基于可量化性能分级的自适应 IP 语音隐写方法

田 晖[1],郭舒婷[1],秦 界[1],黄永峰[2],陈永红[1],卢 璈[3]
(1. 华侨大学计算机科学与技术学院,福建厦门 361021;2. 清华大学电子系,北京 100084;3. 华侨大学网络技术中心,福建厦门 361021)

摘 要: 论文以客观语音质量评价和信噪比为量化手段,分析了参数编码中语音帧的每个比特位对重构语音质量影响的不均衡性,并提出了一种载体可隐藏位的分级方案,以达到充分利用各载体位的目的. 以此为基础,进一步提出了一种基于载体位置分级的自适应 IP 语音隐写方法. 该方法可自适应地选择最佳的隐写位置,以提高隐蔽通信的不可感知性. 以大量的语音样本为载体,对提出的方法进行了实验验证. 结果表明,本文的分级方案是正确可行的,且提出的分级隐写方法较之传统方法具有更好的隐写性能.

关键词: 隐写; IP 语音; 信息隐藏; 性能分级
中图分类号: TP 309 **文献标识码:** A **文章编号:** 0372-2112 (2016)11-2735-07
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2016.11.024

Adaptive Voice-over-IP Steganography Based on Quantitative Performance Ranking

TIAN Hui[1], GUO Shu-ting[1], QIN Jie[1], HUANG Yong-feng[2], CHEN Yong-hong[1], LU Jing[3]
(1. *College of Computer Science and Technology, Huaqiao University, Xiamen, Fujian* 361021, *China*;
2. *Department of Electronic Engineering, Tsinghua University, Beijing* 100084, *China*;
3. *Network Technology Center, Huaqiao University, Xiamen, Fujian* 361021, *China*)

Abstract: In this paper, we first analyze the unequal impacts of various cover bits on the quality of decoded speech for parameter codecs, and further design a ranking scheme for available cover bits to utilize the cover fully. Moreover, we present an adaptive VoIP steganography based upon the performance ranking of cover bits, which can adaptively choose the optimal steganographic positions to enhance the imperceptibility of covert communications. The proposed methods are evaluated and tested with a large number of speech samples as the cover. The experimental results show that the proposed ranking scheme is sound and feasible, and the presented steganogaphic method also outperforms the existing ones.

Key words: steganography; voice over IP (VoIP); information hiding; performance ranking

1 引言

随着网络和计算机技术的飞速发展,越来越多的网络应用已逐渐深入我们生活,人们的生产、工作和生活已经越来越离不开互联网. 然而,在网络给人们带来便利的同时也存在通信内容的泄露、个人信息被窃取等风险. 因此,人们普遍开始关注诸如安全通信、个人隐私保护等信息安全相关问题. 隐写(Steganography)技术是近几年来受到广泛关注的一项隐蔽通信技术,它是利用人类感觉器官的不敏感性(感觉冗余)以及多媒体数字信号本身存在的冗余(数据特性冗余),在不影响载体质量及正常通信的前提下,将隐秘信息隐藏在可公开的媒体信息中,使得隐秘信息不被察觉地传输. 与传统的加密技术相比,隐写技术隐藏了信息的存在性,使得隐蔽通信不易被察觉,从而提高了隐秘信息在特定场合的安全性.

从现有的文献来看,目前的隐写已不仅仅局限于图像、文本、音频等静态媒体,越来越多的学者开始热衷于基于动态流媒体的隐写技术研究,最为代表性的即为基于 IP 语音(Voice over IP, VoIP)的隐写及隐蔽通信

收稿日期:2015-10-18;修回日期:2016-04-20;责任编辑:蓝红杰
基金项目:国家自然科学基金(No. 61302094, No. U1536115, No. U1405254);福建省自然科学基金(No. 2014J01238);福建省高校杰出青年科研人才培育计划(No. MJK2015-54);福建省教育厅中青年教师教育科研项目(No. JA13012);国家留学基金项目(No. 201507540001);华侨大学中青年教师科研提升资助计划(No. ZQN-PY115);华侨大学科技创新团队和领军人才支持计划(No. 2014KJTD13)

技术研究[1,2]. 主流的研究思路是以编码后的语音流作为载体,利用其冗余性实现隐秘信息的隐藏[1~4]. 基于最低有效位(Least Significant Bit,LSB)的隐写,以其低复杂度和高隐藏容量等优点,成为目前在 VoIP 中应用最多的一种技术,但是如何提高其安全性(包括不可感知性和不可检测性)仍然是一个极具挑战性的课题. 迄今为止,已有许多研究者对此进行了研究. 在抵抗检测攻击方面,Kratzer 等人[5]率先主张在 LSB 隐藏前进行加密处理以消除隐秘信息间的相关性,并提出了基于 Twofish 和 Tiger 加密技术的隐写方案. 尽管这一方案有效地提高了安全性,但是不难看出,这种传统加密方式将会给 VoIP 系统带来很大的通信延迟,而这种延迟给语音质量带来的损害,将使得隐蔽通信陷入另一个易于"暴露"的极端. 为此,Tian 等人[6]提出用 m 序列代替 Twofish 和 Tiger 对隐秘信息进行加密,在消除隐秘信息间的相关性的同时,维护 VoIP 的实时性. 在维护 VoIP 的不可感知性方面,Huang 等人[7]引入了 LSB Matching 算法来降低载体的改变量,但是该方法将隐藏容量降低到了传统 LSB 方法的一半. Tian 等人[8,9]首次提出部分相似值的概念以评价隐秘信息与载体间的相似度,并先后提出利用数学变换(逻辑运算和位移运算)来提高载体信息和隐秘信息间的相似性,在不损失载体容量的前提下提高感知透明性[8],以及通过合理设置部分相似值的门限值,结合 m 序列实现可自适应获得较好的不可感知性和较高隐藏容量的最佳平衡[9]. Liu 等人[10]则是将语音帧的 LSB 转换成多进制(如二进制,三进制及五进制)序列,以多进制的方式执行嵌入操作,这种方式不仅提高了隐藏容量,而且减少了对语音质量的影响. 另外,也有研究指出,可在 VoIP 隐写过程中引入各种矩阵编码方法[11~14],以提高隐写效率和隐写的不可感知性.

尽管上述研究在提高隐写安全性方面取得了显著成果,但是这些研究均将不同位置的载体同等对待,忽略了它们之间的差异性. 事实上,在各种语音编码(尤其是参数编码)中,同一语音帧中的不同位置的参数对于重构语音的质量影响是显著不同的. 可以预见,通过充分挖掘在不同载体位置间的差异性,在隐写过程中自适应地选取可隐藏性能好的位置进行嵌入,可大大降低隐写操作对载体语音质量的影响,从而进一步提高隐蔽通信的不可感知性. 有鉴于此,本文以 VoIP 隐写中应用最多的 LSB 方法为背景,首先给出一种基于性能量化的 LSB 分级方案,并以此为基础提出了一种基于 LSB 分级的自适应 VoIP 隐写方法. 以 VoIP 中广泛使用的 G.729a 语音编码为例,对上述分级方案和隐写方法进行了大量而全面的测试. 实验结果表明本文方法的可行性和有效性.

2 基于性能量化的可隐藏位分级方案

本文利用 MOS-LQO(Mean Opinion Score – Listening Quality Objective)值和信噪比 SNR (Signal-to-Noise Ratio)值来评估不同载体位置对于载体语音质量的影响. 其中,MOS-LQO 值是采用 ITU-T P.862 标准(Perceptual evaluation of speech quality,PESQ)[15]给出的一种语音质量客观评价分数,其取值在 1.017 到 4.549 之间,分数越大则语音质量越好;SNR 值定义为纯净语音信号 P_s 与噪声语音信号 P_n 的功率之比,即 $SNR = 10\log_2(P_s/P_n)$,SNR 值越高语音质量越好. 在参数编码中,所谓的可隐藏位是指对其进行修改后对语音质量影响较小的比特位;从空间域信息隐藏的角度看,可将其类比为 LSB. 在载体位置分级前,需首先对各载体位置的性能进行量化,其方法为:以选取的大量语音样本为载体,对各语音帧进行逐比特置反实验,并对置反前后的样本分别进行 PESQ 和 SNR 测试;统计语音帧中各比特对应的平均 MOS-LQO 值和平均 SNR 值,并分别按从高到低排序. 表 1 给出了 ITU G.729a 语音帧中可隐藏位的排序结果(取前 40 位).

表 1 ITU G.729a 语音帧中可隐藏位的排序结果

No	Bit	MOS – LQO	Bit	SNR
1	L3 – 0	4.388	L3 – 0	17.318
2	L3 – 1	4.339	L3 – 1	16.586
3	L3 – 2	4.334	L3 – 2	16.249
4	L3 – 4	4.328	L3 – 4	15.912
5	C1 – 9	4.315	L3 – 3	15.415
6	C2 – 9	4.311	C1 – 9	14.682
7	L3 – 3	4.220	C2 – 9	14.571
8	P2 – 0	4.051	P2 – 0	9.540
9	GB1 – 2	4.012	GB1 – 2	9.134
10	GB2 – 2	4.002	GB2 – 2	9.108
11	GA1 – 2	3.928	C1 – 5	7.916
12	GA2 – 2	3.921	C1 – 3	7.912
13	GB2 – 1	3.850	C1 – 0	7.899
14	C1 – 5	3.847	C1 – 2	7.873
15	C1 – 2	3.841	C1 – 6	7.838
16	C2 – 5	3.837	C2 – 5	7.828
17	GB1 – 1	3.834	C2 – 0	7.819
18	C2 – 2	3.825	C2 – 3	7.819
19	C1 – 8	3.823	C2 – 2	7.774
20	C2 – 8	3.813	C1 – 8	7.772
21	C1 – 12	3.792	C2 – 6	7.767

续表

No	Bit	MOS－LQO	Bit	SNR
22	C2－12	3.785	C2－8	7.717
23	C1－3	3.690	C1－10	7.679
24	C1－0	3.677	C2－10	7.645
25	C2－3	3.677	C1－12	7.573
26	C1－6	3.663	C2－12	7.566
27	C2－0	3.663	C1－4	6.645
28	C2－6	3.653	C1－1	6.634
29	C1－10	3.624	C2－1	6.563
30	C2－10	3.617	C2－4	6.554
31	C1－4	3.613	C1－7	6.551
32	C2－4	3.600	C2－7	6.505
33	C1－1	3.596	L0	6.487
34	C2－1	3.588	GB1－3	6.374
35	C1－7	3.579	C2－11	6.366
36	C2－7	3.572	C1－11	6.345
37	GB1－3	3.540	GB2－3	6.158
38	C2－11	3.534	GB2－1	5.834
39	C1－11	3.533	GB1－1	5.467
40	GB2－3	3.508	P2－1	5.211

上述排序的结果反映了参数编码中语音帧的参数比特对重构语音质量影响的非均衡性. 然而,上述两者排序的结果往往不同. 为此,本文首先依据 MOS-LQO 值对可隐藏位进行初步分级,然后根据 SNR 值排序结果对分级进行调整和优化.

假设语音帧中以平均 MOS-LQO 值和平均 SNR 值分别排序后的隐藏位集合为 $B_1=\{b_{1,1},b_{1,2},\cdots,b_{1,n}\}$ 和 $B_2=\{b_{2,1},b_{2,2},\cdots,b_{2,n}\}$,其中 n 为可隐藏位的总个数;记根据平均 MOS-LQO 值初步分为 x 级后的结果为 $\mathfrak{c}=\{\mathfrak{C}_1,\mathfrak{C}_2,\cdots,\mathfrak{C}_x\}$;记最终的分级结果为 $C=\{C_1,C_2,\cdots,C_r\}$,其中 $C_j=\{c_{j,2},c_{j,1},\cdots,c_{j,L_j}\}$,$1\leqslant j\leqslant r$,$L_j$ 表示集合 C_j 的长度,即第 j 个可隐藏级别中 LSB 的个数. 具体分级方案如下:

(1)设定分级阈值 T(在 G.729a 语音流中可设置为 0.1),对集合 B_1 进行初步分级,令 $\mathfrak{B}=B_1$,初始级数 $J=1$:

STEP 1.1:可隐藏位的预分级. 将集合中的第一个元素分配到子集 $\mathfrak{B}_1$,其余元素则分配到子集 $\mathfrak{B}_2$ 中,即 $\mathfrak{B}_1=\{b_{1,1}\}$,$\mathfrak{B}_2=\{b_{1,2},\cdots,b_{1,n}\}$.

STEP 1.2:细化分级. 计算集合 $\mathfrak{B}_1$ 中所有元素的平均 MOS-LQO 值并记为 $\mathfrak{B}$,并对集合 $\mathfrak{B}_2$ 中的每个元素依次计算绝对值 $a_i=|\varphi_i-\mathfrak{B}|$,$2\leqslant i\leqslant|\mathfrak{B}_2|+1$,$|\mathfrak{B}_2|$ 为集合 $\mathfrak{B}_2$ 中元素的个数,φ_i 为集合 $\mathfrak{B}_2$ 中的元素 $b_{1,i}$所对应的 MOS-LQO 值,并做如下判断:若 $a_i<T$,则集合 $\mathfrak{B}_2$ 中的元素 $b_{1,i}$属于子集 $\mathfrak{B}_1$,需将元素 $b_{1,i}$从集合 $\mathfrak{B}_2$ 移到集合 $\mathfrak{B}_1$;若 $a_i\geqslant T$,则将元素 $b_{1,i}$视为临界点,并将其暂时分配到集合 $\mathfrak{B}_1$;之后,记 $\mathfrak{C}_J=\mathfrak{B}_1$,$J=J+1$,判断集合 $\mathfrak{B}_2$ 是否为空集,若是,则对可隐藏位初步分级结束,执行 STEP 1.4,否则,执行 STEP 1.3.

STEP 1.3:对 STEP 1.2 中的集合 $\mathfrak{B}_2$ 继续分级,即 $\mathfrak{B}=\mathfrak{B}_2$,执行 STEP 1.1.

STEP 1.4:重新分配临界点:对 STEP 1.2 中提及的所有临界点进行重新分配;将当前临界点 Q 的 MOS-LQO 值与下一级的平均 MOS-LQO 值之差的绝对值记为 p,若 $p>T$,则将当前临界点分配到下一级的可隐藏级别中,若 $p\leqslant T$,则当前临界点仍归于当前可隐藏级别中.

(2)根据可隐藏位的平均 SNR 值对上述分级结果进行调整和优化,初始化 $I=1$,$J=1$,具体步骤如下:

STPE 2.1:确定(1)中的初步分级结果的第 I 个可隐藏等级 $\mathfrak{C}_I$ 中隐藏位的个数$|\mathfrak{C}_I|$;取 B_2 中的前$|\mathfrak{C}_I|$个元素构成集合 $\mathfrak{B}'$,做如下判断:如果 $\mathfrak{C}_I=\mathfrak{B}'$,记 $C_J=\mathfrak{C}_I$,从 B_2 去除已划分到 C_J 的所有元素,当还有初步分级待优化,取 $I=I+1$,$J=J+1$,重复 STPE 2.1;如果 $\mathfrak{C}_I\neq\mathfrak{B}'$且 $\mathfrak{C}_I\cap\mathfrak{B}'\neq\varnothing$,取 $\mathfrak{C}_I$ 和 $\mathfrak{B}'$相同的元素构成级别 C_J,并从 B_2 去除已划分到 C_J 的所有元素,执行 STPE 2.2;如果 $\mathfrak{C}_I\cap\mathfrak{B}'=\varnothing$,分级结束.

STPE 2.2:确定 $\mathfrak{C}'=\mathfrak{C}_I-C_J$ 及其包含的元素个数$|\mathfrak{C}'|$;在 B_2 中取前$|\mathfrak{C}'|$个元素与 $\mathfrak{C}'$一起构成集合 $\mathfrak{C}^*$;在 $\mathfrak{C}^*$中依次测试选取 2 到$|\mathfrak{C}^*|$个所有元素组合进行 LSB 替换后的平均 MOS-LQO 值和平均 SNR 值;取符合 MOS-LQO 值和 SNR 值要求(如 MOS-LQO>3.5 且 SNR>7),且元素个数最多的组合,构成级别 C_{J+1},完成分级.

值得注意的是,为保证隐写操作的实时性,上述分级操作均应隐写前完成,且其结果为发送方和接收方所共享.

3　基于可隐藏位分级的自适应隐写

以上述分级结果为依据,本文提出了一种充分利用 LSB 的冗余差异性的自适应隐写方法. 假设发送方将发送 L_M 比特隐秘信息 $M=\{m_i=0\text{ or }1\mid I=1,2,\cdots,L_M\}$,用于隐藏 M 的载体信息集合(本文指载体的所有 LSB 位)为 $C=\{c_i=0\text{ or }1\mid i=1,2,\cdots,L_C\}$,其中 L_C 表示集合 C 的长度. 为了使隐秘信息能够完全嵌入,L_C 与 L_M 需满足:$L_C\geqslant L_M$. 在嵌入过程中,将载体 LSB 集合 C 按上文提出的 LSB 分级方案分成 r 组,即 $C=\{C_1,C_2,\cdots,C_r\}$,其中 $C_j=\{c_{j,1},c_{j,2},\cdots,c_{j,L_j}\}$,$1\leqslant j\leqslant r$,$L_j$ 表示集合 C_j 的长度,即第 j 个可隐藏级别中 LSB 的个数. 根据

上述符号定义,嵌入操作步骤为:

STEP1:计算权重向量 $\boldsymbol{W}$:记权重向量 $\boldsymbol{W}=\{w_i\in[0,1]\mid i=1,2,\cdots,r\}$,其中,$r$ 为可隐藏级别的总数,w_i 为第 i 个可隐藏级别的权重系数,定义为该可隐藏级别在隐藏过程中需选择的 LSB 数与该级别中总 LSB 数之比,其计算方式可表述为:

$$w_i=\begin{cases}0, & \text{当 } x\leqslant 0\\ x, & \text{当 } 0<x<1\\ 1, & \text{当 } x\geqslant 1\end{cases} \tag{1}$$

上式中,x 的计算方式如下:

$$x=\frac{\alpha\cdot L_c-\sum_{j=1}^{i-1}(L_j\cdot w_j)}{L_i} \tag{2}$$

其中,$\alpha=L_M/L_C$ 表示隐秘信息长度 L_M 与载体 LSB 总个数 L_C 的比值,L_i 为第 i 个可隐藏级别中 LSB 的个数.

STEP2:根据权重向量 W 中非零元素的个数 k,将隐秘信息 M 分成 k 组,即 $M=\{M_1,M_2,\cdots,M_k\}$,$M_i=\{m_{i,1},m_{i,2},\cdots,m_{i,l_i}\}$,$1\leqslant k\leqslant r$,$l_i$ 为每组隐秘信息的长度且 $1\leqslant i\leqslant k$,其计算式为 $l_i=L_i*\ w_i$;

隐秘信息的嵌入过程表达式为:

$$C'=\begin{cases}\sum_{i=1}^{L_i}\psi_i+\sum_{i=k+1}^{r}C_i, & k=1\\ \sum_{i=1}^{k-1}\sum_{j=1}^{l_i}c_{i,j}\otimes m_{i,j}+\sum_{i=1}^{L_i}\psi_i+\sum_{i=k+1}^{r}C_i, & k>1\end{cases} \tag{3}$$

其中,$V=\{v_1,v_2,\cdots,v_{L_i}\}$ 为随机生成的选择因子的集合,$v_i=0$ 或 1,$1\leqslant i\leqslant L_k$,且 $\sum_{i=1}^{L_i}v_i=L_k\cdot w_k$;$C'=\{C'_1,C'_2,\cdots,C'_r\}$ 表示嵌入隐秘信息后的载密信息集合,其中 $C'_j=\{c'_{j,1},c'_{j,2},\cdots,c'_{j,L_j}\}$,$1\leqslant j\leqslant r$;符号"$\otimes$"表示替换操作.

$$\psi_i=(1-v_i)\cdot c_{k,i}+v_i\cdot m_{k,t} \tag{4}$$

$$t=\begin{cases}1, & \text{当 } i=1\\ \sum_{j=1}^{i}v_j, & \text{当 } i>1\end{cases} \tag{5}$$

相应地,接收方根据分级结果以及事先约定的每帧嵌入隐秘信息 M 的长度 L_M,确定权重向量 $\boldsymbol{W}$,并计算 W 中非零元素的个数 k;与此同时,根据事先约定的密钥产生选择因子集合 V,并可结合公式(6)提取隐秘信息 M.

$$M=\begin{cases}\sum_{i=1}^{L_i}v_i\cdot c'_{k,i}, & \text{当 } k=1\\ \sum_{i=1}^{k-1}\sum_{j=1}^{l_i}c'_{i,j}+\sum_{i=1}^{L_i}v_i\cdot c'_{k,i}, & \text{当 } k>1\end{cases} \tag{6}$$

4 实验与分析

本文以 VoIP 中广泛使用的 ITUG.729a 编码为例对本文提出的分级方案和隐写方法进行测试. 然而,需要指出的是,本文提出的方法与具体的编码器无关,具有良好的普适性. 实验选取了 1600 个语音样本(包括中文男声,中文女声,英文男声和英文女声)作为载体,对它们的 G.729a 编码版本进行分级实验和相关隐写操作.

4.1 G.729a 编码语音帧的 LSB 分级特性

根据上文所述的 LSB 分级方法,G.729a 语音帧的 LSB 可分成 3 个可隐藏等级,如表 2 所示. 第一级为最优的可隐藏级别,包含 7 个 LSB;第二级次之,包含 3 个 LSB;第三级包含 2 个 LSB.

表 2 G.729a 语音帧的可隐藏位分级

可隐藏等级	可隐藏位 ($Px-y$)
第 1 级	L3-0,L3-1,L3-2,L3-4,C1-9,C2-9,L3-3
第 2 级	P2-0,GB1-2,GB2-2
第 3 级	C1-5,C1-3

为了评估每个可隐藏等级的可隐藏性能,对各可隐藏等级分别进行 LSB 替换测试:以第 i 级的 k 个可隐藏位为载体,测试隐藏容量为 x 比特/帧的所有组合的 LSB 替换($1\leqslant i\leqslant 3$,$x=2,3,4,\cdots,k$,k 表示第 i 级的所有可隐藏位数). 对第 1 级、第 2 级、第 3 级进行 LSB 替换测试的 MOS-LQO 及 SNR 结果,分别如图 1、2、3 和 4 所示. 从图中可看出,(1)在不同级别选取相同载体数进行 LSB 替换所得的平均 MOS-LQO 值和平均 SNR 值不同;隐藏级别越低的其平均 MOS-LQO 值以及平均 SNR 值越低,说明了经过分级之后,不同级别的可隐藏性能不一样,选取不同级别的可隐藏位作为载体进行的 LSB 替换所得的语音质量也不同,验证了对可隐藏位分级的必要性;(2)在同一级别中,对于隐藏容量相同的所有组合的 LSB 替换,它们的平均 MOS-LQO 值以及平均 SNR 相差非常小,说明了在同一可隐藏级别中,对给定隐藏容量可随机选择相同数目的载体.

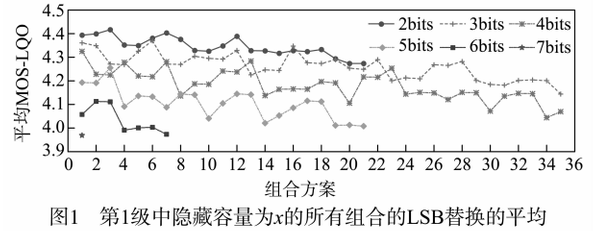


图1 第1级中隐藏容量为x的所有组合的LSB替换的平均MOS-LQO值

为了进一步验证隐藏等级高的可隐藏位的性能优于隐藏级别低的可隐藏位的性能,我们做了如下测试:在相同隐藏容量的前提下,分别从{一个可隐藏等级}、{两个可隐藏等级}、{三个可隐藏等级}这三组中随机选择载体进行 LSB 替换. 图 5 和图 6 所示的是以上三组 LSB 替换的实验结果. 从图 5 可看出,在具有相同隐藏

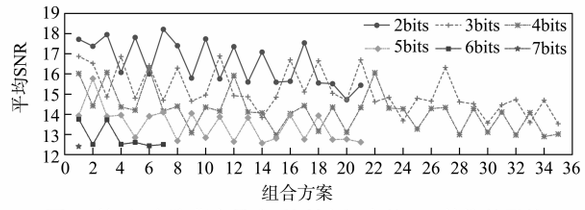
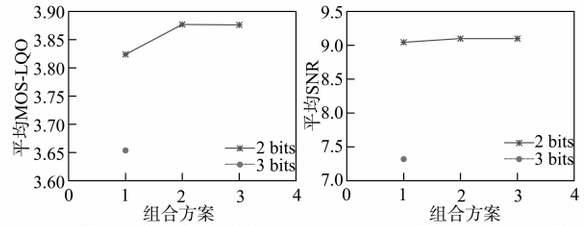
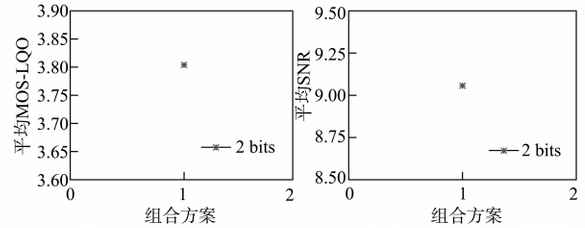


图2　第1级中隐藏容量为x的所有组合的LSB替换的平均SNR值



(*a*) 第2级所有组合LSB替换的MOS-LQO值　(*b*) 第2级所有组合LSB替换的SNR值

图 3　第2级中隐藏容量为x的所有组合的LSB替换的平均MOS-LQO值及平均SNR值



(*a*) 第3级所有组合LSB替换的MOS-LQO值　(*b*) 第3级所有组合LSB替换的SNR值

图 4　第3级中隐藏容量为x的所有组合的LSB替换的平均MOS-LQO值及平均SNR值

容量选择不同可隐藏等级的载体的情况下:选择第 1 级的可隐藏位作为载体的平均 MOS-LQO 值会高于从第 1,2 级和第 1,3 级中随机选择的可隐藏位作为载体的平均 MOS-LQO 值;而从第 1,2,3 级中随机选择的可隐藏位作为载体一组的平均 MOS-LQO 值则最低. 这说明

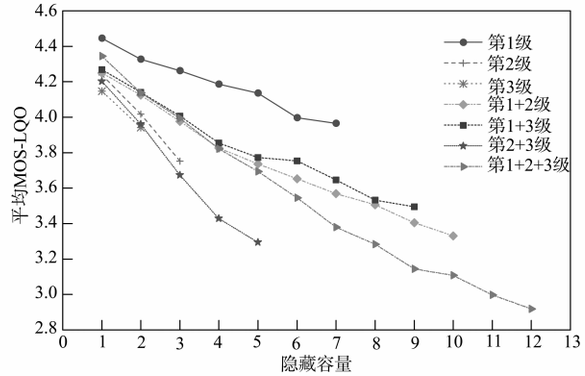


图5　相同隐藏容量下，分别从不同级别中选取载体的LSB替换的MOS-LQO

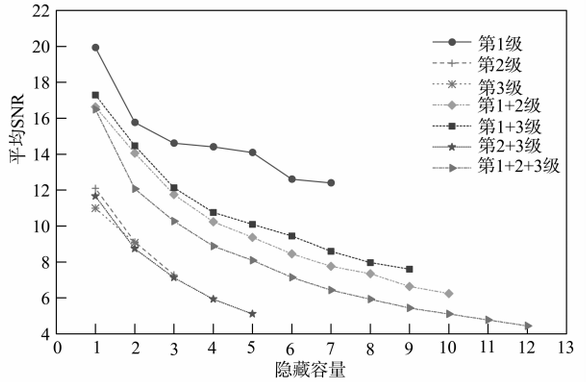


图6　相同隐藏容量下，分别从不同级别中选取载体的LSB替换的SNR

了分别对以上三组载体进行 LSB 替换后的载密语音的语音质量是依次降低的. 同样,由图 6 也可看出,采用信噪比测试的结果与 MOS-LQO 的结论相近,因此,进一步验证了对可隐藏位的分级可提高隐写过程的不可感知性,增强隐蔽通信的安全性.

4.2　隐写性能

为了验证所提出的自适应分级隐写方法的有效性,以随机生成的二进制序列作为隐秘信息,将所提方法与以下六组实验进行比较:(1)选择 Su 等人分析所得的固定码书索引参数作为载体进行 LSB 替换[16];(2)选择三个可隐藏级别中所有可隐藏位作为载体进行随机的 LSB 替换(共 12 比特,记 $m=12$);(3)选择按 MOS-LQO 排序前 12 位可隐藏位作为载体进行随机的 LSB 替换(共 12 比特,记 $m=12$[MOS-LQO]);(4)选择各比特置反后 SNR 大于 7 的位作为载体进行随机的 LSB 替换(共 26 比特,记 $m=26$[SNR]);(5)选择按 MOS-LQO 排序前 26 位可隐藏位作为载体进行随机的 LSB 替换(记 $m=26$[MOS-LQO]);(6)选择各比特置反后 MOS-LQO 大于 3.5 的位作为载体进行随机的 LSB 替换(共 40 比特,记 $m=40$).

以上七组实验中隐藏容量分别从 1 比特/帧到 12 比特/帧的平均 MOS-LQO 值及平均 SNR 比较结果,分别如图 7、8 所示. 根据图 7、8 容易得知,在相同隐藏容量的前提下,本节所提出的自适应分级隐写方法的平均 MOS-LQO 值以及平均 SNR 明显优于其他 6 组,这说明了所提出的隐写方法对载体语音质量的失真影响较小,嵌入隐秘信息后的载密语音质量良好,即具有较高的不可感知性. 此外,由图中可看出,对于不同的隐藏容量,采用自适应的分级隐写方法的语音质量不等,因此,在实际应用中,用户可根据实际需求通过合理的选取载体向量长度以自适应调整不可感知性和隐藏容量间的较佳平衡.

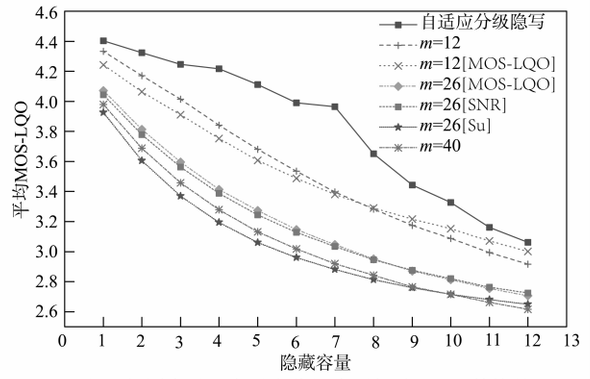


图7 相同容量，自适应分级隐写与随机LSB替换的MOS-LQO比较

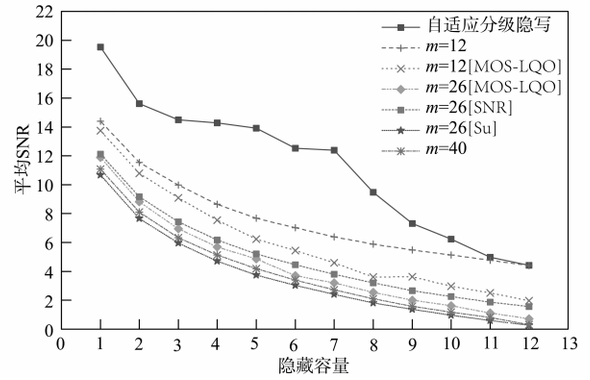


图8 相同容量，自适应分级隐写与随机LSB替换的SNR比较

5 结论与未来的工作

基于IP语音的隐写是当前信息隐藏研究的一个热点.然而,现有研究均将可隐藏位置一视同仁地对待,忽略了其差异性.本文首先通过性能量化的方式,对载体隐藏位置的非均衡性进行了分析;进而给出了一种可隐藏位的分级方法;并以此为基础,提出了一种基于分级的自适应隐写方法.本文代表性地选择广泛使用的G.729a为编码器,以大量的语音样本为载体,对本文提出的分级方案和隐写算法进行了实验测试.实验结果表明,通过对载体LSB进行分级可明显提高嵌入隐密信息后的载体语音质量,从而提高载密语音的不可感知性;并且与目前较流行的随机LSB替换相比,在相同的隐藏容量的前提下,本文算法的不可感知性明显优于随机LSB替换方法.

本文是对于分级隐写的一次初步尝试,尽管获得了一些有益的结果,但后续仍有许多工作值得深入,如进一步研究载体分级的相关理论基础和方法,将分级思想与隐写编码理论相结合探索具有更好性能的隐写方法,以及分析分级隐写的抗隐写分析性能等.

参考文献

[1] Mazurczyk W. VoIP Steganography and its detection:a survey [J]. ACM Computing Survey,2013,2(46):20.

[2] Huang Y, Yuan J, Chen M, Xiao B. Key distribution over the covert communication based on VoIP[J]. Chinese Journal of Electronics,2011,20(2):357 – 360

[3] 钟巍,孔祥维,尤新刚,王波. 基于态函数的离散分数余弦倒谱变换在取证话音信息隐藏中的应用[J]. 电子学报,2012,40(3):595 – 599.
Zhong W, Kong X, You X, Wang B. Forensic speech information hiding using fractional cosine-cepstrum transform [J]. Acta Electronica Sinica,2012,40(3):595 – 599. (in Chinese)

[4] 杨婉霞,余晖,胡萍. 在压缩语音编码中集成信息隐藏方法研究[J]. 电子学报,2014,42(7):1305 – 1310.
Yang W, Yu H, Hu P. Research on steganographic method integrated in the compressed speech codec[J]. Acta Electronica Sinica,2014,42(7):1305 – 1310. (in Chinese)

[5] Kratzer C, Dittmann J, Vogel T, et al. Design and evaluation of steganography for voice-over-IP [A]. Proceedings of the 19th IEEE International Symposium on Circuits and Systems[C]. Kos, Greece:IEEE,2006. 2397 – 2340.

[6] Tian H, Zhou K, Jiang H, et al. An m-sequence based steganography model for voice over IP [A]. Proceedings of the 44th IEEE International Conference on Communications [C]. Dresden, Germany:IEEE,2009. 1 – 5.

[7] Huang Y, Xiao B, Xiao H. Implementation of covert communication based on steganography [A]. Proceedings of the 4th International Conference on Intelligent Information Hiding and Multimedia Signal Processing[C]. Harbin, China:IEEE,2008. 1512 – 1515.

[8] Tian H, Zhou K, Jiang H, et al. Digital Logic based encoding strategies for steganography on Voice-over-IP [A]. Proceedings of the 17th ACM Multimedia Conference[C]. Beijing, China:ACM,2009. 777 – 780.

[9] Tian H, Jiang H, Zhou K, et al. Adaptive partial-matching steganography for voice over IP using triple M sequences [J]. Computer Communications, 2011, 34 (18): 2236 – 2247.

[10] Liu J, Zhou K, Tian H. Least-significant-digit steganography in low bitrate speech [A]. Proceedings of the 47th IEEE International Conference on Communications[C]. Ottawa, Canada:IEEE,2012. 1 – 5.

[11] Tian H, Zhou K, Feng D. Dynamic matrix encoding strategy for voice-over-IP steganography [J]. Journal of Central South University of Technology, 2010, 17(6): 1285 – 1292.

[12] Tian H, Jiang H, Zhou K, et al. Transparency-orientated

encoding strategies for voice-over-IP steganography [J]. The Computer Journal, 2012, 55(6): 702 – 716.

[13] Wu Z J, Cao H J, Li D Z. An approach of steganography in G. 729 bitstream based on matrix coding and interleaving [J]. Chinese Journal of Electronics, 2015, 24(1): 157 – 165.

[14] Tian H, Qin J, Huang Y, et al. Optimal matrix embedding for Voice-over-IP steganography [J]. Signal Processing, 2015, 117: 33 – 43.

[15] ITU-T Recommendation P. 862. Perceptual evaluation of speech quality (PESQ): an objective method for end-to-end speech quality assessment of narrow-band telephone networks and speech codecs [S]. 2001.

[16] Su Y, Huang Y, et al. Steganography-oriented noisy resistance model of G. 729a [A]. Proceedings of IMACS Multi-conference on Computational Engineering in Systems Applications [C]. Beijing, China: IEEE, 2006. 11 – 15.

作者简介

田　晖　男,1982 年生于湖北赤壁,博士,现为华侨大学计算机科学与技术学院副教授. 研究方向为网络与信息安全,多媒体内容安全等. E-mail: htian@ hqu. edu. cn

郭舒婷　女,1989 年生于福建漳州. 华侨大学计算机科学与技术学院硕士研究生. 研究方向为多媒体内容安全,信息隐藏等.