DOI:10.13718/j.cnki.xsxb.2012.09.015

文章编号:1000-5471(2012)09-0109-06

一种改进的回声隐藏算法①

胡大辉, 杜治国

西南大学 信息管理系, 重庆 402460

摘要: 回声隐藏算法利用人类听觉系统的时域掩蔽效应来隐藏水印信息, 其工作原理是人耳基本不能分辨强信号消失前嵌入的弱信号. 针对回声隐藏算法中水印恢复准确率较低的问题, 提出一种基于离散余弦变换和交织编码的隐藏算法. 算法对水印图像进行离散余弦变换使其隐蔽效果更好, 将变换后的信息进行交织编码以提高对常见攻击的免疫. 实验证明, 新算法的水印隐藏效果好、恢复率高, 对常见的恶意攻击具有较好的免疫效果.

关 键 词: 回声隐藏; 离散余弦变换; 交织码; 归一化相关系数

中图分类号: TP391 文献标志码: A

信息隐藏是信息安全领域的热点话题, 它在多媒体信息安全中有不可替代的作用. 版权所有人把秘密信息隐藏在一些公开发行的媒体文件中, 以便于在发生版权纠纷时提供版权归属证据. 信息隐藏两个主要研究方向是隐写术和数字水印技术[1]. 隐写术主要研究信息如何伪装, 数字水印技术则关注嵌入秘密信息后载体的鲁棒性.

水印的嵌入主要依靠算法来实现, 由于人类听觉系统的敏感度远远高于视觉等系统, 所以在音频载体上隐藏信息要比在文本和图像等载体上更难. 音频水印的隐藏算法基本可以分为两大类: 时域算法和变换域算法. 回声隐藏(echo hiding)算法就是一种典型的时域隐藏算法. 回声隐藏具有算法简单、不产生噪声和隐藏效果好等优点, 但当回声幅度减小时, 提取水印的正确率就会降低, 而加大回声幅度就影响秘密信息的隐藏. 本文提出一种改进的回声隐藏方法, 首先对水印信息进行离散余弦变换以利于信息的隐藏, 再将变换后的信息进行编码处理以便于提高提取水印的正确率, 最后将水印信息嵌入已分段的原始音频中. 仿真实验显示, 本方法运算量小、隐藏效果好, 水印提取的正确率有较大提高.

1 算法介绍

Bender 等在 1996 年首次提出一种针对音频载体的隐藏技术, 即回声隐藏技术[2]. 一个强纯音会掩蔽在它周围的弱纯音, 这种效果称为频域掩蔽; 在时间上相邻的声音之间也存在掩蔽现象, 称为时域掩蔽[3]. 回声信息隐藏算法利用了人耳听觉系统(Human auditory system, HAS)的时域掩蔽效应. 经研究发现, 在强信号出现后的 50~200 ms 内的弱信号基本不被察觉. 因此, 回声隐藏利用强信号消失前的这段时间内嵌入较弱的秘密信息, 原信号基本不会改变.

① 收稿日期: 2011-06-09
基金项目: 西南大学青年基金支持项目(2010RCQ003).
作者简介: 胡大辉(1977-), 女, 重庆大足人, 硕士, 讲师, 主要从事信息安全方面的研究.
通信作者: 杜治国, 副教授.

1.1 算法原理

Bender在文献[2]中提出的方法可以用公式(1)表示.

$$h(n)=\delta(n)+\alpha\delta(n-d) \tag{1}$$

$y[n]$是嵌入回声后的信号,是$x[n]$和$h[n]$的卷积.其中,$h[n]$是单位脉冲信号,$x[n]$是原始信号.回声信号由$\alpha\delta(n-d)$引入到原始声音当中,α是衰减系数,d是延迟时间.只要选取合适的参数,人耳就不能分辨加入回声信息后的声音信号.加入秘密信号后的载体信号可用公式(2)表示.

$$y[n]=x[n]*h[n] \tag{2}$$

1.2 算法的演变

Bender提出的方法还存在需要改进的地方,例如对衰减系数α没有做进一步的研究;只考虑向后时延而没有考虑向前时延等.

1.2.1 双向回声核[4]

Kim提出了一种新的回声核,由两个延时时间相同,但方向相反的核构成,称为前向核和后向核.Kim的思想可用公式(3)表示.

$$h(n)=\delta(n)+\alpha\delta(n-d)+\alpha\delta(n+d) \tag{3}$$

公式(3)中,$\delta(n-d)$称为后向回声,$\delta(n+d)$称为前向回声.研究结果表明,针对相同的原始声音信号,采用前后向回声核的效果明显好于单回声核,隐藏信息的恢复率有一定提高.

1.2.2 双极性回声核[5]

Oh等提出了基于双极性回声核的隐藏方法,这种方法比Bender提出的方法在低频区域表现得更平滑,能有效提高嵌入水印后载体的表现效果.Oh提出的方法可用公式(4)表示.

$$h(n)=\delta(n)+\alpha_1\delta(n-d_1)-\alpha_2\delta(n-d_2) \tag{4}$$

公式(4)中,α_1和α_2分别表示两个回声信号相对于原始信号的衰减系数,d_1和d_2分别表示回声的延迟.

1.2.3 基于衰减系数的改进[6]

赵朝阳等提出一种通过调整衰减系数来达到信息隐藏的目的.对于样本数为N,回声延时为d的音频载体,引入衰减系数为α的回声后,原始音频可用公式(5)来表示.

$$y[n]=x[n]+\alpha x[n-d] \tag{5}$$

经测试,只要选择合适的α值,在无攻击情况下,水印信息的提取基本能达到100%.

1.2.4 双向对称时扩回声核[7]

Chous等将前向回声和时扩回声结合起来,提出了双向对称时扩回声核,可用公式(6)来表式.

$$k[n]=\delta[n]+\alpha\cdot p[n-d]+\alpha\cdot p[n+d] \tag{6}$$

这种方法兼顾了双向回声和时扩的特点,与传统回声核相比,隐蔽性有一定的提高,但检测率提高不明显.

2 改进的算法

2.1 已有算法的缺陷

前后双向回声核隐藏方法能有效的增强秘密信息的隐藏效果,但不能提高水印提取的正确率;双极性回声核隐藏方法能够增强回声的不可感知性,但是信息的恢复率较低,特别是在回声幅度较小的时候;调整衰减系数隐藏方法能有效的提高数据回复率,但是在受到恶意攻击后数据恢复率急剧降低;双向对称时扩回声核隐藏方法能有效地提高秘密信息的隐蔽性,但是水印的提取率没有明显的提高并且算法的鲁棒性较差.

2.2 水印处理

首先对图像水印信息进行二值转换,再把转换后的二值图像进行离散余弦变换(DCT),得到矩阵X,

对矩阵 X 进行交织编码，得到 X'. 对于一个 $M\times N$ 的矩阵，其二维离散余弦变换如公式(7) 所示.

$$\mu=\alpha_p\alpha_q\sum_{m=0}^{M-1}\sum_{n=0}^{N-1}X_{mn}\cos\frac{\pi(2m+1)p}{2M}\cos\frac{\pi(2n+1)q}{2N} \tag{7}$$

其中，μ 是 DCT 系数，$0\leqslant m\leqslant M-1$，$0\leqslant n\leqslant N-1$，

$$\alpha_p=\begin{cases}1/\sqrt{M}, & p=0\\ \sqrt{2/M}, & 1\leqslant p\leqslant M-1\end{cases},\ \alpha_q=\begin{cases}1/\sqrt{N}, & q=0\\ \sqrt{2/M}, & 1\leqslant q\leqslant N-1\end{cases}$$

在实际的处理过程中，信道都存在随机错误和突发错误，因此必须考虑同时纠正这两种错误. 交织是一种改造技术，它通过信号设计将原来的突发差错改造为独立差错. 交织码的工作原理如图 1 所示.

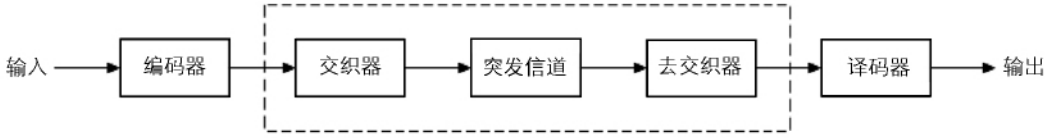

图 1　交织编码原理图

例如，发送信息 $X=[x_1x_2x_3\cdots x_{24}x_{25}]$，首先将 X 送入交织器，同时将交织器设计为按列写入按行取出的 5×5 阵列存储器. 然后从存储器中按行输出送入突发差错的有记忆信道，信道输出送入去交织器，它完成交织器的相反变换，即按行写入按列取出，仍是一个 5×5 阵列存储器. 去交织器的输出，即阵列存储器中按列输出的信息，其差错规律就变成了独立差错.

上例中，$X=x_1x_2x_3\cdots x_{23}x_{24}x_{25}$，则 X 的交织矩阵如公式(8) 所示.

$$\prod\nolimits_1=\begin{bmatrix}y_1 & y_6 & y_{11} & y_{16} & y_{21}\\ y_2 & y_7 & y_{12} & y_{17} & y_{22}\\ y_3 & y_8 & y_{13} & y_{18} & y_{23}\\ y_4 & y_9 & y_{14} & y_{19} & y_{24}\\ y_5 & y_{10} & y_{15} & y_{20} & y_{25}\end{bmatrix} \tag{8}$$

将 X 按公式(8) 进行变换得到 X'.

$X'=x_1x_6x_{11}x_{16}x_{21}x_2x_7\cdots x_{22}x_3\cdots x_{23}x_4\cdots x_{24}x_5\cdots x_{25}$ 假如这时产生两个突发错误，第一个错误在 x_1 到 x_{21}，连续错误 5 个；第二个错误在 x_{13} 到 x_4，连续错误 4 个，则 X 的去交织矩阵如公式(9) 所示.

$$\prod\nolimits_2=\begin{bmatrix}x_1 & x_6 & x_{11} & x_{16} & x_{21}\\ y_2 & y_7 & y_{12} & y_{17} & y_{22}\\ y_3 & y_8 & x_{13} & x_{18} & x_{23}\\ x_4 & y_9 & y_{14} & y_{19} & y_{24}\\ y_5 & y_{10} & y_{15} & y_{20} & y_{25}\end{bmatrix} \tag{9}$$

对公式(9) 的矩阵进行按行写入按列取出，得到 X 如公式(10) 所示.

$$X=x_1x_2x_3x_4\cdots x_{22}x_{23}x_{24}x_{25} \tag{10}$$

由此可见，经过交织矩阵和去交织矩阵的信号变换后，原来信道中产生的突发错误变成无记忆随机性的独立性差错.

2.3　水印的嵌入

回声信息的嵌入步骤是：

① 对水印图像进行 DCT 变换且进行交织编码；

② 由于原始音频是一维的，对编码后的信息进行降维处理，使之成为一维数据；

③ 将原始声音信号分成 N 个含相同样点数的片段，每个片段可嵌入1bit的信息；

④ 利用公式(2)进行每片嵌入，当 $d=d_0$，嵌入bit"0"；当 $d=d_1$，嵌入bit"1". d_0 和 d_1 选择的依据就是HAS，嵌入时的衰减系数设为0.4；.

⑤ 反复进行第④步，直到嵌入工作完成；

⑥ 把含有秘密信息的音频片段重新组合成一个完整的音频序列.

2.4 水印的提取

2.4.1 回声核位置的确定

提取嵌入隐藏信息的本质就是确定回声延时. 因为每个片段中的隐藏信息都是一个卷积性组合信号，所以直接确定回声延时存在困难，但可用卷积同态滤波来处理，将这个卷积性组合信号变为加性组合信号.

对于声音信号 $y[n]$，其复倒谱描述如公式(11)所示.

$$c_y[n]=F^{-1}(\log_e F(y[n])) \tag{11}$$

上式中，F，F^{-1} 分别表示傅立叶变换和傅立叶逆变换. 于是，公式(2)可用公式(12)来表示.

$$c_y[n]=F^{-1}(\log_e x(e^{j\omega}))+F^{-1}(\log_e h(e^{j\omega})) \tag{12}$$

公式(12)分别计算 $x[n]$ 和 $h[n]$ 的复倒谱，然后求和，即 $c_y[n]=c_x[n]+c_h[n]$. 对 $h[n]$ 求复倒谱如公式(13)所示.

$$c_h[n]=F^{-1}(\log_e h(e^{j\omega})) \tag{13}$$

其中，$h(e^{j\omega})=1+\alpha e^{j\omega}$.

由于 $\log_e(1+x)=x-\frac{x^2}{2}+\frac{x^3}{3}-\cdots\cdots(|x|<1)$，又因衰减系数 $0<\alpha<1$，可得公式(14).

$$\log_e h(e^{j\omega})=\alpha e^{-j\omega d}-\frac{\alpha^2}{2}e^{-2j\omega d}+\frac{\alpha^3}{3}e^{-3j\omega d}-\cdots\cdots \tag{14}$$

由公式(13)和公式(14)可推出公式(15).

$$c_n[n]=\alpha\delta[n-d]-\frac{\alpha^2}{2}\delta[n-2d]+\frac{\alpha^3}{3}\delta[n-3d]-\cdots\cdots \tag{15}$$

所以，当回声嵌入方法如公式(2)所示时，嵌入回声信号的复倒谱如公式(16)所示.

$$c_y[n]=c_x[n]+\alpha\delta[n-d]-\frac{\alpha^2}{2}\delta[n-2d]+\frac{\alpha^3}{3}\delta[n-3d]-\cdots\cdots \tag{16}$$

公式(15)中，$c_h[n]$ 中的非零值一定出现在 $d\times n$ 处. 也就是说，在复倒谱域 $c_y[n]$ 中，回声延时信号的位置一定会出现在峰值.

2.4.2 水印信息的恢复

提取后的水印信息是一维数据，将其升维为二维数据. 再将其送入去交织器，得到矩阵 M，对矩阵 M 进行DCT逆变换，就得到原始二值图像. DCT逆变换的方法如公式(17)所示.

$$X_{mn}=\sum_{p=0}^{M-1}\sum_{q=0}^{N-1}\alpha_p\alpha_q\mu\cos\frac{\pi(2m+1)}{2M}\cos\frac{\pi(2n+1)}{2N} \tag{17}$$

3 仿真实验

实验使用采样频率为44 kHz、16bits量化、时长30 s的一段音频，原始音频信息如图2所示. 原始水印图像为 64×64 像素大小，色深24位，原始水印图像如图3所示. 使用本文提出的方法，把水印信息嵌入原始音频后的效果如图4所示.

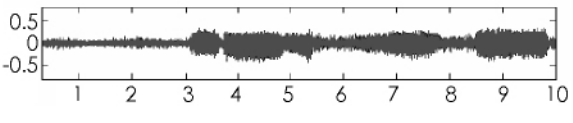

图2 原始音频信息

图 3　原始水印信息

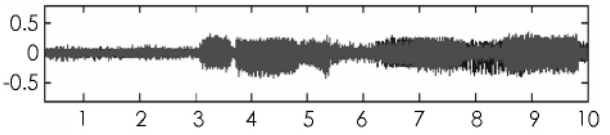

图 4　水印嵌入后的效果

在音频信号中嵌入水印图像，为评价提取的水印信息与原始信息的相似性，一般是用归一化相关系数(NC)作为评价标准，其定义如公式(18)所示，其中 W 为原始水印，W' 为提取出的水印，图像的大小是 $M_1 \times M_2$.

$$NC(W, W') = \frac{\sum_{i=1}^{M_1}\sum_{j=1}^{M_2} W(i, j)W'(i, j)}{\sqrt{\sum_{i=1}^{M_1}\sum_{j=1}^{M_2} W(i, j)^2} \times \sqrt{\sum_{i=1}^{M_1}\sum_{j=1}^{M_2} W'(i, j)^2}} \tag{18}$$

对本文提出的方法进行常见的攻击测试，相关 NC 值如表 1 所示.

把嵌入的水印看作是加载到原始音频上的噪声，通过计算信噪比(SNR)来衡量嵌入的水印信息对原信号的影响程度. 计算信噪比的方法如公式(19)所示，其中 x 为原始水印，x' 为提取出的水印，n 为音频采样的点数，L 为音频信号长度.

$$\mathrm{SNR} = 10 \times \log\left(\frac{I-1\sum_{n=0} x^2(n)}{\sum_{n=0}^{I-1}(x'(n) - x(n))^2}\right) \tag{19}$$

提取各种攻击下信噪比(SNR)的结果如表 2 所示.

表 1　各种攻击及其归一化系数 NC 值

攻击方式	NC
Write_lsbzero	1.000
Write_compressor	1.000
Write_zerocross	0.893
Write_exchange	0.987
Write_flippsample	0.859

表 2　不同方法得到的信噪比 SNR 结果

攻击方式	SNR
无攻击	27.110
加噪	24.683
重采样	24.106
滤波	17.041

4　结　　论

本文在分析已有的回声隐藏方法的各种优缺点后，提出了一种改进的算法. 该方法建立在回声隐藏基本原理之上，采用离散余弦变换提高信息隐藏效果；使用交织编码来纠正隐藏信息中的错误. 经过 MATLAB 仿真实验表明，在设置合理的衰减系数(本文 $\alpha = 0.4$)后，水印隐藏效果良好，算法简单且运算量小. 对嵌入水印的音频载体进行常规攻击后发现，本算法鲁棒性较高，具有一定的实用价值.

参考文献：

[1] 王育民，张　彤，黄继武. 信息隐藏－理论与技术 [M]. 北京：清华大学出版社，2006.

[2] BENDER W, GRUHL D, MORIMOTO N, et al. Techniques for Data Hiding [J]. IBM Systems Journal, 1996, 35(3－4): 313－336.

[3] 唐　升. 回声隐藏技术的研究 [D]. 西安：西北大学，2006.

[4] KIM H J, CHOUS Y H. A Novel Echo-Hiding Scheme with Backward Kernels [J]. IEEE Transactions on Circuits and Systems for Video Technology, 2003, 13(8): 885－889.

[5] OH H O, SEOK J W, HONG J W, et al. New Echo Embedding Technique for Robust and Imperceptible Audio Watermarking [C]. IEEE International Conference on Acoustics, Speech, and Signal Processing. Salt Lake City, USA: IEEE,

2001：1341－1344.

[6] 赵朝阳，刘振华，王 挺. 数字音频信号的回声数据隐藏技术 [J]. 计算机应用研究，2000，7：42－44.

[7] SHUANG-AN CHOUS, SHIH-FU HSIEH, KO-CHIANG LI. A Temporal Masking Technique and Its Performace Analysis for Audio Watermarking [C]. IEEE Intl Conf on Multimedia & Expo，2007，7：1774－1777.

[8] 彭 静，候祥勇，马 燕. 一种自适应图像灰度水印算法 [J]. 西南大学学报：自然科学版，2009，31(7)：171－175.

[9] 李元东. 基于模糊信息的群体多维偏好分析决策模型 [J]. 西南师范大学学报：自然科学版，2009，34(10)：82－87.

An Improved Algorithm for Echo Hiding

HU Da-hui， DU Zhi-guo

Dept. of Information Management，Southwest University，Chongqing 402460，China

Abstract：Echo hiding algorithm can be used to hide the watermark information by means of the time-domain masking effects of human auditory system. It relies on the basic principle that human ear can not distinguish the embedded weak signal before a strong signal disappears. As the recovery accuracy of echo hiding watermark is low，a hiding algorithm based on the discrete cosine transform and interleaving coding is proposed. The algorithm can be used to hide image watermark better after discrete cosine transform. In order to improve immunity against common attacks，the information is transformed into interleaved codes. Experiments show that this algorithm can be used to hide Watermark better and to recover efficiently，which is immune to the common malicious attacks effectively.

Key words：echo hiding；DCT；mixed code；normalized correlation coefficient

责任编辑 汤振金