减去1的二进制表示。具体而言:当误差值为正数时,码元的第一位编为‘1’,其余位为误差值减去1的二进制表示;当误差值小于等于0时,码元的第一位编为‘0’,其余位为误差绝对值的二进制表示。假设码元长度为  $n(n > 1)$ ,码元序列为  $c_1, c_2, \dots, c_n$ ,那么误差值  $d$  与码元序列之间的关系如下:

$$\begin{cases} d = \sum_{i=2}^n c_i \cdot 2^{n-i} + 1, d > 0 \\ |d| = \sum_{i=2}^n c_i \cdot 2^{n-i}, d \leq 0 \end{cases} \quad (11)$$

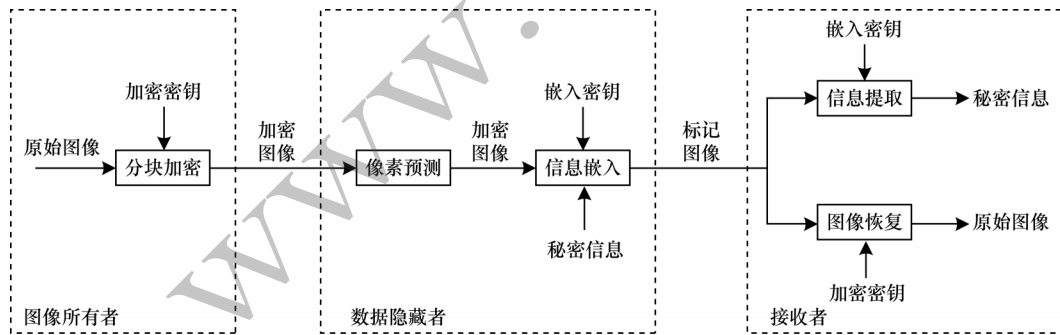


图2 本文算法框架

Fig.2 Framework of the proposed algorithm

### 2.1 图像加密

对于大小为  $M \times N$  的载体图像,首先将图像分为  $m$  个大小为  $3 \times 3$  的图像块,其中  $m = \lfloor (M \times N) / (3 \times 3) \rfloor$ 。依据加密密钥生成伪随机序列  $\{r_1, r_2, \dots, r_m\}$ ,根据该序列对图像块进行置乱,然后对于任一图像块

表1以码元长度为1、2和3为例,说明码元长度  $n$  与误差值  $d$  的对应关系,其中“—”表示码元长度  $n$  无法表示误差值  $d$ 。

表1 码元长度为1、2和3时的对称编码结果

Table 1 Symmetric coding results when the symbol length is 1, 2 and 3

$n$	$d=-3$	$d=-2$	$d=-1$	$d=0$	$d=1$	$d=2$	$d=3$	$d=4$
1	—	—	—	0	1	—	—	—
2	—	—	01	00	10	11	—	—
3	011	010	001	000	100	101	110	111

根据上述规则,不同码元长度表示的误差值范围如式(12)所示,即当码元长度为  $n(1 \leq n \leq 7)$  时,共有  $2^n$  种误差值表示。对于差分编码方法,假设信号源等概率分布,根据式(13)计算得到编码效率为1。

$$\begin{cases} -(2^{n-1} - 1) \leq d \leq 2^{n-1}, n = 2, 3, \dots, 7 \\ 0 \leq d \leq 1, n = 1 \end{cases} \quad (12)$$

$$\eta = \frac{\sum_{i=1}^{2^n} p_i \cdot \lg p_i}{\sum_{i=1}^{2^n} p_i \cdot l_i} \quad (13)$$

其中,  $p_i$  为信号源出现概率,  $l_i$  为信号源长度。

## 2 加密域可逆数据隐藏算法

本文算法框架如图2所示,首先由图像所有者对原始图像进行分块加密,保留图像块内像素间的相关性,然后数据隐藏者在接收到加密图像后,对加密图像分块并对子块内像素值进行预测,若像素预测误差在一定范围内,则对预测误差进行编码,并采用位替换方法嵌入秘密数据,最后接收者使用嵌入密钥可以提取秘密信息,而采用加密密钥可以准确无误地恢复原始图像。

$B_k(k = 1, 2, \dots, m)$ ,将图像块内的像素  $p_{ij}^k$  与同一字节  $r_k$  进行取余运算得到加密像素:

$$e_{ij}^k = \text{mod}(p_{ij}^k + r_k, 256) \quad (14)$$

当  $M$  或  $N$  无法被3整除时,原始图像中并非所有像素均可构成图像块。针对该情况,可对子块之

外的其余像素采用置乱方式进行加密,进一步提高加密图像的安全性。

## 2.2 像素预测与分类

在接收到加密图像后,数据隐藏者首先将数据集中的标准图像作为训练样本,对5组多元线性回归模型进行训练得到回归系数。具体方法为将数据集中的图像划分为大小为 $3 \times 3$ 的图像块,假设训练集中包含 $t$ 个图像块,以图1中心位置 $u_1$ 像素值的回归分析为例,将每个图像块内的 $v_1, v_2, v_3, v_4$ 像素值作为观测自变量,中心位置 $u_1$ 像素值作为观测因变量分别代入式(10),矩阵形式为:

$$U = V \cdot B \quad (15)$$

$$\text{其中, } U = \begin{bmatrix} u_{11} \\ u_{12} \\ \vdots \\ u_{1t} \end{bmatrix}, V = \begin{bmatrix} 1 & v_{11} & v_{21} & v_{31} & v_{41} \\ 1 & v_{12} & v_{22} & v_{32} & v_{42} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & v_{1t} & v_{2t} & v_{3t} & v_{4t} \end{bmatrix}, B = \begin{bmatrix} b_{10} \\ b_{11} \\ b_{12} \\ b_{13} \\ b_{14} \end{bmatrix}.$$

将式(15)结合式(5)可得到相关系数的解完成回归分析。类似地,对式(10)中其他几组模型分别进行回归分析。然后将加密图像划分为 $3 \times 3$ 的图像块,利用训练得到的多元线性回归模型逐块地进行像素预测,计算图像块内目标像素 $u_1, x_1, x_2, x_3, x_4$ 的预测值,设像素预测值为 $p$ ,原始像素值为 $o$ ,预测误差 $d$ 的计算公式如下:

$$d = p - o \quad (16)$$

假设采用 $n$  bit对预测误差进行编码,根据差分对称编码可知,若预测误差满足式(12),则目标像素可进行秘密数据嵌入,否则目标像素不可嵌入秘密信息,因此目标像素被分为可嵌入像素和不可嵌入像素两类。此外,用 $5m$  bit的位置图对目标像素的可嵌入性进行标记。当目标像素可嵌入时,位置图相应位置标记为1,否则标记为0。为预留更多的嵌入空间,还可使用算术编码方法对位置图序列进行压缩。

## 2.3 辅助信息存储

为使接收端无误地提取秘密信息和恢复原始图像,将参数 $n$ 、位置图长度、多元线性回归模型系数以及位置图序列作为辅助信息嵌入加密图像中,即将辅助信息比特流以位替换的方式嵌入参考像素的最低有效位中,而被替换的LSB则与秘密信息共同嵌入可嵌入的像素中,因此待嵌入信息包括秘密信息和参考像素的LSB。

## 2.4 秘密信息嵌入

为保证算法安全性,使用嵌入密钥并通过流加密方式对秘密信息进行加密。对于可嵌入像素,按照差分对称编码方法对预测误差进行编码,以 $n$  bit预测误差码元代替可嵌入像素的高 $n$ 位,使用待嵌入信息替换可嵌入像素的低 $(8-n)$ 位。对于不可嵌入像素,像素值保持不变。例如,当 $n=3$ 时,经秘密信息嵌入后图像块的像素分布如图3所示,待嵌入信息比特流为‘01101...’。对中心位置像素进行预测,假设预测值为102,则预测误差为-3,预测误差符

合式(12),该像素为可嵌入像素。由表1可知,对应预测误差码元序列为‘011’,可嵌入的5 bit信息为‘01101’,位替换后中心位置像素的码元序列为‘01101101’,对应的像素值为109。

125		98
	105	
94		66

→

125		98
	109	
94		66

图3 秘密信息嵌入后图像块的像素分布

Fig.3 Pixel distribution of image block after secret information is embedded

## 2.5 信息提取与图像恢复

在接收端共存在接收者仅拥有嵌入密钥、接收者仅拥有加密密钥和接收者同时拥有加密密钥和嵌入密钥3种情况。当接收者仅拥有嵌入密钥时,可以完全无误地提取嵌入信息,具体步骤如下:

1)将标记图像分块,扫描参考像素的LSB,提取辅助信息。

2)根据位置图确定可嵌入像素的位置,从可嵌入像素的低 $(8-n)$ 位中提取嵌入信息,获取加密后的秘密信息。

3)使用嵌入密钥解密,即可恢复秘密信息。

当接收者仅拥有加密密钥时,可以无失真地重建原始图像,具体步骤如下:

1)将标记图像分块,扫描参考像素的LSB,提取辅助信息。根据辅助信息中的回归系数信息重建多元线性回归模型。

2)根据位置图获取可嵌入像素位置,并在可嵌入像素的低 $(8-n)$ 位中提取嵌入信息,获取参考像素的原始LSB序列,恢复参考像素的像素值。

3)基于参考像素恢复每个图像块内中心位置的像素值,即使用相应的多元线性回归模型对中心像素进行预测,从中心像素的高 $n$ 位处获取预测误差码元,对照编码规则得到预测误差,根据式(17)将像素预测值 $p$ 与预测误差 $d$ 相减可得到原始像素值 $o$ 。

$$o = p - d \quad (17)$$

4)重复步骤3恢复图像块内其余可嵌入像素的像素值,使得加密图像得到恢复。

5)将加密图像分块,根据加密密钥将块内像素值与同一字节进行取余运算,然后对图像块进行反置乱。若图像中有未凑成图像块的像素,则同样使用加密密钥进行反置乱。

当接收者同时拥有两把密钥时,可以按照上述步骤分别提取秘密信息和恢复原始图像。

## 3 实验结果与分析

为验证本文算法的性能,在BOWS-2<sup>[19]</sup>和UCID<sup>[20]</sup>数据集中随机选取大小为 $512 \times 512$ 的标准

测试图像进行实验,如图4所示。从模型有效性、嵌入容量和算法性能的角度对本文算法进行分析。所有实验均在 Matlab2014a 平台上完成。

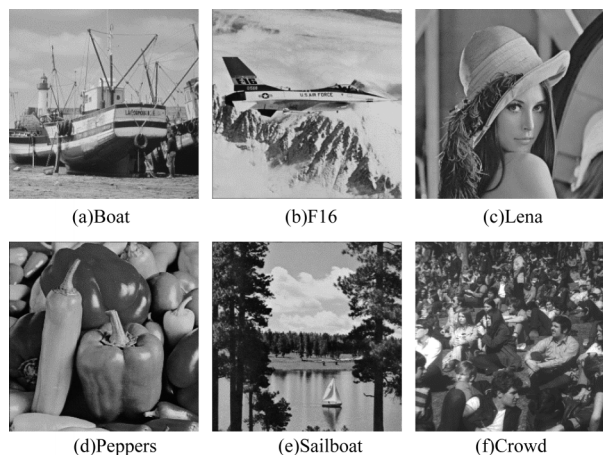


图4 标准测试图像

Fig.4 Standard test images

### 3.1 多元线性回归模型有效性分析

在训练多元线性回归模型时需要足够多的样本,如果模型特征数(即自变量数目)较多而样本数过少,则会造成欠拟合问题或过拟合问题。一般而言,样本数越多,拟合效果越好。在实验过程中,在 BOWs-2<sup>[19]</sup> 数据集中随机选取 100 张大小为 512×512 的灰度图像,将每张图像划分为 3×3 的图像块,将数据集中的图像块作为训练样本,对 5 组多元线性回归模型进行拟合,训练得到回归系数为  $b_{10}=-0.759\ 4$ 、 $b_{11}=0.245\ 3$ 、 $b_{12}=0.257\ 8$ 、 $b_{13}=0.257\ 1$ 、 $b_{14}=0.245\ 3$ 、 $b_{20}=-0.548\ 1$ 、 $b_{21}=0.416\ 0$ 、 $b_{22}=0.174\ 6$ 、 $b_{23}=0.413\ 5$ 、 $b_{30}=-0.616\ 5$ 、 $b_{31}=0.365\ 9$ 、 $b_{32}=0.277\ 6$ 、 $b_{33}=0.361\ 1$ 、 $b_{40}=-0.564\ 6$ 、 $b_{41}=0.414\ 5$ 、 $b_{42}=0.173\ 8$ 、 $b_{43}=0.415\ 9$ 、 $b_{50}=-0.612\ 4$ 、 $b_{51}=0.364\ 1$ 、 $b_{52}=0.277\ 0$ 、 $b_{53}=0.363\ 5$ 。拟合优度是表征多元线性回归模型有效性的重要参数。表2结果了 5 组模型的拟合优度,可以看出 5 组模型的拟合优度均接近或大于 0.98,整体接近 1,由此表明 5 组模型均有效描述了目标像素与邻近像素的相关关系,拟合度较高。

表2 多元线性回归模型的拟合优度

Table 2 Goodness of fit for multiple linear regression models

目标像素	$R^2$
$u_1$	0.979 4
$x_1$	0.989 1
$x_2$	0.987 9
$x_3$	0.989 1
$x_4$	0.987 9

### 3.2 嵌入容量分析

对于本文算法,码元长度  $n$  是影响嵌入容量的重要因素。码元长度越长,表征的预测误差范围越大,同一幅图像内可嵌入像素数量越多,但一个像素内的可嵌入空间越小。为进一步说明码元长度对实

验结果的影响,利用 RDH-EI 算法对部分标准灰度图像在不同码元长度下的嵌入率进行测试,如表 3 所示。可以看出,嵌入率随着码元长度的增加先增大再减少,测试图像的嵌入率在码元长度为 3 或 4 时达到最大,说明可嵌入像素数量和每个像素可嵌入空间在码元长度为 3 或 4 时可达到最佳平衡。

表3 不同码元长度下 RDH-EI 算法的嵌入率比较

Table 3 Comparison of embedding rate of RDH-EI algorithm with different symbol lengths ( $\text{bit} \cdot \text{pixel}^{-1}$ )

图像	嵌入率						
	$n=1$	$n=2$	$n=3$	$n=4$	$n=5$	$n=6$	$n=7$
Boat	0.75	1.05	1.33	1.37	1.21	0.83	0.37
F16	1.25	1.55	1.71	1.60	1.29	0.86	0.39
Lena	0.78	1.13	1.52	1.60	1.32	0.88	0.39
Peppers	0.58	0.85	1.24	1.51	1.30	0.86	0.38
Crowd	1.20	1.36	1.46	1.45	1.24	0.83	0.36

为验证本文算法的普适性和有效性,设置参数  $n=3$ ,在 BOWs-2<sup>[19]</sup> 和 UCID<sup>[20]</sup> 数据集中分别随机选取 100 张图像进行实验,测试图像的嵌入率如图 5 所示。表 4 给出了数据集测试图像的嵌入率统计数据。可以看出:对于来自 BOWs-2 数据集的 100 张随机选取的测试图像,嵌入率的最高值为 2.641 bit/pixel,最低值为 0.578 bit/pixel,平均值为 1.717 bit/pixel;对于来自 UCID 数据集的 100 张随机选取的测试图像,嵌入率的平均值为 1.310 bit/pixel,表明本文算法稳定性较强且嵌入容量较大。

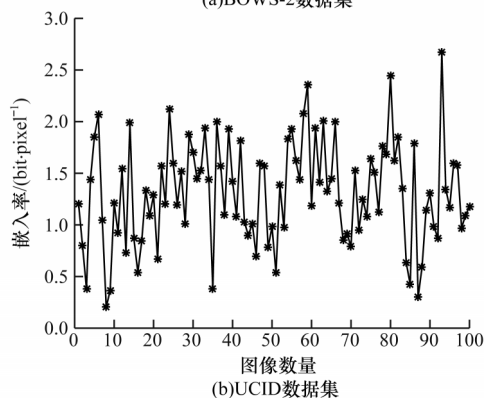
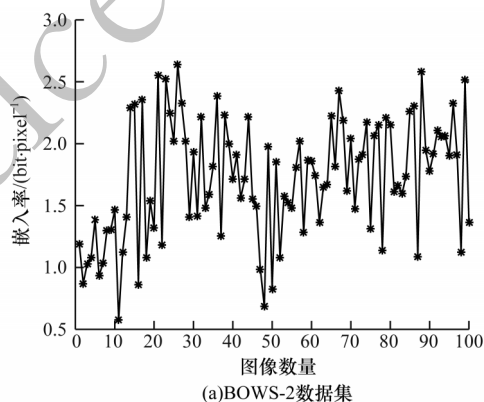


图5 测试图像嵌入率

Fig.5 Embedding rate of test images

表 4 数据集测试图像的嵌入率统计			
Table 4 Statistics of embedding rate for test images in dataset (bit·pixel <sup>-1</sup> )			
数据集	嵌入率		
	最高值	最低值	平均值
BOWS-2	2.641	0.578	1.717
UCID	2.676	0.204	1.310

将本文算法与具有代表性的文献[9,13-14,18]算法进行嵌入率比较,如表 5 所示。文献[9]采用压缩加密像素最低有效位的方式预留嵌入空间,嵌入容量有限。文献[13]提出新型加密框架并使用传统 RDH 方法嵌入秘密信息。文献[14]通过引入多层嵌入增加嵌入容量。与以上 3 种算法相比,本文算法的嵌入率有较大幅度的提升,在 F16、Lena 以及 Peppers 图像上的嵌入率约提高 1 bit/pixel。与文献[18]算法相比,本文算法的嵌入率也有一定程度的提升。

表 5 5 种算法的嵌入率比较					
Table 5 Comparison of embedding rate of five algorithms (bit·pixel <sup>-1</sup> )					
图像	嵌入率				
	文献[9] 算法	文献[13] 算法	文献[14] 算法	文献[18] 算法	本文 算法
Boat	0.012	0.160	0.560	0.958	1.370
F16	0.020	0.118	0.764	0.989	1.710
Lena	0.015	0.092	0.622	0.964	1.601
Peppers	0.007	0.080	0.434	0.976	1.505
Sailboat	0.012	0.080	0.327	0.984	1.133

3.3 算法性能分析

从图像恢复操作无误、信息提取操作无误以及信息提取操作与图像恢复操作可完全分离角度对本文算法进行分析并与经典算法进行比较,如表 6 所示。

表 6 4 种算法的性能比较			
Table 6 Performance comparison of four algorithms			
算法	图像恢复操作 无误	信息提取操作 无误	完全 可分离性
文献[9]算法	否	是	否
文献[13]算法	是	是	否
文献[14]算法	是	是	否
本文算法	是	是	是

本文算法由于在信息嵌入和信息提取过程中对于原始像素的操作是完全可逆的,因此保证了图像恢复操作的无失真。文献[9]算法通过压缩矩阵对加密图像的多个最低有效位平面进行压缩以获取冗余空间,因此在恢复图像操作过程中并不能保证完全无误。此外,本文算法可嵌入像素的高  $n$  位包含了图像恢复操作所需的预测误差信息,低  $(8-n)$  位包含了图像恢复操作所需部分参考像素的原始 LSB 信

息以及信息提取操作所需加密后的秘密信息两部分数据,因此图像恢复操作和信息提取操作所需的信息可以分别提取,保证了两种操作的完全可分离性。文献[13-14]算法原始图像的恢复需要同时拥有嵌入密钥和加密密钥,只有在信息提取操作完成后才能进行图像恢复操作。

4 结束语

本文提出一种基于预测误差编码的加密域可逆数据隐藏算法。在图像块内建立多元线性回归模型,利用数据集中的大量图像训练模型,并采用多元线性回归模型预测目标像素,同时通过差分对称编码方式提高编码效率并间接增加嵌入容量。实验结果表明,该算法具有嵌入容量大、信息提取操作和图像恢复操作可完全分离的特点,能较好地实现秘密信息提取与原始图像重建且安全性较高。后续将探究更有效的可嵌入像素标记方法以增加嵌入容量,同时利用图像块内相邻像素间的相关性,建立更加高效的多元线性回归模型提高像素预测准确率。

参考文献

[ 1 ] MA Kede, ZHANG Weiming, ZHAO Xianfeng, et al. Reversible data hiding in encrypted images by reserving room before encryption [J]. IEEE Transactions on Information Forensics and Security, 2013, 8(3): 553-562.

[ 2 ] ZHANG Weiming, MA Kede, YU Nenghai. Reversibility improved data hiding in encrypted images [J]. Signal Processing, 2014, 94: 118-127.

[ 3 ] CAO Xiaochun, DU Ling, WEI Xingling, et al. High capacity reversible data hiding in encrypted images by patch-level sparse representation [J]. IEEE Transactions on Cybernetics, 2016, 46(5): 1132-1143.

[ 4 ] ZHANG Xinpeng. Reversible data hiding in encrypted image [J]. IEEE Signal Processing Letters, 2011, 18(4): 255-258.

[ 5 ] HONG W, CHEN T S, WU H Y. An improved reversible data hiding in encrypted images using side match [J]. IEEE Signal Processing Letters, 2012, 19(4): 199-202.

[ 6 ] LIAO Xin, SHU Changwen. Reversible data hiding in encrypted images based on absolute mean difference of multiple neighboring pixels [J]. Journal of Visual Communication and Image Representation, 2015, 28: 21-27.

[ 7 ] HONG W, CHEN T S, CHEN J, et al. Reversible data embedment for encrypted cartoon images using unbalanced bit flipping [C]//Proceedings of International Conference on Swarm Intelligence. Washington D. C., USA: IEEE Press, 2013: 208-214.

[ 8 ] LI Ming, XIAO Di, PENG Zhongxian, et al. A modified reversible data hiding in encrypted images using random diffusion and accurate prediction [J]. ETRI Journal, 2014, 36(2): 325-328.

[ 9 ] ZHANG Xinpeng. Separable reversible data hiding in encrypted image [J]. IEEE Transactions on Information Forensics and Security, 2012, 7(2): 826-832.

(下转第 153 页)

(上接第 143 页)

- [10] QIAN Zhenxing, ZHANG Xinpeng. Reversible data hiding in encrypted images with distributed source encoding[J]. IEEE Transactions on Circuits & Systems for Video Technology, 2016, 26(4): 636-646.
- [11] QIAN Zhenxing, ZHANG Xinpeng, FENG Guorui. Reversible data hiding in encrypted images based on progressive recovery[J]. IEEE Signal Processing Letters, 2016, 23(11): 1672-1676.
- [12] WU Xiaotian, SUN Wei. High-capacity reversible data hiding in encrypted images by prediction error[J]. Signal Processing, 2014, 104: 387-400.
- [13] HUANG Fangjun, HUANG Jiwu, SHI Yunqing. New framework for reversible data hiding in encrypted domain[J]. IEEE Transactions on Information Forensics and Security, 2016, 11(12): 2777-2789.
- [14] GE Haoli, CHEN Yan, QIAN Zhenxing, et al. A high capacity multi-level approach for reversible data hiding in encrypted images[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2019, 29(8): 2285-2295.
- [15] LI Zhijia, XIA Wei. Reversible information hiding algorithm in encrypted domain based on difference histogram shifting[J]. Computer Engineering, 2019, 45(11): 152-158. (in Chinese)  
李志佳, 夏玮. 基于差值直方图平移的密文域可逆信息隐藏算法[J]. 计算机工程, 2019, 45(11): 152-158.
- [16] ZHOU Neng, ZHANG Minqing, LIN Wenbing. Separable reversible information hiding algorithm in encrypted domain based on secret sharing[J]. Computer Engineering, 2020, 46(10): 112-119. (in Chinese)  
周能, 张敏情, 林文兵. 基于秘密共享的可分离密文域可逆信息隐藏算法[J]. 计算机工程, 2020, 46(10): 112-119.
- [17] LIU Yu, YANG Bailong, ZHAO Wenqiang, et al. Reversible information hiding algorithm in large capacity ciphertext field based on matrix coding[J]. Computer Engineering, 2018, 44(10): 221-226. (in Chinese)  
刘宇, 杨百龙, 赵文强, 等. 基于矩阵编码的大容量密文域可逆信息隐藏算法[J]. 计算机工程, 2018, 44(10): 221-226.
- [18] PUTEAUX P, PUECH W. High-capacity reversible data hiding in encrypted images using MSB prediction[C]// Proceedings of the 6th International Conference on Image Processing Theory, Tools and Applications. Washington D. C., USA: IEEE Press, 2017: 10-15.
- [19] The BOWS-2 image database[EB/OL]. [2020-01-15]. <http://bows2.ec-lille.fr/>.
- [20] SCHAEFER G, STICH M. UCID: an uncompressed color image database[C]// Proceedings of Storage and Retrieval Methods and Applications for Multimedia. [S. l.]: International Society for Optics and Photonics, 2003: 472-480.

编辑 陆燕菲