

带失真补偿的抖动调制水印算法中的补偿因子研究

肖 俊,王 颖,李象霖

(中国科学院研究生院信息安全国家重点实验室,北京 100049)

摘 要: 带失真补偿的抖动调制水印算法是一种可以获得大容量的量化水印算法,它以量化失真作为补偿来提高抖动调制水印算法的性能,而其中补偿因子是影响该算法性能的关键因素之一.本文从量化水印算法中最小距离解码器的工作原理出发,提出了衡量带失真补偿的抖动调制水印算法鲁棒性的一般模型;在此基础上,应用率失真理论采用高斯信道来模拟有损压缩信道,得到了在有损压缩下使得误码率最低时,选择补偿因子的方法.理论结果表明有损压缩的强度越大时,应该选择的补偿因子越小.实验结果证明了理论结果的正确性.

关键词: 数字水印;量化;补偿因子;有损压缩;误码率

中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112(2007)04-0786-05

Study on the Compensation Factor in the Watermarking Algorithm of Dither Modulation with Distortion Compensation

XIAO Jun, WANG Ying, LI Xiang-lin

(The Graduated School of the Chinese Academy of Sciences, Information Security State Key Laboratory, Beijing 100049, China)

Abstract: Dither modulation with distortion compensation is a quantization watermarking algorithm that can achieve high capacity, and it uses the quantization error as the compensation to improve the performances of dither modulation, while the compensation factor is one of the key factors that affect its performances. This paper establishes a common model measuring the robustness of the algorithm from the principle of the minimum distance decoder in quantization watermarking algorithms. Then, this paper uses rate distortion theory to model the lossy compression channel, and obtains the method that can get the minimum bit error rate under lossy compression. The theoretical result shows that the larger the compression strength is, the smaller the compensation factor should be. The experimental result confirms the validity of the theoretical result.

Key words: digital watermarking; quantization; compensation factor; lossy compression; bit error probability

1 引言

数字水印因其在知识产权保护、认证等方面的重要应用价值,已成为信号处理领域最热门的研究课题之一^[1~5],也产生了各种水印算法,而基于量化的水印算法由于其容量大、容易实现盲检测等特性已成为研究和应用最多的方法之一.量化技术在水印研究早期就被用于算法设计中,然而直到1999年,Chen和Wornell^[6]才首先从理论角度对基于量化的水印算法进行了分析,提出了量化索引调制(Quantization Index Modulation, QIM)方案.1983年Costa提出“脏纸编码”^[7]理论,从理论上证明水印信道容量与载体信息无关,利用边信息编码可以实现大容量的水印嵌入方案.于是Chen和Wornell利用Costa的思想对QIM进行改进,从而产生了带失真补偿的量化索引调制(Distortion-Compensated QIM, DC-

QIM)^[8],其中可以实现的典型DC-QIM算法是带失真补偿的抖动调制(Distortion-Compensated Dither Modulation, DC-DM)算法^[9].DC-DM算法实现简单,容量和鲁棒性等性能也很好,是一种性能优越的量化水印算法.

在设计DC-DM过程中,量化系数、量化步长和补偿因子的选择决定了算法的性能,其中量化系数和量化步长的选择是所有量化算法都要考虑的问题,它们与算法鲁棒性的关系已经明确.而补偿因子的选择既可以影响算法的容量,也可以影响算法的鲁棒性.Chen和Wornell从容量的角度分析了如何选择最优的补偿因子.2000年Eggers等所提出的标量Costa方案^[10]与DC-DM是等价的,也从容量的角度来考虑补偿因子的选择问题.水印算法的容量是衡量水印算法的一个重要因素,然而在很多实际应用场合,要求在数字水印容量和嵌入失真一定的情况下,算法的鲁棒性最佳.基于量化的方法在容

收稿日期:2005-12-19;修回日期:2007-02-22

基金项目:国家863高技术研究发展计划(No. 2003AA144080)

量方面表现出很好特性,其容量一般可以满足应用要求.此时,如何提高算法的鲁棒性成为焦点,因此如何选择最佳的补偿因子使得水印算法的鲁棒性最佳是一个值得研究的问题.

M. Staring 等^[11]研究了在高斯噪声和均匀噪声攻击下如何选择补偿因子使得 DC-DM 算法鲁棒性最优的问题,但是他们没有对常见的有损压缩(JPEG 压缩)进行研究.本文对 JPEG 压缩进行分析,从最小距离解码器的角度建立误码率模型,提出了使鲁棒性达到最优的 DC-DM 补偿因子的选择方法.

2 DC-DM 水印方案及其鲁棒性度量方法

QIM 算法中的量化步长是影响其性能的一个关键因素.量化步长越大,量化算法的鲁棒性越好,但是相应的嵌入失真也越大.量化算法的失真主要是量化误差引起的,DC-QIM 算法利用量化误差修正 QIM 算法中由于量化引起的失真,实现鲁棒性和失真的折衷.

2.1 DC-DM 水印方案

抖动调制(DM)利用水印信息对载体数据进行抖动,然后采用与水印信息相对应的量化器对经过抖动的载体数据进行量化,从而实现水印信息的嵌入.如下式所示

$$Q^m(x) = \text{round}[(x + d(m)) / J] \times J - d(m) \quad (1)$$

其中 x 表示原始载体数据; J 表示量化步长; m 表示水印信息,如果水印是二进制的,则 $m \in \{0, 1\}$; $d(m)$ 是与 m 相对应的抖动量; $Q^m(\cdot)$ 是与 m 相对应的量化器,对于二进制水印,有两类量化器:量化器 0 ($Q^0(\cdot)$) 和量化器 1 ($Q^1(\cdot)$).图 1 给出了二进制抖动调制的示意图,其中圆圈(\circ)表示量化器 0 得到的量化点,叉点(\times)表示量化器 1 得到的量化点.抖动调制的实现也可以用图 2 所示的框图表示.

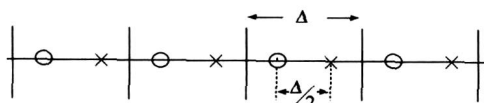


图 1 二进制抖动调制示意图

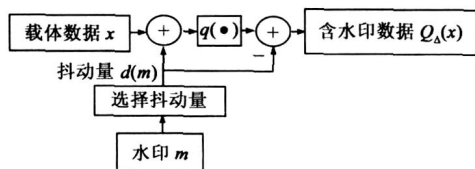


图 2 抖动调制的实现(其中 $q(\bullet)$ 为量化器函数)

利用量化误差对抖动调制进行失真补偿就可以得到性能更优的 DM 算法,即 DC-DM.因此 DC-DM 水印方案的嵌入过程可以用下式表示

$$s = Q^m_c(x) + (1 - \alpha) [x - Q^m_c(x)] \quad (2)$$

其中 s 表示含水印数据; α 表示补偿因子, $\alpha \in [0, 1]$;

$[x - Q^0_c(x)]$ 为量化误差. DC-DM 的实现框图如图 3 所示.

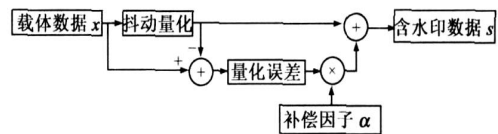


图 3 DC-DM 水印算法的嵌入过程

DC-DM 水印方案在进行解码时,可采用最小距离解码.假设水印信息是二进制的,接收到的数据距离量化器 0 最近时,解码器认为嵌入的水印信息为 0,否则,解码器认为嵌入的水印信息为 1.即解码器的判决按照下式进行

$$\hat{m} = \underset{m \in \{0,1\}}{\text{arg min}} (y - y[m])^2 \quad (3)$$

其中 y 表示解码器接收到的数据; \hat{m} 是提取的水印信息; $y[0]$ 和 $y[1]$ 分别表示采用量化器 0 和量化器 1 对接收到的数据 y 进行抖动调制所得到的量化值.其提取过程如图 4 所示.

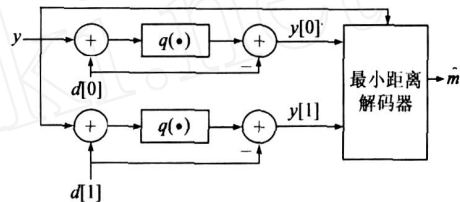


图 4 水印提取过程

2.2 误码率模型

在嵌入水印信息之后,含水印信息经常要遭受各种恶意或者非恶意的攻击,解码器端需要采用一种方式来度量水印算法对抗攻击的鲁棒性.误码率是一种常用的鲁棒性度量方法^[11,12],可以从不同的角度建立误码率模型.M. Staring 等^[11]是从解码器输出值的范围角度来考虑的,Fernando 等^[12]是从量化误差的概率分布角度来考虑的.然而从这两个角度考虑时不直观,而且计算过程较复杂,尤其是 Fernando 等的方法,而本文直接利用提取过程中的最小距离解码器建立误码率的模型,物理概念更清楚、直观,并且易于计算.

假设传输过程中允许的攻击失真限定不超过 $\frac{2}{a}$,即

$$\frac{1}{N} \sum_{i=1}^N (y_i - s_i)^2 \leq \frac{2}{a} \quad (4)$$

其中 s 表示含水印数据, y 表示解码器接收到的数据.

假设 $m \in \{0, 1\}$,即二进制水印信息,并且其中 0、1 出现的概率分别为 p_0 、 p_1 .如果选择误码率来衡量算法对抗攻击失真的鲁棒性,根据最小距离解码器的判决式(3),可以得到解码的错误概率 P_e 为

$$P_e = 1 - p_1 P\{|Q^0(y) - y| > |Q^1(y) - y|\} - p_0 P\{|Q^0(y) - y| < |Q^1(y) - y|\} \quad (5)$$

由图 1 可见,在一个量化单元内,量化器 1 与量化器 0 得到的量化值之间的距离为 $\Delta/2$,则

$$P_e = 1 - p_1 P(|y - Q^1(y)| < \frac{\Delta}{4}) - p_0 P(|y - Q^0(y)| < \frac{\Delta}{4}) \quad (6)$$

因此寻找合适的补偿因子 α 使得鲁棒性最优的过程,就转换为下面的一个条件极值问题,

$$\alpha = \arg \min_{(0,1)} P_e \quad (7)$$

即适当选择 α 使错误概率 P_e 最小.

3 JPEG 攻击信道的等价模型

静止数字图像在其存储和传递过程中经常经历的信号处理是 JPEG 压缩. 与高斯噪声和均匀噪声相比,有损压缩的过程更加复杂,经过处理之后的数据与原始数据之间的关系不像加性噪声情况下简单,因为有损压缩中的量化处理是一个非线性处理.但是,可以通过线性函数来对这一非线性处理进行模拟^[13,14], Chen^[13]从信息率失真的角度来模拟有损压缩, Fei 等^[14]从使量化器输出与线性模拟之间有相同的统计关系的角度来分析有损压缩.从统计关系的角度进行模拟的方法适合于非盲的采用相关检测来提取水印信息的场合,从信息率失真的角度来模拟有损压缩更适用于水印信息的盲提取.本文研究的量化算法可以实现盲提取,所以应用率失真理论采用高斯信道来模拟有损压缩信道.

对于常见的多媒体数据来说,压缩时允许产生一定的失真,只要解压缩之后的数据在一定程度上可以被感官接受即可.因此有损压缩对应于信息论中的限失真编码.假设嵌入水印之后的数据 s 是零均值的白高斯信源信号,有损压缩算法所允许的最大失真为 $\frac{\Delta}{2}$,即

$$\frac{1}{N} \sum_{i=1}^N (y_i - s_i)^2 \leq \frac{\Delta^2}{4} \quad (8)$$

根据率失真理论,此有损压缩所对应的限失真编码问题可以通过以下测试信道来表示^[13,15]

$$s = y + z \quad (9)$$

式中 s 是高斯信源 $N(0, \frac{\Delta^2}{4})$; y 是 s 相对应的信源码字,服从高斯分布 $N(0, \frac{\Delta^2}{4} - \frac{\Delta^2}{4})$; $z \sim N(0, \frac{\Delta^2}{4})$ 是信源编码误差. z 是与 y 独立的,因此 s 与 y 是联合高斯分布的,并且在给定 s 的情况下, y 的条件均值和条件方差为

$$E[y | s] = \frac{\frac{\Delta^2}{4} - \frac{\Delta^2}{4}}{\frac{\Delta^2}{4} - \frac{\Delta^2}{4}} s \quad (10)$$

$$\text{var}[y | s] = (\frac{\Delta^2}{4} - \frac{\Delta^2}{4}) \frac{\Delta^2}{4}$$

因此,可以用下式来表示式(9)所描述的测试信道

$$y = s + z, z \sim N(0, (\frac{\Delta^2}{4} - \frac{\Delta^2}{4})) \quad (11)$$

其中

$$= \frac{\frac{\Delta^2}{4} - \frac{\Delta^2}{4}}{\frac{\Delta^2}{4} - \frac{\Delta^2}{4}} \quad (12)$$

并且 z 与 s 统计独立.

因此,与此类型的有损压缩等价的线性模型是:嵌入水印之后的数据首先与一个尺度因子相乘,然后加上一个独立的高斯噪声.由式(12)可见,在压缩所带来的失真可以预知的情况下,尺度因子是已知的(假设 $\frac{\Delta^2}{4}$ 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).并且,如果在解码器端知道尺度因子,在提取水印信息之前可以做一个预处理,即

$$y = \frac{1}{\alpha} y = s + n \quad (13)$$

其中, $n = z/\alpha$ 是加性的零均值高斯噪声,并且与 s 独立,其方差为

$$\frac{\Delta^2}{n} = \frac{\text{var}[z]}{\alpha^2} = \frac{\frac{\Delta^2}{4}}{1 - \frac{\Delta^2}{4} \frac{\Delta^2}{4}} \quad (14)$$

由式(14)可见,在 $\frac{\Delta^2}{4} \frac{\Delta^2}{4}$ 很大的情况下,此噪声方差趋于压缩失真 $\frac{\Delta^2}{4}$.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.

4 有损压缩下使得误码率最低的补偿因子

采用第三节中的高斯信道来模拟有损压缩信道,要计算式(7)的极值仍然是一个很困难的问题,因为噪声强度与量化器的输出有很大的关系.根据量化器的特点和噪声强度的不同,这里将解码时产生误码与否分为如下两类:第一,不产生误码的情况,它又可以分为两种情况,(1)噪声较弱,解码时,量化器可以将接收到的数据量化到正确的量化值;(2)噪声很强,解码时,量化器将接收到的数据量化到与正确量化值不同但与正确量化值同类的量化值上,此时也不会产生误码;第二,产生误码的情况,噪声较强,解码时,量化器将接收到的数据量化到与正确量化值不同类的量化值上.

根据以上分析,不失一般地,假设嵌入的水印信息为 0,则此时的误码率为

$$P_e = 1 - P(|y - Q^0(y)| < \frac{\Delta}{4})$$

$$= 1 - \int_{-\frac{\Delta}{4}}^{\frac{\Delta}{4}} P\left[\left(k - \frac{1}{4}\right) (1 - \alpha)(x - Q^0) + n < \left(k + \frac{1}{4}\right)\right] dx \quad (15)$$

式中 n 代表噪声, Z 表示整数集.

根据 2.1 节所述,二进制水印需要两类量化器来实现嵌入,由同一类量化器得到的所有量化值称为属于相同类的量化值.

上述第一类中的两种情况分别对应于 $K=0$ 和 $K>0$ 的情况. 如果进行 K 阶近似, 则误码率为

$$P_e^K = 1 - \sum_{k=-K}^K P \left[\left(k - \frac{1}{4} \right) (1 - \rho)(x - Q^0) + n < \left(k + \frac{1}{4} \right) \right] \quad (16)$$

利用与 M. Staring 相类似的计算方法^[11], 先求 $(1 - \rho)(x - Q^0)$ 一定时的条件错误概率, 然后积分获得最后的误码率, 可以得到 $K=0$ 时的误码率为:

$$P_e^0 = 1 - \frac{1+2(1-\rho)}{4(1-\rho)} \operatorname{erf} \left[\frac{1+2(1-\rho)}{4\sqrt{2}n} \right] + \frac{1-2(1-\rho)}{4(1-\rho)} \operatorname{erf} \left[\frac{1-2(1-\rho)}{4\sqrt{2}n} \right] + \frac{\sqrt{2}n}{(1-\rho)\sqrt{\rho}} \left[\exp \left[-\frac{2(1+2(1-\rho))^2}{16n^2} \right] - \exp \left[-\frac{2(1-2(1-\rho))^2}{16n^2} \right] \right] \quad (17)$$

其中 $\frac{2}{n} = \frac{2}{1 - \frac{2}{s}} \frac{1}{s}$, 此时寻找使得鲁棒性最强 (即误码率最低) 的就转化为

$$= \arg \min_{\rho \in [0,1]} P_e^0 \quad (18)$$

直接求解式(18)很困难, 这里仅仅给出其数值解, 如图 5 中实线所示, 其中横轴 WNR, 即 Watermark-to-Noise Ratio, 是指水印噪声比; 纵轴代表补偿因子. 从图 5 可见, 为了使得误码率最小, JPEG 压缩失真越大时, 最优补偿因子越小.

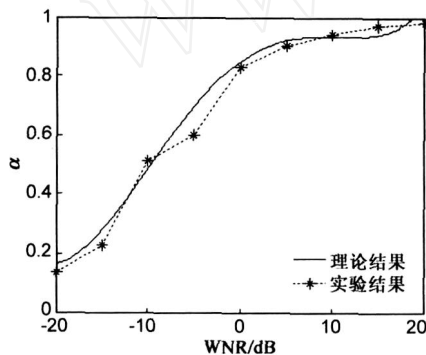


图 5 不同 WNR 下的最优补偿因子

5 仿真实验

为了说明上述误码率模型及对有损压缩信道的模拟的合理性, 本文从实验的角度对最优补偿因子进行研究, 以 256×256 的 Lena 灰度图像作为载体图像, 用 32×32 的二值图像作为水印信息. 实验中先对载体图像做分块 DCT 变换, 选择每块的低频系数嵌入水印信息, 然后进行 JPEG 压缩, 最后用最小距离解码器提取水印信息. 在不同的水印噪声比时, 搜索使得误码率最小的最优补偿因子, 实验结果如图 5 中虚线所示. 图 5 的实验结果说明: 为了使得误码率最小, JPEG 压缩失真越大时, 最优补偿因子越小, 这与理论结果基本一致.

但从图 5 的实验结果与理论计算的比较可见, 理论上的最优补偿因子与实际的最优补偿因子之间存在一定的误差, 这主要是因为, 在理论计算时, 假设嵌入水印之后的数据符合高斯分布, 而实验时所采用的实际图像数据不满足此假设.

在实际应用中, 多采用压缩因子来度量压缩强度, 因此本文也从实验中得到了不同压缩因子下的最优补偿因子, 如图 6 所示, 其中 Q 代表 JPEG 压缩因子, Q 越小, 压缩失

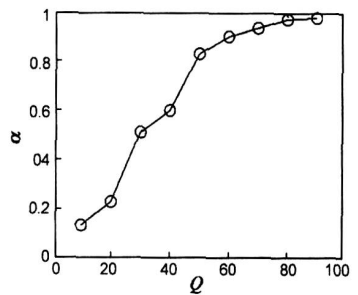


图 6 不同压缩强度下的最优补偿因子
真越大, 图 6 中的结果显示应该选择的补偿因子也越小, 这与上面的分析一致.

6 结论

本文首先在分析最小距离解码器工作原理的基础上, 对 DC-DM 水印算法的误码率进行了建模, 得到了衡量算法鲁棒性的一般模型; 其次采用高斯信道来模拟有损压缩信道, 得到了有损压缩下使得误码率最低的最优补偿因子, 理论结果与实验结果均说明有损压缩的强度越大时, 应该选择的补偿因子越小.

参考文献:

- [1] Cox I J, Miller M L, Bloom J A. Digital Watermarking [M]. Mordan Kaufmann Publishers, 2002. 5 - 15.
- [2] 孙圣和, 陆哲明. 数字水印处理技术 [J]. 电子学报. 2000, 28(8): 85 - 90.
Sun Sheng-he, Lu Zhe-ming. Digital watermarking techniques [J]. Acta Electronica Sinica, 2000, 28(8): 85 - 90. (in Chinese)
- [3] 张冠男, 王树勋, 温泉. 一种嵌入可读水印的自适应盲水印算法 [J]. 电子学报. 2005, 33(2): 308 - 312.
Zhang Guan-nan, Wang Shu-xun, Wen Quan. An adaptive blind watermarking algorithm to embed readable watermark [J]. Acta Electronica Sinica, 2005, 33(2): 308 - 312. (in Chinese)
- [4] 陆哲明, 吴昊天, 刘忠仁, 等. 一种用于版权通知和保护的多功能彩色图像水印算法 [J]. 电子学报. 2004, 32(5): 778 - 781.
Lu Zhe-ming, Wu Hao-tian, Liu Zhong-ren, et al. A multipurpose color image watermarking algorithm for copyright notification and protection [J]. Acta Electronica Sinica, 2004, 32(5): 778 - 781. (in Chinese)
- [5] 张毅刚, 焦玉华, 牛夏牧, 等. 基于指纹特征数字水印算法的身份认证技术研究 [J]. 电子学报. 2004, 31(B12): 2131

- 2134.
Zhang Yi-gang, Jiao Yu-hua, Niu Xi-mu, et al. Authentication based on fingerprint feature watermarking algorithm [J]. Acta Electronica Sinica, 2004, 31 (B12) :2131 - 2134. (in Chinese)
- [6] Chen B, Wornell G W. Provably robust digital watermarking [A]. In Proc of SPIE. Volume 3845 of Multimedia Systems and Applications II [C]. San Jose, USA, 1999, 3845:43 - 54.
- [7] Costa M H. Writing on dirty paper [J]. IEEE Trans on Information Theory, 1983, 29(3) :439 - 441.
- [8] Chen B, Wornell G W. Preprocessed and postprocessed quantization index modulation methods for digital watermarking [J]. Proc of SPIE: Security and Watermarking of Multimedia Contents II, 2000. 48 - 59.
- [9] Chen B, Wornell G W. 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.
- [10] Eggers J J, Su J K, Girod B. A blind watermarking scheme based on structured codebooks [A]. In: Proc of IEEE Conf on Secure Images and Image Authentication [C]. London, UK, 2000. 1 - 6.
- [11] Staring M, Job Oostveen, Ton Kalker. Optimal distortion compensation for quantization watermarking [J]. Image Processing, 2003, 2:727 - 730.
- [12] Fernando Perez-Gonzalez, Pedro Comesaña, Felix Balado. Dither modulation data hiding with distortion compensation: exact performance analysis and an improved detector for JPEG attacks [A]. In International Conference on Image Processing [C]. Barcelona, Spain, 2003. 503 - 506.
- [13] Chen B. Design and analysis of digital watermarking, information embedding, and data hiding systems [D]. England: University of Cambridge, 2000.
- [14] Fei C, Kundur D, Kwong R. The choice of watermark domain in the presence of compression [A]. Proceedings International Conference on Information Technology: Coding and Computing [C]. Los Alamitos, Calif IEEE CS Press, 2001. 79 - 84.
- [15] Cover T M, Thomas J A. Elements of Information Theory [M]. New York, John Wiley & Sons, 1991.

作者简介:



肖俊男, 1981年出生于湖北荆门, 中国科学院研究生院博士研究生. 主要研究领域为图像处理与数字水印技术等.

E-mail: xiao.jun@mails.gucas.ac.cn



王颖女, 博士, 1969年出生于黑龙江, 中国科学院研究生院教授, 计算与通信工程学院常务副院长. 主要研究领域为数字通信、图像处理及信息安全等. E-mail: ywang@gucas.ac.cn

李象霖 男, 1938年出生于北京, 中国科学院研究生院教授. 主要研究领域为图像处理.