

文章编号:1004-9037(2006)03-0330-04

一种抗剪切的鲁棒数字水印

王 丽 赵媛媛 赵 耀

(北京交通大学信息科学所,北京,100044)

摘要:利用 Patchwork 方法并结合量化索引调制(QIM)提出了一个抗剪切的数字水印方案。首先在空域中对原始图像进行 32×32 分块,在每块中用 Patchwork 的方法进行点对的选取和像素值的修改,从而在整幅图像中嵌入若干个相同且不重叠的定位模式。然后,对每一块进行 DCT 变换,并用 QIM 方法对低频系数进行水印的重复嵌入,最后经 DCT 逆变换得到嵌入水印后的图像。提取时根据密钥产生和原图大小相同的定位解码模式,通过定位模式得到可能遭受攻击的水印图像正确的剪切位置,并对剩余的完整分块进行 DCT 变换,重新量化其中低频系数,最后根据最小距离法提取水印。实验表明,该方案对剪切具有很高的鲁棒性,对压缩及加噪声等常见的图像处理也取得了很好的效果。

关键词:数字图像水印;量化;剪切攻击;量化索引调制;Patchwork 方法

中图分类号:TP391

文献标识码:A

Digital Image Watermarking Resistant to Cropping Attacks

Wang Li, Zhao Yuanyuan, Zhao Yao

(Institute of Information Science, Beijing Jiaotong University, Beijing, 100044, China)

Abstract: A novel image watermarking scheme based on Patchwork and quantization index modulation(QIM) is proposed. In the embedding, the image is partitioned into the blocks of 32×32 , and the same locating pattern is embedded by Patchwork method in each block. Then the watermark sequence is embedded in the block DCT coefficients by using the QIM method. In the decoding, the position where the watermarked image is cropped through the locating pattern is obtained, so the right blocks are found and the watermark sequence is extracted from the block DCT coefficients using the minimum distance method. Experimental results show that the scheme is robust to cropping attacks as well as compression, and the additive noise.

Key words: digital image watermarking; quantization; cropping attack; quantization index modulation; Patchwork method

引 言

水印算法主要可分为两类:空间域的算法^[1]和变换域^[2]的算法。空间域算法直接修改图像的像素,该类算法最大特点是算法简单,并可以保留一些位置信息,但鲁棒性较差,嵌入容量有限。相对于空域算法,频域算法有着多种很好的特性,无论是图像质量还是水印容量都比空域算法有很大的提高,也是目前水印算法研究的热点。但是频域算法在没有原始图像的情况下,当图像受到诸如剪切操

作等攻击时,水印嵌入的同步信息被完全破坏,往往无法正确地检测和提取水印信息。

综合空间域和频率域的优点,可以利用空域中的位置信息来抵抗剪切攻击,同时利用频域的特性进行水印的高质量大容量嵌入。基于这种思想,本文提出了一种结合 Patchwork^[1]和量化索引调制(Quantization index modulation, QIM)^[3]的抗剪切的公开水印算法,该算法利用分块 Patchwork 的方法在空域中确定剪切位置,利用 QIM 的方法在 DCT 域中实现多比特水印嵌入。在保证水印不可见性的同时,水印的容量得到了很大的提高,对常见的图像处理操作,特别是剪切具有很好的鲁棒性。

基金项目:国家自然科学基金(60172062)资助项目;霍英东青年教师基金资助项目;留学回国人员科研启动基金资助项目。

收稿日期:2005-04-17; **修订日期:**2006-02-20

1 水印嵌入算法

本文水印嵌入算法见图 1,主要分为 3 步:首先对要嵌入水印的图像进行 32×32 分块,并对所

有的分块图像用 Patchwork 的方法嵌入相同的定位模式^[4];然后,对所有的分块图像进行 DCT 变换并用 QIM 方法重复嵌入水印;最后对分块图像进行反 DCT 变换得到嵌入了水印的图像。

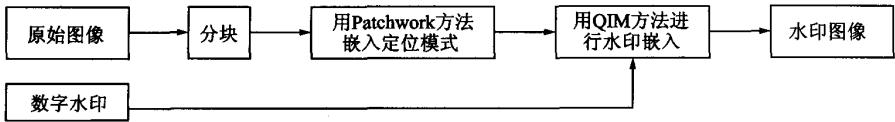


图 1 嵌入水印的过程

1.1 嵌入定位模式

Patchwork 是由 Bender 在 1996 年提出的一种基于伪随机统计过程的方法。在 Patchwork 算法中有如下假设:图像的灰度值服从平均分布,且相互独立。所以对随机选取的若干点对 (a_i,b_i) 的差值和 $S_n = \sum_{i=1}^n (a_i - b_i)$,从统计意义上来说,应该为 0。Patchwork 方法就是利用这个性质,人工地修改 S_n ,使得修改后点对差值的和 S_n' 偏离其期望值 0。

基本的 Patchwork 方法只能进行单比特的水印嵌入,为了提高水印的容量和性能,本文对 Patchwork 方法进行了一些改进。首先对图像进行了分块,然后对所有的块用同一个密钥进行点对的选取和像素值的修改。这样就相当于一幅图像中嵌入了若干个互不重叠的且完全相同的定位模式。如果图像遭受剪切攻击,就可以根据剩余的分块确定剪切位置。

定位模式嵌入的具体过程如下:(1)将原始图像按 32×32 大小分块;(2)用相同的密钥在每一块中用 Patchwork 方法进行点对的选取和像素值的修改;(3)经过上述操作后,就在每一个块中嵌入了一个相同的定位模式。

1.2 有意义水印序列的嵌入

QIM 是由 Brian Chen 等提出的一种非线性水印方法。QIM 方法的主要策略是根据嵌入水印信息 0 或 1 的不同,选择不同的量化器(一般是正交的量化器),对原始信息(可以是空域信息,也可以是频域信息)进行量化。解码端对嵌入水印的数据进行重新量化,根据重新量化的结果与各个量化器间的距离做出判决,从而提取出嵌入的水印信息。

本文采用 DM(Dither modulation)^[5]抖动量化器进行水印嵌入。首先构造一个步长为 Δ 的基本量化器 $q(\cdot)$,然后将基本量化器经平移形成相距

$\Delta/2$ 的量化器 $q_0(\cdot,0)$ 和 $q_1(\cdot,1)$ 。

水印序列嵌入的具体过程如下:

(1)对每一个嵌入过定位模式的 32×32 块进行 DCT 变换。

(2)对每一块,从第二个系数起,选择和水印长度一样的 DCT 系数,根据水印比特值的不同选择不同的量化器按照式(1)的方法对其进行量化。

对每一块都进行相同的水印嵌入是为了提高水印算法的鲁棒性,因为在水印提取的时候,对所有块中位置相同的 DCT 系数用与嵌入时相同的量化器 $q_0(\cdot,0)$ 和 $q_1(\cdot,1)$ 分别进行量化,同时累积该系数的量化误差,根据量化误差来确定水印的 0/1 值。

假设: X 为原始图像; y 为要进行水印嵌入的 DCT 系数; W 为水印信息; l 为水印长度。则水印的嵌入公式为

$$s(X,W) = \begin{cases} q_0(y(k),0) = \\ \qquad q(y(k) + d(k,0)) - d(k,0) \\ \qquad \qquad \qquad w(k) = 0 \\ q_1(y(k),1) = \\ \qquad q(y(k) + d(k,1)) - d(k,1) \\ \qquad \qquad \qquad w(k) = 1 \end{cases}$$

$k = 1, \dots, l$ (1)

抖动序列 $d(k,0)$ 是区间 $[-\Delta/2, +\Delta/2]$ 上的均匀分布, $d(k,1)$ 是由 $d(k,0)$ 生成的且与 $d(k,0)$ 相距 $\Delta/2$ 的均匀分布。

$$d(k,1) = \begin{cases} d(k,0) + \Delta/2 & d(k,0) < 0 \\ d(k,0) - \Delta/2 & d(k,0) \geq 0 \end{cases}$$

$k = 1, \dots, l$ (2)

(3)对嵌入水印后的块进行 IDCT 变换,得到嵌入水印后的图像。

量化器的量化步长对水印算法的鲁棒性影响很大,如果步长过大,图像质量会变差,而且经过反 DCT 后,图像的灰度值改变比较大,会影响到

Patchwork 方法的正确定位。如果量化步长过小,则水印的鲁棒性会很差。经过实验发现,步长在 10 的

时候,图像的质量和水印鲁棒性之间能够达到一个很好的平衡。QIM 方法嵌入水印过程如图 2 所示。

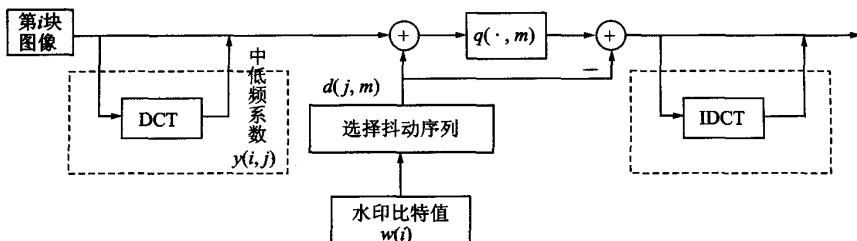


图 2 QIM 方法嵌入水印

2 水印的提取算法

水印提取算法如图 3 所示。

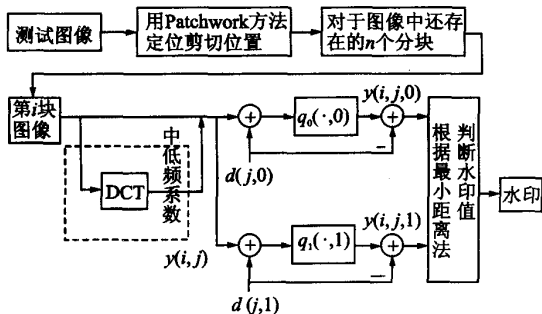


图 3 水印提取

对于可能遭受剪切攻击的水印图像,本文通过下面两个步骤进行水印提取。

(1) 定位剪切位置。根据密钥生成和原始图像大小相同的定位解码模式,用水印图像从解码模式的左上角开始,在 32×32 大小的块中进行平移,每平移到一个位置,根据解码模式定义的点对计算整幅水印图像在该位置的 $S_n' = \sum_{i=1}^n (a_i' - b_i')$ 值,找到最大的 S_n' 所在的相对于解码模式左上角起始点的位置坐标,记为 (x_1', y_1') 。根据 (x_1', y_1') 确定剪切图像中下一个完整的 32×32 分块的位置,也即 $(1 + (32 - x_1' + 1), 1 + (32 - y_1' + 1))$,从而找到原图像正确的分块位置。

(2) 提取水印。对水印图像中还剩下的 n 个完整的块,首先做分块 DCT 变换,并选取和水印嵌入时相同的中低频系数,用量化器 $q_0(\cdot, 0)$ 和 $q_1(\cdot, 1)$ 分别进行量化,最后根据最小距离法进行水印的提取。

假设: l 为水印长度; $i = 1, 2, \dots, n$ 为 32×32 块的序号; $j = 1, 2, \dots, l$ 为水印序列的序号; $y(i, j)$ 为被量化的 DCT 系数; $y(i, j, 0)$ 和 $y(i, j, 1)$ 为量

化器 $q_0(\cdot, 0)$ 和 $q_1(\cdot, 1)$ 量化 $y(i, j)$ 后的值。在第 i 个 32×32 的块中计算:

$$\text{dist}_0(i, j) = (y(i, j, 0) - y(i, j))^2 \quad (3)$$

$$\text{dist}_1(i, j) = (y(i, j, 1) - y(i, j))^2 \quad (4)$$

对所有的块计算

$$\text{dist}_0(j) = \sum_{i=1}^n \text{dist}_0(i, j) \quad (5)$$

$$\text{dist}_1(j) = \sum_{i=1}^n \text{dist}_1(i, j) \quad (6)$$

如果 $\text{dist}_0(j) < \text{dist}_1(j)$, 则 $w(j) = 0$; 反之 $w(j) = 1$ 。

3 实验结果与分析

测试图像为 256×256 的 Lena 灰度图像。水印是 15×20 有意义的黑白图像, Patchwork 方法中灰度值的改变幅度为 2, DM 的量化步长为 10。相对于文献[4]中没有采用 QIM 的 Patchwork 改进方案,本文方案在水印容量和抗剪切的性能上都有所提高,文献[4]的嵌入容量为 55,而本文嵌入容量为 300,文献[4]最多只能抵抗 $1/2$ 的剪切,而本文方案能够抵抗 $1/16$ 的剪切攻击,图 4 给出该水印方案的检测结果。

通过实验可以看出,本方案能很好地抵抗剪切攻击,而单纯的 QIM 方法却无法做到。理论上来说,只要第一层水印定位正确,并且剪切后的图像中至少包含一个完整的 32×32 块,水印都能够正确地提取出来。但是剪切位置的能否正确定位主要取决于剩下的那些块的统计特性,如果剩下的块数太少,则有可能定位出错。例如当剪切图像分别为 $[20 \ 20 \ 65 \ 65]$ 和 $[210 \ 210 \ 256 \ 256]$ 时,前者可以正确地定位剪切位置,而后者却定位出错,也不能正确地提取水印。但从本文的实验结果来看,如果剩余的 32×32 的块数大于 4,水印基本都能够被正确检测出来。

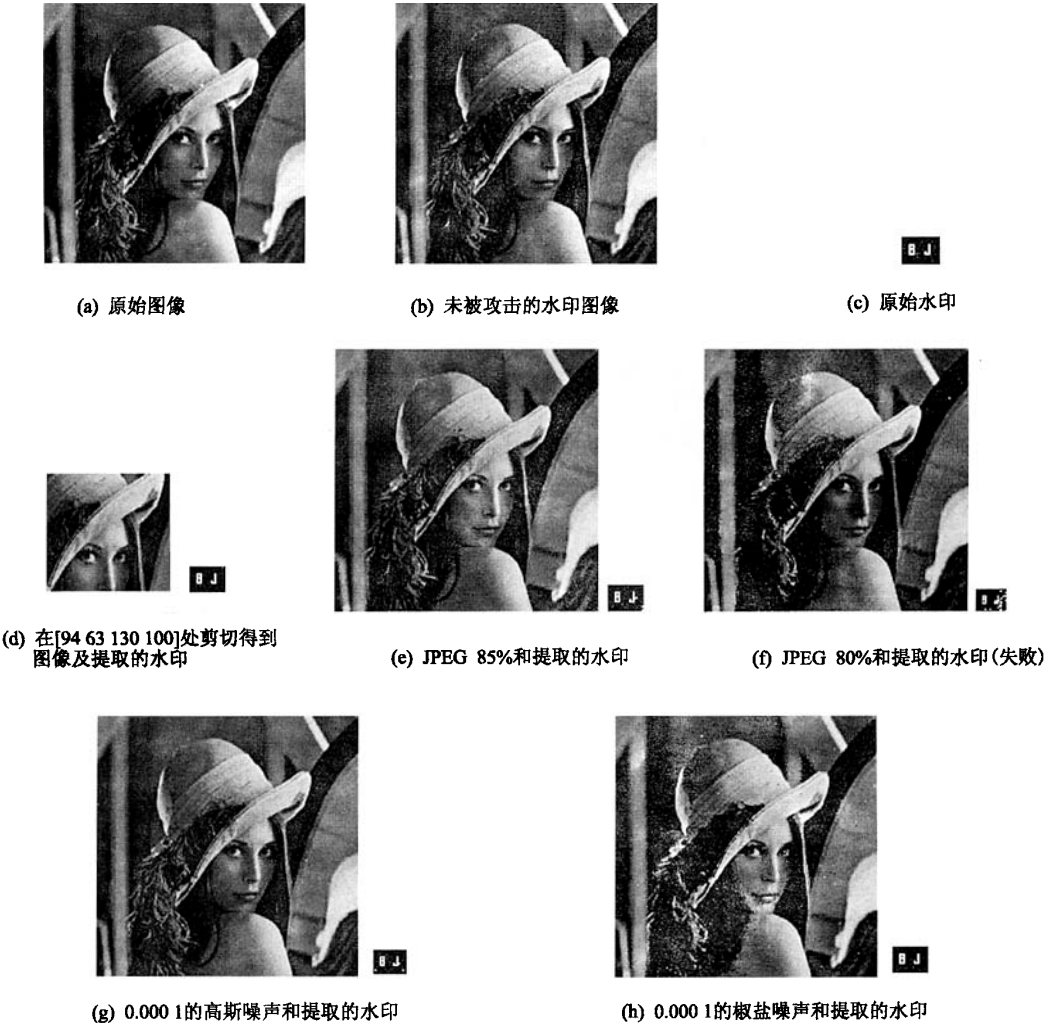


图 4 攻击后的水印图像和提取出的水印

4 结束语

本文提出了一种抗剪切攻击的鲁棒数字图像水印方案,其主要思想是利用 Patchwork 方法确定水印提取时的正确分块位置和 QIM 的大容量来进行嵌入和提取的多比特水印方案。实验结果表明,该方案对剪切具有非常好的鲁棒性,并且对常见的压缩、加噪等多种图像处理操作也具有很好的效果。

参考文献:

[1] Bender R W, Gruhl D. Techniques for data hiding [J]. IBM System Journal, 1996, 35(3-4): 313-336.

[2] Cox I J, Killian J, Leighton F T, et al. Secure spread spectrum watermarking for multimedia [J]. IEEE Trans Image Processing, 1997, 6(12): 1673-1687.

[3] Chen B, Wornell G W. Quantization index modulation methods for digital watermarking and information embedding of multimedia [J]. Proceedings of the Journal of VLSI Signal Processing, 2001, 27(1-2): 7-33.

[4] Butman M. Stand-alone multi-level watermarking [D]. Ramat-Gan, Israel: Dept of Computer Science of Bar-Ilan University, 2000.

[5] Zhao Yuanyuan, Yang Wenxue, Zhao Yao. Improving QIM watermark with soft decision FEC [C]// Proceedings of fourth IASTED International Conference on Visualization, Imaging, and Image Processing. 2004: 814-818.

作者简介:王丽(1980-),女,硕士研究生,研究方向:数字水印, E-mail: kekahu@126.com; 赵媛媛(1981-),女,硕士研究生,研究方向:数字水印; 赵耀(1967-),男,教授,研究方向:数字水印、图像压缩编码、视频图像检索和多媒体信息处理。