

基于视觉模型的迭代 AQIM 水印算法

凌 洁, 刘 琚, 孙建德, 孙兴华

(山东大学信息科学与工程学院, 山东济南 250100)

摘 要: 自适应量化索引调制算法(AQIM)通过 Watson 视觉模型来计算量化步长,使得量化步长可以随着待量化系数自适应变化,从而获取了比传统量化索引调制算法(QIM)更好的不可见性和鲁棒性.但即使在没有干扰的情况下,该算法在检测时计算的量化步长与嵌入时计算的量化步长也不一致,这就导致水印不能够完整可靠地提取.本文在分析该算法存在问题的基础上,提出了一种改进的迭代 AQIM 水印方案,仿真实验表明该方案比原算法具有更好的性能.

关键词: 数字水印; 自适应 QIM; 视觉模型; 迭代嵌入

中图分类号: TN919.8 **文献标识码:** A **文章编号:** 0372-2112 (2010) 01-0151-05

Visual Model Based Iterative AQIM Watermark Algorithm

LING Jie, LIU Ju, SUN Jian-de, SUN Xing-hua

(School of Information Science and Engineering, Shandong University, Jinan, Shandong 250100, China)

Abstract: Adaptive Quantization Index Modulation (AQIM) calculates the quantization step based on the Watson's visual model, in which the quantization step varies adaptively on the quantized coefficient. So AQIM is more reliable and robust than the traditional Quantization Index Modulation (QIM). But even if there is no noise, the embedding step in watermarking is different from the one in detecting, which results in that the watermark can't be integrally extracted. In the paper, an iterative AQIM is advanced to overcome the defect and has better result than AQIM.

Key words: digital watermark; AQIM; visual model; iterative embedding

1 引言

随着网上数字多媒体的传播,如何有效保护数字产品版权成为亟需解决的问题.研究者提出各种嵌入算法,而数字水印算法的不可见性和鲁棒性是解决版权保护的关键.

现在常用水印算法主要包括扩频水印算法和量化索引调制算法(QIM).SS 算法由 Cox 等^[1]首先提出,该算法的主要创新点是水印嵌入到载体的重要位置上,以提高水印鲁棒性,并可根据视觉模型来控制嵌入强度^[2~4],但该算法在盲检测时性能较差^[5],且嵌入水印为 1 比特水印.QIM 算法由 Brian Chen 等^[6]最早提出,该算法具有鲁棒性好,嵌入量大,算法复杂度小且可盲检测等优点,因此在数字水印算法中备受关注.但传统的 QIM 算法是基于固定量化步长的,所以会导致在局部区域具有较差的不可见性,而且对数值测度的变化极其敏感^[7,8].研究者试图在 QIM 算法中采用视觉模型来控制量化步长,来平衡不可见性和鲁棒性.Saravanan 等^[9]提出根据亮度掩蔽特性对不同亮度的分块采用不同量化

间隔,量化步长为亮度的函数的算法,但该算法没有考虑对比度掩蔽特性,量化步长不能随着待量化值的变化而自适应调整.Cox 等^[10,11]提出了一种自适应 QIM (AQIM)算法,该算法基于自适应量化步长,且采用改进的视觉模型使算法对于数值测度的变化具有鲁棒性,较传统的 QIM 算法在相同可信度前提下具有更高的鲁棒性,或者说在相同的鲁棒性下具有更好的可信度.但是该算法存在一个致命的弱点:由于量化步长是待量化系数的函数,因而嵌入水印后的量化步长是利用改变后的已量化系数计算的,这就造成嵌入时使用的量化步长与检测时的量化步长不一致,导致该算法即使在没有干扰的情况下也不能完整地提取出水印.

针对上述问题,我们通过对该算法缺陷产生的原因进行理论分析,提出了一种理论可行的迭代算法.该迭代算法的基本思想是,在水印嵌入过程中同时进行水印检测,观察是否出错,如果出错就在已嵌入水印系数的基础上再次嵌入,以克服算法本身缺陷造成的水印检测差错,而传统的迭代嵌入主要是克服 IDCT 完成后由于取整误差导致的水印提取错误^[12].

2 基于 Watson 视觉模型 AQIM 算法

QIM 是首先利用待嵌入信息(水印)来调制索引或者索引序列,然后使用相应的量化器或量化器序列来量化作品,以达到嵌入信息目的算法:

$$y = q(x, m) \quad (1)$$

式中 x 表示作品中待嵌入信息的载体向量, m 表示待嵌入信息, $q()$ 表示量化函数, y 表示经过量化后的载体向量。

但是,传统的 QIM 算法量化步长与待嵌入信息无关,为了平衡嵌入信息的不可见性和鲁棒性, Cox 等提出 AQIM 算法,采用 Watson 视觉模型^[13,14]中的对比度掩蔽阈值 $s(i, j, k)$ 作为量化步长:

$$step_E = s(i, j, k)$$

$$= \max \left\{ t_L(i, j, k), |C_0(i, j, k)|^{w(i, j)} \cdot t_L(i, j, k)^{1-w(i, j)} \right\} \quad (2)$$

$$t_L(i, j, k) = t(i, j) (C_0(0, 0, k) / C_{0,0})^{\alpha_T} \quad (3)$$

式(2)中, $w(i, j)$ 是一个介于 0 和 1 之间的常数,在 Watson 模型中被取为 0.7, 式(3)中 α_T 为一常数,通常取值为 0.649, $C_0(0, 0, k)$ 为原图中第 k 块的 DC 系数, $C_{0,0}$ 为原图中 DC 系数的平均值, $t(i, j)$ ($i, j = 1, 2, \dots, 8$) 为 Watson 视觉模型定义的敏感度表,反映了人眼对不同频率的敏感程度,具体推导过程见参考文献[13]。

量化步长 $s(i, j, k)$ 为 $|C_0(i, j, k)|$ 的函数,经过量化后得到 $C_w(i, j, k)$, 虽然 $C_w(i, j, k) \approx C_0(i, j, k)$, 但是两者并不完全相等。在信息的提取过程中,由于 $C_0(i, j, k)$ 在检测端未知,只能通过 $C_w(i, j, k)$ 来估计 $s(i, j, k)$, 这样可能造成信息提取错误。

(1) 当 $t_L(i, j, k) \geq |C_0(i, j, k)|^{w(i, j)} t_L(i, j, k)^{1-w(i, j)}$, 即 $t_L(i, j, k) \geq |C_0(i, j, k)|$ 时, $step_E = t_L(i, j, k)$, 这时候量化步长与 $|C_0(i, j, k)|$ 无关,与传统 QIM 一样量化步长恒定,不会造成信息检测错误。

(2) 当 $t_L(i, j, k) < |C_0(i, j, k)|^{w(i, j)} t_L(i, j, k)^{1-w(i, j)}$, 即 $t_L(i, j, k) < |C_0(i, j, k)|$ 时

$$step_E = |C_0(i, j, k)|^{w(i, j)} t_L(i, j, k)^{1-w(i, j)} \quad (4)$$

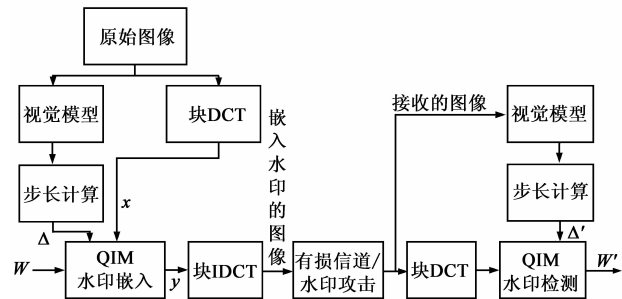


图1 AQIM水印嵌入流程

量化步长随 $|C_0(i, j, k)|$ 变化,就有可能产生检测错误。

基于 Watson 视觉模型的 AQIM 算法流程如图 1 所示。从图 1 可以看到,步长不再使用预先设定值,而是通过 Watson 视觉模型计算得出,同样在检测时也是如此。

3 AQIM 算法缺陷分析

即使在没有干扰的情况下, AQIM 算法在检测时计算的量化步长与嵌入时计算的量化步长也不一致,这就导致水印不能够完整可靠地提取。以下是对这一问题的分析:

在以下的推导中我们将省略 (i, j, k) , 设二进制水印为 W , 嵌入时量化步长为 $step_E$, $q_E = \frac{|C_0|}{step_E}$, $m_E = round(q_E)$, $\delta = q_E - m_E$, 则其中 $|\delta| \leq \frac{1}{2}$ 。

则由式(4)可以得到:

$$|C_0| = t_L \cdot q_E^{\frac{1}{1-w}} = t_L \cdot (m_E + \delta)^{\frac{1}{1-w}} \quad (5)$$

3.1 水印的嵌入过程

Case1: $\text{mod}(m_E, 2) = W$

$$|C_w| = m_E \cdot step_E = m_E \cdot |C_0|^w \cdot t_L^{1-w} = m_E \cdot (m_E + \delta)^{\frac{w}{1-w}} \cdot t_L \quad (6)$$

Case2: $\text{mod}(m_E, 2) \neq W$

(1) 如果 $\delta \geq 0$

$$|C_w| = (m_E + 1) \cdot step_E = (m_E + 1) \cdot |C_0|^w \cdot t_L^{1-w} = (m_E + 1) \cdot (m_E + \delta)^{\frac{w}{1-w}} \cdot t_L \quad (7)$$

(2) 如果 $\delta < 0$

$$|C_w| = (m_E - 1) \cdot step_E = (m_E - 1) \cdot |C_0|^w \cdot t_L^{1-w} = (m_E - 1) \cdot (m_E + \delta)^{\frac{w}{1-w}} \cdot t_L \quad (8)$$

3.2 水印的检测过程

设: $q_D = \frac{|C_w|}{step_D}$, $m_D = round(q_D)$

Case1: $\text{mod}(m_E, 2) = W$

要保证检测正确需要满足 $m_E - \frac{1}{2} < q_D < m_E + \frac{1}{2}$, 也就是要使 $|C_w|$ 满足

$$t_L \cdot \left(m_E - \frac{1}{2}\right)^{\frac{1}{1-w}} < |C_w| < t_L \cdot \left(m_E + \frac{1}{2}\right)^{\frac{1}{1-w}},$$

$$\text{即 } t_L \cdot \left(m_E - \frac{1}{2}\right)^{\frac{1}{1-w}} < m_E \cdot (m_E + \delta)^{\frac{w}{1-w}} \cdot t_L < t_L \cdot \left(m_E + \frac{1}{2}\right)^{\frac{1}{1-w}} \quad (9)$$

可以看出上式与 t_L 无关, 由于 $|\delta| \leq \frac{1}{2}$, 所以上式显然成立, 不会产生水印检测错误。

Case2: $\text{mod}(m_E, 2) \neq W$

(1) $\delta \geq 0$ 时, 要保证检测正确需要满足 $m_E + \frac{1}{2} < q_D < m_E + \frac{3}{2}$. 即:

$$t_L \cdot \left(m_E + \frac{1}{2}\right)^{\frac{1}{1-w}} < (m_E + 1) \cdot (m_E + \delta)^{\frac{w}{1-w}} \cdot t_L < t_L \cdot \left(m_E + \frac{3}{2}\right)^{\frac{1}{1-w}} \quad (10)$$

同样上式成立与否与 t_L 的大小无关.

当 $\delta = 0$ 时

$$(m_E + 1) \cdot m_E^{\frac{w}{1-w}} < \left(m_E + \frac{1}{2}\right)^{\frac{1}{1-w}} \quad (11)$$

该式可以通过函数 $\frac{(x+1) \cdot x^{\frac{w}{1-w}}}{\left(x + \frac{1}{2}\right)^{\frac{1}{1-w}}}$ 的单调性来证明.

当 $\delta = \frac{1}{2}$ 时

$$(m_E + 1) \cdot (m_E + \delta)^{\frac{w}{1-w}} = (m_E + 1) \cdot \left(m_E + \frac{1}{2}\right)^{\frac{w}{1-w}} > \left(m_E + \frac{1}{2}\right)^{\frac{1}{1-w}} \quad (12)$$

$m_E \cdot (m_E + \delta)^{\frac{w}{1-w}}$ 为 δ 的连续函数, 所以存在 $0 < \epsilon < \frac{1}{2}$, 使得

$$(m_E + 1) \cdot (m_E + \delta)^{\frac{w}{1-w}} = \left(m_E + \frac{1}{2}\right)^{\frac{1}{1-w}} \quad (13)$$

在 $0 \leq \delta < \epsilon$ 时检测错误.

(2) $\delta < 0$ 时, 要保证检测正确需要满足 $m_E - \frac{3}{2} < q_D < m_E - \frac{1}{2}$

$$t_L \cdot \left(m_E - \frac{3}{2}\right)^{\frac{1}{1-w}} < (m_E - 1) \cdot (m_E + \delta)^{\frac{w}{1-w}} \cdot t_L < t_L \cdot \left(m_E - \frac{1}{2}\right)^{\frac{1}{1-w}} \quad (14)$$

当 $\delta = 0$ 时

$$(m_E - 1) \cdot (m_E)^{\frac{w}{1-w}} > \left(m_E - \frac{1}{2}\right)^{\frac{1}{1-w}} \quad (15)$$

该式可以通过函数 $\frac{(x-1) \cdot x^{\frac{w}{1-w}}}{\left(x - \frac{1}{2}\right)^{\frac{1}{1-w}}}$ 的单调性来证明.

当 $\delta = -\frac{1}{2}$ 时

$$(m_E - 1) \cdot (m_E + \delta)^{\frac{w}{1-w}} = (m_E - 1) \cdot \left(m_E - \frac{1}{2}\right)^{\frac{w}{1-w}} < \left(m_E - \frac{1}{2}\right)^{\frac{1}{1-w}} \quad (16)$$

$(m_E - 1) \cdot (m_E + \delta)^{\frac{w}{1-w}}$ 为 δ 的连续函数, 所以在存

在 $-\frac{1}{2} < \epsilon' < 0$, 使得

$$(m_E - 1) \cdot (m_E + \delta)^{\frac{w}{1-w}} = \left(m_E - \frac{1}{2}\right)^{\frac{1}{1-w}} \quad (17)$$

在 $\epsilon' < \delta < 0$ 时检测错误.

综上所述, 当 $\text{mod}(m_E, 2) \neq W$ 且 $\epsilon' < \delta < \epsilon$ 时, 水印检测错误.

4 迭代 AQIM 水印算法

为更加清晰地观察水印检测错误情况, 我们在同一幅图中绘制 $|C_0|$ (实线, 直线), $\text{mod}(m_E, 2) \neq W$ (虚线) 与 $\text{mod}(m_E, 2) = W$ 时的 $|C_w|$ (点划线), $t_L \cdot k^{\frac{1}{1-w}}$ (实线, 折线) 及阈值 $\left(m + \frac{1}{2}\right)^{\frac{1}{1-w}} \cdot t_L$ (点线), 如图 2 所示.

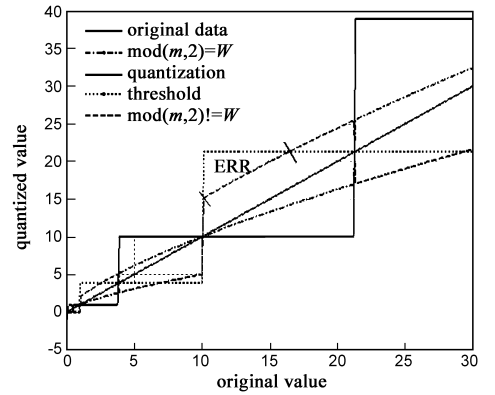


图2 AQIM算法分析

嵌入水印后的值越靠近 $t_L \cdot k^{\frac{1}{1-w}}$, 鲁棒性越好, 越靠近 $|C_0|$ 失真越小, $\left(m + \frac{1}{2}\right)^{\frac{1}{1-w}} \cdot t_L$ 来判断嵌入强度是否足以检测到正确水印, 图中所标 ERR 的区域表示 $\text{mod}(m_E, 2) \neq W$ 且 $0 < \delta < \epsilon$ 时发生检测错误.

通过上述分析, 我们可以看出发生错误的原因在于嵌入水印时, 改变的值没有使 C_w 超过特定的阈值, 需要进一步增大嵌入量才能保证检测正确. 针对该问题我们提出迭代嵌入方案, 迭代嵌入就是在上次嵌入仍然不能检测正确时, 再次进行嵌入. 对检测出错的系数进行迭代嵌入, 公式如下:

当 $\text{mod}(m_E, 2) \neq W$,

(1) 如果 $0 \leq \delta < \epsilon$

$$|C_{nw}| = (m_E + 1) \cdot \text{step}_E = (m_E + 1) \cdot |C_{(n-1)w}|^w \cdot t_L^{1-w} \quad (18)$$

$C_{(n-1)w}$ 表示第 $n-1$ 次嵌入水印后得到的系数, 可以看出 $\{|C_{nw}|\}$ 为递增的序列, 极限为 $t_L \cdot (m_E + 1)^{\frac{1}{1-w}}$, 所以经过有限次迭代之后必然会使得 $|C_w|$ 满足 $|C_w| > t_L \cdot \left(m_E + \frac{1}{2}\right)^{\frac{1}{1-w}}$.

(2)如果 $\epsilon' < \delta < 0$

$$|C_{nw}| = (m_E - 1) \cdot \text{step}_E = (m_E - 1) \cdot |C_{(n-1)w}|^w \cdot t_L^{1-w} \quad (19)$$

$\{|C_{nw}|\}$ 为递减的序列,极限为 $t_L \cdot (m_E - 1)^{\frac{1}{1-w}}$,所以经过有限次迭代之后必然会使得 $|C_w|$ 满足 $|C_w| < t_L \cdot (m_E - \frac{1}{2})^{\frac{1}{1-w}}$.具体嵌入流程如图 3 所示.

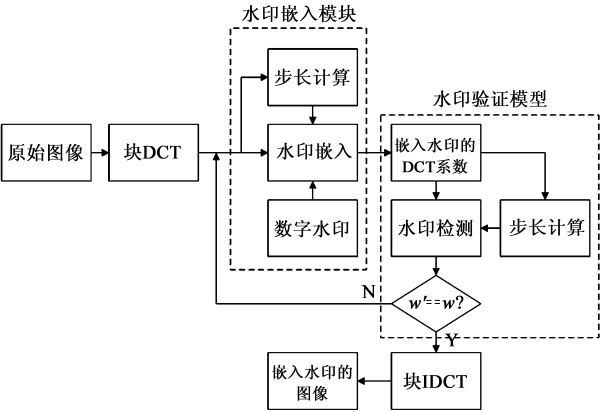


图3 迭代AQIM水印嵌入流程

该迭代嵌入方法仅仅对于那些在检测时会出错的DCT系数进行迭代嵌入而不影响其它的嵌入,需要进行迭代的数据约占 40%,迭代次数不超过 50 次.

5 仿真实验

为证明所提出方案的有效性,我们采用 1000 幅图像进行多次实验,实验中通过调整量化系数的权重使得载体水印比(Document-to-Watermark Ratio, DWR)为 25. DWR 计算公式如下:

$$DWR = 10\log_{10}\left(\frac{\sigma_x^2}{\sigma_\Delta^2}\right) \quad (20)$$

其中 x 代表原始图像, y 代表嵌入水印后的图像,水印为 $\Delta = y - x$.

实验采用归一化相关作为水印检测性能的指标:

$$NC = \frac{\sum_{i=1}^L (2W(i) - 1) \cdot (2W'(i) - 1)}{\sqrt{\sum_{j=1}^L (2W(j) - 1)^2 \sum_{j=1}^L (2W'(j) - 1)^2}} \quad (21)$$

其中, L 为水印长度.

首先,在无干扰情况下我们利用 lena 图像作为载体,比较 AQIM 算法和所提出算法的水印提取情况.图像大小图为 256×256 ,水印为 32×32 的二值图像,水印嵌入前原始图像如图 4(a)所示,(b)为嵌入水印后的图像,水印嵌入后 $DWR = 25$, $PSNR = 38.8387$.图 5(a)为采用 AQIM 算法提取的水印,归一化相关系数为 0.5988,图 5(b)为改进算法提取的水印,与嵌入水印完全一致,

可以看出即使无干扰的情况下,AQIM 也无法提取出完整的水印,而迭代算法很好地解决了该缺陷.



图4

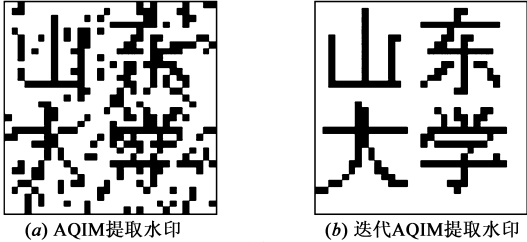


图5

图 6 表示不同强度高斯白噪声干扰下水印的鲁棒性,横坐标为噪声方差,纵坐标为提取水印与嵌入水印之间归一化相关系数,实线表示 AQIM 算法,虚线表示迭代算法,可以看出我们提出的方法在低噪声情况下具有更好的性能,在高噪声情况下,与 AQIM 算法具有近似相同的性能.

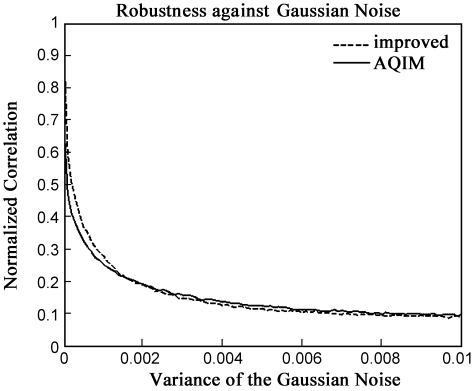


图6 高斯噪声对水印算法的影响

水印鲁棒性另外一个重要体现是对 JPEG 压缩的鲁棒性,对这 1000 幅嵌入水印的图像分别进行压缩因子为 20~100 的 JPEG 压缩,然后检测水印,图 7 中,横坐标表示 JPEG 压缩质量因子,纵坐标为归一化相关系数,可以看出我们的改进方案明显好于原方案.

表 1 其它攻击下水印的鲁棒性

攻击	剪切 1/4	中值滤波 3×3	椒盐噪声 0.005	数值测度变化
迭代 AQIM	0.7471	0.6753	0.6833	1.0000
AQIM	0.5860	0.5276	0.5467	0.7613

其他水印攻击方式下迭代AQIM算法与AQIM算法的水印鲁棒性能比较如表 1 所示,水印存在与否的阈值

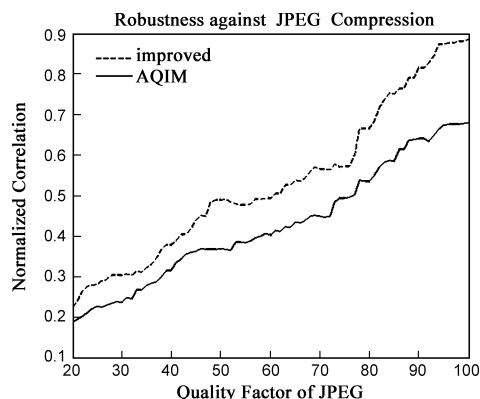


图7 JPEG压缩对水印算法的影响

设为 0.1,可以保证虚警率小于 6.9325×10^{-4} ^[15].

6 结论

针对传统 QIM 算法量化步长单一的缺点, Cox 等提出了 AQIM 水印嵌入算法,该算法较传统 QIM 算法具有更好的鲁棒性,但 AQIM 算法嵌入和检测时采用的步长不同,对此本文没有进行深入的理论分析.本文从理论上详细分析了 AQIM 算法的缺陷,并针对缺陷提出了对该算法改进的迭代策略,实验结果证明该方案较原方案特别是对 JPEG 压缩具有更好的鲁棒性.

参考文献:

- [1] Cox I J, Kilian J, Leighton F T, Shamoon T. Secure spread spectrum watermarking for multimedia[J]. IEEE Transactions on Image processing, 1997, 6(12): 1673 – 1687.
- [2] Podilchuk C I, Wenjun Zeng. Image-adaptive Watermarking using visual models[J]. IEEE Journal of Selected Areas in Communication, 1998, 16(4): 525 – 539.
- [3] Porter J P, Rajan P K. Image adaptive watermarking techniques using models of the human visual system[A]. Proceedings of the 38th Southeastern Symposium on System Theory[C]. Cookeville: Tennessee Technological University, 2006. 354 – 357.
- [4] Rangsaneri Y, Thitimajshima W. Copyright protection of images using human visual masking on DCT-based watermarking[A]. Asia-Pacific Conference on Circuits and Systems[C]. Singapore: APCCAS, 2002. 419 – 422.
- [5] Karybali I, Berberidis K. Blind image-adaptive watermarking[A]. Proceedings of the 2003 10th IEEE International Conference on Electronics, Circuits and Systems[C]. Sharjah: ICECS, 2003. 894 – 897.
- [6] Chen B, Wornell G W. Quantization index modulation: a class of provably good methods for digital watermarking and information embedding[J]. IEEE Transactions on Information Theory, 2001, 47(4): 1423 – 1443.

- [7] Ourique F, Licks V, Jordan R, Perez-Gonzalez F. Angle QIM: a novel watermark embedding scheme robust against amplitude scaling distortions[A]. IEEE International Conference on Acoustics, Speech, and Signal Processing[C]. Philadelphia: ICASSP, 2005. 797 – 800.
- [8] Perez-Gonzalez F, Barni M, Abrardo A, Mosquera C. Rational dither modulation: a novel data-hiding method robust to value-metric scaling attacks[A]. IEEE 6th Workshop on Multimedia Signal Processing[C]. Sienna: IEEE Signal Processing Society, 2004. 139 – 142.
- [9] Saravanan V, Bora P K, Ghosh D. Oblivious image-adaptive watermarking using quantization index modulation[A]. The Eighth National Conference on Communications[C]. Mumbai: Indian Institute of Technology Bombay, 2002. 26 – 27.
- [10] Li Q, Cox I J. Using perceptual models to improve fidelity and provide invariance to volumetric scaling for quantization index modulation watermarking[A]. IEEE International Conference on Acoustics, Speech, and Signal Processing[C]. Philadelphia: ICASSP, 2005, II-1-II-4.
- [11] Li Q, Cox I J. Using perceptual models to improve fidelity and provide resistance to volumetric scaling for quantization index modulation watermarking[J]. IEEE Transactions on Information Forensics and Security, 2007, 2(2): 127 – 139.
- [12] 钟桦, 焦李成. DCT 域半易损水印技术[J]. 计算机学报, 2005, 28(9): 1550 – 1557.
Zhong Hua, Jiao Licheng. DCT based semi-fragile watermarking technique[J]. Chinese Journal of Computers, 2005, 28(9): 1550 – 1557. (in Chinese)
- [13] Watson A B. DCT quantization matrices visually optimized for individual images[J]. Human Vision, Visual Processing and Digital Display, 1993, SPIE-1913: 202 – 216.
- [14] Mannos J L, Sakrison J J. The effects of a visual fidelity criterion on the encoding of image[J]. IEEE Transactions on Information Theory, 1974, IT-4: 525 – 536.
- [15] Lu C S, Liao H M, Kutter M. Denoising and copy attacks resilient watermarking by exploiting prior knowledge at detector[J]. IEEE Transaction on Image Processing, 2002, 11(3): 280 – 292.

作者简介:



凌 洁 女, 1979 年 9 月出生于山东临沂. 2001 年和 2004 年山东大学理学学士和理学硕士学位, 目前为山东大学信息科学与工程学院在读博士研究生, 主要研究方向是数字水印和信息隐藏技术.

E-mail: lingjie@sdu.edu.cn