

在压缩语音编码中集成信息隐藏方法研究

杨婉霞^{1,2}, 余 晖², 胡 萍³

(1. 甘肃农业大学工学院, 甘肃兰州 730070; 2. 清华大学电子工程系, 北京 100084; 3. 清华大学网络科学与网络空间研究院, 北京 100084)

摘 要: 论文针对低速率语音编码过程的特点, 提出了一种基于动态码本生成的信息隐藏方法, 设计了相应的嵌入和提取算法. 该方法解决了现有的基于静态码本分区的信息隐藏方法无法对抗码字统计分析检测的问题. 实验表明该隐藏算法在 13.3Kbps 的载体速率下能获得 450bps 隐藏容量, 而且载密信息的语音质量 PESQ 值下降不到 6%.

关键词: 信息隐藏; 语音编码; 动态码本; 隐藏算法; 隐藏容量; 隐蔽性

中图分类号: TN911.23 **文献标识码:** A **文章编号:** 0372-2112 (2014)07-1305-06

电子学报 URL: <http://www.ejournal.org.cn>

DOI: 10.3969/j.issn.0372-2112.2014.07.010

Research on Steganographic Method Integrated in the Compressed Speech Codec

YANG Wan-xia^{1,2}, YU Hui², HU Ping³

(1. College of Technology, Gansu Agricultural University, Lanzhou, Gansu 730070, China;

2. Department of Electronic Engineering, Tsinghua University, Beijing 100084, China;

3. Institute for Science and Network Space Sciences, Beijing 100084)

Abstract: This paper proposes a kind of information hiding method which is based on dynamic codebook generating technique, together with the corresponding inserting method and extracting algorithm. This method greatly solves the problem of deficiency in anti-testing of code analysis, which is faced by the information hiding that is based on static codebook partition techniques. The experimental result shows that the proposed algorithm can get 450 bps steganographic capacities within 13.3 Kbps carrier rate, while the loss of PESQ value of speech with steganographic information is less than 6%.

Key words: steganography; speech coding; dynamic codebook; steganographic capacity; imperceptibility

1 引言

信息隐藏技术是信息安全领域新兴安全技术, 是加密技术的有力补充. 传统信息隐藏主要采用图像等静态文件作为隐藏载体, 但随着网络流媒体的普遍使用, 基于网络流媒体的信息隐藏技术应运而生, 而且成为当前网络安全领域的研究热点. 语音是人们广泛使用的网络媒体, 当前比较流行的低速率编码有 G.723.1、G.729a 和 iLBC (Internet Low Bit Rate Codec)^[1] 等. 然而, 由于信息隐藏技术是利用媒体信息中的冗余来嵌入秘密信息, 而低速率语音在压缩编码过程中尽可能大的去除冗余信息, 而且人耳对语音极其敏感; 另外, 语音经过低速率编码压缩后, 特征参数相对较少而且比较集中, 对抗统计分析检测的能力比较弱. 因此, 如何在低速率语音中实现信息隐藏是十分具有挑战性的研究方向. 本论文针对低速率语音编码过程中码本动态生成的特点, 提出了一种基于动态码本分组的信息隐藏方法, 并以 iLBC 语音

编码为实例, 设计了一种基于动态码本的信息隐藏的嵌入和提出算法.

论文结构组织如下. 第 2 部分介绍以语音为载体的信息隐藏的研究现状和主要问题. 第 3 部分分析了 iLBC 语音编码原理, 讨论语音编码过程基于动态码本的信息隐藏方法. 第 4 部分对隐藏算法进行了测试和性能分析. 第 5 部分是全文小结.

2 相关研究工作

当前针对低速率压缩编码器的信息隐藏研究成果比较少, 主要成果集中在脉冲编码调制 (Pulse-Code Modulation, PCM)^[2,3] 或动态影像专家组压缩标准音频层面 3 (Moving Picture Experts Group Audio Layer III, MP3) 格式的音频^[4]. 而目前成熟的信息隐藏方法都很难直接应用于低速率压缩语音载体中. 因此, 近几年来有了一些针对低速率语音编码进行信息隐藏的研究工作. 例如, Huang 等人^[5] 对 G723.1 编码标准中静音帧的分析发现, 静音

帧比活动帧更适于隐藏,提出了基于静音帧的信息隐藏算法,并取得了较好的隐藏效果.文献[6,7,9]分别提出了通过修改编码器固定激励码本的搜索过程实现信息嵌入与语音联合编码,并减小失真的方法.上述方法对合成语音质量容易造成较大影响,且易于受到基于统计分析方法的检测.针对这一问题,Xiao 等人^[8]采用量化索引调制(Quantization Index Modulation, QIM)原理,建立了一种针对低速率语音编码的信息隐藏方法,提出了互补邻居顶点算法(Complementary Neighbor Vertex, CNV)用以优化码本分组,该方法对编码的语音质量影响非常小,可以抵抗一般的统计检测算法.

从目前国内外的研究现状来看,虽然有一些针对低速率语音压缩的研究成果,但大部分只是对编码参数简单的 LSB 或改进的 LSB 嵌入算法,虽然有采用 QIM 原理的隐藏方法,如文献[8]中的 CNV 隐藏方法以语音编码中的静态码本为隐藏载体.但有研究成果能检测出来,例如,文献[12]提出了一种针对 CNV 隐藏的检测方法.因此,如何进一步提高低速率语音编码信息隐藏的隐蔽性和隐藏容量是论文研究的动机和目标.

3 信息隐藏方法的设计

目前在许多低速率语音编码过程中采用码本的动态生成编码机制.其中,最典型是 iLBC 编码.下面就选择 iLBC 作为载体,建立一种基于低速率语音编码中码本动态的隐藏方法.

3.1 基于 iLBC 码本生成的隐藏方法

iLBC 语音编码是一种混合参数编码,通过对语音分帧(30ms 和 20ms 两种帧格式).然后以帧为单位,采用码本激励线性预测模型(CELP),对语音进行一系列的分析,得到一组能够表示语音特征的参数,将这些参数编码封装发送.接收方根据接收到的特征参数对语音进行解码.在自适应码本量化编码即 iLBC 编码过程中,需要经历多个处理环节,其中一个重要环节是自适应码本量化编码.在该环节中,对每帧语音的 3 个子帧(20ms 帧)和 5 个(30ms 帧)子帧分别构建动态码本,然后对残差语音信号进行量化编码.

动态码本进行编码时分为如下 3 个阶段,每个阶段结束以后都会对目标向量进行更新,从目标向量中减去增益和匹配向量的乘积,这就保证了在第一阶段和第二阶段量化都是精确的.而且,每帧语音的自适应码本是在编解码过程中进行动态生成和动态分组.这样能够对抗现有的基于特征统计分析的隐藏检测方法,具有比基于静态码本隐藏方法更好的隐蔽性.

(1)初始状态块的选择编码.下面以 iLBC 的 20ms 帧为例,说明码本动态的构建方法.通过在第 K 帧语音 P_k 中寻找 2 个连续的具有较高能量的子帧作为初始状

态块.图 1 是 20ms 帧的子帧能量和初始状态块选择示意图.图中子帧 1 和 2 能量最高,因此,在该帧中选择子帧 1 和 2 作为初始状态块.

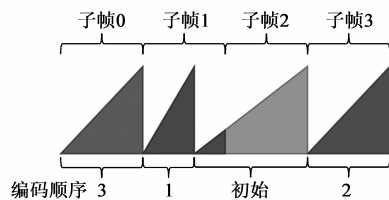


图1 20ms帧的子帧能量和初始状态选择图

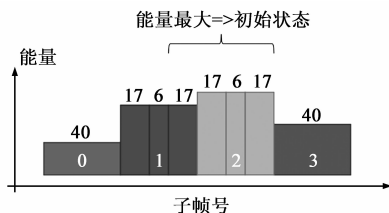


图2 一帧语音中各个子帧的自适应码本生成顺序

在确定了初始状态块的位置标号 $Index_k$ 之后,还需要进一步确定初始状态块的起始位置 S_first .如图 1 所示的 2 个连续子帧(1 和 2)共计有 80 样本点,是选择前 57/58 样点,还是后 57/58 样点作为初始起始状态.

(2)每帧的子帧动态码本构建方法

完成了语音帧 P_k 的初始状态块选择编码后,就可以采用初始状态编码来动态构建每个子帧的码本.动态码本由基本码本和扩展码本两部分组成.基本码本是由加权码本内存中连续目标子帧矢量来生成.扩展码本是对加权码本内存映像用一个 8 阶 FIR 滤波后取中间段来得到.图 2 是在图 1 所示的初始状态下每个子帧的码本生成顺序.

(3)码字搜索和目标矢量化.在每个子帧的自适应码本动态构建完成后,然后基于码本进行目标矢量的量化搜索.进行码本搜索的主要步骤如下:

①计算度量,如式(1)所示:选择码本中的码字向量使其最大.

$$(\text{target} \cdot \text{cbvec})^2 / |\text{cbvec}| \quad (1)$$

式(1)中, cbvec 表示选择的码本向量, target 表示目标码本向量.

②选择的码本向量 cbvec 的绝对值要小于 1.3,即 $|\text{cbvec}| < 1.3$ 增益的计算公式如式(2)所示:

$$\text{gain} = (\text{target} \cdot \text{cbvec}) / |\text{cbvec}|^2 \quad (2)$$

③在第一阶段匹配时,选择最佳码本向量与目标向量的点积必须大于 0,即满足式(3)

$$\text{target} \cdot \text{cbvec} > 0 \quad (3)$$

3.2 隐藏信息的嵌入算法设计

下面以 20ms 长度的语音帧为实例,具体设计嵌入

算法.

假设存在一个 iLBC 语音流 P , P 是由 m 个语音帧 p_k 组成. 可以表示为 $P = \{P_k | i = 1, \dots, m\}$, 机密信息比特流表示 $M = U_{i \in N} \{0, 1\}$.

(1) 秘密信息 M 经过随机函数 $f(M)$ 处理后, 得到秘密信息的伪随机比特流 $E = \{b_0, b_1, \dots, b_L\}$, L 为秘密信息比特流的长度 ($L \leq N$), 设定伪随机数生成器的初始化种子 Seed.

(2) 语音流中的第 K 帧语音表示为 P_K , P_K 是由 3 个子帧组成, 即 $p_k = \{p_k^1, p_k^2, p_k^3\}$. 按照 3.1 节的规则选择初始状态块 Index_k , 并基于初始状态块 Index_k 来对每个子帧 $p_k^i (i = 1, 2, 3)$ 进行动态码本构建, 获得如式(4)所示的自适应码本.

$$MB_k = \{MB_k^1, MB_k^2, MB_k^3\} \quad (4)$$

其中, MB_K 表示第 K 帧语音 P_K 的自适应码本, MB_{iK} 表示每个子帧的码本.

(3) 分别对每个子帧的码本空间进行分组, 即索引号为奇数份的分为第 1 组, 索引号为偶数份的分为第 2 组, 因此, 每个子帧的码本可以表示为式(5).

$$MB_k^i = \{MB_k^{i,1}, MB_k^{i,2}\} \quad (5)$$

(4) 在对语音帧 $p_k = \{p_k^1, p_k^2, p_k^3\}$ 进行动态编码的第一阶段, 根据当前需要嵌入的机密信息 $E = \{b_0, b_1, \dots, b_L\}$ 的 b_i 值来选择所对应的子帧码本搜索范围来进行量化. 具体表示为表达式(6)

$$\begin{aligned} BW \in MB_k^{i,1} & \quad \text{if } b_i = 1 \\ BW \in MB_k^{i,2} & \quad \text{if } b_i = 0 \end{aligned} \quad (6)$$

BW 表示量化过程中搜索的码字. 若 $b_i = 1$, 则量化码字在码本组 $MB_{Ki,1}$ 中搜索; 反之, 若 $b_i = 0$, 则量化码字在码本组 $MB_{Ki,2}$ 中搜索. 在相应的码本组中对目标向量 P_{1K} 与当前码本组中的码字进行匹配, 得到最佳的索引号 Index_{ki} 以及增益值 Gain_{ki} . 然后将目标向量进行更新为下一个子帧 P_{2K} , 并将秘密信息向后移 1 位为 b_{i+1} . 重复该过程, 分别完成 1 帧语音帧 P_K 中 3 个子帧 $p_k = \{p_k^1, p_k^2, p_k^3\}$ 的信息嵌入.

(5) 在 iLBC 动态编码第 2 阶段, 重复(3)和(4)的操作.

(6) 在 iLBC 动态编码第 3 阶段, 重复(3)和(4)的操作.

(7) 若秘密信息已经嵌入完毕 ($i = n$) 或已无载体则结束 ($k = m$), 否则, 回到第(2)步, 继续第 P_{K+1} 帧的信息嵌入. 最后产生载密的编码比特流为 S , $S = \{S_k | k = 1, \dots, m\}$, 其中, S_k 是 1 帧语音的编码比特参数.

3.3 隐藏信息的提取算法设计

iLBC 解码中最重要的步骤是从 1 帧语音编码参数中抽取两个重要的特征参数, 即 57 比特的初始状态

编码 Index_k 和每个子帧的量化码字索引号 Index_{ki} . 然后根据初始状态编码 Index_k 在解码端重新构建每个子帧的 $MB_k = \{MB_k^1, MB_k^2, MB_k^3\}$, 再分别在自适应码本量化编码的解码 3 个阶段, 通过判断码字索引号 Index_{ki} 的奇偶性就可以提取机密信息的比特 b_i . 具体提取算法的设计如下.

(1) 接收端对接收到比特流 $S = \{S_k | k = 1, \dots, m\}$ 进行解析, 提取第 k 帧编码比特参数 S_k .

(2) 从第 k 帧编码比特参数 S_k 中抽取出初始状态编码 Index_k 和每个子帧的量化码字索引号 Index_{ki} . 并根据初始状态编码 Index_k 在解码端重新构建每帧动态码本 $MB_k = \{MB_k^1, MB_k^2, MB_k^3\}$.

(3) 根据每个子帧的量化码字索引号 Index_{ki} 的奇偶来判决当前嵌入的机密信息比特 $b_i = 0$ 或者 $b_i = 1$. 如果 Index_{ki} 为奇数, 则 $b_i = 1$; 否则, Index_{ki} 为偶数, 则 $b_i = 0$.

(4) 重复第(2)和(3), 对所有 $S = \{S_k | k = 1, \dots, m\}$ 的 S_k 进行信息提取. 对所有提取出的秘密信息 b_i 进行整合, 得到 $E = \{b_0, b_1, \dots, b_L\}$. 采用伪随机数生成器的初始化种子 Seed, 通过函数 $M = F^{-1}(E)$ 解码得到最终的机密信息 $M = U_{i \in N} \{0, 1\}^i$.

4 算法实验结果与性能分析

从目前对基于 QIM 信息隐藏算法的研究成果来看, 隐藏算法的复杂性都比较简单, 而且鲁棒性都比较好. 因此, 隐藏算法性能好坏主要取决于隐蔽性和隐藏容量^[12].

4.1 隐藏容量分析

通过分析隐藏算法可以从理论上计算得到 2 种不同帧结构下的机密信息隐藏容量.

(1) 30ms 帧的隐藏容量. 由于每个 30ms 帧分为 5 个子帧, 每个子帧进行了 3 个阶段量化编码, 在每个子帧和每个阶段量化编码, 分别可以嵌入 1 比特的机密. 因此, 可以得到 30ms 帧结构下的信息隐藏容量如式(7)来计算.

$$C_{ap} = 1000/30 * 5 * 3 * 1 = 500\text{bps} \quad (7)$$

(5) 20ms 帧的隐藏容量. 同理, 也可以建立 20ms 帧结构的隐藏容量计算方法, 如式(8)来计算. 由于 20ms 帧结构分为 3 个子帧.

$$C_{ap} = 1000/20 * 5 * 3 * 1 = 450\text{bps} \quad (8)$$

从计算结果可以看出, 这种算法的隐藏容量对低速率语音编码载体 (iLBC 本身的码流速率也只有 13.3 和 15.6Kbps) 来说, 是比较理想的结果.

4.2 隐藏算法的感觉隐蔽性分析

对于以语音为载体的信息隐藏算法, 其感觉隐蔽性的好坏主要对比测试载密和非载密情况的语音质

量. 对语音质量的评价, 国际上常采用标准语音质量评测工具来测试 PESQ 值^[10,11]. 本论文也是采用该方法来评价隐藏算法的感觉隐蔽性.

实验采用 4 组不同类型的语音样本, 分别是中文男声、中文女声、英文男声、英文女声. 每组语音各有 20 段. 首先要判断隐藏信息提取的准确性, 然后通过对只进行编解码不隐藏信息得到的语音质量和进行隐藏后得到的语音质量的比较, 来判断隐藏算法的优劣. 对 iLBC 编码, 有两种帧结构, 下面分别对这两种帧结构进行测试. 其中图 3 是 30ms 帧结构下的隐蔽性测试结果, 分别对比了进行信息隐藏和未信息隐藏时 20 段语音样本对应的 PESQ 值. 图 4 是 20ms 帧结构下的隐蔽性测试结果, 也分别对比了进行信息隐藏和未信息隐藏时 20 段语音样本对应的 PESQ 值.

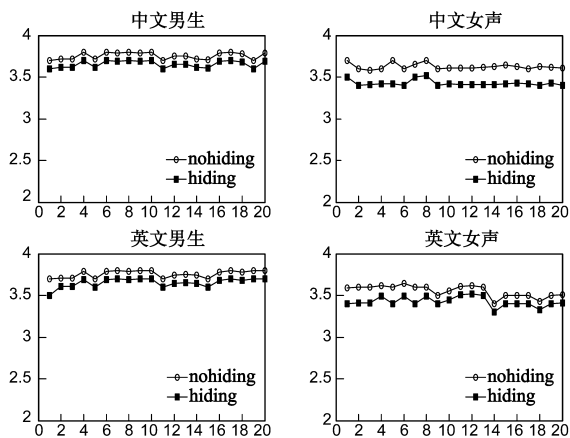


图3 30ms帧的隐藏和不隐藏时的PESQ值

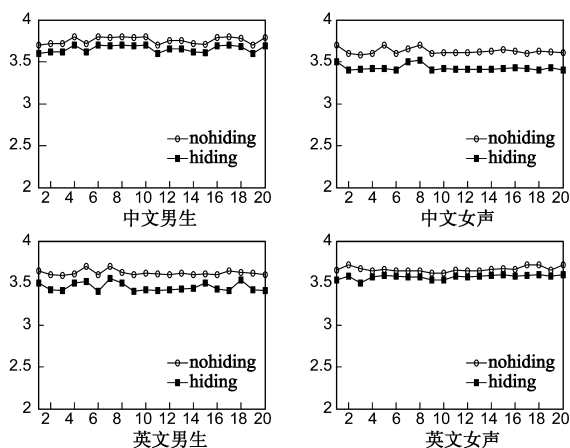


图4 20ms帧的在隐藏和不隐藏时的PESQ值

通过对不同种类的语音载体进行测试, 可以看出在信道良好的条件下, iLBC 语音编码中的隐藏算法能够保证秘密信息的精准度. 同时载体语音的质量也没有受到嵌入机密信息的影响而产生很大变化. 对于环境情况不太好时, 隐藏算法对语音质量改变相对较小,

这是因为秘密信息对于载体语音而言就相当于噪声, 有一部分秘密信息湮没在了噪声中, 因此, 对语音质量改变较小, 隐蔽性会更好些.

另外, 为了更全面地分析隐藏算法的隐蔽性, 我们对测试得到 PESQ 平均值和方差进行了进一步分析. 计算了不同条件的平均值和方差, 从而来进一步评估隐藏算法的隐蔽性能的平稳性. 其中, 表 1 是 4 组语音测得 PESQ 平均值, 并与文献[8]的隐藏算法(CNV)的隐蔽性进行了比较. 表 2 是 4 组语音测得 PESQ 值变化的平均值和方差.

表 1 4 组语音测得 PESQ 平均值

类别	30ms 帧			20ms 帧		
	未隐藏	本文隐藏方法	CNV 方法	未隐藏	本文隐藏方法	CNV 方法
中文男声	3.75505	3.6285	3.6101	3.7735	3.6603	3.6571
中文女声	3.61415	3.4331	3.4012	3.63315	3.4746	3.4501
英文男声	3.66235	3.56585	3.5508	3.67895	3.60195	3.60101
英文女声	3.554263	3.374468	3.3644	3.603526	3.438158	3.4086

表 2 4 组语音测得 PESQ 值变化的平均值和方差

类别	30ms 帧		20ms 帧	
	平均值	方差	平均值	方差
中文男声	0.12655	0.003105	0.1132	0.003797
中文女声	0.18105	0.002673	0.15855	0.004473
英文男声	0.0965	0.002493	0.077	0.00144
英文女声	0.180895	0.005626	0.165368	0.003354

从表 1 可以看出, 论文采用动态码本载体的隐藏方法, 从语音质量的隐蔽性比文献[8]静态载体要好, 文献[8]采用的 CNV 码本隐藏方法是目前国际性能最好方法之一. 另外, 从表 1 表 2 中还可以发现, 相对于非载密情况, 载密条件下语音质量的 PESQ 值的方差增大. 也就是说, 在 iLBC 语音编码使用隐藏算法来隐藏信息情况下, 语音质量更容易受到外界的干扰. 同时, 还可以发现 iLBC20ms 帧结构比 30ms 帧结构更能获得稳定的语音质量.

4.3 信息隐藏算法的统计特征隐蔽性分析

采用当前比较优秀的基于二阶差分衍生的梅尔倒谱系数(Derivative Mel-Frequency Cepstral Coefficients, DM-FCC)特征的支持向量机的通用方法进行了统计分析测试. 该方法对文献[8]提出的基于静态码本的隐藏方法(CNV)有较好的检测效果.

实验样本组中文男生(CSM):500,其中300用于训练,200用于测试;中文女生(CSW):600,其中300用于训练,300用于测试;英文男生(ESM):800,其中600用于训练,200用于测试;英文女生(ESW):800,其中600用于训练,200用于测试;混合语音是指CSM、CSW、ESM和ESW四种样本类的随机抽取.结果如表3和表4所示.

从表3中看出,对于20ms帧模式下检测结果5类样本集中的最大值为58.2%,最小值为48.1%,总的平均值为52.01%,标准差取值都小于2.69%;从表4中看出,对于30ms帧模式下检测结果5类样本集中的最大值为55.2%,最小值为44.7%,总的平均值为50.9%,标准差取值都小于3.56%.这充分说明本文提出的信息隐藏方法,在2种帧模式下都能够很好地抵抗基于DMFCC特征的统计分析检测.

表3 DMFCC对20ms帧模式下的检测结果

窗口长度	CSM(%)	CSW(%)	ESM(%)	ESW(%)	混合(%)
0.1s	51.18	50.00	50.48	48.50	52.19
0.2s	50.82	49.60	52.46	49.31	48.33
0.4s	48.44	48.14	52.65	53.20	49.61
0.8s	54.82	48.13	55.15	51.42	51.44
1.6s	50.84	48.11	54.20	52.28	51.11
3.2s	51.20	51.48	58.24	51.60	52.78
4.8s	54.43	48.51	54.88	50.97	52.64
6.4s	55.56	51.51	57.06	51.90	51.19
8.0s	56.81	51.52	55.38	53.20	53.50
10.0s	52.80	49.23	58.56	48.30	53.50
平均值	52.71	49.62	54.90	51.07	51.74
CNV方法平均值	68.11	65.16	63.71	59.23	62.29

表4 MFCC对30ms帧模式下的检测结果

窗口长度	CSM(%)	CSW(%)	ESM(%)	ESW(%)	混合(%)
0.1s	49.70	54.41	47.95	45.38	49.93
0.2s	49.71	53.60	53.09	50.42	51.62
0.4s	47.10	45.74	52.32	51.72	51.30
0.8s	54.90	49.50	48.68	48.31	51.42
1.6s	50.10	47.87	52.34	48.72	52.50
3.2s	51.080	46.52	50.15	52.16	51.00
4.8s	52.80	53.60	53.30	50.21	53.09
6.4s	52.10	56.26	52.83	50.24	52.35
8.0s	54.50	50.60	54.53	52.65	51.23
10.0s	52.09	54.40	53.07	48.30	51.45
平均值	51.42	51.45	51.83	49.81	52.20
CNV方法平均值	69.11	66.14	65.71	59.63	63.40

另外,对比表3和表4的CNV隐藏方法的检测结果可以证明:采用本文提出的基于动态码本的隐藏方法,具有很好的对抗统计分析的隐藏检测,其性能明显好于CNV方法.

5 小结

论文提出了一种基于码本动态生成的信息隐藏方法,并选择目前广泛应用的iLBC语音为研究实例,制定了相应的嵌入和提取算法.实验结果表明,该算法不仅具有较高隐藏容量,而且语音感觉的隐蔽性和特征统计分析的隐蔽性都很好,特别是在抗特征统计分析方面明显优于基于静态码本的隐藏方法.未来的工作是进一步分析动态码本分组的优化方法,进一步提高隐藏时语音质量.

参考文献

- [1] IETF RFC 3951. Internet Low Bit Rate Codec (iLBC) [S]. <http://datatracker.ietf.org/doc/rfc3951/>, 2011, 12.
- [2] 谭良,吴波,等.一种基于混沌和小波变换的大容量音频信息隐藏算法[J].电子学报,2010,38(8):1812-1818. TAN Liang, WU Bo, et al. An audio information hiding algorithm with high-capacity which based on chaotic and wavelet transform[J]. Acta Electronica Sinica, 2010, 38(8): 1812-1818. (in Chinese)
- [3] L Liu, M Li, Q Li, Y Liang. Perceptually transparent information hiding in G.729 bitstream[A]. Proceedings of the 4th International Conference on Intelligent Information Hiding and Multimedia Signal Processing[C]. Harbin, China: IEEE, 2008. 406-409.
- [4] Lu Z M, Yan B, Sun S H. Watermarking combined with CELP speech coding for authentication[J]. IEICE Transactions on Information and System, 2005, E88-D(2): 330-334.
- [5] Yongfeng Huang, Jian Yuan, Shanyu Tang, C Wang. Steganography in inactive frames of VoIP streams encoded by source codec[J]. IEEE Transactions on Information Forensics and Security, June 2011, 6(2): 296-306.
- [6] 龙敏,彭飞.基于混沌分组的二维工程图信息隐藏算法[J].电子学报,2009,37(1):79-83. LONG Min, PENG Fei. An information hiding algorithm for two-dimensional engineering graphics based on chaotic grouping [J]. Acta Electronica Sinica, 2009, 37(1): 79-83. (in Chinese)
- [7] Rui Miao, Yongfeng Huang. An approach of covert communication based on the adaptive steganography scheme on voice over IP [A]. IEEE International Conference on Communications (ICC2011)[C]. USA: IEEE, 2011. 1-5.
- [8] B Xiao, Y Huang, S Tang. An approach to information hiding in low bit-rate speech stream [A]. Proceedings of the 2008

IEEE Global Telecommunications Conference [C]. New Orleans, LA, USA: IEEE, 2008. 1 - 5.

- [9] Qingzhong Liu, Andrew H Sung, Mengyu Qiao. Temporal derivative-based spectrum and mel-cepstrum audio steganalysis [J]. IEEE Transactions on Information Forensics and Security, 2009, 4(3): 359 - 368.
- [10] Y Huang, J Yuan, S Tang, C Wang. Steganography in inactive frames of VoIP streams encoded by source codec [J]. IEEE Transactions on Information Forensics and Security, 2011, 6(2): 296 - 306.
- [11] Yongfeng Huang, Shanyu Tang, Chunlai Bao, Yau Jim Yip. Steganalysis of compressed speech to detect covert VoIP channels [J]. IEE/IEEE Journal, IET Information Security, 2011, 5(1): 1 - 7.
- [12] Huang Y, Zhang Y, S Tang. Detection of covert VoIP communications using sliding window based steganalysis [J]. IET Communications, IEE/IEEE Journal, 2011, 5(2): 126 - 133.
- [13] Songbin Li, Huaizhou Ta, Yongfeng Huang. Detection of QIM steganography in G. 723. 1 bit stream based on quantization index sequence analysis [J]. Zhejiang Univ-Sci C (Comput & Electron), 2012, 13(8): 624 - 534.

作者简介



杨婉霞 女, 1979 年 1 月出生, 甘肃静宁人, 2002 年、2007 年分别在甘肃工业大学和兰州交通大学获得工学学士和工学硕士学位. 现为甘肃农业大学工学院讲师, 主要从事信息处理, 自动控制等方面的研究工作.

E-mail: yangwanxia@163.com

余 辉 男, 1987 年出生, 清华大学电子工程系硕士研究生. 研究方向: 网络信息处理.



胡 萍 女, 1957 出生, 清华大学网络科学与网络空间研究院研究员, 研究方向为网络信息安全和网络行为计算. 作为负责人先后完成了多项国家 863、973、国际合作等项目, 已在国内外重要期刊和国际会议发表学术论文 30 多篇, 获得省部级等科技成果奖 3 项.