

利用 PCM 量化编码的小波域音频信息伪装算法

张秋余, 黄羿博, 郑兰君

(兰州理工大学 计算机与通信学院, 甘肃 兰州 730050)

摘 要: 以能够同时兼顾隐蔽性与顽健性为目的, 提出了一种利用 PCM 量化编码在小波域来嵌入保密信息的音频信息伪装算法。通过引入 PCM 量化编码将小波系数分段均值量化为二进制序列, 可极大减小量化误差, 使用矩阵编码来嵌入秘密比特, 可提高嵌入效率与嵌入容量。实验结果表明, 该算法不仅具有较好的隐蔽性, 而且对加噪、低通滤波、重采样、Mp3 压缩、同步攻击等有较强的顽健性。

关键词: 信息隐藏; 音频信息伪装; PCM 量化编码; 浊音帧; DWT

中图分类号: TP309

文献标识码: A

文章编号: 1000-436X(2010)9A-0245-06

Audio steganography algorithm using PCM quantization coding in the DWT domain

ZHANG Qiu-yu, HUANG Yi-bo, ZHENG Lan-jun

(School of Computer and Communication, Lanzhou University of Technology, Gansu Lanzhou 730050, China)

Abstract: Considering the concealment and robustness of the audio steganography, using the pulse code modulation (PCM) quantization coding to embed secret message, an audio steganography algorithm was proposed. The PCM quantization coding was introduced to quantify the every segment's mean value of wavelet coefficient to a binary sequence. This method could greatly reduce the quantization error. Using matrix coding to embed secret bits could improve embedding efficiency and embedding capacity. The experimental results show that the algorithm not only has excellent concealment, but also has good robustness against noise addition, lowpass filtering, resampling, MP3 compression and synchronization attack.

Key words: information hiding; audio steganography; pulse code modulation quantization coding; voiced frames; DWT

1 引言

由于人耳听觉系统 (HAS, human auditory system) 的高灵敏性, 以音频为载体的信息隐藏技术的研究比图像信息隐藏更为困难, 其发展也相对滞后, 但近几年随着网络音乐在互联网上的广泛传播以及音频压缩技术的成熟, 对音乐版权保护的呼声越来越高, 从而使音频信息隐藏技术的研究受到了更多关注。

经典的音频信息隐藏算法主要分为时域算法和

变换域算法, 包括 LSB 算法、回声隐藏算法、相位编码算法、扩展频谱算法、DCT/DWT 域算法等, 而目前比较流行的嵌入算法主要有以下几大类, 直接相加法^[1,2]、量化调制法^[3-5]、修改能量比法^[6,7]、修改统计量法^[8]以及 Pathwork 算法^[9], 此外在结合人耳听觉掩蔽特性^[10,11]和抗同步攻击^[12-14]方面也进行了很多研究。通常根据应用需要的不同, 算法的侧重方面也不同, 数字水印侧重于顽健性, 而保密通信则侧重于隐蔽性与嵌入容量。但是大量的实

收稿日期: 2010-08-10

基金项目: 甘肃省自然科学基金资助项目 (0803RJZA024)

Foundation Item: The Natural Science Foundation of Gansu Province (0803RJZA024)

实践发现，对于音频信息隐藏系统，不论何种应用需求，都要同时兼顾顽健性与隐蔽性，尤其是顽健性，否则就不是一个安全的、可用的信息隐藏系统。

本文提出一种能够较好地兼顾顽健性、隐蔽性与嵌入容量的基于 PCM (pulse code modulation) 量化编码的小波域音频信息伪装算法。算法有以下几个特点：1) 在嵌入前使用混沌映射对秘密信息进行调制，使隐写系统符合密码学中的 Kerckhoff 原则，从而提高了算法的安全性；2) 将秘密比特嵌入在利用语音时域参数确定的浊音帧中，利于系统隐蔽性的提高；3) 对嵌入帧的小波低频系数分段，对每段的统计均值进行 PCM 量化编码，而不是单个系数，从而使系统具有较好的稳健性；4) 使用矩阵编码对每段的统计均值末三位中的一位进行修改或不修改来嵌入秘密比特，矩阵编码的应用可提高嵌入效率与嵌入容量，并能够减小修改比例；5) 使用巴克码作为同步码，与每段秘密比特组合依次在浊音帧中嵌入，使得算法具有良好的抗同步攻击性能，并且可实现盲检测。

2 PCM 量化编码

PCM 量化编码是最早也是目前应用得比较广泛的模/数变换的方法，它具体包括抽样、量化和编码 3 个步骤。算法中要将承载秘密比特的数据通过 PCM 量化编码转换为二进制序列。我国 PCM 系统中采用 13 折线近似 A=87.6 的 A 律压扩特性，如图 1 所示。但是在实验中发现，由于存在数值很小的数据，甚至小于所设定的最小量化间隔，从而导致

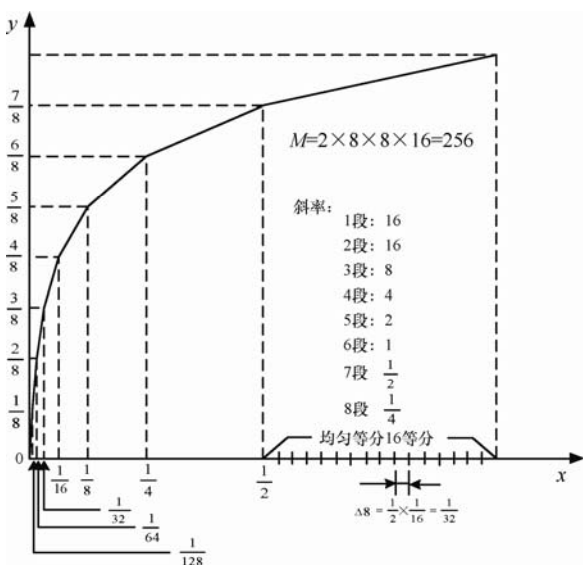


图 1 A 律 13 折线压扩特性

一些幅度微弱的信号经过量化以后幅度变为零，这样的误差会影响语音信号的音质，因此，在对信号做 PCM 量化编码之前，首先使用 μ 律压缩，将微小信号进行一定程度的放大，可以有效地减小量化误差。 μ 律压扩方程为

$$y = \frac{\ln(1 + \mu x)}{\ln(1 + \mu)} \quad 0 \leq x \leq 1 \quad (1)$$

这里 $\mu=255$ ，然后对经过 μ 律压扩以后的数据进行量化编码，最小量化间隔设为最大值的 1/4 096。而编码就是将所有的量化级按其量化电平大小的次序排列起来，列出各自对应的码字，这里采用 8bit 折叠二进制码。

3 水印图像的预处理

为了提高抗干扰能力和安全性，消除二值水印图像的像素空间相关性，在嵌入前对图像进行混沌调制，提取后经混沌解调才能恢复水印图像。混沌序列具有良好的伪随机性，它对初始值极端敏感，改变初始值可以得到任意长度的不同序列。这里采用一维 Logistic 映射^[6]，定义为

$$h_{k+1} = \mu h_k (1 - h_k), k = 0, 1, 2, \dots \quad (2)$$

其中， $h_k \in (0, 1)$ ， $\mu \in [0, 4]$ 。当 $\mu=4$ 时，系统完全处于混沌状态。

通过定义阈值，将混沌序列量化为二值序列 $M=[m(1), m(2), m(3), \dots](m(i) \in \{0, 1\})$ ，即

$$m(x_k) = \begin{cases} 0, & 0 \leq h_k < 0.5 \\ 1, & 0.5 \leq h_k \leq 1 \end{cases} \quad (3)$$

水印图像降维以后形成一维二值序列 $w=[w(1), w(2), w(3), \dots](w(i) \in \{0, 1\})$ ，然后通过式(4)进行调制，得到调制后的序列 s ，将 s 升维便得到一幅完全杂乱无章的图像。

$$s(i) = m(i) \oplus w(i) \quad (4)$$

图 2 为原始水印图像与经过混沌调制以后的水印图像，可以看出，经过置乱以后原始水印再无任何规律可言，第三方非法用户在无初值密钥的情况下无法恢复出有意义的水印信息。



(a) 原始水印信息 (b) 混沌调制后的水印信息

图 2 置乱前后水印信息

4 秘密信息的嵌入

4.1 嵌入帧的选择

由于语音信号的短时平稳特性，采用连续的方式对原始音频分帧，通常一帧的长度取为 10~30ms，每秒的帧数为 33~100，视实际需要确定，每帧的长度记为 N 。本文使用每帧信号的短时能量 E 和短时过零率 Z 这 2 个时域参数来确定浊音帧。

一帧语音信号的短时平均能量为

$$E = \sum_{m=1}^N x^2(m) \quad (5)$$

短时平均能量给出了区分清音段与浊音段的基础，通常 $E^{(清)} \gg E^{(浊)}$ ，而且大致定出浊音语音变为清音语音的时刻，或反之。

一帧信号的短时过零率为

$$Z = \sum_{m=1}^N |\text{sgn}[x(m)] - \text{sgn}[x(m-1)]| \quad (6)$$

其中， $\text{sgn}[\cdot]$ 为符号函数。高频率意味着有高的过零率，低频率意味着有低的过零率， Z 与能量的频率分布有密切的关系，而浊音语音能量约集中在 3kHz 以下，清音语音则多集中于较高的频率上，所以过零率对判断浊/清音段很有用。

关于定量的分析要通过大量的实验统计来得到，依据所选则载体音频的采样率 f_s 和 N 来选取合适的短时能量阈值 T_1 ，短时过零率阈值 T_2 ，当 $E > T_1$ ， $Z > T_2$ 时，确定此帧为浊音段。

4.2 同步码的处理

抗同步攻击的方法有很多，但外加同步码的方法仍然是当前比较简便而稳妥的方法。还有一种研究比较多的自同步法，它是利用载体自身特征来确定嵌入位置，不需要外加同步码，可节省载体资源，但是实施嵌入以后，载体自身特征会发生变化，给正确提取带来困难。因此，选用外加 16bit 巴克码作为同步码，将同步码与秘密比特如图 3 所示组成一个二进制码组，一个同步码组携带一定数量的秘密比特嵌入在一帧载体信号中。同步码的另外一个重要作用就是实现盲检测，因为在接收端，原始信号已被修改，若再次利用寻找浊音帧的方法确定嵌入帧则可能出现错误，而利用同步码就不会出现错误确定嵌入帧的问题。

同步码	秘密比特	同步码	秘密比特	...
-----	------	-----	------	-----

图 3 秘密比特与同步码的组合

4.3 数据的嵌入

首先，将所确定的浊音帧 $Q(n), n=1, 2, \dots, N$ 做 H 级离散小波变换，得到小波变换系数 $\{A_H, D_H, D_{H-1}, \dots, D_1\}$ ，考虑到小波变换的低频分量能够抵御各种干扰，因而选用低频分量 A_H 来嵌入隐密数据，将 A_H 记为一个一维数组 $x(i) = \{c_i | c_i \in (A_H)\}, i=0, 1, \dots, \text{length}(A_H)$ ，对该数组分段，每段长度为 k ，共分为 $d = \lceil \text{length}(A_H)/k \rceil$ 段，即该帧共有 d 个位置承载秘密比特，其中一段记为 $X(j) = \{x(0+kj), \dots, x(k-1+kj)\}, j=0, 1, \dots, d-1$ 。参数 k 可作为另一密钥来提高系统安全性， k 的选择与嵌入强度和嵌入容量相关， k 越大，嵌入强度和嵌入容量越小， k 越小，嵌入强度和嵌入容量越大，当然，嵌入强度越大，稳健性越强，而隐蔽性越低，嵌入强度越小，则稳健性越弱，隐蔽性越高，因而参数 k 的选择直接关系着嵌入水印后的信噪比高低。

分别计算每段的均值 $\bar{X}(j)$ ：

$$\bar{X}(j) = \frac{1}{k} \sum_{i=0}^{k-1} x(i+kj) \quad (7)$$

先用 μ 律压缩，再用 PCM 量化编码方法将 $\bar{X}(j)$ 编码为 8bit 二进制序列，记为 $a_i, i=0, 1, \dots, 7$ 。

矩阵编码是密写编码的一种，目的是使用尽可能少的改动隐藏尽可能多的隐密信息^[15]，使用该方法可以减少对原始信号的修改比例，对提高系统的隐蔽性与嵌入容量有重要作用。算法通过修改或不修改均值二进制表示的末三位中的一位来嵌入 2bit 秘密比特。设同步码与秘密信息的组合为 $tw(j)$ ：

1) 若 $tw(j) = a_5 \oplus a_7, tw(j+1) = a_6 \oplus a_7$ ，不改变原始数据；

2) 若 $tw(j) \neq a_5 \oplus a_7, tw(j+1) = a_6 \oplus a_7$ ，改变 a_5 ；

3) 若 $tw(j) = a_5 \oplus a_7, tw(j+1) \neq a_6 \oplus a_7$ ，改变 a_6 ；

4) 若 $tw(j) \neq a_5 \oplus a_7, tw(j+1) \neq a_6 \oplus a_7$ ，改变 a_7 。

嵌入后做 PCM 解码得到 $\bar{X}'(j)$ ，相应修改该段的各个系数：

$$x'(i+kj) = x(i+kj) + (\bar{X}'(j) - \bar{X}(j)) \quad (8)$$

$$i = 0, \dots, k-1, \quad j = 0, \dots, d-1$$

嵌入后， $x'(i)$ 即为修改后的 A'_H 的各系数，对 $\{A'_H, D_H, D_{H-1}, \dots, D_1\}$ 做小波逆变换，重构得到载密音频。

5 隐秘信息的检测

本文算法属盲检测算法，提取时无需原始音频

信号，检测过程如下：

1) 对载密信号按指定的样点数 N 进行分帧，逐帧做 H 级离散小波变换，提取低频系数 A_H ；

2) 将 A_H 记为 $x(i)=\{c_i|c_i \in (A_H, D_H)\}, i=0,1, \dots, length(A_H)$ ，以长度 k 进行分段，各段为 $X(j)=\{x(0+kj), \dots, x(k-1+kj)\}, j=0,1, \dots, d-1$ ，分别计算每段均值 $\bar{X}(j)$ ；

3) 对 $\bar{X}(j)$ 先做 μ 律压缩，再做 PCM 量化编码，变换为二进制序列 $a_i, i=0,1, \dots, 7$ ，并对末三位做矩阵解码，得到秘密比特 $tw'(j)$ ，如式(9)和式(10)：

$$tw'(j)=a_5 \oplus a_7 \tag{9}$$

$$tw'(j+1)=a_6 \oplus a_7 \tag{10}$$

4) 先提取每帧信号前 16bit 做同步码比对，若与嵌入的巴克码相似度高于 0.98，则判断为嵌入帧，继续提取后面的数据，否则为非嵌入帧，不再继续操作，跳到下一帧检测；

5) 去掉同步码，得到秘密比特 $s'(i)$ ，用初值密钥重新生成混沌序列 h_k ，再量化为二值序列 $M=[m(1),m(2),m(3), \dots](m(i) \in \{0,1\})$ ，用混沌序列对秘密比特解调得到二值序列 $w'(i)$ ：

$$w'(i)=m(i) \oplus s'(i) \tag{11}$$

对 $w'(i)$ 升维完成水印的提取。

6 实验及算法性能分析

实验是在 MATLAB 7.0 平台上完成的，载体音频是采样率为 44.1kHz，分辨率为 16bits 量化的单声道数字音频信号，其内容为“speech that you may say”的一段男生语音，帧长 1024 个样点。水印为 64×64 的二值图像，图像内容为黑底白字“密”。混沌序列初值选取为 0.25011。小波变换采用的常见的 daubechies-4 小波基，小波变换级数选取为 $H=3$ 。同步码选用了码长为 16bit 的巴克码 1111100110101110。

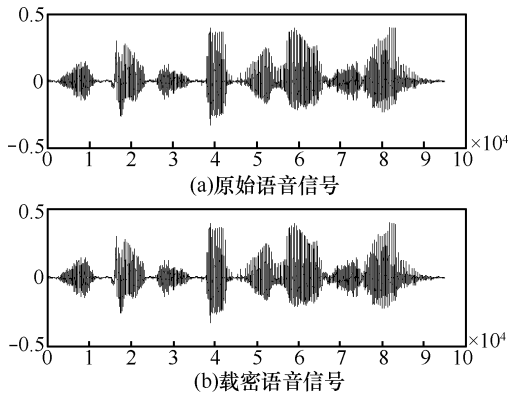


图 4 原始语音与载密语音

在无攻击条件下，原始音频和载密音频的波形如图 4 所示，2 个音频信号差异微小，两者幅度值的最大差值不足 1.7×10^{-3} ，声音试听结果在主观听觉上，原始音频与载密音频几乎没有差异。说明在无攻击情况下算法的不可感知性较好。

本文采用如下 3 个常用的性能指标来客观评价系统性能。

1) 信噪比：用来衡量载密音频的客观音质，即它的隐蔽性。 $x(n)$ 和 $x'(n)$ 分别表示原始音频信号和载密音频信号。

$$SNR = 10 \lg \left\{ \frac{\sum_{n=0}^{N-1} x^2(n)}{\sum_{n=0}^{N-1} [x'(n) - x(n)]^2} \right\} \tag{12}$$

2) 归一化相关系数：对提取出的保密语音和原始经过压缩编码以后的保密语音的相似性做客观评价， $S(i)$ 和 $S'(i)$ 分别表示原始经过压缩编码以后的保密语音和提取出的保密语音。

$$\rho(S, S') = \frac{\sum S(i)S'(i)}{\sqrt{\sum S(i)^2} \sqrt{\sum S'(i)^2}} \tag{13}$$

3) 误码率：错误提取的秘密比特数与总共嵌入的比特数（不包括同步码）的比值。

$$BER = \frac{1}{N} \sum_{i=0}^{N-1} \begin{cases} 1, & s'(i) \neq s(i) \\ 0, & s'(i) = s(i) \end{cases} \tag{14}$$

对含有水印的语音信号分别进行加噪、低通滤波、重采样、随机剪切和 MP3 压缩，处理后提取出的水印如图 5 所示，可以看到本算法对常规信号处理有较好的顽健性。



图 5 几种攻击下提取的水印效果

为了验证本算法的优越性，使用相同的宿主音频，嵌入同样的数据，用 2 个典型变换域隐藏算法与之进行性能测试比较，如图 6 所示。

算法 1^[5] 使用相同的同步信号，用均值量化法嵌入在时域音频样本中，而用相加法将秘密数据

嵌入在小波域低频分量的平均值内。

算法 2^[16] 用量化信噪比自适应确定量化步长，用单值量化嵌入的方法将秘密数据嵌入在小波低频分量绝对值最大的系数中。

算法 3 本文算法。

信息隐藏的嵌入容量与隐蔽性是一对矛盾，取一帧信号对算法 1 和算法 3 进行比较（算法 2 因嵌入量固定，且用单值量化法，在这里不进行比较），只计算所嵌入的有意义秘密数据（除去同步数据量）。

从图 6 可以看到，当嵌入容量较低时，各算法均有良好的隐蔽性，而随着嵌入容量的加大，隐蔽性会受到影响，但受影响程度不同。本算法使用 PCM 量化编码，量化步长非常小，同时又引入了矩阵编码的嵌入方法，提高了嵌入效率并减小了修改比例，因而随着嵌入容量的加大，隐蔽性明显优于算法 1。这也说明本算法在保证良好隐蔽性的前提下具有较大的嵌入容量。

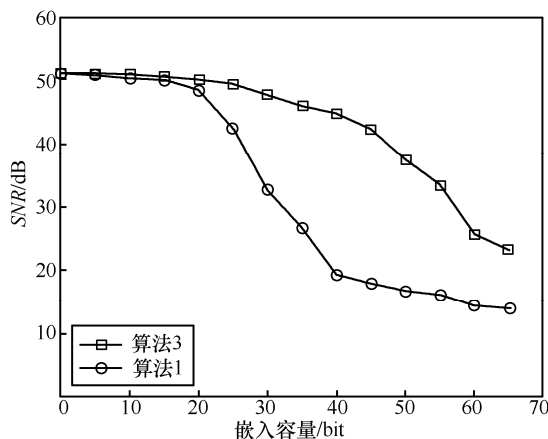


图 6 2 个算法隐蔽性随嵌入量变化的比较

表 1 给出了 3 种算法抗攻击性能的比较结果，从实验得出以下结论。

1) 相比较其他攻击而言，重量化对单值量化算法的影响较大，提取秘密信息的误码率较高，这是

因为重量化再次引入了量化误差。但可以看出，算法 3 和算法 1 抵抗该攻击的性能较好，因为本文是在小波域使用均值量化的方法，重量化对小波系数统计均值的影响微乎其微。

2) 载密音频下采样到 22.05kHz，再上重采样到 44.1kHz,对提取保密数据的影响较小，算法 3 优于文献[16]的算法，但是若下采样到 11.025kHz，再上采样到 44.1kHz，则载密音频的音质会受到一定程度的影响，而且提取秘密数据的误码率过高，因为下采样过度会导致大量数据丢失。

3) 为了抵抗常见的低通滤波，算法 3 将保密信息嵌入在载体音频的低频部分，且语音信号能量主要集中在低频部分，滤除高频对低频的影响很小，实验表明，在经过截止频率在 9kHz 以上的低通滤波后算法仍然保持了很高的恢复率。

4) 在加入高斯白噪声之后，3 个算法都具有较强的抵抗能力，当加入强度过大时，载密音频都会有一定程度的失真，但由于采用的是量化小波系数统计均值的方法，因此当加入的噪声强度适中时，对提取秘密数据的影响非常小。因此，算法 3 对加噪攻击具有较强的顽健性。

5) 算法抵抗延时和回声攻击的顽健性较强，因为延时与回声并不会改变音频样值，而且同步码的使用很好地预防了这类攻击。

6) 将载密音频由 wav 格式转换为 MP3 格式，再由 MP3 格式转换为 wav 格式。从实验结果可见，算法 3 抵抗普通 MP3 攻击的能力很强。

7) 实验验证了巴克同步码的使用对抵抗如随机剪切这种同步攻击非常有效，当剪切比例适中时，对载密音频音质的影响非常小，而且能够较好地提取出保密数据，恢复的水印图像清晰可辨。

通过分析，可知本文算法对常见信号处理与几何攻击有较强的抵抗能力。

表 1 算法对部分常规攻击的抵抗能力

算法	性能指标	未攻击	重量化	重采样 22.05kHz	重采样 11.025kHz	加噪	低通滤波	延时	回声	MP3 压缩	随机剪切 10%
1	ρ	1	0.96	0.98	0.90	0.96	0.98	0.97	0.97	0.89	0.94
	BER/%	0	0.72	0.88	10.13	0.53	0.24	0.65	0.89	2.21	1.98
2	ρ	1	0.92	0.95	0.89	0.95	0.91	0.95	0.94	0.82	0.87
	BER/%	0	3.68	3.32	14.31	2.35	1.07	1.78	1.65	3.32	2.96
3	ρ	1	0.94	0.97	0.90	0.96	0.97	0.98	0.98	0.92	0.96
	BER/%	0	0.89	0.92	10.85	0.66	0.38	0.42	0.31	1.96	1.02

7 结束语

本文提出了一种基于 PCM 量化编码的小波域音频信息伪装算法。在隐蔽性方面, 算法通过选择浊音帧来确定嵌入帧, 并用改动比例较小的矩阵编码来实施嵌入, 这些做法保证了系统的不可感知性。在顽健性方面, 选择嵌入帧小波变换的低频系数作为嵌入位置, 并利用均值 PCM 量化编码的方法, 以及巴克同步码的使用, 这些都是为系统的抗攻击性方面考虑, 实验结果也验证了其优越的顽健性。在嵌入量方面, 矩阵编码的应用大大提高了嵌入效率, 是同类均值量化算法嵌入容量的一倍。同时, 水印图像混沌置乱的应用使该系统符合 Kerckhoff 原则。因此, 本文提出的算法是一个兼顾隐蔽性、顽健性与嵌入量的安全的音频信息伪装算法。

参考文献:

- [1] 刘泉, 高庆. 基于 DWT 的自适应盲音频水印算法[J]. 武汉理工大学学报, 2008, 30(1):68-79.
LIU Q, GAO Q. Adaptive blind digital audio watermarking algorithm based on DWT[J]. Journal of Wuhan University of Technology, 2008, 30(1):68-79.
- [2] CHEN X S, ZHANG X, YANG Y T. Reacher for adaptive audio information hiding approach based on DWT[A]. Proc of CCDC 2008[C]. Yantai, Shandong, 2008. 3029-3033.
- [3] VIVEKANANDA B K, Indranil sengupta, abhijit das audio watermarking based on mean quantization in cepstrum domain[A]. Proc of ADCOM 2008[C]. Chennai, 2008. 73-77.
- [4] KALANTARI N K, AHADI S M, KASHI A. A robust audio watermarking scheme using mean quantization in the wavelet transform domain[A]. Proc of ISSPIT2007[C]. Cairo, Egypt, 2007. 198-201.
- [5] 王向阳, 牛盼盼. 基于音频统计特性的数字水印嵌入算法[J]. 自动化学报, 2008, 34(8):1001-1003.
WANG X Y, NIU P P. A content-based digital audio watermarking scheme[J]. Acta Automatica Sinica. 2008, 34(8):1001-1003.
- [6] 张晓明, 殷雄. 基于混沌序列的小波域语音信息隐藏方法[J]. 系统仿真学报, 2007, 19(9):2113-2117.
ZHANG X M, YIN X. Speech information hiding approach in wavelet domain based on chaotic sequence[J]. Journal of System Simulation, 2007, 19(9):2113-2117.
- [7] 陈雪松, 金七顺, 杨永田. 全球移动通信系统中语音信息隐藏算法的研究[J]. 计算机应用, 2007, 27(4):841-845.
CHEN X S, JIN Q S, YANG Y T. Study on a voice hiding algorithm in GSM communication[J]. Journal of Computer Applications, 2007, 27(4):841-845.
- [8] 戴志强, 俞一彪, 颜祥等. 一种基于多重统计量分析的稳健语音信息隐藏算法[J]. 信号处理, 2008, 24(3):500-503.
DAI Z Q, YU Y B, YAN X, *et al.* A robust information hiding algorithm in wavelet domain of speech signal based on multi-statistic analysis[J]. Signal Processing, 2008, 24(3):500-503.
- [9] SLUCIAK O, VARGIC R. An audio watermarking method based on wavelet patchwork algorithm[A]. Proc of IWSSIP 2008[C]. Bratislava, 2008.117-120.
- [10] 全笑梅, 张鸿宾. 基于小波包域听觉感知分析的统计音频水印算法[J]. 电子学报, 2007, 35(4):673-677.
QUAN X M, ZHANG H B. Statistical audio watermarking algorithm based on auditory analysis in wavelet packet domain[J]. Acta Electronica Sinica, 2007, 35(4):673-677.
- [11] DELFOROUZI A, POOYAN M. Adaptive digital audio steganography based on integer wavelet transform[A]. Proc of IIHMSP2007[C]. Kaohsiung, 2007. 283-286.
- [12] LIN K Z, FAN B, YANG W. Robust audio watermarking scheme based on wavelet transforming stable feature[A]. Proc of CIS2008[C]. Suzhou, 2008. 325-329.
- [13] POOYAN M, DELFOROUZI A. Adaptive and robust audio watermarking in wavelet domain[A]. Proc of IIHMSP2007[C]. Kaohsiung, 2007.287-290.
- [14] 雷赞, 刘建, 严波等. 窄带的自同步音频水印算法[J]. 计算机学报, 2008, 31(7):1283-1290.
LEI Y, LIU J, YAN B, *et al.* Narrowband-based audio watermarking with self-synchronization[J]. Chinese Journal of Computers, 2008, 31(7):1283-1290.
- [15] 王朔中, 张新鹏, 张开文. 数字密写与密写分析[M]. 北京: 清华大学出版社, 2005.
WANG S Z, ZHANG X P, ZHANG K W. Steganography and Steganalysis[M]. Beijing: Tsinghua University Press, 2005.
- [16] 付永庆, 孙滢. 一种新的基于小波变换的自适应量化音频水印算法[J]. 哈尔滨工程大学学报, 2007, 28(9): 1052-1055.
FU Y Q, SUN Y. A new adaptively quantized audio watermark algorithm based on wavelet transform[J]. Journal of Harbin Engineering University, 2007,28(9):1052-1055.

作者简介:



张秋余 (1966-), 男, 河北辛集人, 兰州理工大学研究员, 兰州理工大学计算机与通信学院副院长, 主要研究方向为信息隐藏与隐写分析、图像理解与识别、网络与信息安全。

黄羿博 (1982-), 男, 甘肃兰州人, 兰州理工大学硕士生, 主要研究方向为语音信号处理、信息隐藏和数字水印。

郑兰君 (1983-), 女, 甘肃兰州人, 兰州理工大学硕士生, 主要研究方向为语音信号处理和信息安全。