GSM 移动通信系统中语音隐藏算法研究*

白 剑, 杨 榆, 徐迎晖, 钮心忻, 杨义先
(北京邮电大学 国家重点实验室 //信息安全中心, 北京 100876)

摘 要: 提出了一种能够在GSM 移动通信网络中使用的信息隐藏算法。隐藏容量为 50 bit/s。实验结果表明算法对GSM、ADPCM 等语音压缩编码以及滤波操作有很强的鲁棒性, 携密语音的分段平均信噪比接近 35 dB, 可以达到透明性要求。算法简单易行并且是基于盲检测的, 具有很大的实用性。

关键词: 信息隐藏; 语音隐藏; GSM 移动通信系统
中图分类号: TP391.41 文献标识码: A 文章编号: 0529-6579 (2004) S2-0156-04

当前移动通信网络已经非常普及, 随着移动通信尤其是 GSM 通信的越来越普及, 其带来的安全问题也越来越突出。目前主要的安全问题是移动通信窃听问题。

为了解决移动通信中的保密通话问题, 业界人士提出了一些解决方案。如德国手机制造商 GSMK 公司近日推出了将语音通话加密后再进行传输的手机。这种方式解决了一定的通信保密问题。但是要求通信双方必须同时使用 GSMK 公司的手机, 而且窃听者听到的是噪音, 很容易引起窃听者的怀疑进而重点关注精心破译。

针对上述问题, 有学者提出了利用信息隐藏的方法进行保密通信传输的方法。信息隐藏[1-3] 是把有意义的信息隐藏在另一个称为载体的信息中得到隐密载体, 使窃听者察觉不到隐密载体中隐藏了其他信息, 以达到信息安全传输目的的方法。文献[4] 提出了一种伪装式数字化语音保密通信系统。该系统将需要传输的密文语音信息利用 MELP 算法编码后, 使用 ABS 算法隐藏到一段 GSM 编码的明文语音中传输。这样窃听者听到的是一段正常的明文语音信息, 不容易引起怀疑, 使得密文信息能够安全传输。但是这种方法要求对现有手机的 GSM 语音编码电路进行改造, 在其中嵌入 ABS 算法, 实现难度较大。

为了获得一种能够和现有大多数 GSM 手机兼容的语音隐藏移动通信系统, 要求设计一种算法能够在手机 GSM 语音编码芯片之前完成信息隐藏, 并且能够抵抗 GSM 编码解码, 最终在接收端正常解出隐藏的密文信息。这种算法的关键在于能够抵抗 GSM 语音编解码, 即 GSM 编码解码不会影响隐藏信息的嵌入。经过研究发现一段语音经过 GSM 编解码以后, 输出语音和原始语音的相邻段能量比基本保持一致。基于此性质, 本文提出了一种新的能够抵抗 GSM 语音编码的信息隐藏算法。其原理为将明文语音分段, 根据密文信息调整相邻段之间的能量大小, 在接收端根据相邻段之间的能量大小进行解码。大量仿真试验结果表明该算法能够抵抗 GSM 编码解码, 其明文语音质量下降不多。每秒明文能够嵌入 50bit 的密文信息。是一种简单有效的 GSM 移动通信系统语音隐藏算法。

1 GSM 编码算法特性研究

我们经过对大量语音信号的 GSM 编码前后特性分析研究发现, 一段语音信号经过编解码以后, 能量改变的幅度不大。对大量语音 (采样率 8 kHz, 以 80 个采样点为一个分段) 经过 GSM 编解码前后的每段能量比进行了分析和统计 (见表 1), 结果表明编码前后的能量比集中在 0.9 ~ 1.5, 尤其是 0.9 ~ 1.3 之间。

由以上分析结果可知, 如果我们利用相邻语音段能量比来进行信息隐藏, 将相邻段能量比定位为 1.5 以上, 即可保证经过 GSM 编码解码后信息可以得到 91% 以上的恢复率。为了达到 100% 的恢复率, 可以引入纠错交织编码技术。如使用 Gray 码 (23, 12, 3), 理论可以将 13% 以下误码完全纠正。正是基于该发现, 我们提出了本文的语音隐藏算法。

* 收稿日期: 2004-09-11
基金项目: 国家重点基础研究发展规划资助项目 (TG1999035804); 教育部优秀青年教师资助计划资助项目; "十五" 国家密码发展基金资助项目
作者简介: 白剑 (1979 年生), 男, 博士研究生; E-mail: Baijbupt@263.net

(C)1994-2020 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

表 1　GSM 编解码前后的每段能量比

Tab. 1　Energy ratio of pre-coding and decoding

编码前后能量比	落在该能量比的语音分段数量	占总数量的百分比/%
0.9~1.1	9486	31
1.1~1.3	13715	45
1.3~1.5	4775	15
1.5~2.0	1725	5
其他	1362	4

2　信息嵌入算法

信息嵌入算法的流程框图如图 1 所示：

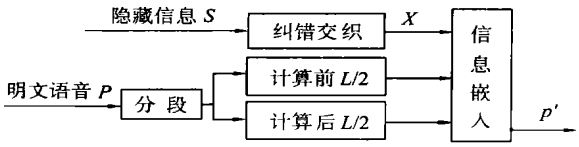

图 1　信息嵌入算法流程框图

Fig. 1　Infomation embedded procession

具体实现流程如下：

(1) 将需要隐藏的信息 S 使用 Gray 码进行纠错交织编码，形成 q bit 的的隐藏信息 X：

$$X=\{x(i),0<i<q\},x(i)\in\{0,1\} \quad (1)$$

(2) 将明文语音 P 进行分段，设 $P=\{p(j),0<j<M\}$ 为 M 个样点的公开语音，分段后表示为：

$$p(k)=p(k\times L+j),\quad 0<k<K \text{ 且 } 0<j<L \quad (2)$$

式中，$p(k)$ 表示第 k 段语音，K 表示明文语音的总段数，L 表示每段样点数。若要保证隐藏信息 X 能够完整嵌入，必须满足不等式：$q\leqslant L$ 或者 $q\times L\leqslant M$。本文取 $L=160$。将 p 分段分别计算前 $L/2$ 个点的能量和后 $L/2$ 个点的能量：

$$E_1=\sum_{j=0}^{L/2-1}(p(k\times L+j))^2 \quad (3)$$

$$E_2=\sum_{j=L/2}^{L}(p(k\times L+j))^2 \quad (4)$$

(3) 在对应段嵌入信息。由于透明性和鲁棒性是一对矛盾，嵌入深度 β 增加，鲁棒性随之提高，但势必导致携密语音 p' 质量的下降，因此 β 依据具体应用条件适当选取。

将 $x(i)$ 嵌入到 p 中的具体过程如下：

首先计算前 $L/2$ 段的放大增益：

$$\beta_1=\begin{cases}\sqrt{\beta\times E_2/E_1} & x(i)=1 \text{ 且 } E_1/E_2<\beta\\ 1 & \text{其他}\end{cases} \quad (5)$$

其次计算后 $L/2$ 段的放大增益：

$$\beta_2=\begin{cases}\sqrt{\beta\times \dfrac{E_2}{E_1}} & x(i)=0 \text{ 且}\dfrac{E_2}{E_1}<\beta\\ 1 & \text{其他}\end{cases} \quad (6)$$

最后根据 β_1、β_2 的值将 $x(i)$ 嵌入到明文语音 P 中

$$P'(k\times L+j)=\begin{cases}P(k\times L+j)\times\beta_1 & 0\leqslant j<L/2\\ P(k\times L+j)\times\beta_2 & L/2\leqslant j\leqslant L\end{cases} \quad (7)$$

从而获得携密的明文语音 p' 进行存储或者传输。

3　信息提取算法

信息提取算法的流程框图如图 2 所示：

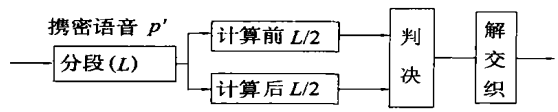

图 2　信息提取算法流程框图

Fig. 2　Information extracted procession

在信息提取时，首先将接收到的携密的明文语音 P' 进行分段处理，每段段长为 L 个采样点。分段后表示为：

$$P'(k)=P'(k\times L+j),\quad 0<k<K \text{ 且 } 0<j<L \quad (8)$$

然后计算前 $L/2$ 点能量 E'_1 和后 $L/2$ 点能量 E'_2：

$$E_1=\sum_{j=0}^{L/2-1}(p(k\times L+j))^2 \quad (9)$$

$$E_2=\sum_{j=L/2}^{L}(p(k\times L+j))^2 \quad (10)$$

然后进行判决获得通过信道的密文信息 X'。判决规则如下：

$$X'(i)=\begin{cases}1 & E'_1>E'_2\\ 0 & E'_2\geqslant E'_1\end{cases} \quad (11)$$

将 X' 经过解交织解纠错编码即可得到恢复的密文信息。

4　性能分析

为了测试该算法的性能，进行了各类仿真实验。实验的数据中均采用 8 kHz 采样，16 bits 量化的语音，语音 S 共 323840 个样点。语音段长 L 为 160 个采样点，嵌入深度 $\beta=1.5$。分别在无攻击和多种攻击情况下分析本文算法的性能。

4.1　性能指标

本文衡量音质的主要性能指标有归一化相关系数、分段平均信噪比[5]。

(C)1994-2020 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

其中归一化相关系数 ρ 的定义为: 对于原始序列 W 和变化后的序列 W', 有:

$$\rho(W, W') = \frac{\sum_i w(i)\, w'(i)}{\sqrt{\sum_i w(i)^2}\ \sqrt{\sum_i w'(i)^2}} \quad (12)$$

分段平均信噪比 SNR 用于衡量中间语音 P' 的客观音质, 定义为各段语音信噪比的平均值。当 $p(i) = p'(i)$ 时, 本段 $p(i)$ 和 $p'(i)$ 信噪比的分母为0, 此时令信噪比为 100。由此可得分段平均信噪比 SNR 定义为:

$$\mathrm{SNR} = \frac{1}{K}\sum_{i=0}^{K-1}\mathrm{SNR}_i \quad (13)$$

其中

$$\mathrm{SNR}_i = \begin{cases} 100 & p(i) = p'(i) \\ \dfrac{\sum_{j=0}^{L-1} p^2(j\times L + i)}{\sum_{j=0}^{L-1}[p(j\times L + i) - p'(j\times L + i)]^2} & p(i) \neq p'(i) \end{cases} \quad (14)$$

4.2 携密语音 P' 的质量

携密语音 P' 质量的好坏反映了算法的透明性指标, 是衡量算法好坏的重要标志。表 2 给出了本文算法在无攻击情况下的分段平均信噪比 SNR (dB) 和原始明文和携密明文归一化相关系数指标。

表 2 无攻击情况下携密语音 P' 的音质

Tab. 2 Embedded audio qnality

算法	分段平均信噪比	$\rho(P, P')$
GSM 能量隐藏算法	34.7	0.984

从主观听觉测试结果表明, 本文所提算法获得的携密语音仅仅比原始明文略多一点噪声, 并不影响整体听觉效果。图 3、4 给出了原始语音 P 和携密语音 P' 之间波形和频谱对比图。

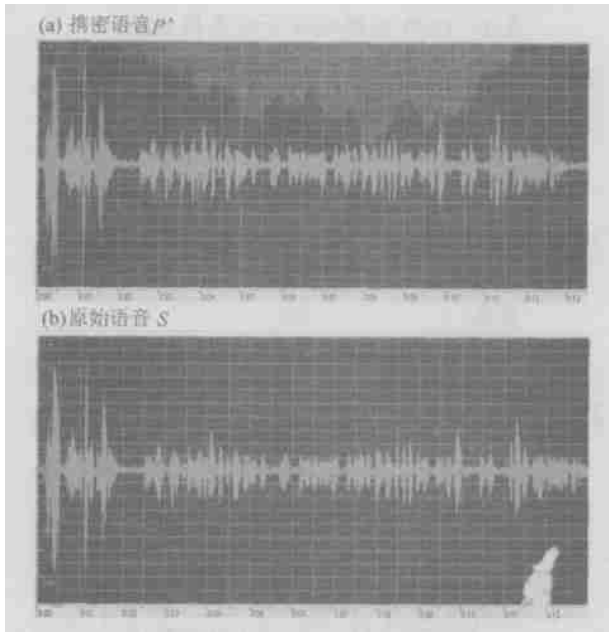

图 3 携密语音和原始语音波形比较图

Fig. 3 Original and embedded audio time domain diagram

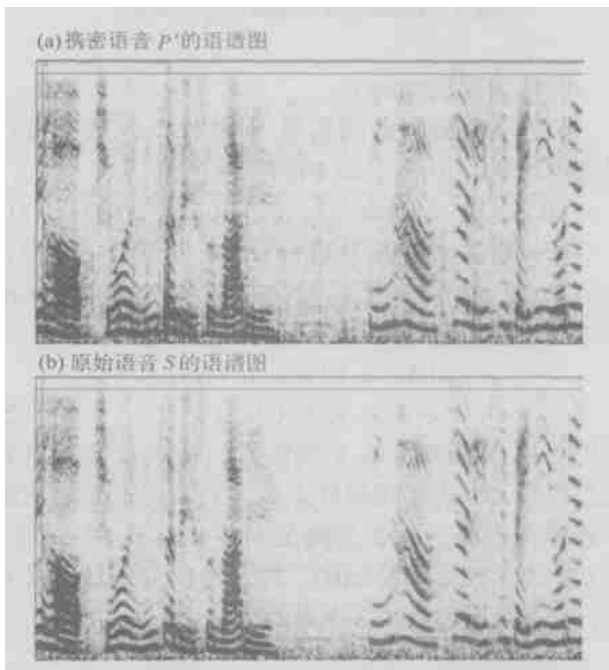

图 4 携密语音和原始语音频谱比较图

Fig. 4 Original and emkedded audio frequercy domain diagram

4.3 抗语音压缩测试

抗压缩能力是衡量算法鲁棒性的重要指标, 也是通信网络环境对实用信息隐藏技术的要求。为了测试本文所提算法抵抗语音压缩的性能, 我们将中间语音 P' 分别使用 GSM 语音编码、G.721 32 kb/s ADPCM 以及 G.723 24/40 kb/s 的 ADPCM 编码进行压缩后再进行信息提取。表 3 显示了经过不同语音编码算法处理以后信息提取的误码率以及经过纠错以后的误码率。

表 3 本文算法抗压缩性能测试结果

Tab. 3 Performance of anti-coding

压缩算法	直接提取信息的误码率/%	经过纠错以后提取信息误码率
GSM 语音编码	5.08	0
24 kb/s ADPCM	0.2	0
32 kb/s ADPCM	0	0
40 kb/s ADPCM	0	0

4.4 抗低通滤波性能

将携密语音 P' 经过截止频率分别为 500~3500

(C)1994-2020 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

Hz 的低通滤波器，滤波后提取隐藏信息。图 5 给出了低通滤波后的性能曲线。图 5 表明即使 P' 在 2 kHz 低通滤波的攻击下，经过纠错编码以后仍能够完全解出隐藏信息。

4.5　抗中值滤波性能

中值滤波是语音处理中常用的操作。为了测试本文所提算法抵抗中值滤波的性能，我们将携密语音 P' 经过 3 点中值滤波后进行信息提取。评测结果表明直接提取后信息的误码率为 0.3%，而经过 Gray 码纠错以后，隐藏信息能够完全恢复。

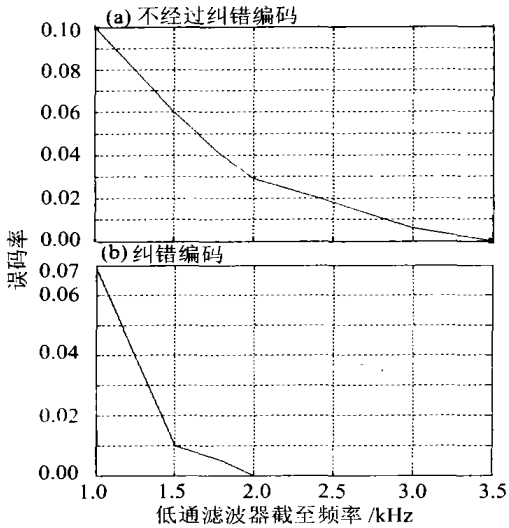

图 5　算法抵抗低通滤波的性能

Fig. 5　Performance of anti-lowpass filter

5　结　论

本文基于 GSM 语音编码对相邻段语音能量比改变不大这一特性，提出了一种能够在 GSM 移动通信网络中使用的信息隐藏算法。并对算法进行了性能测试，实验结果表明算法对 GSM、ADPCM 等语音压缩编码以及滤波操作有很强的鲁棒性，携密语音的分段平均信噪比接近 35dB，可以达到透明性要求。算法简单易行并且是基于盲检测的，具有很大的实用性。本文提出的基于语音的信息隐藏方法可以广泛运用于移动通信网、固定通信网条件下信息安全传输、数字水印、版权保护等领域。

参考文献：

[1] KATZENBEISSER S, PETITCOLAS F A P. Information hiding techniques for stangraphy and digital watermarking [M]. England: Artech House, 1999.

[2] PETITCOLAS F A P, ANDERSON R J, KUHN M G. Information hiding —A survey[J]. Proc IEEE, 1999, 87(7): 1062—1078.

[3] LEE S, JUNG S Z. A survey of watermarking techniques applied to multimedia[J]. Proceedings of ISIE, 2001(1): 272—277.

[4] 杨伟, 王飞, 张中, 等. 伪装式数字化语音保密通信系统[J]. 通信学报, 2004, 25(2): 75—81.

[5] 陈亮, 张雄伟. 基于语音参数模型的语音隐藏算法[J]. 计算机学报, 2003, 26(8): 974—981.

An Audio Hiding Algorithm on GSM Mobile Communication System

BAI Jian, *YANG Yu*, *XU Ying-hui*, *NIU Xin-xin*, *YANG Yi-xian*

(National Key Lab //Information Security Center,

Beijing University of Posts and Telecommunications, Beijing 100876, China)

Abstract: This paper presents an audio hiding algorithm on GSM mobile communication system. The hiding capacity of the algorithm is 50 bit per second. After a lot of experiments, it was proved that this algorithm has strong robustness to many attacks such as GSM, ADPCM compression and filter. The average SNR of the middle speech is close to 35 db, therefore the imperceptibility will be ensured. Moreover the algorithm is based on blind-detection, it is simple and effective.

Key words: information hiding; audio hiding; GSM mobile communication system

(C)1994-2020 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net