

Journal of Image
and Graphics

中国图象图形学报



ISSN1006-8961
CN11-3758/TB

2012 **11**
Vol.17 No.

中国科学院遥感应用研究所
中国图象图形学学会主办
北京应用物理与计算数学研究所

中国图象图形学报

Zhongguo Tuxiang Tuxing Xuebao

2012年11月 第17卷 第11期(总第199期)

目次

综述

数字图像合成技术综述 吴昊, 徐丹(1333)

图像处理和编码

基于群稀疏的结构化字典学习 郭景峰, 李贤(1347)

SSIM 度量虚拟视点绘制失真的深度图帧内编码 喻莉, 张军涛, 邓慧萍, 向森, 周鹏, 左雯, 王宁(1353)

统计量移位的鲁棒无损图像信息隐藏 李晓博, 周诠(1359)

伪造图像典型篡改操作的检测 左菊仙, 刘本永(1367)

图像分析和识别

融合灰度和 SURF 特征的红外目标跟踪 范新南, 丁朋华, 刘俊定, 张学武(1376)

海面温度栅格图的锋面提取与矢量化 崔雪森, 周为峰, 王栋, 张胜茂(1384)

交通场景中车辆的运动检测与阴影消除 王彬, 冯远静, 郭海峰, 张贵军(1391)

基于随机点积图的图像标注改善算法 孙登第, 罗斌, 郭玉堂(1400)

图像理解和计算机视觉

有监督子空间建模和稀疏表示的场景分类 段菲, 章毓晋(1409)

对立色 LBP 模型的目标跟踪 张炯, 宁纪锋, 颜永丰, 于伟(1418)

计算机图形学

联合骨架与边界特征的平面形状分解…………… 蒋建国, 周丹凤, 郝世杰, 郭艳蓉, 詹曙(1425)

屏幕空间自适应的地形 Tessellation 绘制…………… 张兵强, 张立民, 艾祖亮, 张建廷(1431)

遥感图像处理

SAR 图像稀疏优化滤波…………… 杨萌, 张弓(1439)

分段线性动态矩匹配条带去除…………… 秦雁, 邓孺孺, 何颖清, 陈蕾, 陈启东(1444)

基于 Harris 角点和 SIFT 描述符的高分辨率遥感影像匹配算法…………… 陈梦婷, 闫冬梅, 王刚(1453)

第八届图像图形技术与应用学术会议征文通知…………… (1460)

中国图象图形学报

刊名题字: 宋 健

月刊(1996 年创刊)

第 17 卷 第 11 期

2012 年 11 月 16 日出版

主管单位 中国科学院

主 办 中国科学院遥感应用研究所
中国图象图形学学会
北京应用物理与计算数学研究所

主 编 李小文

编辑出版 《中国图象图形学报》编辑出版委员会

北京 9718 信箱 邮编 100101
电子信箱:jig@irsa.ac.cn
电话:010-64807995 010-82614429
网 址:www.cjig.cn

印刷装订 北京北林印刷厂

广告经营许可证 京朝工商广字第 0346 号

总 发 行 北京报刊发行局

订 购 全国各地邮局

国外发行 中国国际图书贸易总公司
(中国国际书店)
(北京 399 信箱 邮编 100044)

Superintended by Chinese Academy of Sciences

Sponsored by Institute of Remote Sensing Application,
CAS China Society of Image and Graphics
Institute of Applied Physics and Computational
Mathematics

Chief editor LI Xiaowen

Editor, Publisher Editorial and Publishing Board
of Journal of Image and Graphics
(P. O. Box 9718, Beijing 100101, China)
E-mail:jig@irsa.ac.cn

Distributed by Beijing Bureau for Distribution of Newspapers
and Journals

Domestic All Local Post Offices in China

Foreign China International Book Trading Corporation
(P. O. Box 399, Beijing 100044, China)

Printed by Beijing Beilin Printing House

ISSN 1006-8961 CN11-3758/TB CODE ZTTXFZ 国内邮发代号: 82-831 国外发行代号: M1406 国内定价: 45.00 元

中图分类号: TP391.9 文献标识码: A 文章编号: 1006-8961(2012)11-1359-08

论文引用格式: 李晓博,周詮. 统计量移位的鲁棒无损图像信息隐藏[J]. 中国图象图形学报,2012,17(11):1359-1366.

统计量移位的鲁棒无损图像信息隐藏

李晓博, 周詮

中国空间技术研究院西安分院空间微波技术重点实验室, 西安 710100

摘要: 鲁棒无损信息隐藏在医学成像、法律取证、遥感等领域有广泛的应用。提出了一种鲁棒无损图像信息隐藏算法。在含密载体图像未受损情况下,正确提取秘密信息后可无损恢复原始载体图像;在含密载体图像受到一定程度JPEG2000压缩攻击后,秘密信息仍然可以被正确提取。首先将原始载体图像分块并计算每个图像块的统计量,再根据统计量绝对值的最大值选择合适的阈值对统计量进行移位,最后利用移位后的统计量来嵌入秘密信息。实验结果表明,该算法在图像视觉质量、嵌入容量和鲁棒性3个方面都具有很好的性能。与其他鲁棒无损嵌入方法相比,在图像视觉质量和鲁棒性大致相当的情况下,该算法的嵌入容量有了很大提高,表明该算法较其他算法具有明显的优势。

关键词: 鲁棒无损信息隐藏;统计量;图像视觉质量;嵌入容量;鲁棒性;JPEG2000压缩

Robust lossless image data hiding with statistical quantity shifting

Li Xiaobo, Zhou Quan

Key Laboratory of Space Microwave Technology, China Academy of Space Technology, Xi'an 710100, China

Abstract: Robust lossless data hiding has extensive applications in medical imaging systems, law enforcement, and remote sensing. A robust lossless image data hiding scheme is proposed in this paper. The original cover image can be recovered without any distortion after the hidden data has been extracted if the stego-image remains intact, and conversely, the hidden data can still be extracted correctly if the stego-image goes through JPEG 2000 compression to some extent. First, the proposed scheme divides a cover image into a number of non-overlapping blocks and calculates the statistical quantity of each block. Then the statistical quantity values are shifted by appropriate thresholds, which are selected according to the maximum absolute value of the statistical quantity. Finally, we can embed secret bits into the blocks by using the statistical quantity values which have been shifted. Simulation results demonstrate that the proposed algorithm can achieve high performances in the visual quality of the stego-images, data embedding capacity, and robustness. Performance comparisons with other existing robust lossless data hiding schemes are provided to demonstrate the superiority of the proposed scheme in embedding capacity when keeping the visual quality and robustness at a similar level.

Key words: robust lossless data hiding; statistical quantity; visual quality of images; embedding capacity; robustness; JPEG2000 compression

0 引言

近年来,无损信息隐藏技术作为版权保护、内容

认证和数字信息安全传递的有效手段之一,在多媒体安全领域发挥着越来越重要的作用。目前国内外已有很多无损信息隐藏算法被提出^[1-6]。然而,大多数无损信息隐藏算法都是针对“无损环境”设计的。

收稿日期:2012-02-07;修回日期:2012-05-20

基金项目:国家重点实验室基金项目(9140C5303020601,9140C5305020706)

第一作者简介:李晓博(1983—),男,中国空间技术研究院西安分院飞行器设计专业博士研究生,主要研究方向为卫星数据传输与信息处理、信息隐藏。E-mail: xbli@yahoo.cn

也就是说,如果在实际传输环境中含有秘密信息的载体图像受到有损压缩,环境噪声等非恶意攻击,接收端将无法从含密载体图像中正确提取秘密信息。因此,人们提出了鲁棒无损信息隐藏技术。鲁棒无损信息隐藏技术是指在嵌入秘密信息时,虽然可能会对原始载体图像的视觉质量造成一定的破坏,但如果隐含秘密信息的载体图像在传输过程没有发生变化,那么接收端可以完全提取出嵌入的秘密信息,并消除失真恢复原始载体图像;如果在传输过程中含密载体图像受到了一定程度的损坏,那么接收端仍然能够从含密载体中正确提取出秘密信息。

2003 年, Vleschouwer 等人^[7]首次提出了鲁棒无损信息隐藏算法,该算法利用 patchwork 理论^[8]和模 256 加法,通过双映射转换的循环解释实现鲁棒无损隐藏,能较好地抵抗 JPEG 压缩,然而该算法容易使含密载体图像产生椒盐噪声,且含密载体图像的峰值信噪比和嵌入容量都较低。2006 年, Zou 等人^[9]提出了一种基于整数小波变换的鲁棒无损信息隐藏方法,利用图像块 HL1 和 LH1 系数的均值的鲁棒性来实现鲁棒无损嵌入,但该算法在嵌入过程中引入了错误比特,必须通过嵌入纠错码(ECC)来纠错,且产生了一些边信息,嵌入容量较低。Ni 等人^[10-11]提出了一种基于统计量直方图修改的鲁棒无损信息隐藏算法,相比前两种方法获得了较高的鲁棒性和峰值信噪比,但该方法也采用了 ECC,这就影响了嵌入容量。2010 年, Zeng 等人^[12-13]改进了 Ni 的方案,该方法引入了两个阈值对统计量进行修改来实现秘密信息的嵌入,避免了 Ni 方法错误比特的引入,在嵌入容量和鲁棒性方面有了很大的提高。然而,该方法在嵌入容量达到理论最大值的情况下,阈值受到图像统计量最大值的限制,使得图像分块较小时嵌入级过大,图像质量无法保证,嵌入容量也受到了限制。此外,还有一些学者对鲁棒无损信息隐藏算法进行了研究^[14-16]。

利用图像块像素值的统计特征,提出了一种基于统计量的鲁棒无损信息隐藏算法。给出了算法的基本原理、秘密信息嵌入、秘密信息提取及原始载体图像恢复的具体过程,并以典型灰度图像为原始载体图像,对算法性能进行了验证。仿真实验结果表明,该算法在图像视觉质量、嵌入容量和鲁棒性方面都获得了很好的性能;且在含密载体图像视觉质量和鲁棒性与其他算法相当的情况下,该算法的嵌入容量较其他鲁棒无损隐藏算法有了很大提高,进一步拓展了无损信息隐藏算法的应用范围。

1 基于统计量的鲁棒无损隐藏算法

1.1 统计量的生成

为了使算法获得鲁棒性, Ni 等人^[10-11]引入了一个统计量作为鲁棒参数来嵌入秘密信息。首先将原始载体图像分为 8×8 的互不重叠的图像块,再将每个图像块的所有像素分为两个像素集合 **A** 和 **B**。如图 1 所示,像素位置标记“+”的归为集合 **A**,并将相应的像素记为 $a_i, i=1, 2, \dots, 32$, 像素位置标记“-”的归为集合 **B**,并将相应的像素记为 $b_i, i=1, 2, \dots, 32$ 。统计量为

$$\alpha = \frac{1}{n} \sum_{i=1}^n (a_i - b_i) \quad (1)$$

式中, $n=32$ 。

+	-	+	-	+	-	+	-
-	+	-	+	-	+	-	+
+	-	+	-	+	-	+	-
-	+	-	+	-	+	-	+
+	-	+	-	+	-	+	-
-	+	-	+	-	+	-	+
+	-	+	-	+	-	+	-
-	+	-	+	-	+	-	+

图 1 差对图

Fig. 1 Difference pair pattern

由于图像块内所有像素无论加或减一个固定的数,图像块的统计量 α 都保持不变,即使块内像素有不同程度的改变,图像块的统计量 α 也变化很小,所以将 α 作为鲁棒参数来嵌入秘密信息,可使嵌入的秘密信息能够抵抗 JPEG2000 有损压缩等非恶意攻击。

将大小为 $M \times N$ 原始载体图像 **I** 分为 $m \times n$ 的互不重叠的图像块(m, n 为偶数),同时产生一个大小为 $m \times n$ 的差对图。类似地,根据差对图中的标记“+”或“-”将每个图像块的所有像素分为两个像素集合 **A** 和 **B**。最终,图像块的统计量可由式(2)得到。

$$\alpha = \sum_{i=1}^{m \times n / 2} (a_i - b_i) \quad (2)$$

式中, $a_i, i=1, 2, \dots, m \times n / 2$ 对应差对图中像素位置标记为“+”的像素, $b_i, i=1, 2, \dots, m \times n / 2$ 对应差对图中像素位置标记为“-”的像素。利用式(2),按一定顺序依次扫描每个图像块,求得 $512 \times 512 \times 8$ 的 Lena 灰度图像的统计量分布如图 2 所示。其中,令统计量绝对值的最大值为 T_{\max} 。

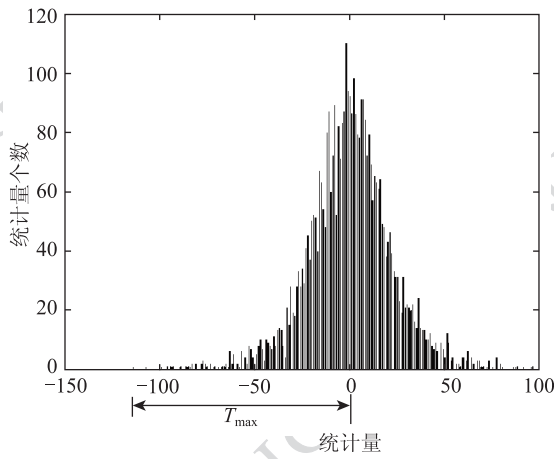


图 2 块大小为 8×8 的 Lena 图像的统计量分布
Fig. 2 The distribution of α with block size 8×8

由图 2 可见,由于一般图像像素灰度值具有很强的局部的相关性和冗余性,所以图像统计量的值大部分都集中于 0 值左右。可以利用这一特性将统计量进行左右移位产生冗余空间来嵌入秘密信息。

1.2 秘密信息的嵌入

首先,引入 4 个可变阈值 T_1, T_2, R_1, R_2 。其中, $0 < T_1 \leq T_{\max}, T_2 = T_{\max} - T_1$ 为统计量阈值, R_1, R_2 为鲁棒阈值。然后按式(3)修改每个图像块的像素值实现统计量移位。

$$II^{(k)}(i,j) = \begin{cases} I^{(k)}(i,j) + \beta_1 & \alpha > T_1 \& \text{mod}(i,2) = \text{mod}(j,2) \\ I^{(k)}(i,j) - \beta_1 & \alpha > T_1 \& \text{mod}(i,2) \neq \text{mod}(j,2) \\ I^{(k)}(i,j) - \beta_1 & \alpha < -T_1 \& \text{mod}(i,2) = \text{mod}(j,2) \\ I^{(k)}(i,j) + \beta_1 & \alpha < -T_1 \& \text{mod}(i,2) \neq \text{mod}(j,2) \\ I^{(k)}(i,j) & \text{其他} \end{cases} \quad (3)$$

式中, $I^{(k)}(i,j)$ 为第 k 块图像坐标为 (i,j) 的像素值, $II^{(k)}(i,j)$ 为相应像素位置修改后的像素值。令 $\beta_1 = \lceil (T_1 + R_1) / (m \times n) \rceil$ 为嵌入级,符号 $\lceil \cdot \rceil$ 代表上取整。 $\text{mod}(x,2)$ 为模 2 运算。根据式(3),对原始载体图像 Lena 的每个图像块进行像素值修改,再计算每个图像块的统计量,得到的移位后的统计量分布图如图 3 所示。由图 3 可见,通过统计量移位,产生了 4 个冗余空间,分别为 $(-\infty, -2T_1 - T_2 - R_1 -$

$R_2]$ 、 $[-2T_1 - R_1, -T_1 - R_1]$ 、 $[T_1 + R_1, 2T_1 + R_1]$ 、 $[2T_1 + T_2 + R_1 + R_2, \infty)$ 。此外, $(-2T_1 - T_2 - R_1 - R_2, -2T_1 - T_2 - R_1)$ 、 $(-T_1 - R_1, -T_1)$ 、 $(T_1, T_1 + R_1)$ 、 $(2T_1 + T_2 + R_1, 2T_1 + T_2 + R_1 + R_2)$ 为 4 个鲁棒空间,鲁棒空间的大小由 R_1, R_2 决定,鲁棒空间越大,受到攻击后图像的统计量互相重叠的概率越低,秘密信息鲁棒性越强。

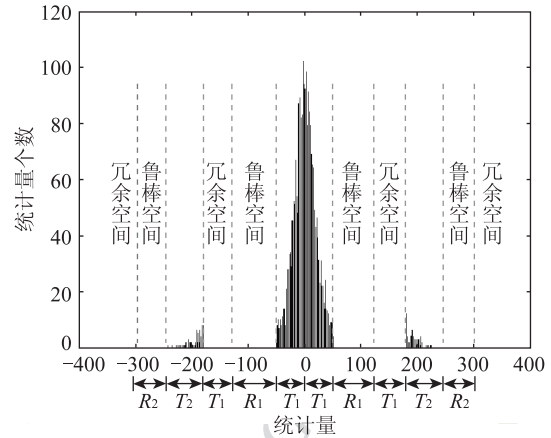


图 3 块大小为 8×8 的 Lena 图像统计量移位
Fig. 3 Distribution of α after shifting

按指定的扫描顺序扫描每个经过统计量移位的图像块,并根据图像块的 α 值进行秘密信息的嵌入。设秘密信息比特流为 $B_l \in \{0, 1\}, l = 1, 2, \dots$, 具体嵌入过程可分为以下两种情况进行:

1) 当 $\alpha > T_1$ 或 $\alpha < -T_1$ 时

如果 $B_l = 1$, 则 $III^{(k)}(i,j) = II^{(k)}(i,j) + \beta_2$;

如果 $B_l = 0$, 则

$$III^{(k)}(i,j) = \begin{cases} II^{(k)}(i,j) + \beta_2 & \alpha > T_1 \& \text{mod}(i,2) = \text{mod}(j,2) \\ II^{(k)}(i,j) - \beta_2 & \alpha > T_1 \& \text{mod}(i,2) \neq \text{mod}(j,2) \\ II^{(k)}(i,j) - \beta_2 & \alpha < -T_1 \& \text{mod}(i,2) = \text{mod}(j,2) \\ II^{(k)}(i,j) + \beta_2 & \alpha < -T_1 \& \text{mod}(i,2) \neq \text{mod}(j,2) \\ II^{(k)}(i,j) & \text{其他} \end{cases} \quad (4)$$

式中, $III^{(k)}(i,j)$ 为嵌入秘密信息后第 k 块图像坐标为 (i,j) 的像素值。令 $\beta_2 = \lceil (T_2 + R_2) / (m \times n) \rceil$ 也为嵌入级。

2) 当 $-T_1 \leq \alpha \leq T_1$ 时

如果 $B_l = 0$, 则 $III^{(k)}(i, j) = II^{(k)}(i, j)$

如果 $B_l = 1$, 则

$$III^{(k)}(i, j) = \begin{cases} II^{(k)}(i, j) + \beta_1 & 0 \leq \alpha \leq T_1 \ \& \ \text{mod}(i, 2) = \text{mod}(j, 2) \\ II^{(k)}(i, j) - \beta_1 & 0 \leq \alpha \leq T_1 \ \& \ \text{mod}(i, 2) \neq \text{mod}(j, 2) \\ II^{(k)}(i, j) - \beta_1 & -T_1 \leq \alpha < 0 \ \& \ \text{mod}(i, 2) = \text{mod}(j, 2) \\ II^{(k)}(i, j) + \beta_1 & -T_1 \leq \alpha < 0 \ \& \ \text{mod}(i, 2) \neq \text{mod}(j, 2) \\ II^{(k)}(i, j) & \text{其他} \end{cases} \quad (5)$$

嵌入秘密信息后的 Lena 图像的统计量分布如图 4 所示。由图 4 可见, 嵌入秘密信息后, Lena 图像的统计量被划分为了 5 个区域, 其中“比特 0 区”和“比特 1 区”分别代表嵌入的秘密信息比特为“0”和“1”。比特区之间的空白区域为鲁棒区间。

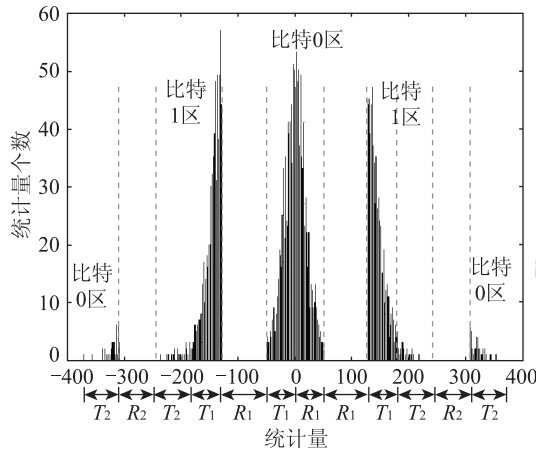


图 4 嵌入秘密信息后 Lena 图像统计量分布
Fig. 4 Distribution of α after embedding data

由以上嵌入过程可知, 每个图像块产生一个 α , 每个 α 可代表一个信息比特 (“0” 或 “1”)。因此, 总的嵌入比特数等于图像块的个数。也就是说, 嵌入容量 $Cap = (M \times N) / (m \times n)$ 。

1.3 秘密信息的提取与原始载体图像的恢复

秘密信息的提取主要分为两种情况进行:

1) 含密载体未受到攻击, 此种情况秘密信息的提取和载体图像的恢复过程是嵌入过程的逆过程, 具体描述如下:

(1) 将含密载体图像 III 分为大小为 $m \times n$ 的互不重叠的图像块 (m, n 为偶数), 同时产生一个大小为 $m \times n$ 的差对图 (如图 1 所示)。

(2) 按嵌入的扫描顺序依次扫描每个图像块, 并计算图像块的 α 值, 可由式 (6) 求得秘密信息。

$$B_l = \begin{cases} 0 & -T_1 \leq \alpha \leq T \ \text{或} \\ & \alpha > 2T_1 + T_2 + R_1 \ \text{或} \\ & \alpha < -2T_1 - T_2 - R_1 \\ 1 & T_1 < \alpha \leq 2T_1 + T_2 + R_1 \ \text{或} \\ & -2T_1 - T_2 - R_1 < \alpha < -T_1 \end{cases} \quad (6)$$

(3) 原始载体图像的恢复可由式 (7) 得到。

$$I^{(k)}(i, j) = \begin{cases} III^{(k)}(i, j) - \beta_1 & T_1 < \alpha \leq 2T_1 + T_2 + R_1 \ \& \ \text{mod}(i, 2) = \text{mod}(j, 2) \\ III^{(k)}(i, j) + \beta_1 & T_1 < \alpha \leq 2T_1 + T_2 + R_1 \ \& \ \text{mod}(i, 2) \neq \text{mod}(j, 2) \\ III^{(k)}(i, j) + \beta_1 & -2T_1 - T_2 - R_1 \leq \alpha < -T_1 \ \& \ \text{mod}(i, 2) = \text{mod}(j, 2) \\ III^{(k)}(i, j) - \beta_1 & -2T_1 - T_2 - R_1 \leq \alpha < -T_1 \ \& \ \text{mod}(i, 2) \neq \text{mod}(j, 2) \\ III^{(k)}(i, j) - \beta_1 - \beta_2 & \alpha > 2T_1 + T_2 + R_1 \ \& \ \text{mod}(i, 2) = \text{mod}(j, 2) \\ III^{(k)}(i, j) + \beta_1 + \beta_2 & \alpha > 2T_1 + T_2 + R_1 \ \& \ \text{mod}(i, 2) \neq \text{mod}(j, 2) \\ III^{(k)}(i, j) + \beta_1 + \beta_2 & \alpha < -2T_1 - T_2 - R_1 \ \& \ \text{mod}(i, 2) = \text{mod}(j, 2) \\ III^{(k)}(i, j) - \beta_1 - \beta_2 & \alpha < -2T_1 - T_2 - R_1 \ \& \ \text{mod}(i, 2) \neq \text{mod}(j, 2) \\ III^{(k)}(i, j) & \text{其他} \end{cases} \quad (7)$$

2) 含密载体受到了一定程度的非恶意攻击, 当含密载体图像受到一定程度攻击后统计量的分布图如图 5 所示。

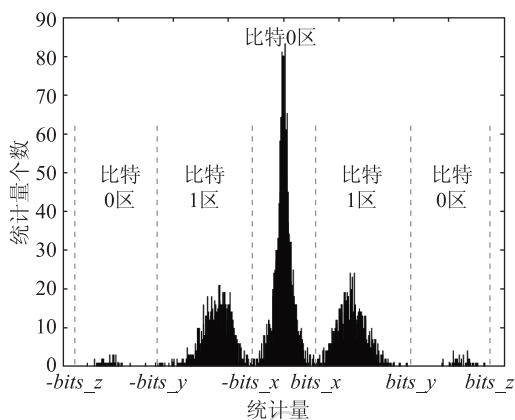


图 5 受到一定程度攻击的含密载体图像统计量分布
Fig. 5 Distribution of α of a stego-image that has gone through attack to some extent

由图 5 可见,部分统计量交织在了一起,在这种情况下采用文献[12]提出的办法,利用嵌入时 0 和 1 的个数,同时考虑到 0 主要集中在比特 0 区,1 主要集中在比特 1 区的趋势,对含密载体图像统计量分布重新划区来提取秘密信息。与文献[12]相比所不同的是,在嵌入秘密信息时要记录嵌入中间比特 0 区的比特 0 个数 $bits_0a$,嵌入的比特 0 总个数 $bits_0b$,还有比特 1 总个数 $bits_1$ 。由图 5 可见,只要保证 $[-bits_x, bits_x]$ 、 $[-bits_y, bits_y]$ 和 $[-bits_z, bits_z]$ 的数目分别为 $bits_0a$ 、 $bits_0a + bits_1$ 和 $bits_0b + bits_1$,则由式(8)可提取秘密信息 B_l 。

$$B_l = \begin{cases} 0 & -bits_x \leq \alpha \leq bits_x \text{ 或} \\ & \alpha > bits_y \text{ 或 } \alpha < -bits_y \\ 1 & -bits_y \leq \alpha < -bits_x \text{ 或} \\ & bits_x < \alpha \leq bits_y \end{cases} \quad (8)$$

1.4 溢出问题的考虑

由于灰度图像像素值的范围为 $[0, 255]$,修改像素灰度值可能导致像素值溢出(小于 0 或者大于 255),使得原始载体图像无法无损恢复。为了解决溢出问题,采用图像直方图平移技术^[3],将图像像素值小于 L (和大于 $255-L$, L 为像素的最大改变量, $L = \beta_1 + \beta_2$)的像素值都加 L 。并建立一个与原始图像大小一致的定位图。如果原始载体图像像素值介于 $(L, 255-L)$,定位图对应位赋值为 0,否则,赋值为 1。对于大多数自然图像而言,像素值小于 L (或者大于 $255-L$)的像素相对较少,且它们都是邻近的。所以,可采用行程编码对定位图进行无损压缩,并将压缩后的定位图同秘密信息一同嵌入到原始载体图像中进行传输。

2 实验与分析

2.1 仿真结果

实验采用 6 幅 $512 \times 512 \times 8$ 的国际标准灰度测试图像作为原始载体图像(测试图像来源于 CVG-UGR 图像数据库^[17]),如图 6 所示。秘密信息采用伪随机发生器产生的二进制比特流。由于本文算法在“无损环境”情况下可以无损恢复秘密信息和原始载体图像,所以实验主要研究含密载体图像在受到攻击时的性能。实验中,采用 JPEG2000 压缩算法对含密载体图像进行不同程度的有损压缩,压缩工具采用 JASPER 软件^[18]。通过不断增加压缩率(以 0.5 倍为最小递增单位),并从受到攻击的含密载体图像中提取秘密信息,当秘密信息位出错率(BER)小于 1% 时,令此时的压缩率为最大压缩率,并将其作为衡量算法鲁棒性的指标。即最大压缩率越大,鲁棒性越好。嵌入秘密信息后含密载体图像的视觉质量采用峰值信噪比(PSNR)来衡量。首先将原始载体图像分为 8×8 的小块,并计算每一小块的统计量 α 值,选择合适的阈值 T_1 、 T_2 、 R_1 、 R_2 对统计量直方图进行移位,最后嵌入秘密信息比特流。6 幅原始载体图像的测试结果如表 1 所示。

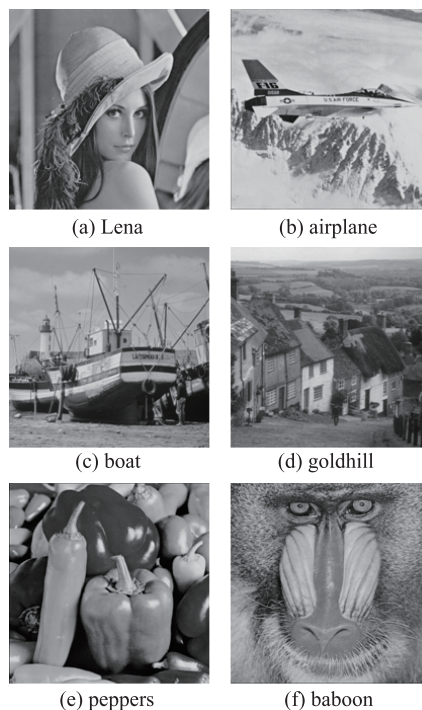


图 6 实验所用的测试图像

Fig. 6 Original six test images used for performance evaluation

表 1 图像块大小为 8×8 时本文算法的测试结果
Table 1 The performance of the proposed scheme with block size 8×8

图像	PSNR/dB	容量/bit	阈值(T_1, T_2)	阈值(R_1, R_2)	嵌入级(β_1, β_2)	最大压缩率/倍	BER/%
Lena	38.77	4 096	(64, 50)	(192, 78)	(4, 2)	13.5	0.195
airplane	38.29	4 096	(64, 56)	(192, 72)	(4, 2)	11	0.098
boat	38.66	4 096	(64, 37)	(192, 91)	(4, 2)	10	0.171
goldhill	38.40	4 096	(64, 45)	(192, 83)	(4, 2)	9.5	0.098
peppers	37.72	4 096	(128, 36)	(128, 92)	(4, 2)	14	0.269
baboon	36.01	4 096	(192, 196)	(128, 60)	(5, 4)	4.5	0.342

由表 1 可见,在秘密信息位出错率小于 1% 且嵌入的秘密信息达 4 096 比特的情况下,6 幅图像可抵抗的最大压缩率为 4.5 倍到 14 倍,含密载体图像的峰值信噪比为 36.01 dB 到 38.77 dB,表明该算法在图像视觉质量,嵌入容量及鲁棒性 3 方面都获得了很好的性能。其中“Baboon”图像的峰值信噪比最低,这是由于其嵌入级大于其他 5 幅图像的缘故。由 1.2 节可知,嵌入级(β_1, β_2)由阈值(T_1, T_2)和(R_1, R_2)决定。嵌入级越大,对图像像素的改变量越大,也就使得含密载体图像的峰值信噪比越低。嵌入级与含密载体 PSNR 的关系如图 7(以 Lena 图像为例)。由图 7 可见,当保持 $\beta_2 = 2$ 不变,增大 β_1 时图像质量迅速降低;当保持 $\beta_1 = 4$ 不变,随着 β_2 的增大图像质量下降较缓。这是由于大部分图像块的统计量都集中于 $[-T_1, T_1]$ 之间(如图 3 所示),在秘密信息的嵌入过程中大部分图像块像素值改变量为 β_1 ,而只有统计量位于区间 $[-2T_1 - R_1 - T_2, -2T_1 - R_1]$ 和 $[2T_1 + R_1, 2T_1 + R_1 + T_2]$ 之间的图像块的像素值改变量为 β_2 ,因此含密载体图像的峰值

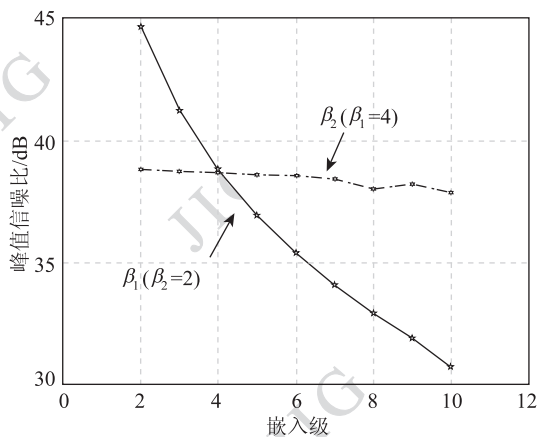


图 7 嵌入级与含密载体图像峰值信噪比的关系

Fig. 7 The relationship between embedding level and PSNR

信噪比主要由 β_1 决定。此外,由于阈值(T_1, T_2)取决于统计量绝对值的最大值 T_{\max} ($T_{\max} = T_1 + T_2$),所以当某些图像(例如 Baboon 图像)的 $T_{\max} = 388$ 很大时,导致阈值(T_1, T_2)较大,此时即使阈值(R_1, R_2)选择很小,也使得嵌入级很大,结果使含密载体图像的 PSNR 较低。

对于同一幅载体图像,嵌入级的大小也影响着含密载体图像可抵抗的最大压缩率。图像分块采用 8×8 ,且在秘密信息位出错率小于 1% 情况下,当保持 $\beta_2 = 2$ 不变(baboon 图像保持 $\beta_2 = 4$ 不变)时,嵌入级 β_1 与含密载体图像可抵抗的最大压缩率的关系如图 8 所示。由图 8 可见,随着嵌入级 β_1 的增大,含密载体图像可抵抗的最大压缩率也逐渐增大,也就是说秘密信息抗压攻击的鲁棒性越好。这是由于随着 β_1 的增大,使得嵌入秘密信息后含密载体图像统计量分布图中(如图 4 所示)中间比特 0 区与比特 1 区之间的鲁棒空间增大,若含密载体图像受到攻击,则含密载体图像统计量分布图中中间比

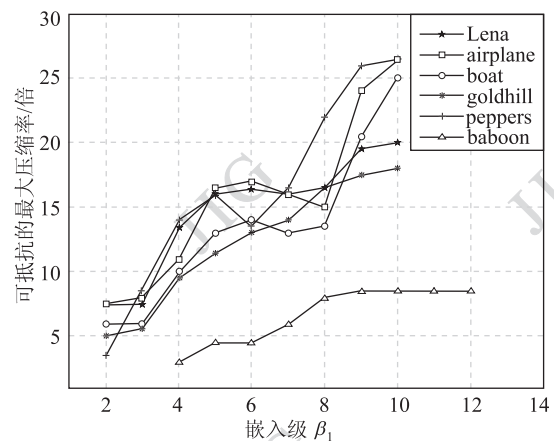


图 8 嵌入级 β_1 与可抵抗的最大压缩率之间的关系

Fig. 8 The relationship between the robustness against maximum JPEG2000 compression and the embedding level β_1

特 0 区与比特 1 区之间越不容易混叠,提取的秘密信息错误比特数就越少。保持 $\beta_1 = 4$ 不变 (Baboon 图像保持 $\beta_1 = 5$ 不变) 时,嵌入级 β_2 与含密载体图像可抵抗的最大压缩率的关系如图 9 所示。由图 9 可见,在 β_1 一定情况下, β_2 基本对含密载体图像可抵抗的最大压缩率没有影响。由前面的分析可知,嵌入秘密信息后图像块的统计量主要集中在分布图的中间比特 0 区和比特 1 区,左右两边的比特 0 区的统计量很少 (如图 4 所示),即嵌入的秘密信息很少,所以秘密信息的鲁棒性主要由嵌入级 β_1 决定。

图像分块的大小同样对算法的性能有影响。由表 2 可见,在嵌入级相同且提取出的秘密信息位出错率小于 1% 时,图像块越大,秘密信息可抵抗的最大压缩率越大。然而,图像块的大小又决定了嵌入容量的大小,所以随着图像块的增大,原始载体图像可嵌入的秘密信息比特数就越少。因此,用户可根据具体要求在嵌入容量与鲁棒性两方面进行权衡。

2.2 与其他算法的比较

表 3 列出了本文算法与 Ni 等人^[10-11]算法和 Zeng 等人^[12]算法的比较结果。为了更好地和其他算法进行比较,在此也采用存活率 (单位为 bit/pixel)

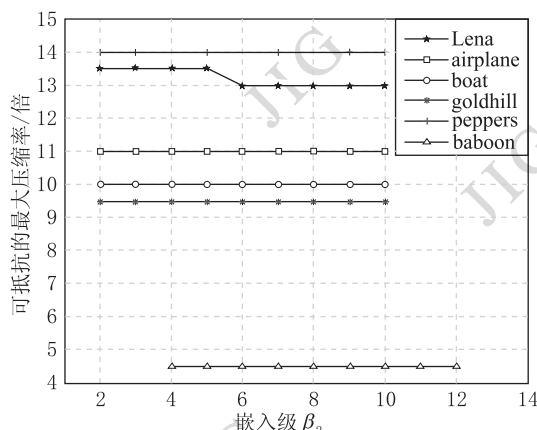


图 9 嵌入级 β_2 与可抵抗的最大压缩率之间的关系

Fig. 9 The relationship between the robustness against maximum JPEG2000 compression and the embedding level β_2

作为衡量算法鲁棒性的指标。存活率与最大压缩率之间的转换关系为:存活率 = 8/最大压缩率。由表 3 可见,在提取的秘密信息位出错率小于 1% 且鲁棒性和含密载体图像峰值信噪比与其他算法相当的情况下,本文算法的嵌入容量远大于其他两种算法,表明本文算法具有明显的优势。

表 2 Lena 图像在分块大小不同的情况下本文算法的性能

Table 2 The performance of the proposed scheme with different block size on image 'Lena'

图像分块大小	PSNR/dB	容量/bit	阈值 (T_1, T_2)	阈值 (R_1, R_2)	嵌入级 (β_1, β_2)	最大压缩率/倍	BER/%
4 × 4	36.761 0	16 384	(64, 56)	(16, 24)	(5, 5)	7.5	0.616
4 × 8	36.916 3	8 192	(64, 34)	(96, 62)	(5, 3)	14.0	0.293
8 × 4	36.910 9	8 192	(64, 62)	(96, 34)	(5, 3)	15.0	0.232
8 × 8	36.889 6	4 096	(64, 50)	(256, 78)	(5, 2)	16.0	0.049
8 × 16	36.515 2	2 048	(64, 68)	(576, 188)	(5, 2)	17.5	0.098
16 × 8	36.852 6	2 048	(128, 69)	(512, 187)	(5, 2)	18.0	0.000

表 3 与其他鲁棒无损隐藏算法的比较

Table 3 Performance comparison between others algorithm and the proposed scheme

图像 (512 × 512)	Ni 等人 ^[10-11] 算法			Zeng 等人 ^[12] 算法				本文算法			
	PSNR /dB	容量 /bit	存活率 /(bit/pixel)	PSNR /dB	容量 /bit	存活率 /(bit/pixel)	BER /%	PSNR /dB	容量 /bit	存活率 /(bit/pixel)	BER /%
Lena	40.19	792	0.80	38.07	2 048	0.80	0.015	38.77	4 096	0.59	0.195
airplane	40.17	792	0.80	38.09	2 048	0.80	0.013	38.29	4 096	0.73	0.098
boat	40.47	560	1.00	38.09	2 048	1.00	0.182	38.66	4 096	0.80	0.171
goldHill	40.18	792	1.08	38.10	2 048	1.08	0.157	38.40	4 096	0.84	0.098
peppers	40.48	560	0.61	38.12	2 568	0.61	0.047	37.72	4 096	0.57	0.269
baboon	38.68	585	1.60	38.05	850	1.60	0.243	36.01	4 096	1.78	0.342

3 结 论

提出了一种鲁棒无损图像信息隐藏算法。当含密载体图像未受损情况下在正确提取秘密信息后可完全无损恢复原始载体图像;当含密载体图像受到诸如 JPEG2000 压缩等非恶意攻击时也能正确提取秘密信息。实验结果表明,本文算法在图像视觉质量、嵌入容量和鲁棒性 3 个方面都具有很好的性能。在保持图像视觉质量和鲁棒性与其他鲁棒无损隐藏算法相当的情况下,本文算法获得了较高的嵌入容量。此外,本文算法的嵌入过程主要执行扫描和平移操作,算法复杂度低,执行速度快。因此,该方案可以应用到医学成像、法律取证、遥感等领域。

参考文献 (References)

- [1] Tian J. Reversible data embedding using a difference expansion [J]. IEEE Transactions on Circuits Systems Video Technology, 2003, 13(8):890-896.
- [2] Ni Z C, Shi Y Q, Ansari N, et al. Reversible data hiding [J]. IEEE Transactions on Circuits Systems Video Technology, 2006, 16(3): 354-362.
- [3] Chang C C, Tai W L, Chen K N. Lossless data hiding based on histogram modification for image authentication [C]// Proceedings of IEEE/IFIP International Conference on Embedded and Ubiquitous Computing. Shanghai: Shanghai Jiao Tong University and Shanghai Computer Society, 2008:506-510.
- [4] Tai W L, Yeh C M, Chang C C. Reversible data hiding based on histogram modification of pixel differences [J]. IEEE Transactions on Circuits Systems Video Technology, 2009, 19(6): 906-910.
- [5] Qiu Y Q. Image reversible data hiding with modified integer transform [J]. Journal of Image and Graphics, 2011, 16(7): 1146-1152. [邱应强. 利用改进整数变换实现图像无损信息隐藏[J]. 中国图象图形学报, 2011, 16(7):1146-1152.]
- [6] Wang L, Geng Z X, Chen L, et al. Reversible information hiding algorithm for remote sensing image with high radiometric resolution [J]. Journal of Image and Graphics, 2011, 16(6):1094-1101. [王兰, 耿则勋, 陈路, 等. 高辐射分辨率遥感影像可逆信息隐藏算法[J]. 中国图象图形学报, 2011, 16(6):1094-1101.]
- [7] Vleeschouwer C D, 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.
- [8] Bender W, Gruhl D, Morimoto N, et al. Techniques for data hiding [J]. IBM Syst. J., 1996, 35(3-4): 313-336.
- [9] Zou D, Shi Y, Ni Z, et al. A semi-fragile lossless digital watermarking scheme based on integer wavelet transform [J]. IEEE Trans. on Circuits Syst. Video Technol, 2006, 16(10): 1294-1300.
- [10] Ni Z, Shi Y, Ansari N, et al. Robust lossless image data hiding [C]// Proceedings of IEEE Int. Conf. on Multimedia Expo. Taipei, Taiwan, China: IEEE ICME, 2004:2199-2202.
- [11] Ni Z, Shi Y, Ansari N, et al. Robust lossless image data hiding designed for semi-fragile image authentication [J]. IEEE Trans. on Circuits Syst. Video Technol, 2008, 18(4): 497-509.
- [12] Zeng X T, Ping L D, Pan X Z. A lossless robust data hiding scheme [J]. Pattern Recognition, 2010, 43(4), 1656-1667.
- [13] Zeng X T, Pan X Z, Ping L D, et al. Robust lossless data hiding scheme [J]. Journal of Zhejiang University-Science C (Computers & Electronics), 2010, 11(2):101-110.
- [14] Kim K S, Lee M J, Suh Y H. Robust lossless data hiding based on block gravity center for selective authentication [C]// Proceedings of IEEE International Conference on Multimedia and Exp. Cancun, Mexico: IEEE Computer Society, Signal Processing Society, Circuits and Systems Society, and the Communications Society, 2009:1022-1025.
- [15] Dhavale S V, Patnaik L M. High capacity, robust lossless EPR data hiding using CDCS with ROI tamper detection [C]// Proceedings of Int'l Conf. on Computer & Communication Technology. Allahabad, India: Motilal Nehru National Institute of Technology, 2010:108-112.
- [16] An L L, Gao X B, Yuan Y. Robust lossless data hiding using clustering and statistical quantity histogram [J]. Neurocomputing, 2012, 77:1-11.
- [17] University of Granada. CVG-UGR image database [DB/OL]. (2012-03-27) [2012-04-15]. <http://decsai.ugr.es/cvg/dbimages/index.php>.
- [18] Michael Adams. The Jasper Software [CP/OL]. (2006-12-07) [2012-04-15] <http://www.ece.uvic.ca/~frodo/jasper/>.