对基于量化水印的两频带滤波攻击的估计

王津申，王执铨

(南京理工大学自动化学院 南京 210094)

【摘要】提出了一种基于量化水印的两频带幅值比例攻击的估计算法。基于量化的水印算法在有加性噪声攻击的情况下可以达到信道容量，然而对线性时不变滤波攻击没有鲁棒性。该文集中考虑一种使用滤波器组调整信号频谱的多频带幅值比例攻击，给出受攻击信号的概率密度函数(PDF)模型；使用这个PDF模型的简化近似；给出两频带滤波攻击幅值比例因子的最大似然估计方法。以合成的音频信号进行实验，结果显示出所提出的估计技术的有效性。

关 键 词 最大似然估计； 多频带； 量化; 水印

中图分类号 TP 309 **文献标识码** A

Two-Band Amplitude Scale Estimation for QIM Watermarks

WANG Jin-shen，WANG Zhi-quan

(School of Automation, Nanjing University of Science & Technology Nanjing 210094)

Abstract This paper presents a scheme for estimating two-band amplitude scale attack within a quantization-based watermarking context. Although quantization-based watermarking schemes achieve the channel capacity in terms of additive noise attacks, these schemes are not robust against linear time invariant filtering attacks. We concentrate on a multi-band amplitude scaling attack that modifies the spectrum of the signal using an analysis/synthesis filter bank. First we derive the probability density function (PDF) of the attacked data. Second, using a simplified approximation of the PDF model, we derive a maximum likelihood (ML) procedure for estimating two-band amplitude scaling factor. Finally, experiments are performed with synthetic audio signals showing the good performance of the proposed estimation technique under realistic conditions.

Key words maximum likelihood estimation; multi-band; quantization; watermarking

基于量化理论的水印算法作为一种信息理论研究的结果[1]最近被提出来。对于加性噪声攻击，该算法已经被证明比传统的扩频水印性能更好。然而，基于量化的水印算法对线性时不变滤波攻击没有鲁棒性。对滤波操作没有鲁棒性是一个严重的缺点，因为许多对图像和音频的正常操作都明确地使用滤波器。在立体声系统中的低音、高音调节是简单的滤波操作应用。还有许多其他的操作，即使没有明确使用滤波器，但是可以看作是滤波器的模型。如音频通过扩音器的播放可以近似为一个滤波操作。本文集中讨论了多频带幅值比例问题结合加性噪声攻击。

1 多频带幅值比例攻击问题

水印系统的结构图如图1所示。

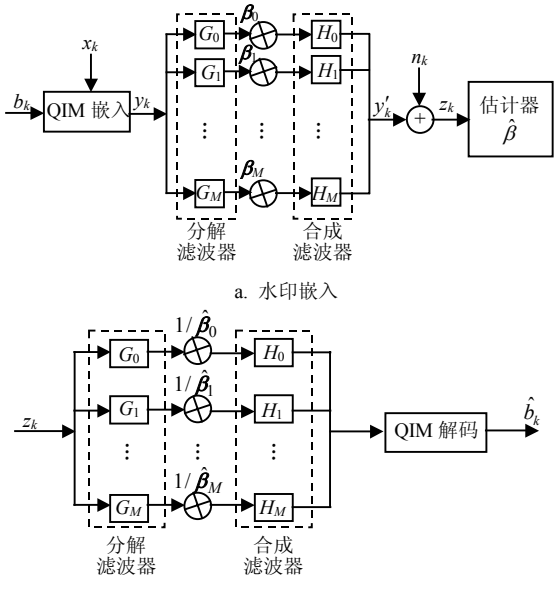


图1 系统结构图

收稿日期：2006 – 04 – 25；修回日期：2006 – 10 – 11
基金项目：国家自然科学基金(60374066)
作者简介：王津申(1978 –)，男，博士生，主要从事信息隐藏与信号处理方面的研究.

系统分为：基于量化的水印嵌入和解码、多频带幅值比例攻击、估计器和校正器。基本的嵌入和解码过程是基于文献[1]提出的具有失真补偿的量化索引调制水印算法[1]。在水印编码器中，$b_k\{0,1\}$表示嵌入在载体信号中的信息比特；$\boldsymbol{x}$是载体信号，其方差是σ_x^2；$\boldsymbol{y}$是加水印后的信号。

多频带幅值比例攻击包含一个分解、合成滤波器组和存在于每个频带中的比例因子。另外，设均值为0，方差为σ_N^2的加性白噪声$\boldsymbol{n}$加入到滤波器的输出信号$\boldsymbol{y}'$中，其中$\boldsymbol{n}$与$\boldsymbol{y}'$独立。设$\boldsymbol{\beta}=[\boldsymbol{\beta}_1,\ \boldsymbol{\beta}_2,\cdots,\boldsymbol{\beta}_i,\cdots,\boldsymbol{\beta}_M]$表示多频带幅值比例因子向量，其中对所有的$i=1,2,\cdots,M$，$\boldsymbol{\beta}_i>0$；$M$是频带数目。根据这个模型，$\boldsymbol{y}'$的Fourier变换可以写为：

$$\begin{aligned}Y'(\mathrm{e}^{\mathrm{j}\omega})=T(\mathrm{e}^{\mathrm{j}\omega})Y(\mathrm{e}^{\mathrm{j}\omega})=\\ [\beta_0G_0(\mathrm{e}^{\mathrm{j}\omega})H_0(\mathrm{e}^{\mathrm{j}\omega})+\beta_1G_1(\mathrm{e}^{\mathrm{j}\omega})H_1(\mathrm{e}^{\mathrm{j}\omega})+\cdots+\\ \beta_MG_M(\mathrm{e}^{\mathrm{j}\omega})H_M(\mathrm{e}^{\mathrm{j}\omega})]Y(\mathrm{e}^{\mathrm{j}\omega})\end{aligned}\tag{1}$$

式中 $G(\mathrm{e}^{\mathrm{j}\omega})$和$H(\mathrm{e}^{\mathrm{j}\omega})$分别是低通滤波器和高通滤波器的传递函数。那么，受攻击向量为：

$$\boldsymbol{z}=\boldsymbol{y}'+\boldsymbol{n}\tag{2}$$

2 PDF模型

本文导出滤波器输出信号$\boldsymbol{y}'$的PDF模型及噪声攻击后信号$\boldsymbol{z}$的PDF模型，两个PDF模型是多频带幅值比例因子向量$\boldsymbol{\beta}$的函数。从式(1)可以看出传递函数$T(\mathrm{e}^{\mathrm{j}\omega})$含有$\boldsymbol{\beta}$的信息。因为目标是导出频带幅值比例攻击后信号$\boldsymbol{y}'$的PDF模型，所以使用式(1)的时域表达更合适。那么$\boldsymbol{y}'$可以表示为：

$$\begin{aligned}\boldsymbol{y}'(k)=t(k)*y(k)=\\ t(0)y(k)+t(1)y(k-1)+\\ t(2)y(k-2)+\cdots+t(k)y(0)\end{aligned}\tag{3}$$

式中 $t(k)$表示$T(\mathrm{e}^{\mathrm{j}\omega})$的脉冲响应。注意估计器已知脉冲响应$t(k)$。

可以看出整体的滤波操作的输出是加水印后信号$\boldsymbol{y}$采样点的加权和。为了导出多频带幅值比例攻击后信号$\boldsymbol{y}'$的PDF函数，设载体信号和加水印后信号都是独立同分布(i. i. d.)的信号。需要指出的是，该假设只是真实情况的近似。因此，多频带幅值比例攻击信号的样本点y_k'是独立同分布的随机变量Y_{yk}的加权和。在文献[2]中已经给出加水印后信号$\boldsymbol{y}$的PDF模型，即$f_Y(y)$。那么，可以给出$\boldsymbol{y}'$的PDF模型：

$$f_{Y'}(\boldsymbol{y}')=\frac{1}{|t(0)|}f_Y\left(\frac{y}{t(0)}\right)*\frac{1}{|t(1)|}f_Y\left(\frac{y}{t(1)}\right)*\cdots*\frac{1}{|t(k-1)|}f_Y\left(\frac{y}{t(k-1)}\right)\tag{4}$$

为了简化多频带幅值比例攻击问题，可考虑使用一个简化的模型，即两频带滤波器组，并且比例因子仅出现在高频带，即比例因子向量$\boldsymbol{\beta}=[1,\beta]$。

考虑加性噪声$\boldsymbol{n}$，可以得到受噪声攻击后信号$\boldsymbol{z}$的PDF模型：

$$f_Z(z)=f_N(n)*f_{Y'}(y')\tag{5}$$

其中卷积*是根据加性噪声$\boldsymbol{n}$和$\boldsymbol{y}'$的独立性。

3 最大似然估计

可以根据式(5)使用最大似然估计来解决这个问题。根据文献[3]中定义3，比例因子β的最大似然估计$\hat{\beta}$是：

$$\hat{\beta}=\arg\max_{\beta}f_{Z_1,Z_2,\cdots,Z_N}(z_1,z_2,\cdots,z_N\mid\beta)\tag{6}$$

然而，从z_k的概率密度函数导出联合概率密度函数很困难。在导出式(4)时，假设多频带幅值比例攻击后信号向量具有独立同分布的元素，因此可以合理的认为向量$\boldsymbol{z}$也近似地具有独立同分布的元素。

因此，联合概率密度函数可以近似地写作边缘概率密度函数的乘积，也就是：

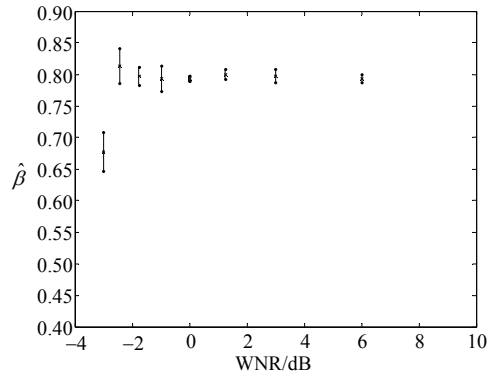
$$\begin{aligned}\hat{\beta}=\arg\max_{\beta}\prod_{i=1}^{N}f_{Z_1}(z_i\mid\beta)=\\ \arg\max_{\beta}\sum_{i=1}^{N}\lg f_{z_i}(z_i\mid\beta)\end{aligned}\tag{7}$$

4 实验结果

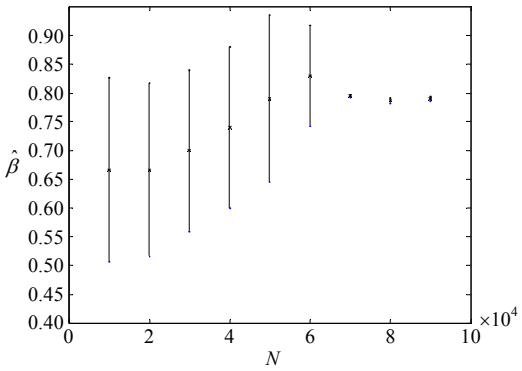
本文从水印噪声比(watermark to noise ratio，WNR)、参数β以及所需要的信号样本数目N三方面以检验所提出方法的估计准确性。实验中所用的载体信号是合成的音频信号，采样频率为48 kHz。

图2给出关于WNR和信号样本数目N的估计结果。设在估计端载体信号的PDF模型是Laplacian模型，其均值为0，方差等于载体信号、水印信号和攻击信道中噪声信号方差的和，即$L(0,\sigma_X^2+\sigma_W^2+\sigma_N^2)$。这是根据实际情况作出的合理假设，因为解码器可以使用接收到的数据并且可以估计其方差。实际上大多数音频信号具有类似于Laplacian的PDF模型。图3给出用不同的音频信号作为载体信号时$\beta-\hat{\beta}$对β的函数。

图中，十字形代表估计均值，直线表示在两个方向上估计的标准差，DWR= 15 dB，估计端信号PDF模型是$X\sim L(0,\sigma_X^2+\sigma_W^2+\sigma_N^2)$。



a. 不同的WNR对应的 $\hat{\beta}$



b. 不同的信号样本数目N对应的 $\hat{\beta}$

图2　不同的WNR和信号样本数目N对应的 $\hat{\beta}$

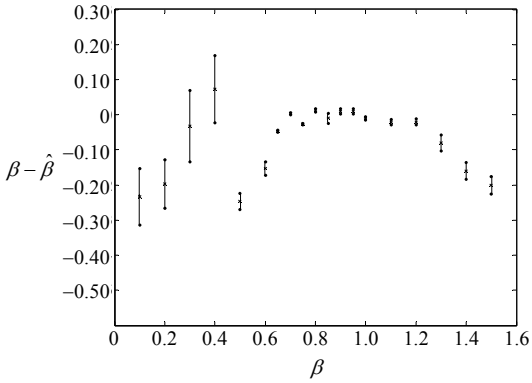


图3　不同的β所对应的 $\beta-\hat{\beta}$

图中，十字形代表估计均值，直线表示在两个方向上估计的标准差，DWR=15 dB，WNR=0 dB，估计端信号PDF模型是 $X \sim L(0,\sigma_X^2+\sigma_W^2+\sigma_N^2)$。

5　结 论

本文给出一种估计两频带幅值比例因子的最大似然估计方法。该方法对参数 β 在加性噪声的情况下和在相对较大的取值范围里都有较好的估计性能。缺点是为了可靠的估计 β，需要相对较大数量的信号采样；另由于该方法计算量较大目前还不适用于实时应用。

参 考 文 献

[1] CHEN B, WORNELL G. Quantization index modulation: A class of provably good methods for digital watermarking and information embedding[J]. IEEE Transactions on Information Theory, 2001, 47:1423-1443.

[2] SHTEREV I, LAGENDIJK R. Maximum likelihood amplitude scale estimation for quantization-based watermarking in the presence of dither[C]//SPIE Security, Steganography, and Watermarking of Multimedia Contents VII. San Jose CA: [s.n.], 2005.

[3] POOR H. An Introduction to signal detection and estimation[M]. [S.l.]: Springer-Verlag, 1994.

[4] EGGERS J, BAUML R, GIROD B. Estimation of amplitude modifi- cations before SCS watermark detection[C]//SPIE Security and Watermarking of Multimedia Contents IV. San Jose CA, USA: [s.n.], 2002: 387-398.

[5] MILLER M, DOERR G, COX J. Dirty-paper trellis godes for water- marking[C]//IEEE International Conference on Image Processing. Rochester, USA: [s.n.], 2002.

[6] BRADLEY B. Improvement to CDF grounded lattice codes[C]//SPIE Security, Steganography, and Watermarking of Multimedia Contents VI. San Jose CA, USA: [s.n.], 2004.

[7] COSTA M. Writing on dirty paper[J]. IEEE Transactions on Information Theory, 1983, 29(3): 439-441.

[8] 王　卓, 赵千川. 基于能量量化的音频水印算法[J]. 计算机工程与应用, 2004, 26(40): 48-51, 55.

[9] 熊淑华, 卜　云, 周激流, 等. 一种基于小波变换的非均匀量化索引调制水印算法[J]. 四川大学学报(工程科学版), 2006, 38(3): 140-143.

[10] 王　丽, 赵媛媛, 赵　耀. 一种抗剪切的鲁棒数字水印[J]. 数据采集预与处理, 2006, 3(21): 330-333.

编　辑　张　俊