

小波域基于差分统计量直方图平移的图像 鲁棒可逆信息隐藏算法*

梁幸源, 项世军

暨南大学 信息科学技术学院/网络空间安全学院 广州 中国 510632

摘要 随着互联网技术的飞速发展和5G时代的到来,数字多媒体的交流和传播变得越来越便捷。为了解决网络环境下,数字图像的版权保护、完整性认证和篡改定位等问题,本文提出了一种小波域基于差分统计量直方图平移的图像鲁棒可逆信息隐藏算法,其主要思想为:1)对载体图像进行Haar小波变换;2)对变换后所得到的低频子带进行分块并计算分块的差分统计量以构造差分统计量的直方图;3)通过平移直方图将秘密信息嵌入到图像的低频子带中,并通过Haar小波逆变换得到带秘密信息的图像;4)在接收方,通过计算低频子带的分块差分统计量可以将秘密信息准确地提取出来,并且通过执行直方图平移的逆操作可以无损地还原出原始的低频子带,从而无失真地恢复出原始载体图像;5)带秘密信息的图像在遭到一定程度的图像处理操作的攻击后,被嵌入的秘密信息仍然可以被有效地提取出来,例如压缩因子为30的JPEG压缩和标准差为30的加性高斯噪声。与现有的几种鲁棒可逆信息隐藏算法相比,本文算法有更强的鲁棒性。实验结果验证了本文算法的有效性。

关键词 鲁棒可逆信息隐藏; Haar小波变换; 差分统计量; 直方图平移; 完整性认证; 版权保护
中图法分类号 TP309 **DOI号** 10.19363/J.cnki.cn10-1380/tn.2020.05.09

Robust and Reversible Data Hiding Algorithm Based on Histogram of Difference Statistics Shifting in Wavelet Domain*

LIANG Xingyuan, XIANG Shijun

School of Information Science and Technology / School of Cyber Security, Jinan University, Guangzhou 510632, China

Abstract With the rapid development of Internet technology and the arrival of 5G, it is becoming more and more convenient to disseminate digital multimedia. In order to solve the problems of copyright protection, integrity authentication and tamper localization of digital images in the network, this paper proposes an robust and reversible data hiding algorithm based on the histogram of differential statistics shifting in the wavelet domain, including five aspects: 1) perform Haar wavelet transform on the original image; 2) the low frequency sub-band obtained by Haar wavelet transform is divided into a number of non-overlapping blocks, and the difference statistic of each block is calculated to construct a histogram of the difference statistics; 3) the additional data can be embedded into the low frequency sub-band of the image by shifting the histogram, and the image with additional information can be obtained by inverse Haar wavelet transform; 4) on the receiver side, the additional information can be accurately extracted by calculating the difference statistics of the blocks in the low-frequency sub-band, and by using the inverse operation of histogram shifting, the original low frequency sub-band can be restored losslessly, so that the original image can be restored without distortion; 5) the embedded additional information can still be effectively extracted from the image with additional information which is attacked by some typical image processing operations to some extent, such as JPEG compression with a compression factor of 30 and additive Gaussian noise with a standard deviation of 30. Compared with several existing robust and reversible data hiding schemes, the proposed scheme is more robust. Experimental results verify the effectiveness of the proposed scheme.

Key words robust and reversible data hiding; haar wavelet transform; difference statistic; histogram shifting; integrity authentication; copyright protection

通讯作者: 项世军, 博士, 教授, Email: shijun_xiang@qq.com。

本课题得到国家自然科学基金(No. 61772234)和广东省科技创新战略专项资金(“攀登计划”专项资金)项目(No. pdjh2020a0060)的资助。

收稿日期: 2019-12-31; 修改日期: 2020-02-20; 定稿日期: 2020-4-20

1 引言

可逆信息隐藏技术是信息隐藏技术的一个重要分支, 与传统信息隐藏技术有所不同的是, 传统信息隐藏技术主要关注秘密信息, 而可逆信息隐藏技术更注重原始的载体信息^[1]。可逆信息隐藏技术利用数字载体中的冗余, 将秘密信息嵌入到数字载体中, 接收方在得到含秘密信息的数字载体后, 可以在提取出秘密信息的同时, 无失真地恢复出原始数字载体^[2]。该技术可以用于数字载体的内容识别、完整性认证和版权保护, 已广泛用于对数字载体的保密性、安全性和保真度有着较高要求的领域, 如法律认证、军事图像、遥感图像以及医学图像等^[3]。可逆信息隐藏算法大致可以分为以下四类: 无损压缩^[4-5]、差值扩展^[6-7]、直方图平移^[8-13]和预测误差扩展^[14-18]。

由于可逆信息隐藏技术通常不考虑鲁棒性, 因此大多数现有的可逆信息隐藏算法是脆弱的, 当含秘密信息的数字载体在遭到噪声的干扰或信号处理操作的攻击后, 会丢失所隐藏的秘密信息。然而在实际生活中, 当带秘密信息的数字载体在网络上传送时, 可能会遭受到噪声或信号处理操作的干扰或攻击, 于是在许多应用场景中, 用户希望嵌入的秘密信息具有一定的鲁棒性。因此, 鲁棒可逆信息隐藏技术已经成为了信息隐藏领域里的另一个重要研究方向。在鲁棒可逆信息隐藏技术中, 如果含秘密信息的数字载体是完好无损的, 则接收方可以在正确地提取出秘密信息的同时, 无损地恢复出原始数字载体; 如果含秘密信息的数字载体受到噪声或信号处理操作的干扰或攻击时, 接收方可以从受攻击的数字载体中有效地出秘密信息^[19]。近年来, 国内外的研究学者已经提出了一些鲁棒可逆信息隐藏算法^[19-29]。

最早在文献[19], Vleeschouwer 等人提出了一种基于双映射的循环实现的鲁棒可逆水印算法。该算法将图像进行分块, 并将选中的分块分成两个区域, 然后将两个区域的灰度值直方图映射到两个圆上, 通过调整两个圆的质心来嵌入水印。该算法对 JPEG 压缩具有一定的鲁棒性, 但为了避免溢出问题, 算法在加法和减法中采用了模 256 加的方案, 导致在水印的嵌入过程中会引入椒盐噪声, 使得嵌入水印后的图像质量较差。为了解决在水印的嵌入过程中所引入的椒盐噪声并提高带水印图像的视觉质量, Vleeschouwer 等人对文献[19]中的方案进行了改进, 提出了文献[20]。为了避免在嵌

水印的过程中引入椒盐噪声, Ni 等人^[21-22]提出了一种空域下的统计量直方图平移的鲁棒可逆信息隐藏算法。该算法实现了对 JPEG/JPEG2000 以及高斯噪声的鲁棒性, 但在进行秘密信息的嵌入时会引入错误比特, 需要利用纠错码(Error Correction Code, ECC)来纠正错误比特, 导致算法的嵌入容量较低。文献[21]提出了一个基于直方图平移的鲁棒可逆信息隐藏算法框架, 此后绝大多数的鲁棒可逆信息隐藏方案都是基于此框架设计的。在文献[24]中, Gao 等人对 Ni 等人的方法进行了改进, 所提出的算法在提取秘密信息的过程中不再需要 ECC 来纠正错误比特, 同时选用了更为有效的统计量作为鲁棒特征, 提高了算法的鲁棒性。在文献[25]中, Zeng 等人选择图像分块的差分统计量作为鲁棒特征, 并通过引入两个阈值(T, G)以及新的直方图平移方式来嵌入秘密信息, 提高了算法的鲁棒性。在文献[26]中, An 等人提出了一种小波域统计量直方图平移和聚类的鲁棒可逆信息隐藏算法, 该算法首先对图像进行整数小波变换, 然后对中频子带 HL 子带进行分块并计算统计量, 秘密信息通过平移统计量直方图嵌入, 同时为了提高提取秘密信息的准确性, 算法采用 k-means 聚类方法来提取秘密信息。文献[27]中, Xiang 等人提出了一种基于同态加密系统的图像鲁棒可逆水印算法, 实现了在加密域中嵌入鲁棒可逆水印。

除此之外, Coltuc 等人^[28]设计出了一种基于两阶段嵌入的鲁棒可逆水印算法框架。在该框架中, 水印的嵌入过程分为两个阶段, 在第一阶段中, 将鲁棒水印 W 嵌入到原始图像 X 中以生成带鲁棒水印的图像 Y , 然后在第二阶段中, 通过使用可逆水印算法, 将 Y 与 X 的差值 M 嵌入到图像 Y 中以得到图像 Z 。如果图像 Z 是完好无损的, 则接收方可以在将差值 M 提取出来的同时无损地恢复图像 Y , 然后鲁棒水印 W 可以从图像 Y 中准确地提取出来, 并且根据 M 和 Y , 接收方可以无失真地恢复出原始载体图像 X ; 如果图像 Z 遭到一定程度的攻击, 则接收者可以正确地将鲁棒水印 W 提取出来。在利用该框架进行水印的嵌入时所选用的鲁棒水印算法和可逆水印算法可以不局限于特定的算法, 具有一定的先进性和开创性。

Wang 等人^[29]根据文献[28]中所提出的算法框架, 提出了一种独立嵌入域基于两阶段嵌入的鲁棒可逆水印算法, 算法的流程图如图 1 所示。该算法首先通过 Haar 小波变换将载体图像 X 分为两个独立的嵌入域 X^l 和 X^h , 其中 X^l 是图像 X 的低频

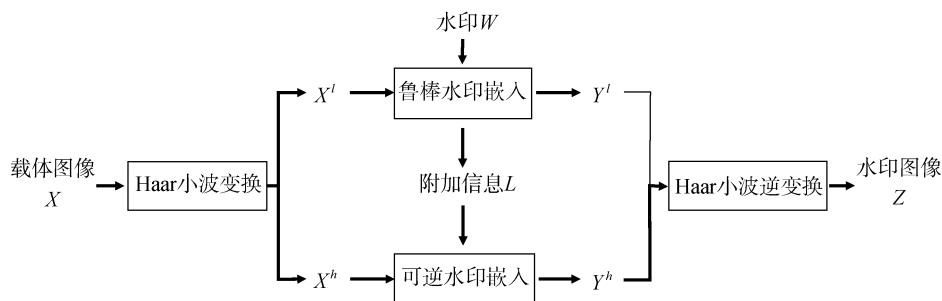


图1 独立嵌入域基于两阶段嵌入的鲁棒可逆水印算法的流程图

Figure 1 Sketch of independent embedding domain based two-stage robust reversible watermarking

子带, X^h 是图像 X 的高频子带。水印的嵌入过程分为两个阶段, 在第一阶段中, 通过使用鲁棒水印算法, 将水印 W 嵌入到 X^l 中以生成带鲁棒水印的低频子带 Y^l ; 在第二阶段中, 通过使用可逆水印算法, 将第一阶段产生的附加信息 L 嵌入到 X^h 中生成带可逆水印的高频子带 Y^h , 其中附加信息 L 由阈值 ζ 、原始差值的集合 D 以及溢出像素的位置图 ℓ 组成。最后, 对 Y^l 和 Y^h 进行 Haar 小波逆变换以生成带鲁棒可逆水印的图像 Z 。在接收方, 通过对图像 Z 进行 Haar 小波变换可以得到 Y^l 和 Y^h 。如果图像 Z 是完好无损的, 接收方可以从 Y^h 中提取出附加信息 L 并还原出原始高频子带 X^h , 以及从 Y^l 中提取出水印 W , 并且根据附加信息 L , 接收方可以将 Y^l 还原为原始低频子带 X^l , 然后对 X^l 和 X^h 进行 Haar 小波逆变换可以无失真地恢复出原始载体图像 X 。如果图像 Z 存在一定程度的失真, 接收方可以从 Y^l 中提取出水印 W 。该算法通过将水印嵌入到两个独立的嵌入域中, 有效地提高了水印图像的质量和鲁棒性, 但由于在第一阶段中, 水印 W 的嵌入会产生大量的附加信息 L , 导致在第二阶段中, 附加信息 L 的嵌入会产生较大的嵌入失真, 对图像质量造成较大的影响。

本文借鉴文献[29]所提出的算法, 提出了一种小波域基于差分统计量直方图平移的图像鲁棒可逆信息隐藏算法。该算法首先对载体图像进行 Haar 小波变换, 其次将变换后所得到的低频子带进行 $m \times n$ 分块并计算出分块的差分统计量以构造差分统计量的直方图, 然后通过可逆的整数变换实现直方图平移, 从而将秘密信息嵌入到图像的低频子带中, 最后通过 Haar 小波逆变换得到带秘密信息的图像。在接收方, 通过对图像的低频子带进行相同分块操作并计算分块的差分统计量, 秘密信

息可以被正确地提取出来, 同时根据提取出的秘密信息, 接收方可以无失真地恢复出原始载体图像。此外, 如果带秘密信息的图像遭到一定程度的图像处理操作攻击(例如 JPEG/JPEG2000 或高斯噪声等), 接收方根据差分统计量, 仍然可以有效地提取出秘密信息以用于版权保护和完整性认证。实验结果表明, 在不出现溢出的情况下, 本文算法在秘密信息的嵌入过程中不产生任何附加信息, 载体图像在嵌入秘密信息后不需要再嵌入附加信息, 使得带秘密信息的图像具有良好的不可感知性, 同时本文算法具有良好的鲁棒性, 当图像的 PSNR 值为 34dB 时, 算法对压缩因子为 30 的 JPEG 压缩、存活率为 1bbp 的 JPEG2000 压缩、标准差为 30 的高斯噪声以及标准差为 50 的椒盐噪声是鲁棒的。

本文接下来的安排如下, 第二部分是本文所提出的鲁棒可逆信息隐藏算法进行详细介绍, 第三部分是实验仿真, 并对实验结果进行分析和比较, 最后是对全文进行总结, 并对将来的工作进行展望。

2 小波域基于差分统计量直方图平移的图像鲁棒可逆信息隐藏算法

本文提出了一种小波域鲁棒可逆信息隐藏算法, 算法中图像所有者嵌入秘密信息的流程图如图 2 所示, 接收方提取秘密信息的流程图如图 3 所示。在秘密信息的嵌入过程中, 首先, 图像所有者需要对载体图像进行 Haar 小波变换。其次将变换后所得到的低频子带分成若干个互不重叠的分块, 每个分块的尺寸为 $m \times n$ 。然后计算每个分块的差分统计量以构建差分统计量的直方图, 接着根据嵌入密钥 T 进行统计量直方图的平移以实现将秘密信息嵌入到载体图像的低频子带中。在不出现溢出的情况下, 秘密信息的嵌入不产生附加信息。最后, 通过 Haar 小波

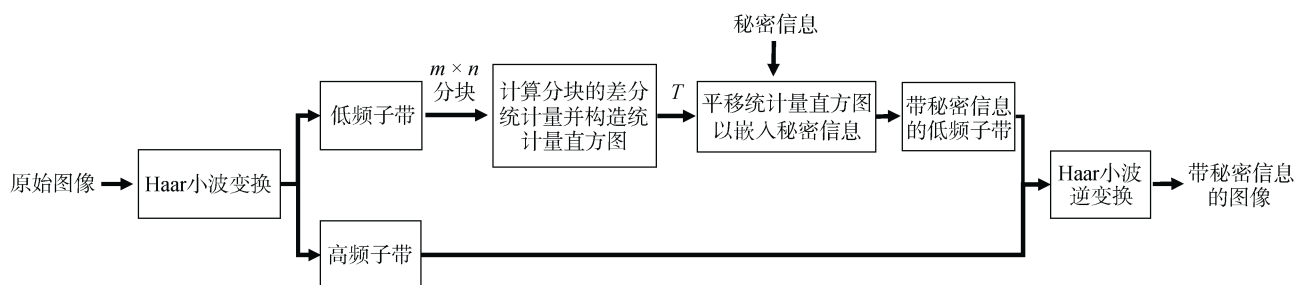


图 2 嵌入额外信息的流程图

Figure 2 Sketch of the additional data embedding

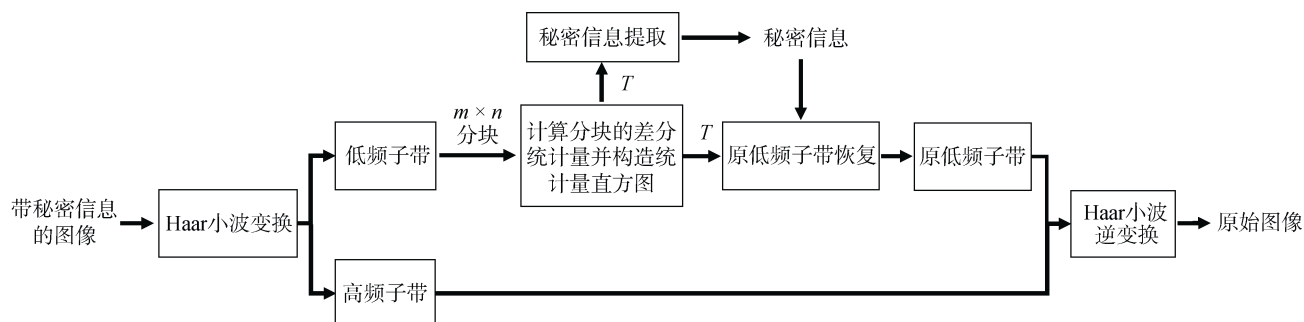


图 3 提取额外信息的流程图

Figure 3 Sketch of the additional data extraction

逆变换得到含秘密信息的载体图像。在秘密信息的提取过程中, 首先, 接收方同样需要对含秘密信息的载体图像进行 Haar 小波变换, 并对低频子带进行相应地分块操作, 然后通过计算每个分块的差分统计量, 秘密信息可以被准确地提取出来, 同时, 根据所提取出的秘密信息以及嵌入密钥 T , 通过对统计量的直方图进行与嵌入过程相反的平移操作可以将原始低频子带无失真地恢复出来, 最后, 通过 Haar 小波逆变换可以无损地恢复出原始载体图像。此外, 当含秘密信息的载体图像遭到一定程度的攻击时, 秘密信息仍可以有效地提取出来。

2.1 信息嵌入

2.1.1 Haar 小波变换

Tian^[6]提出了一种 Haar 小波变换的实现方式, 它可以将原始图像 I 分成 1 个低频子带 I^L 和 1 个高频子带 I^H , 两个子带的尺寸大小相等并为原始图像 I 的一半, 例如, 对大小为 512×512 的 Lena 图像进行 Haar 小波变换将得到大小为 512×256 或 256×512 的低频子带 I^L 和高频子带 I^H , 变换过程如图 4 所示。具体变换过程如下所述, 记 (x_1, x_2) 是由原始图像 I 中的两个相邻的像素 x_1 和 x_2 组成的

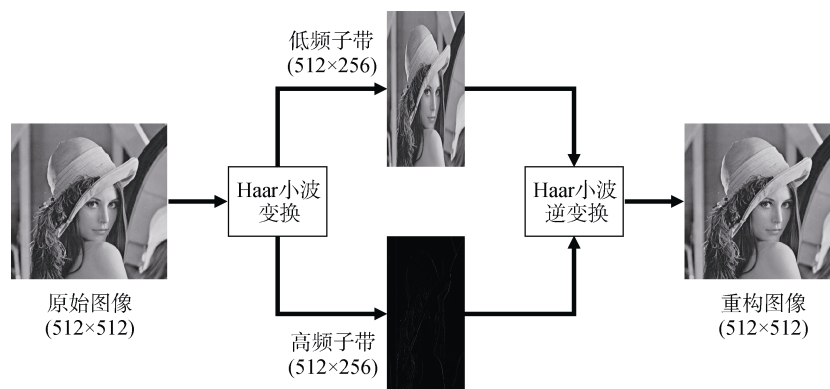


图 4 Haar 小波变换

Figure 4 Haar wavelet transform

像素对, 对像素对 (x_1, x_2) 进行 Haar 小波变换:

$$\begin{cases} x^l = \left\lfloor \frac{x_1 + x_2}{2} \right\rfloor, \\ x^h = x_1 - x_2, \end{cases} \quad (1)$$

其中, x^l 是低频子带 I^L 中的小波系数, x^h 是高频子带 I^H 中的小波系数。该变换是可逆的, 通过对低频子带 I^L 和 高频子带 I^H 进行 Haar 小波逆变换可重构出原始图像 I , 逆变换过程如图 4 所示, 具体逆变换过程如下所述, 对 I^L 和 I^H 中的小波系数 x^l 和 x^h 进行 Haar 小波逆变换:

$$\begin{cases} x_1 = x^l + \left\lfloor \frac{x^h + 1}{2} \right\rfloor, \\ x_2 = x^l - \left\lfloor \frac{x^h}{2} \right\rfloor, \end{cases} \quad (2)$$

可还原出原始像素对 (x_1, x_2) , 从而重构出原始图像 I 。

在本文所提算法中, 图像拥有者首先利用 Haar 小波变换将载体图像 I 分成低频子带 I^L 和高频子带 I^H , 由于低频信号对于多种图像处理操作 (例如 JPEG/JPEG 2000 压缩和高斯噪声) 具有更强的鲁棒性, 因此图像拥有者将把秘密信息嵌入到低频子带 I^L 中。

2.1.2 计算差分统计量

Zeng^[25]提出了一种计算图像分块的差分统计量的方法。该方法首先将图像分为若干个互不重叠的图像分块, 每个图像分块的大小为 $m \times n$ 。其次, 对于一个图像分块 I_1 , 定义一个与之对应的大小 $m \times n$ 为的矩阵 Z :

$$Z(i, j) = \begin{cases} 1, & \text{mod}(i, 2) = \text{mod}(j, 2), \\ -1, & \text{mod}(i, 2) \neq \text{mod}(j, 2), \end{cases} \quad (3)$$

其中 $i \in [1, m]$, $j \in [1, n]$, $\text{mod}(x, 2)$ 是对 x 进行模 2 运算。例如, 大小为 2×2 的矩阵 Z 如图 5 所示。

1	-1
-1	1

图 5 2×2 矩阵 Z 示意图
Figure 5 Block Z sized 2×2

然后, 计算图像分块的差分统计量 α :

$$\alpha = \sum_{i=1}^m \sum_{j=1}^n (I_1(i, j) \times Z(i, j)) \quad (4)$$

其中, $I_1(i, j)$ 为图像分块 I_1 中的像素值。

在本文所提算法中, 由于需要将秘密信息嵌入到图像的低频子带 I^L 中, 故图像拥有者在获得低频子带 I^L 后, 首先将低频子带 I^L 划分成若干个互不重叠的分块, 分块的大小为 $m \times n$, 然后利用上述方法计算出每个分块的差分统计量。记 $I_{(k)}^L$ 为低频子带 I^L 中第 k 个分块, $\alpha(k)$ 为分块 $I_{(k)}^L$ 的差分统计量, 则 $\alpha(k)$ 为:

$$\alpha(k) = \sum_{i=1}^m \sum_{j=1}^n (I_{(k)}^L(i, j) \times Z(i, j)) \quad (5)$$

其中, $I_{(k)}^L(i, j)$ 为分块 $I_{(k)}^L$ 中的小波系数。

通过计算出低频子带 I^L 内所有分块的差分统计量 α , 图像拥有者可以构造出低频子带的差分统计量 α 的直方图, 例如, 对大小为 512×512 的 Lena 图像的低频子带 (大小为 512×256) 进行 8×16 分块后得到的差分统计量 α 的直方图分布如下图 6 所示。图像拥有者将通过平移差分统计量 α 的直方图将秘密信息嵌入到载体图像的低频子带中。

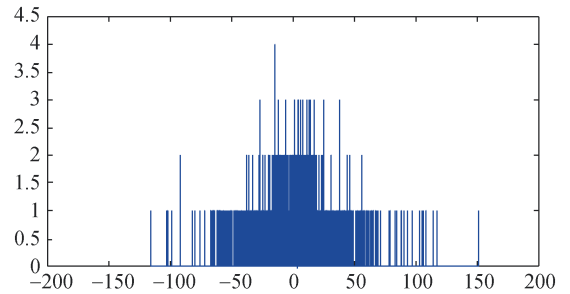


图 6 Lena 图像的低频子带的差分统计量直方图
Figure 6 Histogram of difference statistics of low frequency sub-band of image Lena

2.1.3 平移差分统计量直方图

图像拥有者首先需要选取一个正整数 T 作为嵌入密钥, 在所提出的算法中, 图像拥有者将通过嵌入密钥 T 来控制算法的鲁棒性。为了实现可逆性, T 的选取需要满足:

$$T \geq \frac{\alpha_{\max}}{m \times n} \quad (6)$$

其中, α_{\max} 是差分统计量 α 的绝对值的最大值。

在本文所提出的算法中, 秘密信息将通过平移差分统计量 α 的直方图的方式嵌入到载体图像 I 的低频子带 I^L 中。在低频子带 I^L 中, 每个分块的容量为 1 比特。对于低频子带 I^L 中的第 k 个分块

$I_{(k)}^L$, 图像拥有者将通过分块内的小波系数 $I_{(k)}^L(i, j)$ 进行整数变换以平移分块的差分统计量

$\alpha(k)$, 从而将 1 比特的秘密信息 $w(k) \in \{0, 1\}$ 嵌入到分块 $I_{(k)}^L$ 中:

$$I_{w(k)}^L(i, j) = \begin{cases} I_{(k)}^L(i, j) + (2 \times w(k) - 1)(T - \lfloor \frac{\alpha(k)}{m \times n} \rfloor), & \text{if } \alpha(k) \geq 0 \text{ and } \text{mod}(i, 2) = \text{mod}(j, 2), \\ I_{(k)}^L(i, j) - (2 \times w(k) - 1)(T + \lfloor \frac{\alpha(k)}{m \times n} \rfloor), & \text{if } \alpha(k) \geq 0 \text{ and } \text{mod}(i, 2) \neq \text{mod}(j, 2), \\ I_{(k)}^L(i, j) + (2 \times w(k) - 1)(T - \lfloor \frac{\alpha(k)}{m \times n} \rfloor), & \text{if } \alpha(k) < 0 \text{ and } \text{mod}(i, 2) = \text{mod}(j, 2), \\ I_{(k)}^L(i, j) - (2 \times w(k) - 1)(T + \lfloor \frac{\alpha(k)}{m \times n} \rfloor), & \text{if } \alpha(k) < 0 \text{ and } \text{mod}(i, 2) \neq \text{mod}(j, 2), \end{cases} \quad (7)$$

其中, $i \in [1, m]$, $j \in [1, n]$, $I_{w(k)}^L$ 为嵌入秘密信息后的分块, $I_{w(k)}^L(i, j)$ 为分块 $I_{w(k)}^L$ 中的小波系数, $\lfloor \cdot \rfloor$ 为向下

取整函数, $\lceil \cdot \rceil$ 为向上取整函数, 该整数变换是可逆的, 通过逆变换可以恢复出原始的小波系数 $I_{(k)}^L(i, j)$:

$$I_{(k)}^L(i, j) = \begin{cases} I_{w(k)}^L(i, j) - (2 \times w(k) - 1)(T - \lfloor \frac{\alpha(k)}{m \times n} \rfloor), & \text{if } \alpha(k) \geq 0 \text{ and } \text{mod}(i, 2) = \text{mod}(j, 2), \\ I_{w(k)}^L(i, j) + (2 \times w(k) - 1)(T + \lfloor \frac{\alpha(k)}{m \times n} \rfloor), & \text{if } \alpha(k) \geq 0 \text{ and } \text{mod}(i, 2) \neq \text{mod}(j, 2), \\ I_{w(k)}^L(i, j) - (2 \times w(k) - 1)(T - \lfloor \frac{\alpha(k)}{m \times n} \rfloor), & \text{if } \alpha(k) < 0 \text{ and } \text{mod}(i, 2) = \text{mod}(j, 2), \\ I_{w(k)}^L(i, j) + (2 \times w(k) - 1)(T + \lfloor \frac{\alpha(k)}{m \times n} \rfloor), & \text{if } \alpha(k) < 0 \text{ and } \text{mod}(i, 2) \neq \text{mod}(j, 2). \end{cases} \quad (8)$$

由于该整数变换是可逆的且逆变换的实现不需要附加信息, 因此在不出现溢出的情况下, 秘密信息的嵌入不会产生附加信息。

记 $\alpha_w(k)$ 为嵌入秘密信息 w 后的分块 $I_{w(k)}^L$ 的差分统计量, 通过公式(5)可计算出 $\alpha_w(k)$:

$$\begin{aligned} \alpha_w(k) &= \sum_{i=1}^m \sum_{j=1}^n (I_{w(k)}^L(i, j) \times M(i, j)) \\ &= \alpha(k) + (2 \times w(k) - 1) \times mnT \\ &= \begin{cases} \alpha(k) + mnT, & \text{if } w(k) = 1, \\ \alpha(k) - mnT, & \text{if } w(k) = 0. \end{cases} \end{aligned} \quad (9)$$

根据公式(9)可以知道, 在嵌入秘密信息 $w(k)=1$ 后, 原分块的差分统计量 $\alpha(k)$ 将向右平移 mnT 个单位, 在嵌入秘密信息 $w(k)=0$ 后, 原分块的差分统计量 $\alpha(k)$ 将向左平移 mnT 个单位。同时, 根据公式(6), 可以推出:

$$\alpha_w(k) = \begin{cases} \alpha(k) + mnT \geq 0, & \text{if } w(k) = 1, \\ \alpha(k) - mnT < 0, & \text{if } w(k) = 0. \end{cases} \quad (10)$$

根据公式(10)可以知道, 在嵌入秘密信息 $w(k)=1$ 后, $\alpha_w(k)$ 将在范围 $[0, 2mnT]$ 内, 我们将

范围 $[0, 2mnT]$ 称为比特 1 区; 在嵌入秘密信息 $w(k)=0$ 后, $\alpha_w(k)$ 将在范围 $(0, -2mnT]$ 内, 我们将范围 $(0, -2mnT]$ 称为比特 0 区。例如, 图 5 中 Lena 图像的低频子带在进行 8×16 分块后得到的 $\alpha_{\max} = 151$, 选取嵌入密钥 $T = 2$, 在嵌入 1024 比特的秘密信息后的差分统计量 α_w 的直方图如图 7 所示。

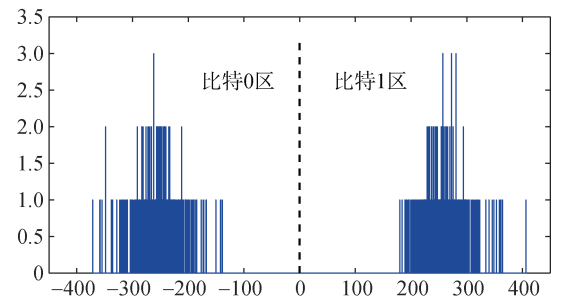


图 7 带秘密信息的低频子带的差分统计量直方图
Figure 7 Histogram of difference statistics of low frequency sub-band with additional information

最后, 图像拥有者将所有分块重新整合生成带秘密信息的低频子带 I_w^L , 并对低频子带 I_w^L 和高

频子带 I^H 进行 Haar 小波逆变换以生成带秘密信息的图像 I_w 。

2.2 信息提取

2.2.1 提取秘密信息和回复原始图像

与秘密信息的嵌入过程相同, 首先, 接收方需要对带秘密信息的图像 I_w 进行 Haar 小波变换以得到带秘密信息的低频子带 I_w^L 和高频子带 I^H , 然后对低频子带 I_w^L 进行 $m \times n$ 分块, 并通过公式(5)计算出分块的差分统计量 α_w 。对于分块 $I_{w(k)}^L$, 根据该分块的差分统计量 $\alpha_w(k)$, 接收方可以从 $I_{w(k)}^L$ 中提取出秘密信息 $w(k)$:

$$w(k) = \begin{cases} 1, & \text{if } \alpha_w(k) \geq 0, \\ 0, & \text{if } \alpha_w(k) < 0. \end{cases} \quad (11)$$

随后, 接收方可以根据嵌入密钥 T 、差分统计量 α_w 以及提取出的秘密信息 w , 将原始的低频子带 I^L 不失真地恢复出来, 具体方法如下:

首先, 接收方需要根据嵌入密钥 T 、差分统计量 α_w 以及提取出的秘密信息 w 计算出原始低频子带 I^L 的差分统计量 α 。对于分块 $I_{w(k)}^L$, 根据公式(9), 可以计算出嵌入秘密信息前的差分统计量 $\alpha(k)$:

$$\begin{aligned} \alpha(k) &= \alpha_w(k) - mnT \times (2 \times w(k) - 1) \\ &= \begin{cases} \alpha_w(k) - mnT, & \text{if } w(k) = 1, \\ \alpha_w(k) + mnT, & \text{if } w(k) = 0. \end{cases} \end{aligned} \quad (12)$$

然后, 根据提取出的秘密信息 w 以及差分统计量 $\alpha(k)$, 接收方可以通过公式(8)对分块 $I_{w(k)}^L$ 内的小波系数 $I_{w(k)}^L(i, j)$ 进行处理以得到 $I_{(k)}^L(i, j)$, 从而恢复出原始的分块 $I_{(k)}^L$ 。

最后, 接收方将所有分块重新整合, 恢复出原始的低频子带 I^L , 并对低频子带 I^L 和高频子带 I^H 进行 Haar 小波逆变换以恢复出原始载体图像 I 。

2.2.2 在受攻击的图像中提取秘密信息

带秘密信息的图像在互联网上进行传送时, 可能会遭到一些的图像处理操作以及噪声的干扰和攻击, 因此嵌入的秘密信息需要具有一定的鲁棒性。由于图像在遭到攻击后, 原始图像是无法复原的, 此时接收方只需提取出秘密信息即可。通过选用载体图像的低频子带的差分统计量的直方图作为鲁棒特征, 将秘密信息嵌入到差分统计量的

直方图中, 可以使得秘密信息对常见的图像处理操作(JPEG/JPEG2000 压缩和加性高斯噪声等)具有一定的鲁棒性。从图 7 中可以看出, 在比特 1 区与比特 0 区之间存在着一个鲁棒区域, 因此, 在带秘密信息的图像 I_w 遭到一定程度的图像处理操作的攻击后, 如果图像的低频子带 I_w^L 的差分统计量 α_w 没有因为攻击所造成的变动而落入到错误的比特区内, 接收方仍然可以根据差分统计量 α_w 以及公式(11)将秘密信息 w 正确地提取出来。例如, 带秘密信息的 Lena 图像在经过 JPEG2000 压缩后的图像低频子带的差分统计量的直方图如图 8 所示。

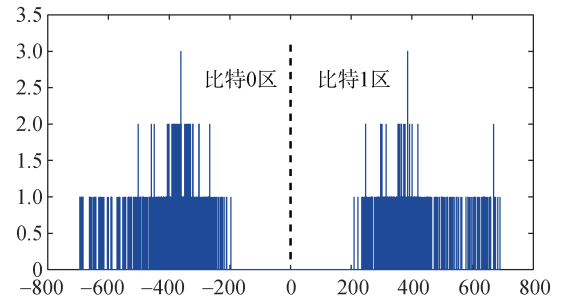


图 8 JPEG2000 压缩后带秘密信息的低频子带的差分统计量直方图

Figure 8 Histogram of difference statistics of low frequency sub-band with additional information after JPEG2000 compression

2.3 溢出处理

对于一幅 8 比特的灰度图像 I , 像素 $I(i, j)$ 的值在范围 $[0, 255]$ 内, 其中 $i \in [1, M]$, $j \in [1, N]$, M 和 N 是图像的尺寸。在嵌入秘密信息后, 像素 $I_w(i, j)$ 的值可能会大于 255 或小于 0, 这意味着会出现溢出问题。为了解决溢出问题, 本文通过使用位置图和像素调整的方法来进行溢出处理。

首先, 图像拥有者需要对得到的带秘密信息的图像 I_w 进行扫描, 生成一个与图像像素一一对应的大小为 $M \times N$ 的位置图 L :

$$L(i, j) = \begin{cases} 1, & \text{if } I_w(i, j) > 255 \text{ or } I_w < 0 \\ 0, & \text{else} \end{cases} \quad (13)$$

其中, $i \in [1, M]$, $j \in [1, N]$, 通过使用位置图 L 可以记录下产生溢出的像素坐标。然后, 图像拥有者需要对产生溢出的像素进行像素调整, 对于出现溢出问题的图像, 其像素值的范围是 $[0 - d_1, 255 + d_2]$, 其中, $d_1 \geq 0$ 为下溢出最大值, $d_2 \geq 0$ 为上溢出最大值, d_1 和 d_2 不能同时为 0。记 d 为溢出的最大值, 则 d 为:

$$d = \max\{d_1, d_2\} \quad (14)$$

像素调整操作为:

$$I_w(i, j)' = \begin{cases} I_w(i, j) - d, & \text{if } I_w(i, j) > 255, \\ I_w(i, j) + d, & \text{if } I_w(i, j) < 255, \end{cases} \quad (15)$$

其中, $I_w(i, j)'$ 为溢出处理后的像素。随后, 图像拥有者需要将位置图 L 和溢出的最大值 d 作为附加信息 λ , 并对 λ 进行无损压缩。最后, 用一种低失真的可逆信息隐藏方案将压缩后的附加信息嵌入到图像的高频子带 I^H 中。

在接收方, 首先从 I^H 中提取出嵌入的附加信息 λ , 然后根据位置图 L 找到经过溢出处理的像素 $I_w(i, j)'$, 并根据溢出的最大值 d , 将像素 $I_w(i, j)'$ 进行还原:

$$I_w(i, j) = \begin{cases} I_w(i, j)' + d, & \text{if } I_w(i, j)' > 125, \\ I_w(i, j)' - d, & \text{if } I_w(i, j)' < 125. \end{cases} \quad (16)$$

在将像素 $I_w(i, j)'$ 还原成 $I_w(i, j)$ 后, 接收方可以根据第 2.2 小节中描述的方法将秘密信息提取出来并恢复出原始的载体图像 I 。

对于大多数的 8 比特灰度图像, 其像素值大多都是集中在范围 $[25, 230]$ 内, 在本文提出的算法中, 嵌入失真的大小与嵌入密钥 T 的值有关, 只要选取合适的嵌入密钥 T , 可以有效地避免溢出问题的发生。当有溢出发生时, 根据本文所提出的溢出处理操作, 可以有效地解决溢出问题。

3 实验结果及分析

在实验部分, 本文将使用 50 张标准的 8 比特灰度图像^[30]作为测试图像进行实验以评估本文所提算法的性能, 并选取其中 8 幅具有代表性的图像进行效果展示, 8 幅图像如图 9 所示。

在本文所提出的算法中, 每个分块的嵌入容量是 1 比特, 对于一个尺寸大小为 $M \times N$ 的图像, 在经过 Haar 小波变换后所得到的低频子带的尺寸为 $(M \times N)/2$, 由于每个分块的大小为 $m \times n$, 则图像的最大嵌入容量为:

$$C_{\max} = \frac{(M \times N)/2}{m \times n}. \quad (17)$$

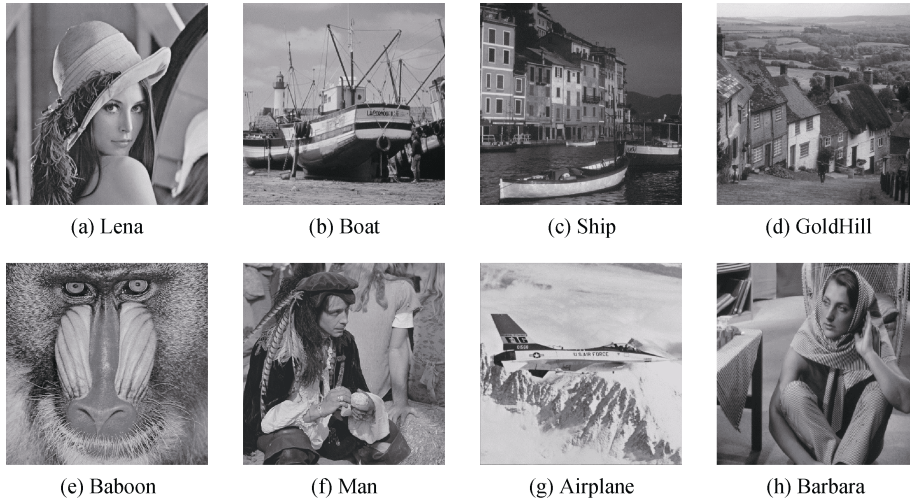


图 9 8 幅测试图像

Figure 9 Eight test images

3.1 可行性分析

首先, 本文将以 Lena 图像作为载体图像进行实验, 并将所获得的实验结果进行展示以验证本文所提算法的可行性。为了评估载体图像在嵌入秘密信息后的图像质量(即不可感知性), 本文采用峰值信噪比(Peak Signal to Noise Ratio, PSNR)来对图像质量进行评估, PSNR 的值越高, 则图像质量越好, 对嵌入的秘密信息的不可感性也越强。对于载体图像 I 和带秘密信息的图像 I_w , 两者之间的 PSNR 为:

$$PSNR = 10 \times \lg \frac{M \times N \times 255^2}{\sum_{i=1}^M \sum_{j=1}^N [I(i, j) - I_w(i, j)]^2}, \quad (18)$$

其中, M 和 N 是图像的尺寸, $I(i, j)$ 是载体图像 I 在坐标 (i, j) 处的灰度值, $I_w(i, j)$ 是带秘密信息的图像 I_w 中与 $I(i, j)$ 相对应的像素值。另外, 为了评估所提取的秘密信息的正确性以及本文所提算法的鲁棒性, 本文采用比特误差率(Bit Error Rate, BER)来进行衡量, BER 的值越低, 则提取秘密信息的正确性就高。BER 的计算公式为:

$$BER = \frac{\sum_{k=1}^L (w(k) \otimes w'(k))}{L}, \quad (19)$$

其中, L 为嵌入的秘密信息的总比特数, $w(k)$ 为嵌入的秘密信息 w 中的第 k 个比特, $w'(k)$ 为提取出的秘密信息 w' 中的第 k 个比特。

实验中, 本文选用尺寸大小为 512×512 的 Lena 图像(如图 10(a)所示)作为测试图像, 该图像为 8 比特的灰度图像, 低频子带的分块大小设置为 8×16 , 嵌入的秘密信息是一段 1024 比特的伪随机序列, 嵌入密钥 T 设置为 2, 实验结果如图 10 所示。在嵌入过程中, 首先, 对载体图像 I (如图 10(a)所示)进行 Haar 小波变换得到低频子带 I^L 和高频子带 I^H ; 其次, 选取低频子带 I^L 进行 8×16 分块并计算每个分块的差分统计量以构建差分统计量的直方图; 然后, 根据嵌入密钥 T , 通过平移直方图将秘密信息嵌入到载体图像中得到带秘密信息的低频子带 I_w^L ; 最后, 对低频子带 I_w^L 和高频子带 I^H 进行 Haar 小波逆变换得到带秘密信息的图像 I_w (如图 10(b)所示), 该图像的 PSNR 值为 42.11dB; 在提取过程中, 首先, 对带秘密信息的图像 I_w 进行 Haar 小波变换得到低频子带 I_w^L 和高频子带 I^H ; 其次, 选取低频子带 I_w^L 进行 8×16 分块并计算每个分块的差分统计量; 然后, 根据嵌入密钥 T 和差分统计量提取出秘密信息并恢复原始的低频子带 I^L ; 最后, 通过 Haar 小波逆变换恢复出载体图像 I (如图 10(c)所示), 恢复出的载体图像的 PSNR 值为 $+\infty$, 这意味着原始载体图像被无失真地恢复出来; 图 10(d)展示了所嵌入的秘密信息和所提出的秘密信息的差值, 从图 10(d)中可以看出, 两者的差值为 0, 这意味着所嵌入的秘密信息被正确地提取出来。实验结果表明, 本文所提算法实现了可逆性, 在带秘密信息的图像是完好无损的情况下, 可以正确地提取出秘密信息并无损地恢复出原始的载体图像。

3.2 不可感知性测试

为了测试本文所提出的算法在不可感知性方面的性能, 在实验中, 本文选用了 50 幅标准的 8 比特灰度图像^[30](其中的 8 幅图像如图 9 中所示)作为测试图像, 每幅图像的大小均为 512×512 , 低频子带的分块大小设置为 8×16 , 嵌入的秘密信息是一段 1024 比特的伪随机序列。

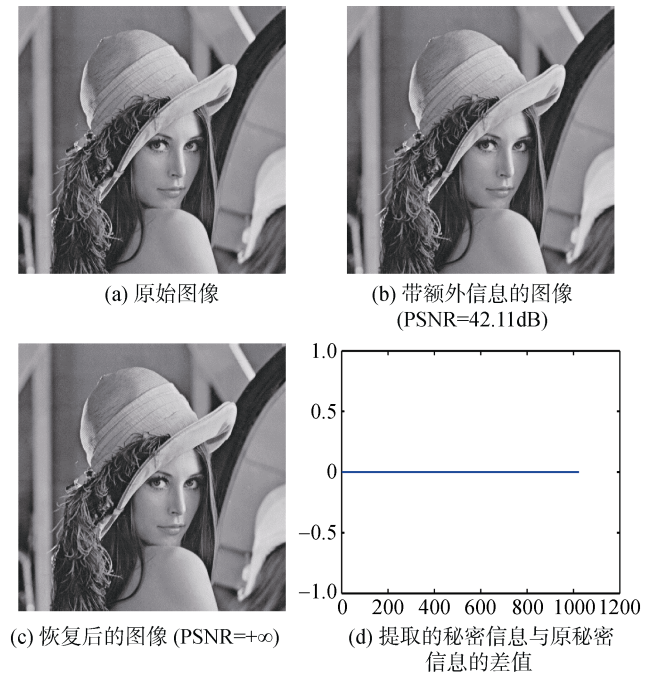


图 10 以 Lena 图像为载体时的秘密信息嵌入和提取测试

Figure 10 Additional data embedding and extraction testing results with image Lena

不可感知性主要受嵌入秘密信息时产生的嵌入失真所影响, 嵌入失真越大, 则不可感知性越差。根据公式(7)可知, 嵌入失真主要与嵌入密钥 T 的值有关, 因此, 本小节将主要研究嵌入密钥 T 对不可感知性的影响。本文测试了 50 幅图像在不同嵌入密钥 T 下的 PSNR 值, 50 幅图像的 PSNR 值的平均值与嵌入密钥 T 的关系如图 11 所示。实验发现, 50 幅图像以相同的嵌入密钥 T 进行秘密信息的嵌入时, 带秘密信息的图像的 PSNR 值基本相同, 并且从图 11 中可以看出, PSNR 值随着嵌入密钥 T 的增加而减小, 这意味着不可感知性随着嵌入密钥 T 的增加而下降, 原因是随着嵌入密钥 T 的增加, 嵌入失真越大, 导致不可感知性下降。

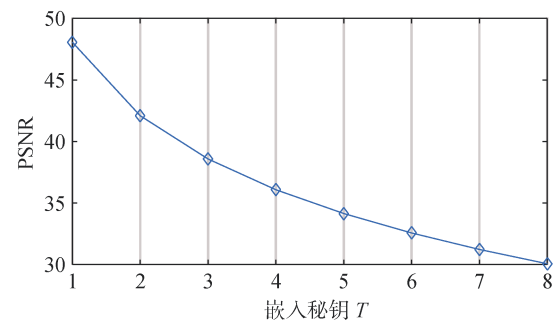


图 11 嵌入密钥 T 和 PSNR 值的关系

Figure 11 Relationship between the hiding key T and PSNR value

3.3 鲁棒性测试

在本文所提出的算法中, 图像拥有者主要通过嵌入密钥 T 来控制算法的鲁棒性。在 JPEG 压缩实验中, 本文采用了 ACDsee 14.0 软件对带秘密信息的图像进行 JPEG 压缩处理, 选用了 8 幅大小为 512×512 的图像(如图 9 所示)作为测试图像, 低频子带分块大小设置为 8×16 , 嵌入的秘密信息是一段 1024 比特的伪随机序列。图 12 展示的是以 Lena 图像作为载体图像时, 在不同的嵌入密钥 T 下, 图像在不同的压缩质量因子的处理下提取秘密信息的比特误差率 BER, 从图 12 可以看出, 在嵌入密钥 T 固定时, 随着压缩质量因子数值的降低(即表示压缩程度逐渐增加), BER 会逐渐上升; 在相同的压缩质量因子下, BER 随着 T 的增加而降低, 这意味着随着嵌入密钥 T 的增加, 算法对 JPEG 的鲁棒性将会增强。图 13 展示了 8 幅图像在不同的嵌入密钥 T 下可以正确提取秘密信息(即 BER=0)的最小 JPEG 压缩质量因子, 对于一幅图像, 压缩质量因子越小说明抗 JPEG 的鲁棒性越强, 从图 13 可以看出, 随着 T 的增加, 8 幅图像的最小 JPEG 压缩质量因子逐渐减小, 在 $T=8$ 时, 8 幅图像的最小 JPEG 压缩质量因子均为 0。图 14 展示了在压缩质量因子分别为 60, 40, 20 时, 8 幅图像在不同的嵌入密钥 T 下提取秘密信息的比特误差率 BER, 从图 14 可以看出, 在相同的压缩质量因子下, 随着 T 的增加, 8 幅图像的 BER 逐渐减小为 0。然而, 根据小节 3.2 可知, 随着嵌入密钥 T 的增加, 嵌入失真将会增加, 从而导致 PSNR 值的下降, 因此, 需要选取合适的 T 值使得图像在图像质量和鲁棒性之间有着更好的平衡性。

在 JPEG2000 压缩实验中, 本文同样采用了 ACDsee 14.0 软件对带秘密信息的图像进行

JPEG2000 压缩处理, 选用了 8 幅大小为 512×512 的图像(如图 9 所示)作为测试图像, 低频子带分块大小设置为 8×16 , 嵌入的秘密信息是一段 1024 比特的伪随机序列。为了评估所提出的算法对 JPEG2000 压缩的鲁棒性, 本文采用了存活率(surviving bit rate)来进行衡量:

$$\text{存活率} = \frac{8}{\text{压缩率}}, \quad (20)$$

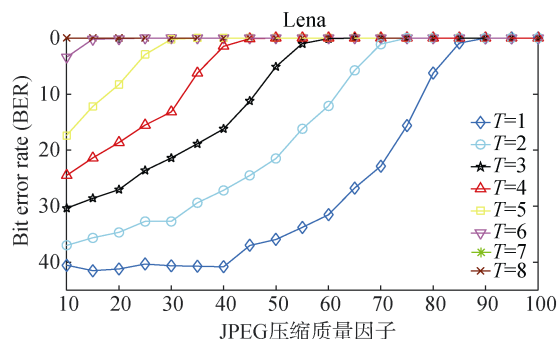


图 12 嵌入密钥 T 对秘密信息抗 JPEG 压缩的影响
Figure 12 Effect of the hiding key T on the robustness to JPEG Compression

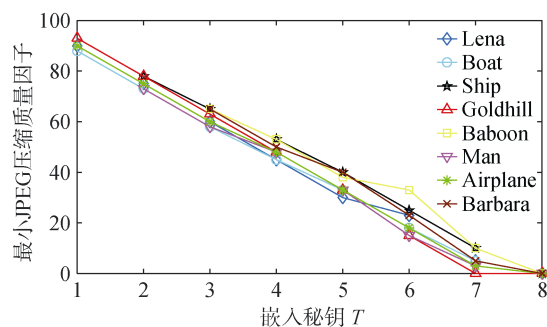


图 13 嵌入密钥 T 与最小 JPEG 压缩质量因子的关系
Figure 13 The relationship between the minimum JPEG compression quality factor and the hiding key T

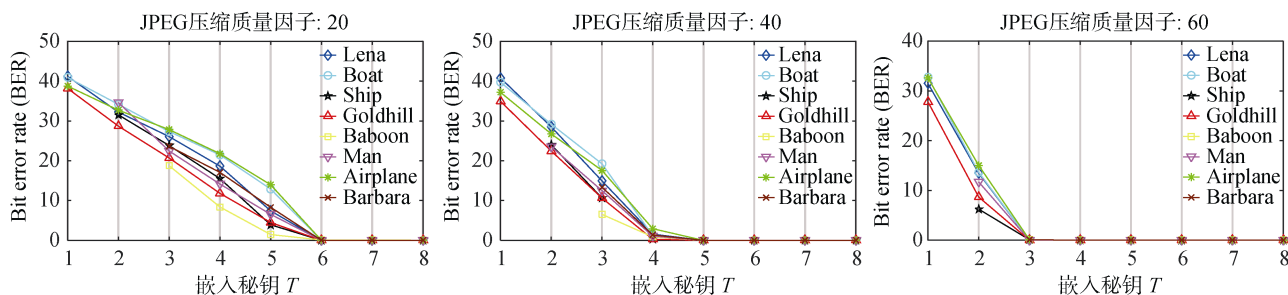


图 14 在不同压缩质量因子下嵌入密钥 T 与比特误差率 BER 的关系
Figure 14 The Relationship between the hiding key T and BER at different compression quality factors

JPEG2000 的压缩率越大, 存活率越小, 则鲁棒性越强。图 15 展示了 8 幅图像在不同的嵌入密钥 T 下可以正确提取秘密信息(即 BER=0)的最小存

活率, 即对于同一图像, 在相同的嵌入密钥 T 下, 若存活率高于最小存活率, 即压缩率小于最小存活率所对应的压缩率时, 均可以正确地提取出秘

密信息(即 BER=0)。从图 15 可以看出, 随着嵌入密钥 T 的增加, 8 幅图像的最小存活率逐渐减小, 这意味着随着嵌入密钥 T 的增加, 算法对 JPEG2000 的鲁棒性将会增强。

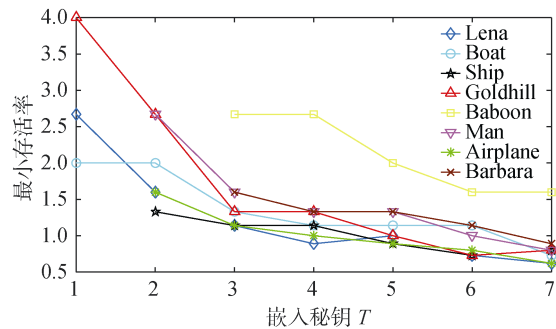


图 15 嵌入密钥 T 对秘密信息抗 JPEG2000 压缩的影响
Figure 15 Effect of the hiding key T on the robustness to JPEG2000 Compression

为了研究低频子块的分块尺寸对鲁棒性的影响, 本文选用了 3 幅大小为 512×512 的图像(Lena 图像、Baboon 图像、Airplane 图像)作为测试图像, 以不同的分块尺寸进行秘密信息的嵌入。表 1 展示了在不同分块大小下, 算法在 3 幅测试图像上的性能。从表 1 可以看出, 对于同一幅图像, 在 PSNR 值基本相同的情况下, 随着分块尺寸增大, 即分块内小波系数的数量增加, 算法可以抵抗的最小 JPEG 压缩质量因

子和最小存活率逐渐减少, 并且, 当分块内小波系数的数量相同时, 算法的性能基本相同, 这意味着鲁棒性随着分块尺寸的增大而增强, 且在分块内小波系数的数量相同时, 分块的形状对算法的鲁棒性影响不大。然而, 随着分块尺寸增大, 嵌入容量将会减少, 实验结果表明, 当分块尺寸为 8×16 或 8×32 时, 算法在图像质量、嵌入容量和鲁棒性之间有着较好的平衡性。

为了测试本文所提出的算法针对其它图像处理操作的鲁棒性, 本文采用了 MATLAB 软件对带秘密信息的图像叠加椒盐噪声和加性高斯噪声, 选用了 8 幅大小为 512×512 的图像(如图 9 所示)作为测试图像, 低频子带分块大小设置为 8×16 , 嵌入密钥 T 设置为 5, 嵌入的秘密信息是一段 1024 比特的伪随机序列。表 2 展示了 8 幅带秘密信息的图像在遭到不同的图像处理操作的攻击后提取秘密信息的比特误差率(BER)(%)。从表 2 可以看出, 在嵌入密钥 T 相同时, 8 幅图像的 PSNR 基本相同, 均约为 34dB; 对于压缩质量因子为 30 的 JPEG 压缩, 所有图像的 BER 均小于 0.5%; 对于存活率为 1bpp 的 JPEG2000 压缩, 除 Baboon 图像外, 其余 7 幅图像的 BER 均小于 1.5%; 对于标准差为 30 的加性高斯噪声, 所有图像的 BER 均小于 1%; 对于对标准差为 50 的椒盐噪声, 所有图像的 BER 均小于 0.5%。实验结果表明, 本文所提出的算法在图像质

表 1 不同分块尺寸下 3 幅图像的性能
Table 1 The performance of 3 images at different block sizes

测试图像	分块尺寸	嵌入容量(bit)	T	PSNR (dB)	JPEG 压缩因子	存活率 (bpp)
Lena	8×8	2048	5	34.15	43	0.89
	16×8	1024	5	34.15	30	0.89
	8×16	1024	5	34.15	35	1
	16×16	512	5	34.15	25	0.89
	32×8	512	5	34.15	28	0.89
	8×32	512	5	34.15	28	0.73
Baboon	8×8	2048	5	34.08	73	4
	16×8	1024	5	34.12	38	2.66
	8×16	1024	5	34.13	40	2
	16×16	512	5	34.15	23	1.6
	32×8	512	5	34.15	25	1.6
	8×32	512	5	34.15	23	1.6
Airplane	8×8	2048	5	34.15	40	1
	16×8	1024	5	34.15	33	0.89
	8×16	1024	5	34.15	30	0.89
	16×16	512	5	34.15	30	0.89
	32×8	512	5	34.15	28	1
	8×32	512	5	34.15	30	0.89

表 2 本文算法在几种常见图像处理操作下的鲁棒性

Table 2 Robustness of the proposed scheme against several image processing operations

测试图像	T	PSNR(dB)	JPEG 压缩(质量因子 30)	JPEG2000 压缩(存活率 1bbp)	高斯噪声 (标准差 30)	椒盐噪声(标准差 50)
Lena	5	34.14	0.2	0	0.44	0.26
Boat	5	34.14	0.09	0.88	0.35	0.37
Ship	5	34.14	0.09	0	0.4	0.38
Goldhill	5	34.14	0.09	0	0.34	0.36
Baboon	5	34.14	0.29	21.88	0.51	0.37
Man	5	34.14	0	1.07	0.42	0.33
Airplane	5	34.14	0	0	0.43	0.45
Barbara	5	34.14	0.29	1.46	0.51	0.36

量上有着较好的表现, 并且能够有效地抵抗一定程度下的 JPEG/ JPEG2000 压缩、高斯噪声和椒盐噪声的攻击, 同时, 相对于纹理复杂的图像, 算法在纹理较为平滑的图像上有着更好的性能表现。

3.4 性能对比

为了进一步说明本文算法的性能, 我们与现有的几种鲁棒可逆信息隐藏算法^[24-26,29]进行了性能比较。文献[24]和文献[25]提出了两种在时域下的鲁棒可逆信息隐藏算法, 文献[26]和文献[29]提出了两种小波域鲁棒可逆水印算法。

在针对不可感知性的对比实验中, 我们选用了 3 幅大小为 512×512 的图像(Lena 图像、Baboon 图像、

Airplane 图像)作为测试图像, 秘密信息是一段 1024 比特的伪随机序列。表 3 展示了在不同的嵌入密钥 T 下, 本文所提出的算法和文献[29]所提出的算法在 3 幅测试图像上的 PSNR 值。从表 3 可以看出, 对于同一幅测试图像, 在相同的嵌入密钥 T 下, 本文算法的 PSNR 值要高于文献[29]所提出的算法。原因是文献[29]所提出的算法在水印的嵌入过程中会产生大量的附加信息, 使得附加信息的嵌入会造成较大的嵌入失真, 导致图像的 PSNR 值下降, 而本文算法在不出现溢出的情况下, 秘密信息的嵌入不产生附加信息, 不需要进行附加信息的嵌入, 减少了嵌入失真, 从而获得更高的 PSNR 值。

表 3 在不同嵌入密钥 T 下与文献[29]的 PSNR 比较

Table 3 Performance comparison of PSNR with [29] at different hiding key T

T	文献[29]			本文算法		
	PSNR(dB)			PSNR(dB)		
	Lena	Baboon	Airplane	Lena	Baboon	Airplane
1	43.5	43.2	43.7	48.1	47.7	48.1
2	40.2	39.6	39.7	42.1	41.9	42.1
3	37.2	37.5	36.6	38.6	38.5	38.6
4	34.7	34.9	34.9	36.1	36.1	36.1
10	27.6	27.4	27.6	28.1	28.1	28.1

在针对 JPEG 压缩的对比实验中, 我们选用了 3 幅大小为 512×512 的图像(Lena 图像、Baboon 图像、Airplane 图像)作为测试图像, 秘密信息是一段 1024 比特的伪随机序列。在秘密信息的嵌入过程中, 对于每一种算法, 需要调节相应的分块大小使得秘密信息可以嵌入到测试图像的全部区域中, 例如, 对于文献[25], 分块大小需设置为 16×16。图 16 展示了在不同的 JPEG 压缩质量因子下, 4 种算法在 3 幅测试图像上的性能, 其中, 3 幅图像的 PSNR 值均约为 34dB。从图 16 可以看出, 在 PSNR 值基本相等的情况下, 本文算法针

对压缩因子大于 30 的 JPEG 压缩的鲁棒性要优于文献[24-26, 29]。

在针对高斯噪声和高斯低通滤波器的对比实验中, 我们选用了 8 幅大小为 512×512 的图像(如图 9 所示)作为测试图像, 秘密信息是一段 1024 比特的伪随机序列。表 4 和表 5 分别展示了高斯噪声的标准差分别为 10、20、30、40 时, 以及高斯低通滤波器的窗口尺寸分别为 3×3、5×5、7×7 时, 本文算法和文献[25]所提出的算法在 8 幅测试图像上提取秘密信息的比特误差率(BER)(%), 其中高斯低通滤波器的标准差设置为 0.7。从表 4 可以看

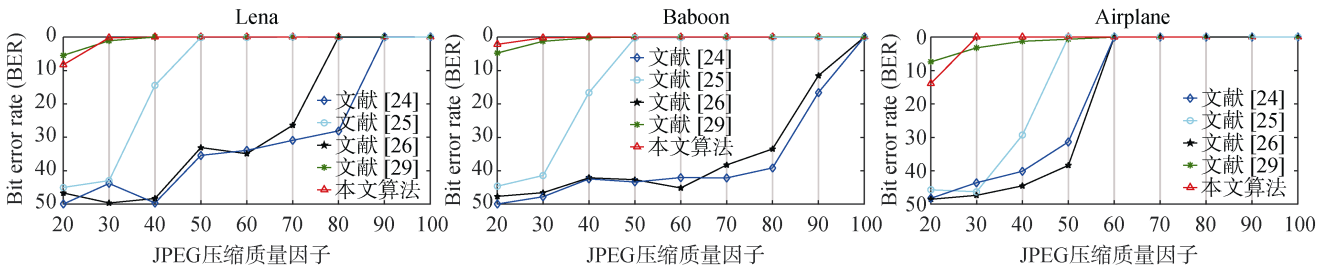


图 16 不同 JPEG 压缩因子下的鲁棒性比较

Figure 16 Performance comparison at different JPEG compression quality factors

表 4 在不同标准差的高斯噪声处理下与文献[25]的鲁棒性比较

测试图像	文献[25]					本文算法				
	PSNR (dB)	高斯噪声				PSNR (dB)	高斯噪声			
		10	20	30	40		10	20	30	40
Lena	33.65	0.07	1.79	9.35	18.29	34.14	0	0.004	0.34	2.36
Boat	33.65	0.07	1.82	9.77	19.04	34.14	0	0	0.10	2.38
Ship	33.65	0.03	1.7	8.73	17.35	34.14	0	0.008	0.45	2.39
Goldhill	33.65	0.04	2	9.41	18.4	34.14	0	0.004	0.45	2.34
Baboon	33.65	0.09	1.85	9.34	18.07	34.14	0	0.003	0.57	2.55
Man	33.65	0.23	1.66	9.51	18.21	34.14	0	0.004	0.45	2.42
Airplane	33.65	0.04	1.96	10.22	19.31	34.14	0	0	0.38	2.46
Barbara	33.65	0.06	1.73	9.20	18.45	34.14	0	0.004	0.47	2.62
平均	33.65	0.08	1.81	9.44	18.39	34.14	0	0.003	0.40	2.44

表 5 在不同窗口尺寸的高斯低通滤波器处理下与文献[25]的鲁棒性比较

测试图像	文献[25]				本文算法			
	PSNR (dB)	高斯低通滤波器(标准差 0.7)			PSNR (dB)	高斯低通滤波器(标准差 0.7)		
		3×3	5×5	7×7		3×3	5×5	7×7
Lena	33.65	4.49	3.03	3.13	34.14	0.1	0	0
Boat	33.65	3.13	1.95	2.05	34.14	0	0	0
Ship	33.65	3.13	1.76	1.76	34.14	0.1	0.1	0.1
Goldhill	33.65	1.95	0.29	0.29	34.14	0	0	0
Baboon	33.65	4.39	3.32	3.32	34.14	0.39	0	0
Man	33.65	3.71	2.54	2.34	34.14	0	0	0
Airplane	33.65	2.93	1.95	1.95	34.14	0.1	0	0
Barbara	33.65	2.73	1.07	1.07	34.14	0	0	0
平均	33.65	3.31	1.99	1.99	34.14	0.0863	0.0125	0.0125

出,对于高斯噪声攻击,文献[25]中的算法在标准差为 30 和 40 时,BER 均大于 5%,而本文所提出的算法在标准差为 40 时,BER 均低于 3%,在标准差为 30 及以下时,BER 均低于 1%,且在标准差为 10 时可以实现零错误率;从表 5 可以看出,对于高斯低通滤波器攻击,文献[25]中的算法在 8 幅测试图像上的平均 BER 高于 1.5%,而本文算法的平均 BER 低于 1%,且在大多数情况下能实现零错误率,

这说明本文算法对高斯噪声和高斯低通滤波器的鲁棒性要优于文献[25]。

4 结论

本文提出了一种小波域基于差分统计量直方图平移的鲁棒可逆信息隐藏算法。在秘密信息的嵌入过程中,本文算法对载体图像进行了 Haar 小波变换,通过将秘密信息嵌入到图像的低频子带,可

以使得秘密信息具有更强的鲁棒性,同时本文采用了差分统计量作为鲁棒特征,通过平移差分统计量的直方图实现秘密信息的嵌入,可以更好地利用像素之间的相关性以提高算法的鲁棒性。另外,本文采用了一种可逆的整数变换来实现直方图的平移,减少了秘密信息嵌入时产生的附加信息。在接收方,如果带秘密信息的图像是完好无损的,则根据嵌入密钥,接收方可以准确地将秘密信息提取出来,并无损地恢复出原始图像;当带秘密信息的图像遭到一定程度的攻击时,接收方仍然可以有效地提取出秘密信息以用于版权保护、完整性认证以及篡改定位。

实验结果表明,本文所提出的算法实现了可逆性,具有足够的嵌入容量,并且由于算法的嵌入失真较小,带秘密信息的图像有着较好的图像质量。此外,算法对常见的图像处理操作(JPEG/JPEG2000 和高斯噪声等)有一定的鲁棒性,例如,当带秘密信息的图像的 PSNR 值为 34dB 时,算法对压缩因子为 30 的 JPEG 压缩、存活率为 1bbp 的 JPEG2000 压缩、标准差为 30 的高斯噪声以及标准差为 50 的椒盐噪声是鲁棒的。值得注意的是,低频子带的分块尺寸对算法的鲁棒性有一定的影响,分块尺寸越大,鲁棒性越强,而嵌入容量越小,当分块尺寸为 8×16 或 8×32 时,算法在图像质量、嵌入容量和鲁棒性之间有着较好的平衡性。与现有的 4 种鲁棒可逆信息隐藏算法相比,本文提出的算法有更强的鲁棒性。

在今后的工作中,我们将会在现有的基础上继续对鲁棒可逆信息隐藏算法进行研究,通过选取更为合适的统计量作为鲁棒特征,以进一步提高算法的鲁棒性,同时,如何设计出抗几何攻击的鲁棒可逆信息隐藏算法也是今后的研究重点之一。

致谢 在此向本文成文中给予指导的老师、提供帮助的同学和给本文提出建议的评审专家表示感谢。本文研究得到国家自然科学基金(No. 61772234)和广东省科技创新战略专项资金(“攀登计划”专项资金)项目(No. pdjh2020a0060)的资助。

参考文献

- [1] Lu Z M, Nie T Y, Ji A G. Introduction to Information Hiding[M]. Beijing: Publishing House of Electronics industry, 2014. (陆哲明, 聂廷远, 吉爱国. 信息隐藏概论[M]. 北京: 电子工业出版社, 2014.)
- [2] C.W. Honsinger, P. Jones, M. Rabbani, et al. Lossless Recovery of an Original Image Containing Embedded Datas. US Patent application, Docket No: 77102/E-D, 1999.
- [3] Feng J B, Lin I C, Tsai C S, et al. Reversible Watermarking: Current Status and Key Issues[J]. *International Journal of Network Security*, 2006, 2(3): 161-170.
- [4] Fridrich J, Goljan M, Du R. Lossless Data Embedding—New Paradigm in Digital Watermarking[J]. *EURASIP Journal on Advances in Signal Processing*, 2002, 2002(2): 185-196.
- [5] Celik M U, Sharma G, Tekalp A M, et al. Lossless generalized-LSB Data Embedding[J]. *IEEE Transactions on Image Processing*, 2005, 14(2): 253-266.
- [6] Tian J. Reversible Data Embedding Using a Difference Expansion[J]. *IEEE Transactions on Circuits and Systems for Video Technology*, 2003, 13(8): 890-896.
- [7] Thodi D M, Rodriguez J J. Expansion Embedding Techniques for Reversible Watermarking[J]. *IEEE Transactions on Image Processing*, 2007, 16(3): 721-730.
- [8] Ni Z C, Shi Y Q, Ansari N, et al. Reversible Data Hiding[J]. *IEEE Transactions on Circuits and Systems for Video Technology*, 2006, 16(3): 354-362.
- [9] S. K. Lee, Y. H. Suh, Y. S. Ho, Reversible image authentication based on watermarking[C]. *IEEE Int. Conf. Multimedia Expo(ICME'06)*, 2006: 1321-1324.
- [10] Tai W L, Yeh C M, Chang C C. Reversible Data Hiding Based on Histogram Modification of Pixel Differences[J]. *IEEE Transactions on Circuits and Systems for Video Technology*, 2009, 19(6): 906-910.
- [11] Hu X C, Zhang W M, Li X L, et al. Minimum Rate Prediction and Optimized Histograms Modification for Reversible Data Hiding[J]. *IEEE Transactions on Information Forensics and Security*, 2015, 10(3): 653-664.
- [12] Wang W Q, Ye J Y, Wang T Q, et al. A High Capacity Reversible Data Hiding Scheme Based on Right-left Shift[J]. *Signal Processing*, 2018, 150: 102-115.
- [13] Jia Y J, Yin Z X, Zhang X P, et al. Reversible Data Hiding Based on Reducing Invalid Shifting of Pixels in Histogram Shifting[J]. *Signal Processing*, 2019, 163: 238-246.
- [14] Hong W, Chen T S, Shiu C W. Reversible Data Hiding for High Quality Images Using Modification of Prediction Errors[J]. *Journal of Systems and Software*, 2009, 82(11): 1833-1842.
- [15] Li X L, Yang B, Zeng T Y. Efficient Reversible Watermarking Based on Adaptive Prediction-Error Expansion and Pixel Selection[J]. *IEEE Transactions on Image Processing*, 2011, 20(12): 3524-3533.
- [16] Liu M L, Seah H S, Zhu C, et al. Reducing Location Map in Prediction-based Difference Expansion for Reversible Image Data Embedding[J]. *Signal Processing*, 2012, 92(3): 819-828.
- [17] Ou B, Li X L, Zhao Y, et al. Efficient Color Image Reversible Data Hiding Based on Channel-dependent Payload Partition and Adaptive Embedding[J]. *Signal Processing*, 2015, 108: 642-657.
- [18] Zheng H C, Wang C T, Wang J X, et al. A New Reversible Watermarking Scheme Using the Content-adaptive Block Size for Prediction[J]. *Signal Processing*, 2019, 164: 74-83.
- [19] de Vleeschouwer C, Delaigle J E, Macq B. Circular Interpretation of Histogram for Reversible Watermarking[C]. *2001 IEEE Fourth Workshop on Multimedia Signal Processing (Cat. No.01TH8564)*,

- Cannes, France. Piscataway, 2001: 345-350.
- [20] de Vleeschouwer C, Delaigle J F, Macq B. Circular Interpretation of Bijective Transformations in Lossless Watermarking for Media Asset Management[J]. *IEEE Transactions on Multimedia*, 2003, 5(1): 97-105.
- [21] Z.C. Ni, Y. Q. Shi, N. Ansari, et al. Robust lossless image data hiding[C]. *IEEE Int. Conf. Multimedia Expo(ICME'04)*, 2004: 2199-2202.
- [22] Ni Z C, Shi Y Q, Ansari N, et al. Robust Lossless Image Data Hiding Designed for Semi-Fragile Image Authentication[J]. *IEEE Transactions on Circuits and Systems for Video Technology*, 2008, 18(4): 497-509.
- [23] Zou D, Shi Y Q, Ni Z C, et al. A Semi-Fragile Lossless Digital Watermarking Scheme Based on Integer Wavelet Transform[J]. *IEEE Transactions on Circuits and Systems for Video Technology*, 2006, 16(10): 1294-1300.
- [24] Gao X B, An L L, Yuan Y, et al. Lossless Data Embedding Using Generalized Statistical Quantity Histogram[J]. *IEEE Transactions on Circuits and Systems for Video Technology*, 2011, 21(8): 1061-1070.
- [25] Zeng X T, Ping L D, Pan X Z. A Lossless Robust Data Hiding Scheme[J]. *Pattern Recognition*, 2010, 43(4): 1656-1667.
- [26] An L L, Gao X B, Li X L, et al. Robust Reversible Watermarking Via Clustering and Enhanced Pixel-Wise Masking[J]. *IEEE Transactions on Image Processing*, 2012, 21(8): 3598-3611.
- [27] S.J. Xiang, L. Yang, Robust and Reversible Image Watermarking Algorithm in Homomorphic Encrypted Domain[J]. *Ruan Jian Xue Bao/Journal of Software*, 2018, 29(4): 957-972.
- (项世军, 杨乐. 基于同态加密系统的图像鲁棒可逆水印算法[J]. *软件学报*, 2018, 29(4):957-972.)
- [28] D. Coltuc, J. M. Chassery, Distortion-Free Robust Watermarking: a Case Study[J]. *Security, Steganography, and Watermarking of Multimedia Contents IX*, 2007, 6505(23): 588-595.
- [29] Wang X, Li X L, Pei Q Q. Independent Embedding Domain Based Two-stage Robust Reversible Watermarking[J]. *IEEE Transactions on Circuits and Systems for Video Technology*, 2019, 3(4): 1-5.
- [30] CVG-UGR Image Database [Online]. Available: <http://decsai.ugr.es/cvg/dbimages/index.php>.



梁幸源 于2017年在南昌航空大学获得电子信息工程学士学位。现在暨南大学通信与信息系统专业攻读硕士学位。研究领域为可逆信息隐藏、鲁棒可逆信息隐藏。
Email: 496687570@qq.com



项世军 于2006年于中山大学获得计算机软件与理论专业博士学位。现任暨南大学信息科学技术学院教授。研究领域为多媒体信息安全。研究兴趣包括加密域信息隐藏、可逆水印和鲁棒可逆信息隐藏等。
Email: shijun_xiang@qq.com