文章编号:1001 - 9081(2006)10 - 2326 - 02

基于 DWT 的盲音频水印算法研究

曹建春[1],沈淑娟[2]
(1. 黄河水利职业技术学院 信息工程系,河南 开封 475003; 2. 郑州大学 信息工程学院,河南 郑州 450052)
(cjcssj@126.com)

摘 要:提出了一种基于离散小波变换的盲音频数字水印算法,该算法采取分段重复嵌入方式在能量最强的小波系数内隐藏水印信号。仿真实验结果表明,该算法具有较强的鲁棒性和不可感知性,能有效抵御各种常见攻击,并且在水印检测时不需要原始的音频信号。

关键词:数字水印;小波变换;数字音频信号;鲁棒性
中图分类号: TP309 **文献标识码**:A

Study of blind audio digital watermarking algorithm based on DWT

CAO Jian-chun[1], SHEN Shu-juan[2]
(1. *Department of Information Engineering, Yellow River Conservancy Technical Institute, Kaifeng Henan* 475003, *China*;
2. *College of Information Engineering, Zhengzhou University, Zhengzhou Henan* 450052, *China*)

Abstract: A new watermarking algorithm based on DWT transform was proposed to offer copyright protection for digital audio signals. A digital watermark is embedded into the significant wavelet coefficients repeatedly. The experimental results show that the imbedded watermark has good imperceptibility and robustness against common signal processing manipulations and the watermark can be extracted without original data.

Key words: digital watermarking; wavelet transform; digital audio signal; robustness

0 引言

随着数字音频压缩技术的成熟,使得以 MP3 为代表的网络音乐在互联网上广泛传播,音乐制品的版权保护问题已迫在眉睫。数字水印技术以其较好的不可感知性、鲁棒性、可检测性及安全性,成为知识产权保护的一种有效手段。数字音频水印技术就是利用人类听觉系统的冗余,在不影响原始音频质量的条件下,向其中嵌入与版权所有者相关的秘密信息,以证实音乐制品的版权归属[1,2]。现有的数字音频水印算法按照对数字音频信号的处理方式不同,可以分为时域算法和频域算法。前者将水印信息直接嵌入到音频信号的采样数据中以隐藏信息;后者首先对音频信号的采样数据进行适当的变换,然后将水印信息嵌入到变换域选定的系数上,最后通过相应的逆变换恢复出含有水印信息的音频信号。总体而言,频域水印的不可感知性及抗攻击能力优于时域水印[3,4],目前占主导地位。

小波变换是将信号分解到时域和尺度域上的一种变换,尺度域可以对应于频域。小波变换具有良好的能量压缩能力,数字音频信号经小波变换后,能量主要集中于逼近信号中,将水印嵌入到能量强的信号分量上,可以有效地提高其稳健性。基于此,本文提出一种鲁棒的数字音频水印算法。仿真实验表明,该算法抗攻击能力强并可实现盲检测。

1 数字音频水印的嵌入

1.1 水印预处理

为了具有更好的实用价值,本文嵌入的水印信号为一幅有意义的二值图像,可表示为:

$$W = \{w(i,j), 0 \leqslant i < P, 0 \leqslant j < Q\},\ W(i,j) \in \{0,1\}$$

由于水印序列是二维图像,要将其嵌入到一维的数字音频信号中,必须先进行降维处理,变为一维序列 V,即:

$$V = \{v(k) = w(i,j), 0 \leqslant i < P, 0 \leqslant j < Q, k = i \times Q + j\}$$

为了提高数字水印算法的鲁棒性,使得所加入的水印能够抵抗剪切、重采样等一系列的信号处理方法的攻击;同时为了达到安全和保密的目的,使得只有掌握密钥的人才能提取并正确地恢复出水印,本文使用线性移位寄存器对一维序列 V 进行置乱变换,其中寄存器的初始状态作为密钥 K[5]。置乱后得到由 V 转换而来的新的一维二进制序列 $X = \{x(i), 0 \leqslant i < P \times Q\}$。

1.2 音频信号的分段小波变换

设 S 是原始数字音频信号,为讨论方便,将 S 分解成两部分,即 $S = S_e + S_r$,其中 S_e 是与水印嵌入相关的部分; S_r 是与水印嵌入无关的部分。为提高水印检测的可靠性,将水印信息分段连续嵌入 m 次,为此,将 S_e 分成 m 段,其中 $S_e(k)$ 是第 k 个音频段。对每一音频段 $S_e(k)$ 分别进行 L 级小波分解,提取出尺度 L 的低频系数 $C_e(k)(l)$,从中选取绝对值最大的前 $P \times Q$ 个系数 $C(i)$ 用于水印嵌入。由于该部分是音频信号的主要部分,对它的恶意攻击如果强度过大,则会破坏信号的品质,因此在一定程度上可限制对水印的攻击,进而增强水印的稳健性[6,7]。

1.3 水印信号的嵌入

水印嵌入是对所选择的小波系数进行特殊量化完成的[8]。设 $C(i)$ 表示待量化小波系数,$C'(i)$ 表示量化处理后含有水印信息的小波系数,$x(i)$ 为待嵌入水印比特,Δ 表示量化

收稿日期:2006 - 05 - 30 **基金项目**:国家自然科学基金资助项目(60472044)
作者简介:曹建春(1970 -),男,河南开封人,讲师,硕士,主要研究方向:数字音频水印、计算机安全; 沈淑娟(1972 -),女,河南信阳人,讲师,硕士,主要研究方向:数字图像处理、数字音频水印.

步长。通过量化处理嵌入水印的方法为:把系数 $C(i)$ 分为图1所示的两类 A 和 B。当 $x(i)$ 为1时,$C(i)$ 量化为与之最接近的 A 类的中点;而当 $x(i)$ 为0时,$C(i)$ 量化为与之最接近的 B 类的中点。

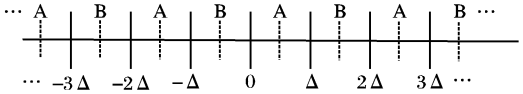

图1　量化系数嵌入水印

1.4　含水印音频信号的生成

对嵌入水印后的音频信号分段进行小波逆变换得到时域中含有水印信息的音频信号 $S'_e(k)$,将 $S'_e(k)$ 代替 $S_e(k)$,最终得到含水印的数字音频信号 $S_W = S'_e + S_r$。

2　数字音频水印的提取

假设 S_s 是待检测的数字音频信号,提取水印的过程如下:

1)对待检测数字音频信号作分段处理,即 $S_s = S_{se} + S_{sr}$,然后对含水印部分 S_{se} 作分段小波变换。

2)根据嵌入水印过程中所生成的用于嵌入水印的小波系数位置信息,确定出含有水印信息的小波系数 $C'(i)$,提取调制水印序列 V'。

$$v'(i) = \begin{cases} 1, & C'(i) \in A \\ 0, & C'(i) \in B \end{cases} \quad (0 \leqslant i < P \times Q)$$

由于水印重复嵌入了 m 次,分别提取 m 组含水印信号的比特流,采用“少数服从多数”的方法决定所提取的每个比特位是“0”还是“1”。

3)根据密钥 K 对所提取的数字水印序列 V' 进行逆置乱和升维,最终计算出嵌入的二值水印图像。

$$W' = \{w'(i,j), 0 \leqslant i < P, 0 \leqslant j < Q\}$$

为了消除观察者的主观因素,通常采用归一化相关系数对提取水印 W' 和原始水印 W 的相似性进行定量的评价,其定义为:

$$NC(W, W') = \frac{\sum_{i=0}^{P-1}\sum_{j=0}^{Q-1} w(i,j)w'(i,j)}{\sqrt{\sum_{i=0}^{P-1}\sum_{j=0}^{Q-1} w^2(i,j)} * \sqrt{\sum_{i=0}^{P-1}\sum_{j=0}^{Q-1} w'^2(i,j)}}$$

水印含有与否的判断标准为:若 $NC > T$,可以判定被测音频信号含有水印,否则不含水印。阈值 T 的选择要同时考虑虚警概率和漏警概率。本文 T 取值为 0.5。

3　实验结果及评价

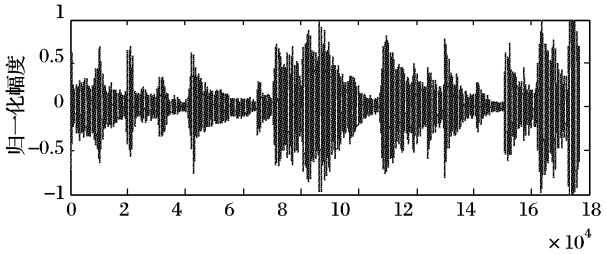

图2　原始数字音频信号

实验选取的原始数字音频信号是 44.1kHz 采样率、16bit 的单声道乐曲,二值图像大小为 64×64。将水印信号每隔 5s 嵌入一次,利用 Db−4 小波基对原始音频信号进行 3 级小波分解,量化步长 Δ 取值为 0.05。图 2 为原始音频信号,图 3 为嵌入水印后的音频信号(信噪比 SNR 为 43.2),和原始音频信号听起来几乎没有差别。

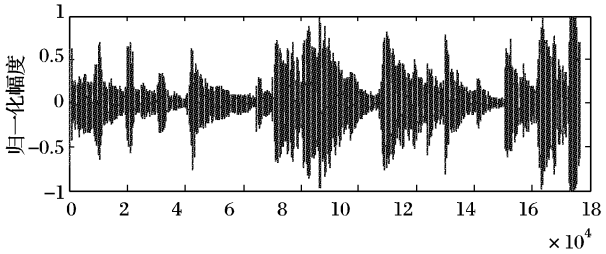

图3　含水印数字音频信号

NC=0.9989　NC=0.8976　NC=0.9486　NC=0.9068　NC=0.9317　NC=0.8694

(a) 原始水印　(b) 未受任何攻击　(c) 叠加噪声　(d) 低通滤波　(e) 重新量化　(f) 重新采样　(g) 有损压缩

图4　原始数字水印与信号处理后的数字水印对比

为验证算法的鲁棒性,对含水印的音频信号进行攻击测试,包括低通滤波、叠加噪声、重新采样、重新量化、有损压缩等,并对处理后的数字音频信号进行水印检测及相似度计算。图 4 给出了原始数字水印与信号处理后的数字水印对比。其中:

叠加噪声　加入高斯白噪声,均值为 0,方差为 0.01。

低通滤波　采用 10 阶截止频率为 4kHz 的 CHBYSHEV 滤波器。

重新量化　将信号从 16 比特量化为 8 比特,再量化为 16 比特。

重新采样　分别对信号进行一次抽取和一次插值处理,抽取和插值的系数为 2。

有损压缩　对信号进行压缩,压缩比为 12∶1,再解压缩。

4　结语

本文以小波变换具有良好的能量压缩能力为基础,提出了一种鲁棒的音频水印算法。该算法在逼近系数内隐藏水印信息,即是把水印信号放在音频信号能量的最大部分——低频部分。一方面由于低频系数的幅值一般远大于高频系数,从而具有较大的感觉容量,使水印不易被察觉[4];另一方面,为了保留原始音频信号的音质,一般信号处理(如滤波、加噪、压缩、变换等)影响的大部分是音频的高频部分,即使水印信号受到影响,但还是能够检测出它的存在。仿真实验结果证明了算法的稳健性和不可觉察性。此外,在水印检测时不需要原始音频信号的参与,实现了盲检测,提高了算法的适用性。

参考文献:

[1] SWANSON MD, KOBAYASHI M, TEWFIK AH. Multimedia data embedding and watermarking technologies[J]. Proceedings of the IEEE, 1998, 86(6):1064−1087.

[2] LACY J, REIBMAN A, SNYDER J. ISO/IEC JTC1/SC29/WG11/M2829, Watermarking as a protection mechanism for IPR in MPEG-4[S]. Fribourg, Switzerland, 1997.

(下转第 2335 页)

步骤 4　A 对消息 M_4 的验证。

A 读取 M_4 中 Signature 字段内容,用 PK_B 对其做 RSA 解密运算,即:

$$DeRSA(PK_B, RSA(SK_B, HASH(M_4))) \quad (11)$$

对 M_4 做 Hash 运算,即 $HASH(M_4)$ (12)

比较(11)、(12)两式内容,如相同,可得结论:M_4 是完整、未经篡改的,且经过 B 数字签名。

A 读取 M_4 中 Validate 字段内容与其保留的 M_3 中的 R_{A2} 比较,如相同,可得结论:M_4 由 B 发出,而非攻击者采用重放攻击发出。

A 读取 M_4 中 Test - Random 字段的内容,用 SK_A 对其做 RSA 解密运算,得测试随机数 R_{B2}。

至此,A、B 双方完成了一次信令信息交互过程,接下来 A、B 间的信令交互与上述的四个步骤相同,在此不再赘述。

3　安全性分析

3.1　数字证书的安全性分析

本模型引入认证中心将 SIP 实体的公用地址和公钥、认证中心的公钥及认证中心对前三项内容 Hash 值的数字签名绑定生成数字证书。由于通过单项散列函数 Hash 提取了 SIP - URL、PK 和 PK_C 三个域内容的特征值,而求具有相同 Hash 值的两个不同消息已被证明不可能,这就保证了数字证书的完整性。又由于认证中心的数字签名不可伪造,从而保证了数字证书的不可否认性。SIP 实体只要将数字证书 SIP - URL + PK + PK_C 内容的 Hash 值和用 PK_C 对数字证书 Verification 域内容做 RSA 解密运算后的值进行比较即可判断数字证书的真伪,从而有效地抵御攻击者伪装合法 SIP 实体的攻击。

3.2　智能卡的安全性分析

智能卡自身的安全一般受 PIN 码保护,PIN 码是由数字组成的口令,只有输入 PIN 码后才能对智能卡进行操作,所以基于智能卡的认证系统实际上是“PIN 码 + 智能卡”的双因素认证系统。PIN 码有一个最大重试次数,当输入错误的 PIN 码的次数达到这个值时,智能卡就会被锁死,防止了猜测攻击。智能卡内置的 SmartCOS 的安全模块可防止非法数据的侵入和篡改,也可防止非法软件对智能卡进行操作。同时,智能卡内置的所有算法都在其内部完成,保证了保密数据的安全性。

3.3　SIP 扩展部分安全性分析

本模型通过对 SIP 做出扩展,将强认证技术有机地融入 SIP,从而提高了 SIP 的安全性。

HELLO 和 ACK-HELLO 消息通过 Certificate 字段实现了会话双方数字证书的交换,使任何 SIP 实体不需要通过认证中心即可判断数字证书的真伪,从而抵御攻击者伪装认证中心的攻击。

Signature 字段用于保存消息发送方对 SIP 消息 Hash 值的数字签名,它作为 SIP 消息的后缀一同发送给接收方。由于求具有相同 Hash 值的两个不同消息已被证明不可能,这就保证了消息的完整性。又由于发送方对消息 Hash 值的数字签名不可伪造,这就保证了消息的不可否认性。消息接收方只要将消息的 Hash 值和用发送方的公钥对消息后缀做 RSA 解密运算得到的值进行比较,即可判断消息的真伪。

Test-Random 字段和 Validate 字段用于抵御消息认证过程中存在的重放攻击问题。在本模型中,消息发送方必须将接收方在 Test-Random 字段中预先给出的测试随机数作为验证随机数加入 SIP 消息 Validate 字段中,接收方收到消息以后只要将 Validate 字段的内容与之前给出的测试随机数进行比较,即可判定消息是由发送方放出还是攻击者采用重放攻击发出的。由于接收方将测试随机数用发送方的公钥加密,而只有发送方才能将其解密,攻击者无法预知测试随机数,从而有效地抵御了重放攻击。

4　结语

本文针对 SIP 的典型安全威胁,提出了基于强认证技术的 SIP 安全认证模型,通过智能卡和数字证书强组合实现强认证,并据此对 SIP 做出扩展,将强认证技术有机地融入 SIP,提高了 SIP 的安全性,具有较高的理论意义和实用价值。基于本模型的 VoIP 实验系统可在 Windows 平台下运行,测试结果表明该认证模型能够有效地抵御 SIP 的典型安全威胁。

参考文献:

[1] 司端锋,潘爱民. SIP 标准中的核心技术与研究进展[J]. 软件学报,2005,16(2):239 - 249.

[2] ROSENBERG J, SCHULZRINNE H, CAMANILO G. SIP: Session initiation protocol[S]. Internet RFC 3261, 2002.

[3] SCHULZRINNE H, ROSENBERG J. The session initiation protocol: Internet-Centric signaling [J]. IEEE Communication Magazine, 2000. 134 - 141.

[4] STEFANO S, LUCA V, DONALD. SIP security issues: The SIP authentication procedure and its processing load[J]. IEEE Network, 2002: 38 - 44.

[5] TAT C, SENTHIL S. On applying SIP security to networked appliances[A]. In: Proc. of the IEEE 4th Int'l Workshop on Networked Appliances[C]. New York: IEEE Press, 2002. 31 - 40.

[6] 张文华,刘忠信,陈增强,等. 基于 SIP 协议的 3G 网络安全认证机制[J]. 计算机工程与应用,2004,40(13):163 - 166.

[7] 施荣华. 基于数字签名的安全认证存取控制方案[J]. 软件学报,2002,13(5):1003 - 1006.

[8] DIFFE W, HELLMAN ME. New Directions in Cryptography[J]. IEEE transactions on Information Theory. 1976, IT - 22(6): 644 - 654.

[9] 施荣华. 一种基于复合问题的双重认证存取控制方案[J]. 小型微型计算机系统,1998,19(7):49 - 52.

[10] GARDENER M. A New Kind of Cipher That Would Take Millions of Years to Break[J]. Scientific American, 1977, 237(8): 120 - 124.

(上接第 2327 页)

[3] SWANSON MD, ZHU B, TEWFIK A. Current state of the art, challenges and future directions for audio watermarking[A]. International Conference on Multimedia Computing and Systems-Proceedings[C]. 1999, 1. 19 - 24.

[4] ARNOLD M. Audio watermarking: features, applications and algorithms[A]. Proceedings of IEEE International Conference on Multimedia & Expo[C]. New York, USA, 2000, 2. 1013 - 1016.

[5] 陈琦, 王炳锡. 一种基于 DCT 变换的语音数字水印算法研究[J]. 信号处理, 2001, 17(3): 238 - 241.

[6] COX I J, KILIAN J, LEIGHTON T. Secure spread spectrum watermarking for multimedia[J]. IEEE Transactions on Image Processing, 1997, 6(12): 1673 - 1687.

[7] 钮心忻, 杨义先. 基于小波变换的数字水印隐藏与检测算法[J]. 计算机学报, 2000, 23(1): 21 - 27.

[8] 王秋生, 孙圣和. 基于量化数字音频信号频域参数的水印嵌入算法[J]. 声学学报, 2002, 27(4): 379 - 385.