第 35 卷 第 7 期 计 算 机 工 程 2009 年 4 月
Vol.35 No.7 Computer Engineering April 2009
·安全技术· 文章编号：1000—3428(2009)07—0147—03 文献标识码：A 中图分类号：TP309.2

基于逼近信号特征抗 MP3 攻击的音频零水印

吴 翔[1]，杨晓元[1,2]，张敏情[1]，周鸿飞[1]
(1. 武警工程学院电子技术系网络与信息安全武警部队重点实验室，西安 710086；
2. 西安电子科技大学综合业务网国家重点实验室，西安 710071)

摘 要：提出一种基于逼近信号统计特征和线性伸缩恢复技术的音频数字零水印算法。对原始水印采用重复码进行纠错编码，将密钥通过伪随机序列发生器产生与重复编码等长的 PN 序列 P，用 P 对编码后的水印进行调制以提高水印检测的正确率。检测时采用线性伸缩恢复技术来消除时间轴上线性伸缩带来的影响，并实现了盲检测。实验结果证明，该算法对于各种攻击尤其对剪切和 MP3 攻击具有较好的鲁棒性。

关键词：音频数字水印；零水印；纠错码；统计特征；线性伸缩恢复

Audio Zero Watermark Based on Feature of Approximation Signal for Avoiding MP3 Attack

WU Xiang[1], YANG Xiao-yuan[1,2], ZHANG Min-qing[1], ZHOU Hong-fei[1]
(1. Network and Information Security Key Lab of the APF, Electronics Technology Dept., Engineering College of the APF, Xi'an 710086;
2. Sate Key Lab. of Integrated Service Networks, Xidian University, Xi'an 710071)

【Abstract】This paper presents an audio zero-digital watermark algorithm based on statistical feature of approximation signal and the technology of restoration of the linear scaling. The original watermark is error corrected coded with repetition code. In order to enhance the correct probability of detecting, the recoded watermark is modulated with PN sequence P which is produced by the key through Pseudo-random sequences generator, with the same length of the recoded code. During the process of detecting, the technology of restoration of the linear scaling is used to eliminate the influence brought by linear scaling on time axis, and a blind detecting is realized. Experiment confirms the expected high robustness to many kinds of attacks especially to cutting-attack and MP3-attack.

【Key words】 audio digital watermark; zero watermark; error correction code; statistical feature; restoration of the linear scaling

1 概述

目前提出的数字水印算法，多数都是在时/空域或频域上对原始数字作品进行修改来嵌入水印信息，而这些信息的嵌入都会导致一定程度的失真，造成数字水印不可感知性和鲁棒性之间的矛盾。“零数字”水印[1]作为解决这对矛盾的有效方法得到了研究者的广泛关注。但目前对其研究主要集中在图像领域，且“嵌入”的水印大都是无意义的。无意义的水印只能通过统计的方法来判断水印是否存在，不能直观地给出版权标志信息。

针对以上问题，本文利用逼近信号小波系数的统计特征和线性伸缩恢复技术向音频数据“嵌入”有意义零水印，算法不修改原始作品的任何数据，具有良好的不可感知性，且实现了盲检测。

2 嵌入算法

2.1 水印调制

为增强算法的鲁棒性，实现水印的盲检测，提高水印系统的可靠性，本文采用的水印调制策略为如下：

(1)对原始水印 W 中的每一位 w_i ($0<i\leqslant N$ ，其中，N 为水印数据的长度)进行重复纠错编码，设重复编码长度为 L 即得水印

$$W'=\left\{w'_k \middle| w'_{(i-1)\times L+j}=w_i,(0<i\leqslant N,\ 0<j\leqslant L)\right\}$$

(2)将密钥 K 通过伪随机序列发生器产生与重复编码长度等长(即为 L)的 PN 序列 $P=\left\{p_j \middle| 0<j\leqslant L\right\}$，$p_j\in\{0,1\}$；

(3)用 P 调制经重复纠错编码后的水印序列 W' 即得到调制后的水印序列，设调制后的水印序列为

$$W_m=\left\{w_m \middle| w_m=w'_{(i-1)\times L+j}\oplus p_j,\ (0<i\leqslant N,\ 0<j\leqslant L)\right\}$$

其长度为 NL。

2.2 水印嵌入

本文利用小波变换后的逼近信号统计特征与给定阈值之间的关系来表示单个水印比特，将水印信息“嵌入”音频作品中，并获得一个索引向量，再根据索引来提取水印信息。该算法不修改原作品的任何数据，具有良好的不可感知性，并且实现了盲检测。

小波变换是一种新型的信号处理技术，尤其适用于对音频这样的非平稳信号进行分析和处理。它在时域和频域的局部化定位观测与人耳的听觉分辨特性很类似[2]。在音频分析

基金项目：国家自然科学基金资助项目(60573032)；国家部委基金资助项目
作者简介：吴 翔(1983－)，男，硕士研究生，主研方向：数字水印；杨晓元、张敏情，教授；周鸿飞，硕士研究生
收稿日期：2008-08-02 **E-mail：**wuxiangwj@sina.com

和分类中，为减少特征矢量的维数，文献[3]采用每个子带中小波系数绝对值的平均值作为小波域的统计特征(这些特征提供音频信号频率分布的信息)来生成特征矢量。为便于水印嵌入，本文直接采用逼近信号中的小波系数平均值而非其绝对值的平均值作为统计特征。该统计特征从逼近信号的小波系数计算得到，这些系数又代表音频信号感知上最重要的低频分量，因此，完全可认为它对一般信号处理如 MP3 压缩、低通滤波等是稳定的[2]。而且，由于相邻音频样本点或小的音频片断之间具有高度的相关性，随机剪切掉少数样本点即使引起个别小波系数发生较大的改变，也不会使统计平均值发生很大变化。这样，该统计平均值对时间域的随机剪切也应该是稳定的。因此，逼近信号的小波系数平均值可以作为一个很好的嵌入水印的物理量[2]。

本文的嵌入算法为:

(1)将原始音频 S 分成 X ($X \geqslant NL$) 段，对每一段音频数据进行小波变换，并求出其逼近信号小波系数的统计平均值 $E_i(1 \leqslant i \leqslant X)$。

(2)依据下列条件，对 E_i 进行分类，并分别记录 2 个类型中的数据在原始音频中的索引段号 i。

A 类: $E_i \geqslant T$

B 类: $E_i < T$

其中，T 为给定的阈值，与原始音频信号和水印信息有关。具体选法为:

1)分别计算水印比特序列中 0 与 1 的个数 C_0, C_1 及它们的比值 $r = C_0/C_1$ 。

2)将 $E_i(1 \leqslant i \leqslant X)$ 中的元素按从小到大进行排序，得到集合 $E' = \{E_1, E_2, \cdots, E_i, \cdots, E_X\}$ ，其中 $E_1 < \cdots E_i < \cdots E_X$ 。

3)根据比值 r 来选择临界值 $T = E_k$,其中: $k = \left\lfloor \dfrac{r}{r+1} \times X \right\rfloor$ 。

(3)将水印比特 1 映射到 A 类集合中，而将 0 映射到 B 类集合中。依据嵌入的比特位是 1 还是 0，从 A 类和 B 类分别选取相应的元素，并记录该元素在原始音频中的段号 i，最终生成一个嵌入索引向量 N。

当水印 W_m 全部嵌入音频文件之后，获得一个嵌入向量 N。提取水印时需要将索引向量 N、每段音频的样点数 M 及阈值 T 作为密钥发送到接收端。

3 检测算法

3.1 水印提取

音频文件经 MP3 压缩与解压缩之后，文件的长度通常会不一致，因此，须进行线性伸缩恢复。假设 $S' = \{s'(0),\ s'(1), \cdots,\ s'(L'-1)\}$ 为待检测的音频信息，长度为 L'，L 为原始音频的长度，当 $L' \neq L$ 时需采用下式[4]进行线性伸缩恢复，该过程可看作是一个插值过程:

$$s''(i) = \begin{cases} s'(0) & i = 0 \\ (1-\beta) \cdot s'(\lfloor \alpha \cdot i \rfloor) + \beta s'(\lfloor \alpha \cdot i \rfloor + 1) & 0 < i < L-1 \\ s'(L'-1) & i = L-1 \end{cases} \quad (1)$$

其中，$S'' = \{s''(0),\ s''(1), \cdots,\ s''(L'-1)\}$ 为线性伸缩恢复后的音频信息，$s''(i)$ 和 $s'(j)$ 分别是 S'' 和 S' 的第 i 个和第 j 个样本，$0 \leqslant i \leqslant L-1$, $0 \leqslant j \leqslant L'-1$, $\beta = \alpha \cdot i - \lfloor \alpha \cdot i \rfloor \in [0,\ 1]$, $\alpha = (L'/L)$ 为线性伸缩因子。经过线性伸缩恢复后再将音频信息分段(每段长度与嵌入时等长)，根据嵌入索引向量 N 提取出相应的音频段，并对该音频段进行与嵌入时相同的小波变换，计算其逼近信号小波系数的统计平均值 E_i'，并与 T 进行比较: 若 $E_i' \geqslant T$ ，则 $w''(i)$ 为 1; 相反若 $E_i' < T$ 则认为 $w''(i)$ 为 0。提取出的水印为

$$W'' = \{w''(i),\ 1 \leqslant i \leqslant NL\} , w''(i) \in \{0,\ 1\}$$

3.2 水印解调

利用与嵌入时相同的密钥通过伪随机序列发生器生成 PN 序列 $P = \{p_j | 0 < j \leqslant L\}$, $p_j \in \{0,1\}$ ；并依 PN 序列的长度 L 对 W'' 进行分段，$W'' = (w_1'', w_2'', \cdots, w_j'', \cdots, w_L'')$, $0 < j \leqslant L$ ，将每段的水印数据与 PN 序列按位取异或得到水印 $W' = \{w_i' | w_i' = w_i'' \oplus P\}$ ，然后在段内相加，若得到的结果大于 $\lfloor L/2 \rfloor$ 则判定水印位为 1，否则为 0。最终恢复出水印 W。如此能从正确率达 50%以上的水印序列中还原出与原始水印 W 相似度很高的水印 W^m[5]。这样，只要提取的水印序列的错误率小于 50%，经解调后的水印和原始水印的相似度仍是很高的，而且水印提取时不需要原始音频。

4 仿真实验

本文利用 Matlab7.0 进行仿真实验，采用 16 位量化精度、44.1 kHz 采样率的单声道数字音频信号，波形如图 1 所示。

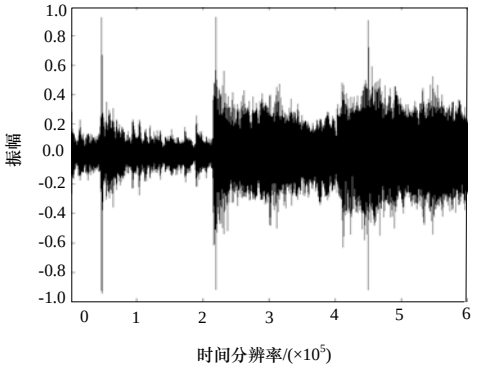

图 1 原始音频波形

以 512 点为帧长对音频信号进行分段，采用 db1 对各段音频信号进行 3 级小波变换。嵌入水印为自制的(48×48) bmp 二值图像如图 2(a)所示，其中比特 0 的个数 C_0 为 523，比特 1 的个数 C_1 为 1781。经计算得 k=599，从 E' 中提取出 $T = E_k$ = –0.007 158 6 ，对水印采用 5 倍重复编码。图 2(b)为未经过任何攻击提取出的水印图像。

图 2 水印图像

为检测算法的鲁棒性，对嵌入水印信息的音频信号进行重新采样、重新量化、低通滤波、附加噪声、回声干扰、MP3 压缩以及剪切攻击(选择 Cool Edit Pro 2.1 作为模拟攻击工

具)，如图 2 所示。

重新采样：先将音频信号由原来的 44.1 kHz 下采样到 16.0 kHz，再恢复采样率至 44.1 kHz，提取水印如图 2(c)所示。

重新量化：先将音频信号量化为 8 bit，再重新量化到 16 bit，提取水印如图 2(d)所示。

低通滤波：采用阶数为 9，截止频率为 4.0 kHz 的 CHBYSHEV 滤波器，提取水印如图 2(e)所示。

附加噪声：在音频信号中加入均值为 0，方差为 0.01 的高斯白噪声，提取水印如图 2(f)所示。

MP3 压缩：先将音频信号压缩至 128 kb/s，再解压缩到 WAV 格式，提取水印如图 2(g)所示。

回声：对音频信号采用回声攻击后提取的水印如图 2(h)所示。

随机剪切：随机剪切掉音频中若干样本点，提取出的水印如图 2(i)~图 2(k)所示，其中图 2(i)、图 2(j)、图 2(k)分别为随机剪切 100, 200, 500 个样本点提取出的水印。

综合攻击：将上述攻击(除剪切攻击)依次对音频信号进行攻击，提取出的水印如图 2(l)所示。

由图 2 可以看出，算法对常见的攻击如滤波、重采样、随机剪切、回声干扰和 MP3 压缩等都具有较好的鲁棒性。在音频质量有明显下降的情况下仍能有效地提取出水印信息。对于剪切攻击，因嵌入位置为高能量处，所以盗版者通常不会剪切到该区域，且由于相邻音频样本点或小的音频片断之间具有高度的相关性，即使随机剪切掉少数样本点逼近信号统计平均值也不会受很大影响，再者由于采用了重复编码，算法在音频信号的不同位置多次嵌入水印信息，所以从理论和现实处理的可能性来看都会有较完整的水印信息保留下来，因此，本算法对剪切攻击具有较高的鲁棒性。对于 MP3 攻击，由于逼近信号平均值对 MP3 压缩的稳定性，线性伸缩恢复技术对时间轴上线性伸缩带来的影响的消除能力使算法能够抵抗 MP3 攻击。另外，算法不修改原始音频信号的任何数据，具有很好的不可感知性。

5 结束语

本文以逼近信号小波系数统计特性和线性伸缩恢复技术为基础，结合纠错编码技术构造音频数字零水印。在完全不影响感知性的同时对各种常见攻击尤其对剪切攻击和 MP3 攻击具有较高的鲁棒性，可实现对音频作品版权的有效保护。

参考文献

[1] Anderson J P. ESD-TR-7 3-5 1-1972 Computer Security Technology Planning Study[S]. 1972.

[2] 李　伟. 鲁棒性数字音频水印算法研究[D]. 上海：复旦大学, 2004.

[3] Tzanetakis G, Essl G, Cook P. Audio Analysis Using the Discrete Wavelet Transform[C]//Proc. of Int. Conf. on Acoustics and Music: Theory and Applications. Skiathos, Greece: [s. n.], 2001.

[4] Lu Hongwei, Pi Bingfeng. Audio Zero-digital Watermarking Algorithm Based on Energy Difference of Wavelet Coefficient[J]. Computer Applications, 2007, 27(3): 605-607.

[5] Wang Rangding, Jiang Gangyi, Chen Jin'er. A New Method of Audio-digital Watermarking Based on Trap Strategy[J]. Journal of Computer Research and Development, 2006, 43(4): 613-620.

编辑　金胡考

（上接第 143 页）

即使攻击者获得正确的口令，也不能计算已有的会话密钥，原因是 $K_h = MAC_K(\alpha^{K_H} \| K)$，即 K_h 依赖于 K，因此，协议满足完美前向安全性。

综上所述，本协议是安全的。

5 计算代价和通信代价分析

计算代价和通信代价分析是 2 个用于分析基于口令的认证协议的重要方面，包括协议步骤数、指数运算次数、对称加解密次数、哈希函数运算次数和随机数生成次数。本协议将与如下协议做比较：LR-AKE[2], PAK-X[3]以及 SKA[4]。性能比较结果如表 1 所示。

表 1　性能比较结果

协议	协议步骤	指数运算			随机数生成	哈希计算
		客户机	服务器	总计		
LR-AKE	3	3	2	5	2	6
PAK-X	3	5	4	9	2	10
SKA	3	2	3	5	2/4	7
本文协议	3	3	2	5	2	9

从表 1 可以看出，与其他协议相比，本文协议的协议步骤和指数运算都是最小的，并且需要 2 次随机数生成、9 次哈希函数运算，而 PAK-X 需要更多。与 SKA 协议相比，协议的哈希运算多 2 次，然而计算 K_h 的 2 次额外 MAC 运算使协议更加安全；与 LR-AKE 相比，本协议需要 1 次额外的哈希运算，原因是 LR-AKE 协议仅协商共享密钥 K，而没有协商一个共同的会话密钥 K_s。

6 结束语

本文提出了一个安全高效的带认证的无线局域网密钥协商协议，具有双方相互认证功能以及密钥建立机制，安全性分析表明，本方案易于实现，对于主动和被动攻击来说都是安全的，还能抵抗多种攻击，与经典协议相比，其计算代价和通信代价都是最低的，可广泛应用于无线网络通信中。

参考文献

[1] 赵宗渠, 刘艳霞. 一种可证安全性的无线网络密钥协商协议[J]. 计算机工程, 2008, 34(14): 174-175.

[2] Hideki I, Seonghan S, Kobara K. Authenticated Key Exchange for Wireless Security[C]//Proc. of IEEE Wireless Communications & Networking Conference. Tokyo, Japan: IEEE Computer Society, 2005.

[3] Mackenzie P. More Efficient Password Authenticated Key Exchange[C]//Proc. of the 2001 Conference on Topics in Cryptology. London, UK: Springer-Verlag, 2001.

[4] Ryu Eun-Kyung, Kim Kee-Won, Yoo Kee-Young. A Simple Key Agreement Protocol[C]//Proc. of the 37th Annual International Carnahan Conference. Taipei, China: IEEE Computer Society, 2003.

[5] Blake-Wilson S, Johnson D, Menezes A. Key Agreement Protocols and Their Security Analysis[C]//Proc. of the 6th IMA International Conference on Cryptography and Coding. [S. l.]: Springer-Verlag, 1997.

编辑　张　帆