文章编号:1001-506X(2011)01-0213-04

JPEG 压缩下图像量化水印的鲁棒性估计

曾高荣[1,2], 裘正定[2], 章春娥[2], 孙冬梅[2]
(1. 江西师范大学物理与通信电子学院, 江西 南昌 330022;
2. 北京交通大学信息所, 北京 100044)

摘 要: 当嵌有水印的图像经受压缩时,水印检测可能出现错误。与通过各种仿真测试不同,提出以互信息为代价函数评测图像量化水印联合图像专家组(joint photographic experts group, JPEG)规范压缩下的鲁棒性,该方法以线性高斯模型近似 JPEG 压缩过程,推导了 JPEG 下的度量鲁棒性的互信息函数计算式,并仿真计算不同压缩因子对应的鲁棒性。实验中以分块离散余弦变换(discrete cosine transform, DCT)中频系数为量化载体进行水印嵌入和检测,结果表明当压缩因子变化时,互信息函数与实验误码率之间是匹配的,应用该方法可以评估和预测图像量化水印算法在 JPEG 压缩下的鲁棒性。

关键词: 量化水印; JPEG; 鲁棒性; 互信息
中图分类号: TP 391 **文献标志码**: A **DOI**:10.3969/j.issn.1001-506X.2011.01.43

Evaluation of robustness for image quantization watermarking under JPEG compression

ZENG Gao-rong[1,2], QIU Zheng-ding[2], ZHANG Chun-e[2], SUN Dong-mei[2]
(*1. College of Physics and Communication Electronics, Jiangxi Normal University, Nanchang 330022, China;*
2. Institute of Information Science, Beijing Jiaotong University, Beijing 100044, China)

Abstract: A detectable error may happen when the watermarked image suffered from joint photographic experts group (JPEG) compression. Different from various simulation tests, a mutual information function is defined as a criterion measuring the robustness of image quantization watermarking against JPEG. Based on a linear Gaussian analog model of JPEG compression, a calculation formula of the mutual information function is derived to evaluate the robustness of watermarking under quantization index modulation (QIM) scheme. In the simulation experiment, the mutual information function is calculated in terms of quality factors, and the middle frequency AC coefficients are selected as the host and are quantified according to watermark bit series in the block-based DCT domain. The statistic bit error rate (BER) is derived under the QIM watermarking scheme and JPEG compression. Experiment results show the evaluation conclusion of the mutual information method is matched with that of the empiric BER against the quality factor. With the analog model, the mutual information method can evaluate and predict the robustness of QIM image watermarking under JPEG compression.

Keywords: quantization watermarking; joint photographic experts group (JPEG); robustness; mutual information

0 引 言

多媒体技术和网络技术的飞速发展,使得图像、音频、视频以及文档等数字多媒体内容的分发和传播变得便捷和高效,然而随之突显出来的问题是,数字内容的任意篡改与无损剽窃,这给数字媒体创作者的利益造成潜在威胁。为了克服这个问题,数字水印是一种有效的解决办法。它通过在原始数据中嵌入秘密信息——水印,来实现版权保护、拷贝控制、数字指纹、交易跟踪、内容标识、隐秘通信、视频广播监控等功能[1]。由于多媒体内容数据量大,对其压缩是数据存储和分发过程经常采用的处理方式。在经受压缩处理后检测算法能否正确提取水印,属于水印算法抗压缩的鲁棒性问题。现有的关于水印鲁棒性评估的理论分析主要集中在加性噪声信道背景。如:文献[2]提出的经典扩频水印方案及文献[3]提出的相关改进版本,文献[4]提出的量化索引调制(quantization index modulation, QIM)水印方案及文献[5-6]

收稿日期:2009-10-12; **修回日期**:2010-06-11。
基金项目:国家科技支撑计划项目(2008BAH33B01);国家高技术研究发展计划(863 计划)(2007AA01Z460);博士启动基金资助课题
作者简介:曾高荣(1976-),男,博士,主要研究方向为数字水印与多媒体信息隐藏。E-mail:loch.zeng@gmail.com

提出的相关改进版本。嵌有水印的载体在经受压缩等其他处理后的鲁棒性评估主要通过仿真实验来验证[7-11]，通过联合图像专家组(joint photographic experts group, JPEG)或JPEG2000等压缩测试，统计正确检测率评估算法鲁棒性。这种实例验证的评测方式，测试条件和测试的次数难以把握，并且需要大量的测试数据作为评估依据。

JPEG压缩是数字图像在存储和传递过程中经常采用的一种压缩处理，虽然其量化处理是个非线性过程，但文献[12]和文献[13]分别从率失真的角度和统计关系的角度认为可以用线性函数来模拟量化器的输入输出特性。文献[14]利用这个模拟关系的近似模型，分析了失真补偿抖动调制水印算法中补偿因子和误码率之间的关系。本文借鉴上述JPEG压缩的线性近似模型，分析QIM水印在JPEG下的鲁棒性。本文通过定义一个互信息函数来描述和度量水印系统的鲁棒性，提出一种评测JPEG压缩下水印鲁棒性的方法，并仿真计算QIM水印在JPEG线性近似模型下的鲁棒性。实验以512×512的Lena图像为载体，统计QIM水印算法在JPEG压缩下的误码率来验证该评估方法的有效性。

1 QIM水印及鲁棒性评测模型

1.1 QIM水印方案

一个简单的QIM水印方案可以由一个步长为Δ的标量均匀量化器$Q(s)=\Delta\lfloor s/\Delta \rfloor$，其中，符号$\lfloor\cdot\rfloor$表示下取整；产生两个抖动量化器$Q_b(\cdot)$来实现水印信息的嵌入。

$$Q_b(s)=Q(s-d_b)+d_b,\ b=0,1 \tag{1}$$

式中，b为二元水印信息位；$d_0=-\dfrac{\Delta}{4}$；$d_1=\dfrac{\Delta}{4}$；s为载体系数。

水印嵌入函数为

$$x=\begin{cases}Q_0(s),\ b=0\\ Q_1(s),\ b=1\end{cases} \tag{2}$$

式中，x表示嵌入水印后的信号。当含水印信号x在被检测前受噪声n污染时，接收端收到的信号为

$$y=x+n \tag{3}$$

水印译码函数为

$$\hat{b}=\arg\min_{b\in\{0,1\}} dist(y,\Lambda_b) \tag{4}$$

式中，$dist(y,\Lambda_b)=\min\limits_{s\in\Lambda_b}|y-s|$。

1.2 鲁棒性评测模型

水印过程类似数据通信过程，水印检测类似通信中从接收信号中提取出传输的信号。由通信的理论可知，要从接收内容中提取水印信息，则接收内容必须包含水印的信息。由于JPEG等信号处理攻击的影响，接收内容包含的水印信息可能会减少，接收内容包含多少水印信息量，意味着多大程度上能从检测器中获取水印信息。接收内容包含的水印信息量可由接收内容(用变量Y表示)和水印信息(用变量B表示)之间的互信息$I(B;Y)$表示。互信息越大，包含越多的水印信息，算法的鲁棒性就越强，正确提取水印的可能性就越大。Y，B的实现分别用y，b表示。

从译码规则可看出，检测时无需原始载体和水印信息参与，并且当$|n|<\Delta/4$，水印信息可以无差错被检测，即$\hat{b}=b$。但当$|n|>\Delta/4$时，水印检测可能出现错误。令$T=Y\bmod\Delta$检测时作为分析变量，在高分辨率的假设前提下，载体分布可以看成是平滑的[15]，这样的模减操作对译码不会减少信息[16]，即有$I(B;Y)=I(B;T)$。

当$b=0$时，$y\bmod\Delta=-\dfrac{\Delta}{4}+n$，此时$T$的条件概率密度函数由噪声分布确定，即

$$f_T(t\mid b=0)=f_n\left(t+\frac{\Delta}{4}\right) \tag{5}$$

类似地，当$b=1$时，也可以确定T相应的条件概率密度函数，即

$$f_T(t\mid b=1)=f_n\left(t-\frac{\Delta}{4}\right) \tag{6}$$

当n为高斯噪声时，不妨设其均值为0，方差为σ_n^2，即$n\sim N(0,\sigma_n^2)$，此时由式(5)和式(6)可求得$f_T(t|b=0)$，$f_T(t|b=1)$分别取均值为$-\dfrac{\Delta}{4}$，$\dfrac{\Delta}{4}$，方差为σ_n^2的高斯分布。由式(7)可求得T的概率密度函数为

$$f(t)=p(b=0)f_T(t\mid b=0)+p(b=1)f_T(t\mid b=1)=\frac{1}{2}N\left(-\frac{\Delta}{4},\sigma_n^2\right)+\frac{1}{2}N\left(\frac{\Delta}{4},\sigma_n^2\right) \tag{7}$$

由信息论基础[17]，对b等概率取值0或1，可求得

$$I(B;T)=D(f_{BT}(b,t)\parallel f_T(t)p_B(b))=\frac{1}{2}\sum_{b=0}^{1}D(f_{T|B}(t\mid B=b)\parallel f_T(t)) \tag{8}$$

式中，$D(\cdot)$表示相对熵。

由$f(t)$对称性和b值的均匀性，有

$$D(f_{T|B}(t\mid B=1)\parallel f_T(t))=D(f_{T|B}(t\mid B=0)\parallel f_T(t)) \tag{9}$$

所以有

$$I(B;T)=D(f_{T|B}(t\mid B=0)\parallel f_T(t))=\int f_{T|B}(t\mid B=0)\log_2\left(\frac{f_{T|B}(t\mid B=0)}{f_T(t)}\right)\mathrm{d}t=1-\int\frac{1}{\sqrt{2\pi}\sigma_n}\mathrm{e}^{\frac{-\left(t+\frac{\Delta}{4}\right)^2}{2\sigma_n^2}}\log_2\left(1+\mathrm{e}^{\frac{t\Delta}{2\sigma_n^2}}\right)\mathrm{d}t \tag{10}$$

由式(10)可知，当信道条件为高斯噪声时，只要知道量化步长和噪声方差，则可计算水印通过该信道的鲁棒性。下面通过对JPEG压缩进行高斯线性近似，估算JPEG压缩下水印鲁棒性。

2 JPEG压缩下水印鲁棒性估计

由于JPEG攻击是不可逆的非线性过程，不能像加性噪声那样简单地处理。但是，根据文献[12-14]的研究，可以用一个线性高斯模型来近似JPEG压缩过程。下面先简单介绍JPEG攻击信道的近似模型，然后在这个近似模型的基础上计算度量鲁棒性的互信息函数。

2.1 JPEG攻击信道的近似模型

假设压缩前后数据分别为x和y，数据长度为N，所允许的最大压缩失真为σ_z^2，即

$$\frac{1}{N}\| y-x \|^2 \leqslant \sigma_z^2 \tag{11}$$

从信源编码的角度,有损压缩属于限失真编码问题。根据率失真理论,该编码问题可以表示为[12,17]

$$x = y' + z \tag{12}$$

式中,x 是高斯信源 $N(0,\sigma_x^2)$;y'是 x 对应的信源码字,服从高斯分布 $N(0,\sigma_x^2-\sigma_z^2)$,$z\sim N(0,\sigma_z^2)$是信源编码误差,$z$ 与 y'统计独立,一般的数字水印场合,σ_z^2 远小于 σ_x^2,因此 x 与 y'可看作联合高斯分布,并且在给定 x 的条件下,$y'|x$ 的分布也是高斯的,且条件均值和条件方差为

$$E[y' \mid x] = \frac{\sigma_x^2-\sigma_z^2}{\sigma_x^2}x \tag{13}$$

$$\mathrm{var}\,[y' \mid x] = (\sigma_x^2-\sigma_z^2)\frac{\sigma_z^2}{\sigma_x^2} \tag{14}$$

式(12)可以等价建模为

$$y' = \beta x + z' \tag{15}$$

式中,$\beta=\frac{\sigma_x^2-\sigma_z^2}{\sigma_x^2}$,$z'\sim N(0,\mathrm{var}\,[y'|x])$,并且 z'与 βx 统计独立。

就水印算法抗压缩过程而言,σ_x^2 是知道的,因为信号方差仅仅依赖于嵌入函数,不依赖于压缩算法。因此,在压缩所带来的失真可以预知的情况下,尺度 β 是可确知的。如果在解码器端知道尺度因子,在提取水印信息之前可以作一个预处理,即

$$y = \frac{1}{\beta}y' = x + n \tag{16}$$

式中,$n=z'/\beta$是加性的零均值高斯噪声,并且与 x 独立,其方差为

$$\sigma_n^2 = \frac{\mathrm{var}\,(z')}{\beta^2} = \frac{\sigma_z^2}{1-\sigma_z^2/\sigma_x^2} \tag{17}$$

由式(17)可知,在 σ_x^2/σ_z^2 很大的情况下,此噪声方差趋向于压缩失真 σ_z^2。从这个意义上来说,可以用加性高斯噪声信道来模拟有损压缩信道,但解码器端要有一个前置的缩放。

2.2　JPEG 近似模型下 QIM 水印的鲁棒性估计

将 2.1 节的 JPEG 线性近似模型中等价的高斯噪声 $n\sim N\left(0,\frac{\sigma_z^2}{1-\sigma_z^2/\sigma_x^2}\right)$代入式(10),可以求得 QIM 水印在 JPEG 攻击下的鲁棒性估计。图 1 为压缩失真在[0～12.67]范围内对应的鲁棒性估计结果。压缩失真越大,互信息函数越小,说明正确提取水印的可能性越小。

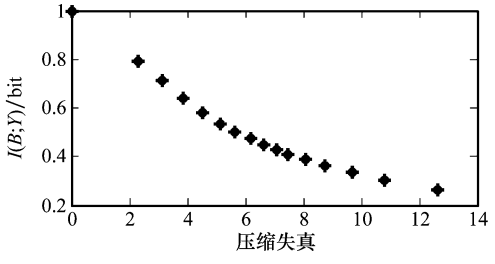

图 1　互信息函数与压缩失真的关系

3　实验与讨论

为了验证 JPEG 压缩下鲁棒性估计的合理性,本文从实验的角度统计 QIM 水印在 JPEG 攻击下的误码率。实验以 512×512 的 Lena 灰度图像为载体图像,用 32×32 的二值图像作为水印信息。先对载体图像作分块 8×8DCT 变换,选择每块中频系数 AC(3,3)作为量化载体嵌入水印信息,然后对生成的含水印图像进行 JPEG 压缩,最后用最小距离解码器提取水印信息。对不同的 JPEG 压缩因子(取值范围为[0,100],压缩因子越大,图像质量越好),计算相应的压缩失真 σ_z^2 和峰值信噪比(peak signal-to-noise ratio, PSNR),图 2 为量化步长取 20 的情况下,不同压缩因子下的 Lena 图像压缩失真和峰值信噪比。从图 2 可知,压缩因子越小,压缩失真越大,峰值信噪比 PSNR 越小。

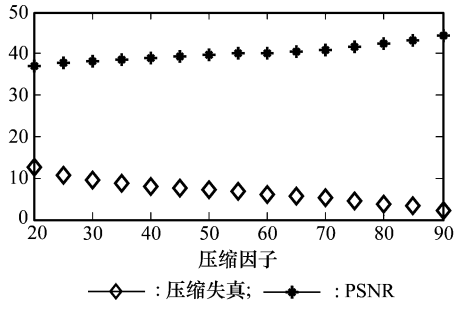

图 2　压缩失真或峰值信噪比与压缩因子的关系

通过 QIM 算法嵌有水印的 Lena 图像,选择 20～100 的质量压缩因子,分别统计检测水印时的误码率,图 3 为检测误码率(bit error rate, BER)随压缩因子变化的曲线示意图。为便于比较,将度量鲁棒性的互信息函数随压缩因子变化的曲线也绘于图 3 中。

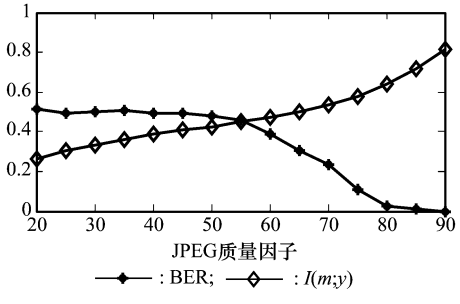

图 3　误码率或 $I(B;Y)$与压缩因子的关系

从图 3 可看出,当压缩因子较大时,如图中 70～90 范围内,误码率随压缩因子的减小而增大,度量鲁棒性的互信息函数随压缩因子减小而减小,在这个范围内,两者对鲁棒性的估计结论是一致的。但是,当压缩因子继续变小后,误码率在 0.5 附近呈现波动现象,这是由于选用固定量化步长时,压缩因子越小,压缩失真越大,不仅图像块高频部分被压缩,甚至一些能量较低的图像块的中频部分包括选中的水印嵌入位置 AC(3,3)也被压缩。这部分压缩后的

AC(3,3)系数被置为 0,由于 0 离两个量化器的距离相等,都为 $\Delta/4$,根据译码规则,提取的水印等可能取 0 或 1,误码率将达到 0.5,此时对应的互信息为限定条件下恢复水印的最小互信息。当互信息低于该最小值时,检测器将无法正确提取水印。至于压缩因子大于 90 的情形,因为压缩率小,丢失的信息也少,互信息较大,此时表现出 QIM 水印算法无差错译码的优势,可以出现零误码率的情况。由于考虑的 JPEG 压缩是有损压缩,随着压缩因子减小,载体丢失的信息增多,载体中包含的水印信息也可能越少,从第 1 节推导的计算公式和图 3 数值仿真的曲线结果看,互信息函数表现出随压缩因子单调减少的趋势。

4 结 论

本文提出了一种 JPEG 压缩下水印鲁棒性的估计方法。该方法首先定义互信息函数作为描述和度量水印系统鲁棒性的代价函数,通过线性高斯信道模拟非线性的压缩过程,推导出 JPEG 信道下 QIM 水印鲁棒性的计算式。该方法只要给定压缩处理参数,无需测试实验就可以估算水印系统的鲁棒性。数值与实验仿真结果表明,互信息函数模型不仅能匹配误码率,而且能单调地匹配图像压缩强度,应用该方法可以评估和预测算法在 JPEG 下的鲁棒性。

参考文献:

[1] Cox I J, Miller M, Bloom J, et al. *Digital wtermarking and steganography*[M]. 2nd ed. Morgan Kaufmann, 2007: 1 - 30.

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

[3] Malvar H S, Dinei A, Florencio F. Improved spread spectrum: a new modulation technique for robust watermarking[J]. *IEEE Trans. on Signal Processing*, 2003, 51(4): 898 - 905.

[4] Chen B, Wornell G. Quantization index modulation: a class of provably good methods for digital watermarking and information embedding[J]. *IEEE Trans. on Information Theory*, 2001, 47(4): 1423 - 1443.

[5] Boyer J P, Duhamel P, Blanc-Talon J. Performance analysis of scalar DC-QIM for zero-bit watermarking[J]. *IEEE Trans. on Information Forensics and Security*, 2007, 2(6): 283 - 289.

[6] Vila-Force J E, Voloshynovskiy S, Koval O. Quantization-based methods: additive attacks performance analysis [J]. *LNCS Trans. on Data Hiding and Multimedia Security*, 2008, 4920: 70 - 90.

[7] Kang X G, Huang J W, Zeng W J. Improving robustness of quantization-based image watermarking via adaptive receiver[J]. *IEEE Trans. on Multimedia*, 2008, 10(6): 953 - 959.

[8] Mairgiotis A K, Galatsanos N P, Yang Y Y. New additive watermark detectors based on a hierarchical spatially adaptive image model[J]. *IEEE Trans. on Information Forensics and Security*, 2008, 3(1): 29 - 37.

[9] Agreste S, Andaloro G. A new approach to pre-processing digital image for wavelet-based watermark[J]. *Journal of Computational and Applied Mathematics*, 2008, 221(2): 274 - 283.

[10] Lin W H, Wang Y R. A blind watermarking method using maximum wavelet coefficient quantization[J]. *Expert Systems with Applications*, 2009, 36(9): 11509 - 11516.

[11] 许文丽,李磊,王育民. 抗噪声、几何失真和 JPEG 压缩攻击的鲁棒数字水印方案[J]. 电子与信息学报, 2008, 30(4): 933 - 936. (Xu W L, Li L, Wang Y M. Robust digital watermarking scheme resistant to gaussian noise, geometric distortion and JPEG compression attacks [J]. *Journal of Electronics & Information Technology*, 2008, 30(4): 933 - 936.)

[12] Chen B, Wornell G. Quantization index modulation: a class of provably good methods for digital watermarking and information embedding [J]. *IEEE Trans. on Information Theory*, 2001, 47(4): 1423 - 1443.

[13] Fei C, Kundur D, Kwong R. The choice of watermark domain in the presence of compression[C]// *Proc. of International Conference on Information Technology: Coding and Computing*, 2001: 79 - 84.

[14] 肖俊, 王颖, 李象霖. 带失真补偿的抖动调制水印算法中的补偿因子研究[J]. 电子学报, 2007, 35(4): 786 - 790. (Xiao J, Wang Y, Li X L. Study on the compensation factor in the watermarking algorithm of dither modulation with distortion compensation[J]. *Acta Electronica Sinica*, 2007, 35(4): 786 - 790.)

[15] Gray R M, Neuhoff D L. Quantization[J]. *IEEE Trans. on Information Theory*, 1998, 44(6): 2325 - 2383.

[16] Pérez-Freire L, Pérez-González F. Security of lattice-based data hiding against the watermarked-only attack [J]. *IEEE Trans. on Information Forensics and Security*, 2008, 3(4): 593 - 610.

[17] Cover T M, Thomas J A. *Elements of information theory*[M]. New York: Wiley, 2006: 140 - 165.