

基于 DCT 域 QIM 的音频信息伪装算法

陈铭^{1,2,3}, 张茹^{1,2,3}, 刘凡凡^{1,2,3}, 钮心忻^{1,2,3}, 杨义先^{1,2,3}

(1. 北京邮电大学 网络与交换技术国家重点实验室信息安全中心, 北京 100876;

2. 北京邮电大学 网络与信息攻防技术教育部重点实验室, 北京 100876; 3. 灾备技术国家工程实验室, 北京 100876)

摘要: 音频与图像相比具有信息冗余大、随机性强的特点, 在音频中实现无误码的信息提取的难度更大。提出一种基于 DCT 域 QIM(quantization index modulation)的音频信息伪装算法, 算法特点如下: 应用 QIM 原理, 以量化的方式嵌入信息, 根据量化区间与信息比特的映射关系提取信息, 可实现盲提取; 采用改进的 QIM 方案, 针对信息提取的误码, 在嵌入端与提取端进行容错处理, 保证了隐藏信息的强顽健性; 隐藏容量大, 可达 357.6bit/s。实验表明, 算法与传统 QIM 方法相比具有更好的不可感知性, 100%嵌入的载密音频的信噪比在 30dB 以上, 并且对于 MP3 压缩、重量化、重采样、低通滤波等攻击具有很强的顽健性, 同时算法运算量小, 易于实现, 实用性强。

关键词: 信息隐藏; 音频信息伪装; QIM; DCT; 强顽健性

中图分类号: TP309

文献标识码: B

文章编号: 1000-436X(2009)08-0105-07

Audio steganography by quantization index modulation in the DCT domain

CHEN Ming^{1,2,3}, ZHANG Ru^{1,2,3}, LIU Fan-fan^{1,2,3}, NIU Xin-xin^{1,2,3}, YANG Yi-xian^{1,2,3}

(1. Information Security Center, State Key Laboratory of Networking and Switching Technology,

Beijing University of Posts and Telecommunications, Beijing 100876, China; 2. Key Laboratory of Network and Information

Attack & Defense Technology of MOE, Beijing University of Posts and Telecommunications, Beijing 100876, China;

3. National Engineering Laboratory for Disaster Backup and Recovery, Beijing 100876, China)

Abstract: Audio signal has more information redundancy than image signal, but its randomness is stronger. It is more challenge to extract embedded bit with non-error from audio. A novel audio steganography based on QIM (quantization index modulation) in the DCT (discrete cosine transform) domain was proposed. The merits of the algorithm were as follows: based on the principle of QIM, the message was embedded by quantization method and was extracted by the mapping between message bit and quantization interval. The extraction was executed blindly; the robustness of the hidden message was ensured well by the improved QIM, which employed the error-tolerance operation during embedding and extracting; the capacity was large as 357.6bit/s. The experimental results show that the proposed method achieves better imperceptibility than normal QIM and the SNR (signal to noise ratio) of the stego audio with the embedding rate of 100% is above 30dB. The embedded message has good robustness against MP3 compression, requantization, resampling and lowpass filtering. Moreover, the algorithm is easy to implement and highly practicable.

Key words: information hiding; audio steganography; QIM; DCT; strong robustness

收稿日期: 2009-01-04; 修回日期: 2009-06-10

基金项目: 国家重点基础研究发展计划(“973”计划)基金资助项目(2007CB311203); 国家自然科学基金资助项目(60821001, 90604022); 高等学校博士学科点专项科研基金资助项目(20070013007)

Foundation Items: The National Basic Research Program of China (973 Program) (2007CB311203); The National Natural Science Foundation of China (60821001, 90604022); The Specialized Research Fund for the Doctoral Program of Higher Education (20070013007)

1 引言

信息隐藏技术起源于古老的隐写术,以图像、音频、视频等数字媒体为载体的信息伪装技术与检测技术构成了现代信息隐藏技术研究的主体。基于音频的隐藏技术在信息伪装技术中占有重要地位,目前主要包括时域、频域、扩频以及相位编码的隐藏方法^[1~7]。

QIM 是由 Chen 等^[8]提出的一种基于指标量化的隐藏方法,构造一个或一组包含索引集的量化器,以隐藏信息去调制索引集中的索引值,再对载体信号以相应的量化器进行量化,以量化的方式嵌入信息,QIM 在隐藏容量、顽健性以及不可感知性 3 个方面达到了很好的折衷。

传统的 QIM 技术采用均匀量化的方法^[9~12],固定量化步长,将量化对象直接量化至量化步长的中点值,传统方法的最大的缺点是引入了较大的量化噪声,因此对于量化噪声引起的数据波动而导致的提取误码不够顽健。针对这一缺陷,本文提出一种改进的 QIM 方案,构造音频 DCT 域 QIM 量化器,量化器针对 QIM 的固有量化噪声进行了容错处理,提高了嵌入信息的顽健性,并且信息提取无需原始载体音频信息,可实现盲提取。

2 DCT 特性分析

DCT 作为一种性能优良的正交变换方式,具有如下特性。

1) 熵保持特性,信号在 DCT 前后信息保持不变;

2) 能量保持与集中特性,信号在 DCT 前后总能量保持不变,同时对能量重新分配,能量集中特性是 DCT 的一个显著特点,这使得只用少量系数就可代表信号的大部分能量;

3) 稳定性,对音频信号施加小的扰动,对应到 DCT 域中的变换系数将不会产生大的变化,反之,DCT 域中的变换系数发生小的变动,对应到时域信号会将变动分散到整个信号中,也不会产生大的变化。

结合 DCT 的能量集中特性和稳定性,将所要隐藏的信息以一种弱噪声的形式,嵌入到音频信号的主要能量分量中,既可保证信息的嵌入不会引起大的信号失真,同时也使隐藏信息获得较好的顽健性。

3 QIM 方案设计

结合 DCT 的稳定性,本文构造了音频 DCT 域的 QIM 量化器,在 DCT 系数中应用 QIM 量化器,以量化的方式嵌入信息。

令 C 为载体音频信号: $C = \{c_i, 0 \leq i \leq L\}$, 其中 $c_i \in \{0, 1, \dots, 2^p - 1\}$ 表示采样点值, L 为采样点总数, p 为每个采样点的编码比特数,对 C 做分段 DCT,记每个分段的长度为 l ,以 $F_i = \{f_i(k) | f_i(k) = \text{DCT}(C_i), 0 \leq i \leq L/l, 0 \leq k \leq l\}$ 表示各个分段 C_i 的 DCT 结果,其中 $f_i(k)$ 表示第 i 个音频分段的第 k 个系数,以 Δ 表示量化器的量化步长,以 $E = \{e_i, 0 \leq i \leq N\}$ 表示待隐藏的信息,其中 $e_i \in \{0, 1\}$ 为信息比特, N 为秘密信息比特数。音频信号 C 的一维 l 点 DCT 和 IDCT 定义如式 (1), 其中

$$\begin{cases} F(k) = a(k) \sum_{i=0}^{l-1} c_i \cos \frac{(2i+1)k\pi}{2l}, & k = 0, 1, \dots, l-1 \\ c_i = \sum_{k=0}^{l-1} a(k) F(k) \cos \frac{(2i+1)k\pi}{2l}, & i = 0, 1, \dots, l-1 \end{cases} \quad (1)$$

3.1 QIM 方案

QIM 方案首先是构造一个步长为 Δ 的量化器,量化器包括对量化区间划分和区间序号分配,量化器如图 1 所示。量化器对系数的整个取值区间以 0 为起点,以 Δ 为量化步长分别向正负方向将取值区间分割为若干个量化区间,对每一个量化区间赋予一个区间序号 S_i ,序号定义方式如式(2),其中 $\lfloor \cdot \rfloor$ 表示向下取整。

$$S_i = \begin{cases} \lfloor f_i(k) / \Delta \rfloor, & f_i(k) \geq 0 \\ \lfloor f_i(k) / \Delta \rfloor - 1, & f_i(k) < 0 \end{cases} \quad (2)$$

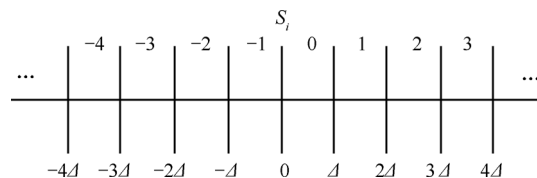


图 1 QIM 量化器

QIM 方案的核心步骤是利用量化器建立量化区间与信息比特的映射关系,利用映射关系嵌入信息,映射关系定义为:以量化区间序号 S_i 的 LSB 代表信息比特 e_i ,即 $e_i = \text{LSB}(S_i)$ 。本文的 QIM 方案

具体描述如下: 以 $f_i'(k)$ 表示嵌入信息后的系数, 信息比特 e_i 对应的嵌入位置的系数 $f_i(k)$ 所在的量化区间为 S_i , 当 $e_i = LSB(S_i)$ 时, 系数 $f_i(k)$ 保持不变, 即 $f_i'(k) = f_i(k)$; 否则将系数 $f_i(k)$ 调整至与其最接近的量化区间内, 调整幅度是将 $f_i(k)$ 移至与最相邻的量化区间边界距离为 δ 的位置。以 $mid = (2S_i + 1)2/\Delta$ 表示区间 S_i 的中点, 上述 QIM 方案的数学形式表述为

$$f_i'(k) = \begin{cases} f_i(k), & \text{if } e_i = LSB(S_i) \\ (S_i + 1)\Delta + \delta, & \text{if } e_i \neq LSB(S_i), \\ & mid < f_i(k) < (S_i + 1)\Delta \\ S_i\Delta - \delta, & \text{if } e_i \neq LSB(S_i), S_i\Delta < f_i(k) < mid \end{cases} \quad (3)$$

3.2 量化噪声误差分析

嵌入与提取需要对音频信号做两次 DCT, 而 QIM 方案不可避免地引入了量化噪声, 从而引起数据波动, 使得嵌入信息后和提取信息前的两次 DCT 结果之间产生系数波动, 最终导致提取时出现误码, 因此需要在嵌入端和提取端进行容错处理, 以提高隐藏信息对数据波动的顽健性, 保证信息提取无误码。

由 QIM 方案可知, 在信息嵌入端只改动所在区间序号的 LSB 与信息比特不同的系数, 即 $e_i \neq LSB(S_i)$ 的系数, 而对 $e_i = LSB(S_i)$ 的系数保持不变, 但对于临近量化区间边界而又满足 $e_i = LSB(S_i)$ 的系数, 由于很接近量化区间的边界, 一旦在两次 DCT 之间产生波动, 将会发生系数越界现象, 如图 2 所示。假设嵌入位置 i 的系数 $f_i(k)$ 满足 $e_i = LSB(S_i)$, $f_i(k)$ 与最接近的量化区间边界距离为 ρ , 嵌入信息后 $f_i(k)$ 不变, 但在信息提取端对载密音频做 DCT 后位置 i 的系数 $f_i'(k)$ 相对于 $f_i(k)$ 产生了大小为 ε 的波动, 当 $f_i'(k)$ 在最接近的量化区间边界方向上的波动大于与边界之间的距离时, 即当 $\varepsilon > \rho$ 时, $f_i'(k)$ 就发生越界而位于 S_i 相邻的量化区间内, 嵌入信息比特后的区间序号 S_i' 变为 S_{i+1} 或者 S_{i-1} , 此时按照映射关系 $e_i' = LSB(S_i')$ 提取信息比特就将产生误码, 使得 $e_i' = e_i + 1$ 或 $e_i' = e_i - 1$ 。

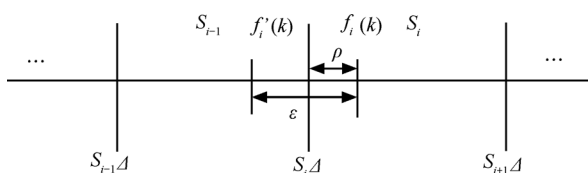


图2 系数波动导致的越界现象

3.3 改进的 QIM 方案

依据对量化噪声误差的分析, 嵌入端对于满足 $e_i = LSB(S_i)$ 的系数 $f_i(k)$ 不做改动, 改进的 QIM 方案将针对保持不变的系数做容错处理, 判断系数与最接近的量化区间边界的距离是否小于某个预设值, 是则将系数与区间边界间的距离增大至预设值, 否则依然保持系数不变, 预设值设为式(3)中的系数改动距离 δ , 改进的 QIM 方案表述为

$$f_i'(k) = \begin{cases} f_i(k), & \text{if } e_i = LSB(S_i), \rho > \delta \\ S_i\Delta + \delta, & \text{if } e_i = LSB(S_i), \rho < \delta, \\ & S_i\Delta < f_i(k) < mid \\ (S_i + 1)\Delta - \delta, & \text{if } e_i = LSB(S_i), \rho < \delta, \\ & mid < f_i(k) < (S_i + 1)\Delta \\ (S_i + 1)\Delta + \delta, & \text{if } e_i \neq LSB(S_i), \\ & mid < f_i(k) < (S_i + 1)\Delta \\ S_i\Delta - \delta, & \text{if } e_i \neq LSB(S_i), \\ & S_i\Delta < f_i(k) < mid \end{cases} \quad (4)$$

嵌入端加入容错处理后, 嵌入位置的每个系数与最接近的量化区间边界的距离至少为 δ , 但在提取端仍存在少量系数因发生波动而越界, 因此提取端同样需要容错处理。

经过大量实验发现, 提取端发生越界的系数总是波动至与其最相邻的量化区间边界的一个很小的范围之内, 因此对载密音频的系数 $f_i'(k)$ 采取如下容错处理: 判断 $f_i'(k)$ 与最接近的区间边界的距离 ρ' 是否在某个小区间 δ' 之内, 是则将 $f_i'(k)$ 所对应的区间序号 S_i' 修改为 S_{i+1}' 或者 S_{i-1}' , 否则保持 S_i' 不变, 改进的 QIM 方案的提取方式由 $e_i = LSB(S_i)$ 改进为如下

$$e_i = \begin{cases} LSB(S_i'), & \text{if } \rho' > \sigma' \\ LSB(S_i' + 1), & \text{if } \rho' < \sigma', mid < f_i'(k) < (S_i' + 1)\Delta \\ LSB(S_i' - 1), & \text{if } \rho' < \sigma', S_i'\Delta < f_i'(k) < mid \end{cases} \quad (5)$$

4 信息隐藏与提取算法

基于改进的 QIM 方案, 本文算法框架包括载体音频做分段 DCT→在每个 DCT 分段中选取嵌入位置→在嵌入位置应用改进的 QIM 方案嵌入信息→分段做 IDCT 得到载密音频, 秘密信息在嵌入前进行加密以提高安全性, 整体框架如图 3 所示。

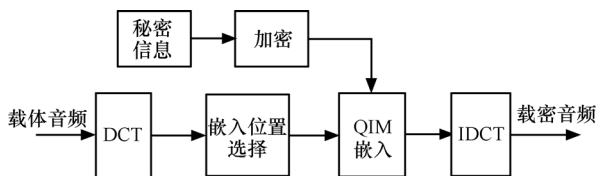


图3 嵌入算法框架

4.1 嵌入算法

根据上述的相关定义和改进的 QIM 方案，嵌入算法具体描述如下。

- 1) 对载体音频 C 分段做 DCT，分段长度为 l ，共分割为 L/l 个分段；
- 2) 输入秘密信息并进行加密，形成待嵌入信息序列 E ，每个音频段嵌入 1bit 信息，因此要求 $L/l > N$ ，对每一个信息比特 e_i 对应的音频分段 F_i 选定一个嵌入位置 pos ；
- 3) 从 pos 开始每隔 10 个系数选出一个系数，每个音频分段选出 r 个系数，利用量化器确定系数的量化区间序号，根据 e_i 与区间序号的映射关系，利用式(4)将 e_i 重复嵌入到 r 个系数中，完成在一个音频分段中嵌入 1bit 信息；
- 4) 判断 N 个信息比特是否嵌入完毕，未嵌入完毕则转至步骤 3)，嵌入完毕则对每个音频分段做 IDCT，得到载密音频信号，至此嵌入过程结束。

4.2 提取算法

根据改进的 QIM 方案，按式(5)提取嵌入的信息，提取过程不需要原始载体音频，为盲提取，具体描述如下。

- 1) 对载密音频 C' 做 l 点分段 DCT，共分割为 L/l 个分段；
- 2) 对每个嵌入信息的分段从 pos 开始每间隔 10 个系数取出 r 个系数，计算系数所在的量化区间序号，按式(5)提取信息比特 e_i ，对提取出的 r 个 0、1bit 做判决，当 0 的个数超过 $r/2$ 时，判 e_i 为 0，否则判 e_i 为 1；
- 3) 对嵌入信息的分段重复步骤 2)，直至提取完毕。

5 实验结果

为测试算法的性能，对不同类型的音频样本进行了实验：自然语音片段(voice)、古典乐曲(classic)和流行歌曲(song)。音频格式均为 44.1kHz 采样，16bit 编码，单声道，时长为 $10+\theta$ s ($\theta \in [0, 0.4]$)。以信噪比(SNR, signal to noise ratio)作为音频质量

退化的客观评价，以误码率(BER, bit error ratio)衡量算法的抗误码性能，为使实验结果更具一般性，以伪随机的 0、1 序列作为隐藏信息，分别测试了算法对重量化、非整数倍重采样、低通滤波和 MP3 压缩的顽健性。沿用算法的相关定义，载体音频 C 包含 L 个采样点，共嵌入 N bit 的秘密信息 E ， c_i 与 c'_i 分别为载体音频与载密音频的采样点值，错误提取的信息比特数为 m ，对 SNR 和 BER 分别定义如下

$$SNR = 10 \lg \frac{\sum_{i=0}^{L-1} c_i^2}{\sum_{i=0}^{L-1} (c_i - c'_i)^2} \quad (6)$$

$$BER = \frac{m}{N} \times 100\% \quad (7)$$

对音频信号 C 以长度 l 做分段 DCT，共得到 L/l 个音频分段，每个音频分段嵌入 1bit 信息，因此音频信号 C 的隐藏容量即为 L/l bit ($N \leq L/l$)，以式(8)定义嵌入率(ER, embedding rate)。

$$ER = \frac{N}{L/l} \times 100\% \quad (8)$$

量化器的量化步长 Δ 与算法的不可感知性和顽健性密切相关，较小的 Δ 可保证较好的不可感知性，但降低了顽健性，较大的 Δ 可获得更高的顽健性，但不可感知性较差。为兼顾不可感知性与顽健性，本文确定 Δ 的原则是在保证一定的听觉质量前提下， Δ 取尽可能大的值，经过大量实验， Δ 取值为 0.0916，其余参数设置如下：音频分段长度 $l=128$ ，单比特信息在每个分段中的重复嵌入次数 $r=10$ ，嵌入起始位置 $pos=2$ ，式(4)与式(5)中的参数设置为 $\delta=0.0305$ ， $\delta'=1.526 \times 10^{-4}$ 。上述 Δ 、 δ 、 δ' 均为归一化取值，对于 16bit 编码的 wav 音频，归一化标准为 32767。

图 4 的(a)与(b)、(c)与(d)、(e)与(f)分别示意实验样本 classic、voice 和 song 的载体音频与未受攻击的嵌入率为 100% 载密音频的时域波形图，表 1 给出了本文的改进 QIM 方案与传统的 QIM 算法在 50% 和 100% 的嵌入率下，载密音频与载体音频的信噪比，传统的 QIM 算法将系数量化至相邻量化区间的中点。实验中对载密音频进行以下顽健性测试：分别以 8bit 和 24bit 重新量化，以 1.088 43 倍和 0.885 倍的采样率(即 48kHz 和 39kHz)做非整数倍的上采样和下采样，以 22.05kHz 为截止频率

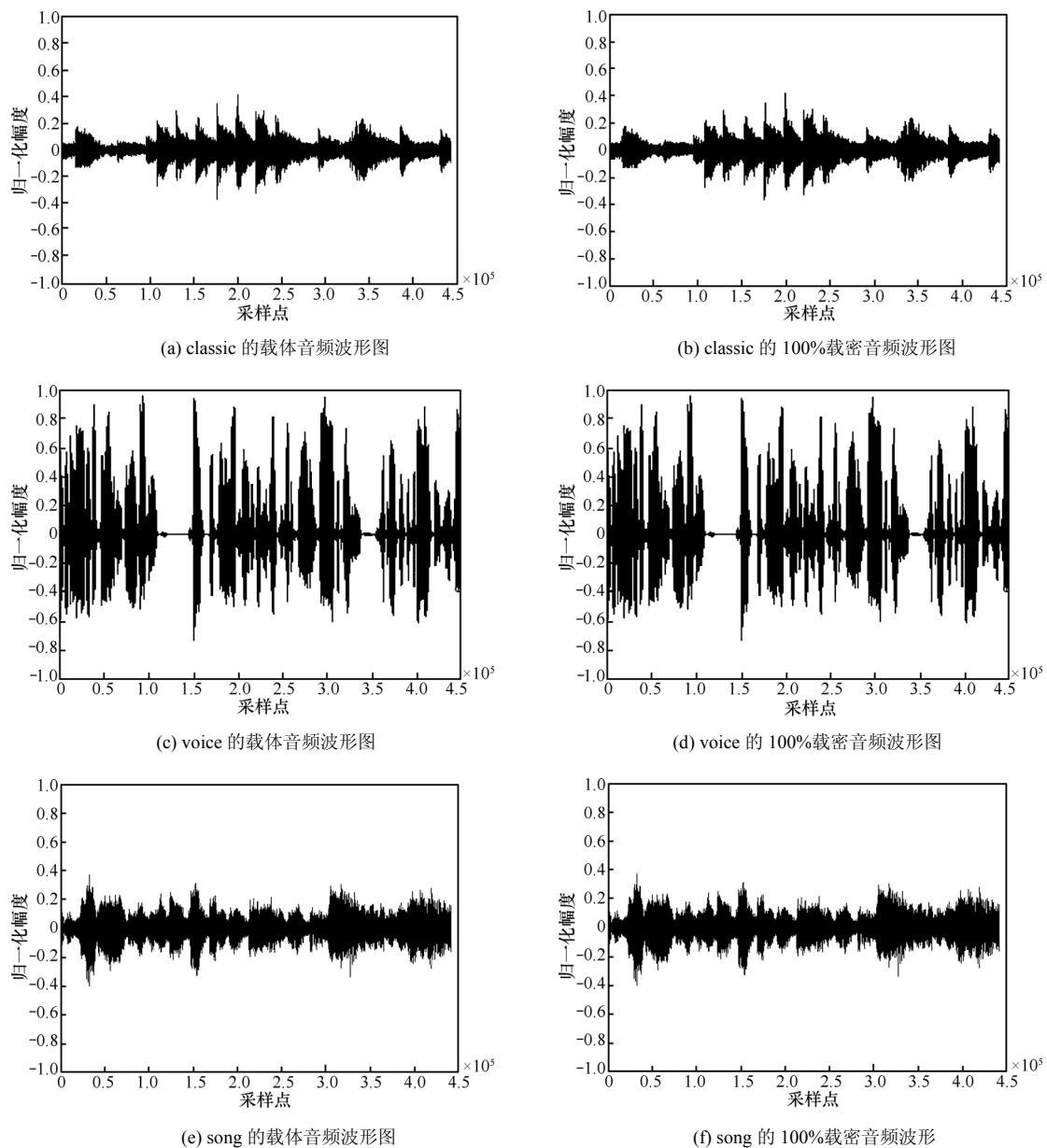


图 4 时域波形图（载密音频嵌入率均为 100%）

做低通滤波，以及分别在 128kbit/s、96kbit/s 和 64kbit/s 的比特率下进行 MP3 压缩/解压。在经过上述处理的载密音频中提取信息，将提取的信息与原始的嵌入信息进行比较，按照式(5)计算误码率，表 2 与表 3 给出 2 种嵌入率的载密音频对上述攻击方式的误码率。

表 1 嵌入率为 50%、100%的载密音频与载体音频的信噪比

嵌入率/%	classic		voice		song	
	本文改进的 QIM	传统 QIM	本文改进的 QIM	传统 QIM	本文改进的 QIM	传统 QIM
50	34.30	31.64	45.21	42.09	36.89	33.88
100	31.32	28.63	42.16	39.06	33.95	30.929 2

表 1 的数据表明本文的 QIM 方案与传统 QIM 算法相比，相同的嵌入量下在信噪比方面平均可获得 2.93dB 的增益，具有更好的音频质量，同时载密音频的信噪比都在 30dB 以上，从图 4 可看出，不同类型的音频样本以 100%嵌入率嵌入信息后都很好地保持了时域波形，从听觉上也无法辨别出原始音频与载密音频的任何差异。表 2 与表 3 的误码率说明本文的算法对于多种攻击方式都具有很强的顽健性，对于重量化和低通滤波可实现无误码提取，对于非整数倍的重采样和不同比特率的 MP3 压缩，误码率最高为 2.85%和 0.41%。以音频样本 song 与 classic 为例，时长均为 10.38s，分段长度为

128 个采样点, 嵌入率为 50% 时嵌入量为 1 788bit, song 对重采样的误码率为 2.85%, classic 对 64kbit/s 的 MP3 压缩的误码率为 0.41%, 即在 178.8bit/s 的隐藏容量下, 两段音频错误提取的信息分别为 50bit 和 7bit, 而在 100% 满嵌情况下, 即 357.6bit/s 的隐藏容量下, 错误提取的信息分别为 51bit 和 12bit, 针对这样的误码率, 只要加入弱纠错能力的纠错码即可完全恢复出隐藏信息, 纠错码的纠错能力只需满足在 100bit 的码元内纠错能力达到 3bit 的纠错码即可达到要求, 例如 (31,26,1) 的 BCH 纠错码, 31bit 码元中只需纠错 1bit 码元, 就可正确恢复出 26bit 的有效隐藏信息。

表 2 嵌入率为 50%、100% 的载密音频对重量化、重采样和低通滤波的误码率

攻击方式	classic		voice		song	
	50%	100%	50%	100%	50%	100%
8bit 重量化	0	0	0	0	0	0
24bit 重量化	0	0	0	0	0	0
低通滤波	0	0	0	0	0	0
1.088 倍上采样	0.29	0	0.56	0.30	0.17	0.34
0.885 倍下采样	0.98	0.92	2.57	1.82	2.85	1.45

表 3 嵌入率为 50%、100% 的载密音频对不同比特率的 MP3 压缩的误码率

比特率/(kbit·s ⁻¹)	classic		voice		song	
	50%	100%	50%	100%	50%	100%
128	0	0	0	0	0	0
96	0	0	0	0	0	0.26
64	0.41	0.35	0.34	0.20	0.41	0.20

6 结束语

本文提出了一种基于 DCT 域 QIM 的音频信息伪装算法, 其特点如下。

1) 提出了一种改进的 QIM 方案, 构造了一种音频 DCT 域的 QIM 量化器, 实现了隐藏信息的盲提取;

2) 通过分析量化噪声对信息提取误码的影响, 改进的 QIM 方案采取容错处理, 包括在音频分段中重复嵌入单个信息比特, 改进量化器的量化方式与提取方式, 保证了隐藏信息的强顽健性;

3) 隐藏容量大, 在 357.6bit/s 的隐藏容量下, 载密音频仍保持了良好的听觉质量, 信噪比在

30dB 以上, 与传统 QIM 方法相比平均可获得 2.93dB 的增益, 同时算法运算量小, 易于实现, 实用性强。

大量实验结果表明, 本文算法在实现了大容量的信息隐藏的同时, 对重量化、非整数倍上/下采样、低通滤波和不同比特率的 MP3 压缩等多种攻击方式均具有很强的顽健性, 信息提取的误码率最高仅为 2.85%。此外, 量化器设计是算法的关键, 其中的量化步长 Δ 与算法的顽健性和不可感知性密切相关, 不同的 Δ 将会得到不同的结果, 针对不同类型和强度的音频信号, 如何得到最佳的 Δ 值是一个值得进一步探讨的问题, 如何使 Δ 能够根据音频信号的特点, 自适应地找到最佳值, 以获得顽健性与不可感知性之间的理想平衡, 将是本文的进一步研究方向。

参考文献:

- [1] CVEJIC N, SEPPANEN T. Increasing robustness of LSB audio steganography using a novel embedding method[A]. Proc of the International Conference on Information Technology: Coding and Computing[C]. Las Vegas: IEEE Computer Society, 2004. 533-537.
- [2] NIAN G J, WANG S X, GE Y L. Research of improved echo data hiding: audio watermarking based on reverberation[A]. Proc of the International Conference on Acoustics, Speech and Signal Processing[C]. Hawaii: IEEE Signal Processing Society, 2007. 177-180.
- [3] SHIRALI-SHAHREZA S, MANZURI-SHALMANI M T. Adaptive wavelet domain audio steganography with high capacity and low error rate[A]. Proc of the International Conference on Information and Emerging Technologies[C]. Karachi: IEEE Computer Society, 2007. 1-5.
- [4] GOPALAN K. Audio steganography by cepstrum modification[A]. Proc of the IEEE International Conference on Acoustics, Speech, and Signal Processing[C]. Philadelphia: IEEE Computer Society, 2005. 481-484.
- [5] 马冀平, 韩纪庆. DCT 域音频水印: 嵌入对策和算法[J]. 电子学报, 2006, 34(7): 1260-1264.
MA Y P, HAN J Q. Audio watermarking in dct:embedding strategy and algorithm[J]. Acta Electronica Sinica, 2006, 34(7): 1260-1264.
- [6] MATSUOKA H. Spread spectrum audio steganography using sub-band phase shifting[A]. Proc of IHH-MSP2006[C]. Pasadena: IEEE Computer Society, 2006. 3-6.
- [7] TAKAHASHI A, NISHIMURA R. Multiple watermarks for stereo audio signals using phase-modulation techniques[J]. IEEE Transactions on Signal Processing, 2005, 53(2): 806-815.

- [8] CHEN B, WORNELL G. Quantization index modulation: a class of provably good methods for digital watermarking and information embedding[J]. IEEE Transactions on Information Theory, 2001, 47(4):1423-1443.
- [9] LIU Y W, SMITH J O. Watermarking sinusoidal audio representations by quantization index modulation in multiple frequencies[A]. Proc of IEEE International Conference on Acoustics, Speech, and Signal Processing[C]. Canada: IEEE Computer Society, 2004.373-376.
- [10] HOGAN M T, BALADO F G, HURLEY C M, *et al.* Secure and robust steganography using side information at the encoder[A]. Proceedings of Information Security[C]. 2006.
- [11] SHTEREV I D, LAGENDIJK R L. Amplitude scale estimation for quantization-based watermarking[J]. IEEE Transactions on Signal Processing, 2006, 54(11): 4146-4155.
- [12] SOROOSH R, ALI R. A secure quantization-based watermarking scheme using an improved statistical model in the wavelet domain[A]. Proc of International Conference on Information and Communication Technology[C]. Dhaka, Bangladesh, 2007. 242-245.

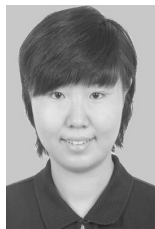
作者简介:



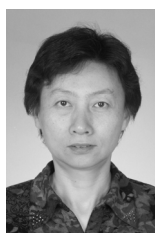
陈铭 (1979-), 男, 云南个旧人, 博士, 北京邮电大学信息安全中心博士后, 主要研究方向为信息安全、信息隐藏、隐写分析。



张茹 (1976-), 女, 山东济南人, 博士, 北京邮电大学副教授, 主要研究方向为密码学、信息隐藏、数字水印。



刘凡凡 (1980-), 女, 北京人, 北京邮电大学信息安全中心博士生, 主要研究方向为信息与信号处理、信息安全、数字水印。



钮心忻 (1963-), 女, 浙江湖州人, 北京邮电大学教授、博士生导师, 北京邮电大学信息安全中心副主任, 北京邮电大学数字内容安全中心主任, 主要研究方向为数字水印、信息隐藏、隐写分析。



杨义先 (1961-), 男, 四川盐亭人, 北京邮电大学教授、博士生导师, 北京邮电大学计算机学院院长, 北京邮电大学信息安全中心主任, 长江学者特聘教授, 主要研究方向为密码学、计算机网络与信息安全。