抗随机几何失真攻击的音频水印方案

周振宇 张新鹏 王朔中
(上海大学通信与信息工程学院, 上海 200072)

摘 要 随机几何失真攻击是指在数字音频中恶意地插入跳跃,或通过重采样等手段使相位等特性发生随机抖动,从而对音频数字水印构成严重威胁的行为。为防止这种攻击提出了一种利用音频信号采样点之间的相关性,同时根据信号局部特征生成水印信号并进行自同步嵌入的新方案。实验表明,该方案不仅对一般信号处理具有稳健性,也能够很好地抵御随机几何失真攻击。

关键词 数字水印 音频信号 随机几何失真
中图法分类号: TP309.2 **文献标识码**: A **文章编号**: 1006-8961(2005)11-1466-05

Audio Watermarking Scheme Against Random Geometric Distortion Attacks

ZHOU Zhen-yu, ZHANG Xin-peng, WANG Shuo-zhong
(*School of Communication and Information Engineering, Shanghai University, Shanghai* 200072)

Abstract Geometric distortion is a simple and effective attack to digital audio watermarking. This paper proposes a novel watermarking scheme, in which the correlation between samples of audio signal is used and watermark signal derived from the local characteristic of host signal is embedded self-synchronously. Simulation results show the proposed scheme, with robustness enough against general signal processing, can effectively resist geometric distortion attacks.

Keywords digital watermarking, audio signal, random geometric distortion

1 引 言

随着数字化音像制品和音乐制品的大量制作和发行,音频数据的版权保护也越来越重要。近年来,音频数字水印技术也得到了迅速发展,主要方法有相位法、回声法、时域法、频域法等,其中,相位方法是利用人类听觉系统对绝对相位不敏感的特性,将水印信息隐藏在声音信号的绝对相位中,而相对相位则尽量保持不变[1,2];回声方法则是将载体数据以一定衰减程度延迟一定时间叠加到原始载体数据上,并用不同的延迟时间来标志水印数据的"0"和"1"[1];时域法,在时域嵌入水印时,可以采用 LSB (least significant bit) 方法,即用水印信息替换最不重要比特位上的载体数据,这种方法虽然实现简单,但稳健性不好,另外还可以通过在时域上叠加经过处理的伪随机序列来嵌入水印[3];频域方法也是音频水印的重要方法,它是将某一频段的系数完全替换[4]、在原系数上叠加[5]或只对频域系数进行局部调整[6]来进行水印嵌入。另外,在水印嵌入时,利用人耳的掩蔽效应,可以进一步提高水印信号的隐蔽性[7]。

音频信号不同于图像,它在时间上是不断延续的流,由于不可能对每一段信号都尝试检测/提取水印,因此同步问题就非常重要。文献[8]提出了一种原始信号与加载了水印的信号之间的匹配同步模型。为了解决同步问题,该模型既可以在嵌入水印的同时,嵌入同步标识信号[4];也可以根据载体信

基金项目:国家自然科学基金项目(60372090);上海市科委基础研究重点项目(04JC14037);上海市教委青年基金项目(04AC93)
收稿日期:2005-08-20;改回日期:2005-09-15

第一作者简介:周振宇(1981~),男。2004 年获上海大学学士学位,现为上海大学通信与信息工程学院硕士研究生。研究方向为信号处理、信息隐藏。E-mail: rinick@163.com

号局部特性来选择嵌入位置[9]。

音乐制品在传播过程中会经常受到压缩、重量化、重采样等信号处理,由于目前出现的音频水印方案大多已考虑了这方面因素,因此能够有效抵御这些常见的信号处理。但是,实用的水印系统还必须能够抵抗恶意的攻击。随机几何失真就是一种简单而有效的恶意攻击手段,对音频载体来说,其实现方法包括加入跳跃信号和使采样频率随机漂移,并可在几乎不影响听觉效果的情况下,破坏水印的同步和检测。

本文针对随机几何失真攻击,提出了一种利用音频信号局部特征设计水印信号(该水印信号相邻采样点之间具有相关性),并自同步嵌入水印的新方案。该方案不但对通常信号处理具有稳健性,而且能够有效地抵御几何失真攻击。

2　随机几何失真攻击

对数字图像而言,随机几何失真是指在不同局部产生不同的微小随机几何畸变。随机几何失真很容易实现,却能使水印的同步变得非常困难。音频水印也面临着类似的问题。音频信号中的随机几何失真有以下两种典型的实现方法:一种是在音频信号中加入跳跃信号(jitter),即每隔一段时间便随机复制或删除一个采样点;另外一种是对音频信号进行重采样,并使采样频率发生随机漂移。虽然这两种攻击方法对听觉的影响都很小,却可以有效地改变信号的时/频特性,从而使水印信号失步而无法检测。

如果在一帧音频信号中加入跳跃信号,假设跳跃信号前的音频信号为 S_1,跳跃信号后的音频信号为 S_2,那么跳跃信号会改变 S_2 的绝对位置以及 S_2 对 S_1 的相对位置。另外,跳跃信号也会使频域特性发生较大变化。假设 S_1 的频谱为 $F_1(\omega)$,S_2 的频谱为 $F_2(\omega)$,未加跳跃信号时这一帧音频信号的频谱 $F(\omega) = F_1(\omega) + F_2(\omega)$;加跳跃信号后,$F_1(\omega)$保持不变,而 $F_2(\omega)$的相位则会发生变化,而且频率越高变化越大,由于整帧信号的频谱是两部分的叠加,所以也会发生变化,尤其在较高的频段,变化较大。不幸的是,由于隐蔽性的要求,水印信号一般隐藏在较高频段,而且很有可能在同一帧音频信号会含有多个跳跃信号,所以这种攻击能有效破坏水印检测。

采样频率漂移在时域上表现为信号被拉长或缩短,且采样点的绝对和相对位置都发生了变化。在频域上表现为频谱被压缩或被扩展,即频谱值偏离了原来的频率位置。如果采样频率的变化是固定的,则可以采用有效的办法进行补偿。例如可以嵌入测试信号,检测时,即可根据测试信号的变化估计出采样频率的变化。但是,如果采样频率的变化是随机的,即在不同时刻采样频率是不同的,那么对随机漂移的补偿将很困难。

从上面的分析可以看出,由于随机几何失真会使信号在时域和频域上都发生畸变,从而影响水印的检测。但是不管怎样,由于信号相邻采样点之间的相关性和信号的局部特征变化是不大的,否则信号会产生较大失真,因此可以利用这个特性来设计水印信号,并将其以自同步方式嵌入,使之能够抵御随机几何失真攻击。

3　数字水印方案

考虑到几何失真对音频信号时域、频域特性的破坏,采用以下方法来设计和嵌入水印信号:

(1)首先将原始信号分为许多短时帧,并计算每帧信号的能量,然后判断每帧的能量是否大于阈值 T,如是,则在该帧中嵌入水印,如不是,则表示该帧信号接近于静音,不宜嵌入水印;

(2)根据密钥产生一个伪随机滤波器,即用一个长度为 l 的伪随机序列 $\boldsymbol{h}$ 作为滤波器的冲激响应,该滤波器不必具有带通特性;

(3)用滤波器 $\boldsymbol{h}$ 对原始信号 $\boldsymbol{x}$ 进行滤波,设结果为 $\boldsymbol{X}$

$$X(n) = x(n) * h(n) \tag{1}$$

式中 * 表示卷积。$\boldsymbol{X}$ 中相邻样点之间的相关性也是很强的,并可将 $\boldsymbol{X}$ 看作音频信号 $\boldsymbol{x}$ 的局部特性;

(4)设 $\boldsymbol{x}$ 的长度为 M,并设 $\boldsymbol{X}$ 中与原始采样点 $x(m)$具有相同对应位置的数据为 $X(m)$。将由 $\boldsymbol{X}$ 产生的二进制序列 $\boldsymbol{w}$ 作为水印信号

$$w(m) = (-1)^{\text{round}\{\frac{X(m)-r}{\Delta}\}}, m = 1,2,\cdots,M \tag{2}$$

式中,Δ 是由水印系统确定的参数,r 是由水印系统确定的处于 $(0, \Delta)$ 之间的数值,round( )表示取最接近的整数。参数 Δ 和 r 可以作为密钥的一部分;

(5)在那些能量大于阈值 T 的帧中,以如下方法嵌入水印,

$$x_w(m) = x(m) + \alpha \cdot w(m) \cdot |x(m)|,$$

$$m = 1,2,\cdots,M \tag{3}$$

α 是系统参数，代表水印嵌入的强度；x_w 即已嵌入水印的信号。

水印检测时，可用密钥生成同样的滤波器响应 h，与待检信号 y 卷积来得到 Y。设 y 的长度为 M_y，并设 Y 中与待检信号采样点 $y(m)$ $(1 \leqslant m \leqslant M_y)$ 具有相同位置的数据为 $Y(m)$，则用类似于步骤(2)的方法可得到

$$w_y(m) = (-1)^{\mathrm{round}\{\frac{Y(m)-r}{\Delta}\}}, m = 1,2,\cdots,M_y \tag{4}$$

然后计算

$$\rho = \frac{1}{M_y}\sum_{m=1}^{M_y} y(m) \cdot w_y(m) \tag{5}$$

同时用一系列不同于 h 的伪随机滤波器 $g^{(k)}$，$k = 1, 2, \cdots, K$（K 可以很大，例如1 000）来产生 $w_y^{(k)}$，并将其代入式(5)就可得到 K 个 $\rho^{(k)}$。如果所有这些随机得到的 $\rho^{(k)}$ 都小于 ρ，则认为 y 中含有水印。

下面说明本方案对随机几何失真攻击的有效性。由于原始信号相邻样点之间的相关性很强，所以经随机滤波器处理后的信号 X 的相邻相关性仍然很强，这样由 X 得到的水印信号 w 的相邻相关性也很强，即具有连续 +1 或连续 −1 的特性。而一般情况下，只要 Δ 取得较小，则由式(2)得到的 w 就是与原始信号 x 不相关的，即

$$\frac{1}{M}\sum_{m=1}^{M} x(m) \cdot w(m) = 0 \tag{6}$$

而且

$$\frac{1}{M}\sum_{m=1}^{M} x(m) \cdot w_y(m) = 0 \tag{7}$$

嵌入水印的过程正是使 w 与 x_w 具有相关性。由于 w 是由局部特性得到的，并被即时地嵌入，而且 w 和含有水印的音频信号 x_w 都具有相邻样点相关性，所以即便含有水印的音频信号被加入到跳跃信号或被随机漂移地重采样和采样点发生一定偏移，而由 Y 得到的 w_y 与 y 也会具有一定的相关性。这种相关性就是用来判决是否含有水印信号的依据。

4 实验结果

为验证本文方案的有效性，采用长度为 60s 的 Beethoven 第 5 交响曲（命运）为原始音频信号来进行实验，采样频率为 44.1kHz，采样值为 16bit 量化。实验中先将左右声道相加来得到单声道信号，然后取滤波器 h 的长度为 127 个采样值，每个采样值根据密钥由标准正态分布互相独立地伪随机取得（如图 1 所示）。伪随机滤波后的信号片段如图 2(a)所示，由其生成的相同位置的部分水印信号如图 2(b)所示，这里取 $\Delta = 0.15$、$r = \Delta/2$。从图 2 可以看出，滤波后信号和水印信号的相邻相关性仍然很强，这种相关性正是保证本方案有效的必要条件。

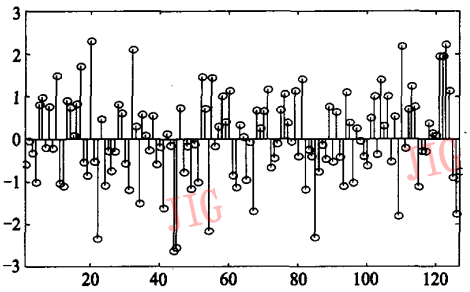
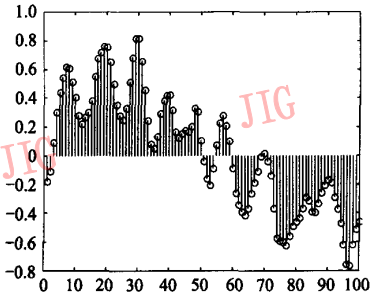
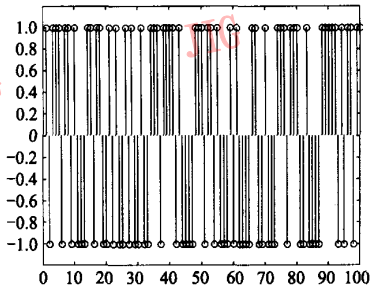


图 1 伪随机滤波器的冲激响应

Fig. 1 Impulse response of pseudo-random filter



(a) 伪随机滤波后的部分信号



(b) 对应的水印信号

图 2 伪随机滤波后的部分信号和对应的水印信号

Fig. 2 Signal after pseudo-randomly filtering and the corresponding watermark signal

由于原始信号的绝大多数帧都是非静音区，可以嵌入水印，所以，嵌入水印信号后相应帧的信噪比（signal to noise ratio，SNR）与水印嵌入强度参数 α

有如下关系式:

$$SNR = 10 \cdot \ln(1/\alpha^2) \tag{8}$$

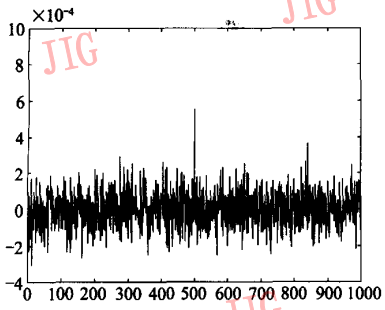
为保证水印信号的隐蔽性,本文将水印信号引起的局部信噪比控制在 33dB,由式(8)可得 $\alpha = 0.022$。按这样的强度嵌入水印后再进行主观评价,就无法察觉原始信号与含水印信号的差别。

当含水印的信号未受攻击时,即 $\boldsymbol{y} = \boldsymbol{x}_w$,而 $\boldsymbol{w}$ 由 $\boldsymbol{x}$ 的局部特征得到,而 $\boldsymbol{w}_y$ 则由 $\boldsymbol{y}$(即 $\boldsymbol{x}_w$)的局部特征得到,但两者会有差别,由式(3)、式(5)、式(7)知:

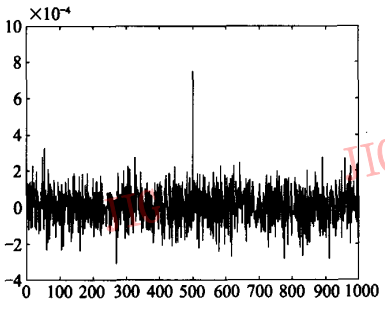
$$\mathrm{E}(\rho) \leqslant \frac{\alpha}{M} \cdot \sum_{m=1}^{M} | x(m) | \tag{9}$$

经计算,上式右边为 1.0×10^{-4},而实验测得的 ρ 值为 9.3×10^{-4}(式中,E 代表数学期望)

对嵌入了水印的信号先分别进行加入跳跃信号和采样频率随机偏移两种几何失真攻击,然后进行水印检测,其结果如图 3 所示。



(a) 跳跃信号攻击测试



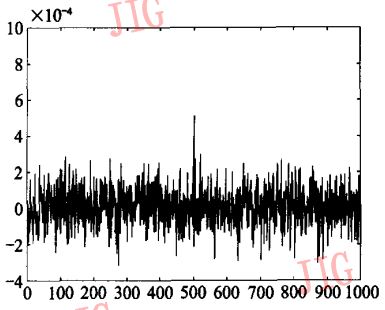
(b) 采样频率随机偏移测试

图 3　抗几何攻击测试

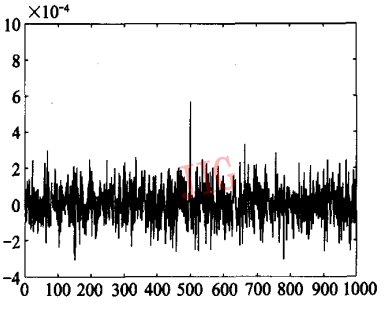
Fig. 3　Experimental results under geometric distortion

由图 3 可见,跳跃信号攻击是在每 50 个样点(即 1.1ms)加入或删除一个样点,已对听觉造成较严重影响。在另外一种攻击中,采样频率的偏移率在正负 2% 之间随机变化,攻击后信号也已较严重地失真。从图 3 中可以看到,当使用不同的伪随机滤波器(即不同的密钥)进行检测时,ρ 值在 -3×10^{-4} 和 $+3 \times 10^{-4}$ 间波动。而使用正确的伪随机滤波器对攻击后的含水印信号进行检测,其得到的两个 ρ 值分别为 5.6×10^{-4}、7.5×10^{-4}。与未受攻击的情况相比,虽然 ρ 值都有所下降,但仍明显大于其它 1000 个不同伪随机滤波器得到的 ρ 值,说明能够检测出水印的存在。可见本方案在随机几何失真已很严重时,依然具有稳健性。

对含水印的信号先进行传输码率为 128kbps、压缩率为 5.5:1 的 MP3 压缩,然后进行水印检测,结果见图 4(a)。类似地,在含水印的信号中加入非常明显的随机噪声($SNR = 23.5$dB)后,水印检测的结果见图 4(b)。图 4 中的 ρ 值分别为 5.1×10^{-4}、5.7×10^{-4}。另外,本方案对抗低通滤波与抗重量化也有很好的性能,限于篇幅,这里将实验结果略去。



(a) 抗 MP3 压缩测试



(b) 抗噪声测试

图 4　抗 MP3 压缩测试和抗噪声测试

Fig. 4　Experimental results under MP3 compression and experimental results under additive noise

5 讨 论

随机几何失真是当前数字水印技术面临的一个重要问题,它不仅实现简单,并且可以在不过分影响感觉效果的情况下,对大多数水印技术进行有效攻击,这就构成了对数字水印的严峻挑战。针对这一类攻击的研究成果报道还不多。文献[3]提出的时域水印嵌入方法虽可低于重采样等几何攻击,却无法抵抗随机几何失真。本文着重考虑了随机几何失真的问题,利用音频信号采样点之间的相关性和原始信号的局部特性来生成水印信号,并将其自同步地嵌入到原始载体中,实验验证该方案的有效性。在本方案中,伪随机滤波器 h 的长度越长,可选的密钥空间就越大,则可以嵌入的水印种数就越多。Δ 的选取要大小适中,因为过大会有损水印信号 w 与原始信号 x 的统计独立性;过小则有损 w 的邻域相关性。

本文提出的方法利用了大量数据的统计特性,因此所需原始信号的长度较大,这是为抵抗随机几何失真付出的代价。如何减小代价将是下一步研究内容。

参考文献(References)

1 Bender W, Gruhl D, Morimoto N, *et al.* Techniques for data hiding [J]. IBM System Journal, 1996, **35**(3,4): 313 ~ 336.

2 XU Chang-sheng, WU Jian-kang, Sun Qi-bin, *et al.* Applications of digital watermarking technology in audio signals[J]. Journal Audio Engineering Sociaty, 1999, **47**(10): 805 ~ 812.

3 Bassia P, Pitas I, Nikolaidis N. Robust sudio watermarking in the time fomain[J]. IEEE Transactions Multimedia, 2001,**3**(2): 232 ~ 241.

4 Tilki J F, Beex A A. Encoding a hidden digital signature onto an audio signal using psychoacoustic masking[A]. In: 7th International Conference on Signal Processing Applications and Technology[C], Boston, MA, USA. 1996, **2**: 476 ~ 480.

5 WANG Ye. A new watermarking method of digital audio content for copyright protection[A]. In: Proceedings of ICSP[C], Beijing, China, 1998: 1420 ~ 1423.

6 WANG Shuo-zhong, ZHANG Xin-peng, ZHANG Kai-wen. Data hiding in digital audio by frequency domain dithering[A]. In: Proceedings of Second International Workshop pn Mathematical Methods, Models, and Arechitectures for. Computer Network Security, Lecture Notes in Computer Science[C], St. Petersburg, Russia, 2776, 2003: 383 ~ 394.

7 Swanson M D, Zhu Bin, Tewfik A H, *et al.* Robust audio watermarking using perceptual masking[J]. Signal Processing, 1998, **66**(3): 337 ~ 355.

8 XU Chang-sheng, WU Jian-kang, SUN Qi-bin. Audio registration and its application in audio watermarking[J]. Proceedings of SPIE Security and Watermarking of Multimedia Contents II, 2000, **3971**: 393 ~ 401.

9 WU Chung-ping, Su P-C, Kuo C-C J. Robust and efficient digital audio watermarking using audio content analysis[J]. Proceedings of SPIE *Security and Watermarking of Multimedia Contents* II, 2000, **3971**: 382 ~ 392.