文章编号:1001 - 9081(2007)04 - 0841 - 02

全球移动通信系统中语音信息隐藏算法的研究

陈雪松[1,2],金七顺[2],杨永田[1]
(1. 哈尔滨工程大学 计算机科学与技术学院,黑龙江 哈尔滨 150001;
2. 大庆石油学院 电气信息工程学院,黑龙江 大庆 163318)
(chenxuesong@dqpi.edu.cn)

摘 要:提出了一种可在全球移动通信系统(GSM)中使用的语音信息隐藏算法,即基于分析合成的能量比调整算法。算法采用了分析合成(ABS)技术,在嵌入过程中根据输入明文语音实时的调整嵌入强度,使得隐藏效果和解码效果都达到最佳值。

关键词:语音信息隐藏;分析合成;能量比
中图分类号: TP309.7 **文献标识码**:A

Study on a voice hiding algorithm in GSM communication

CHEN Xue-song[1,2], JIN Qi-shun[2], YANG Yong-tian[1]
(1. *College of Computer Science and Technology, Harbin Engineering University, Harbin Heilongjiang* 150001, *China*;
2. *Faculty of Electrical and Information Engineering, Daqing Petroleum Institute, Daqing Heilongjiang* 163318, *China*)

Abstract: A voice hiding algorithm that can be used in Global System for Mobile Communication (GSM) was proposed. It is speech-hiding algorithm based on the Analysis-by-Synthesis Energy Ratio. The algorithm is based on the technique of Analysis-By-Synthesis (ABS) and can adjust adaptively the strength of the security information component according to public speech to achieve the best performance of hiding and encoding.

Key words: voice hiding; Analysis-By-Synthesis (ABS); energy ratio

0 引言

信息隐藏技术即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,使非法者察觉不到隐密载体中隐藏了其他信息。所用的载体可以是文字、图像、声音和视频等[1]。信息隐藏技术必须满足不可感知性、稳健性和安全性等要求,即含有秘密信息的载体必须首先保证本身的质量没有发生明显变化,如语音的音效等。信息隐藏学科分为正反两方面:信息隐藏技术和信息隐藏分析技术。一个安全的在语音信号中进行信息隐藏的系统应该具备鲁棒性、不可检测性、透明性、安全性和自恢复性[2]。信息隐藏按嵌入域分类有:空域方法和变换域方法。空域方法具有实现简单,隐藏信息量较大等优点,但简单的信号处理技术均可导致嵌入信息的丢失。相比较而言,变换域方法抗干扰能力较好,不仅能使嵌入的信息能量分布到整个载体中,而且人的感知系统的某些掩蔽特性可以更方便地结合到编码过程中。

当前语音隐藏的主要方法有以下几种:1)最低有效位(LSB)方法。该方法可以隐藏较多的数据,但稳健性较差,无法抵抗音频数据处理所带来的破坏;2)相位编码法。该算法通过修改音频数据的傅里叶系数的相位值将数据隐藏到音频数据中;3)频谱变换法。该算法借鉴扩频通信的原理,将数据作为噪声隐藏到载体数据的频谱中,具有较高的健壮性;4)回声隐藏法。该算法通过改变语音回声的延迟来隐藏水印数据。此外,还有其他多种语音伪装算法,但可以看作以上算法的改进。

要想在 GSM 移动通信系统中使用语音信息隐藏技术,则要求语音信息隐藏算法具有抵抗 RPE-LTP 语音编码、噪声攻击等性能。由于 RPE-LTP 算法采用了脉冲激励线性预测的算法进行语音编码,对携密语音的波形进行了重构,因此现有的很多语音隐藏算法尤其是时域波形隐藏算法在经过 GSM 中的 RPE-LTP 编码解码后不能正确解码。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,本文设计一种能够在手机 GSM 语音编码芯片之前完成信息隐藏的算法,且该算法能够抵抗 GSM 中的 RPE-LTP 编码解码。

1 GSM 编码算法的研究

本文提出的能量比调整(ABS[3,4] Energy Ratio Adjust)算法利用 GSM 中的 RPE-LTP 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的特性来进行信息隐藏。同时采用了 ABS 技术,在隐藏算法中根据输入明文语音实时的调整相邻段能量比,使得隐藏效果和解码效果都达到最佳值。大量仿真试验结果表明,该算法能够抵抗 GSM 中的 RPE2LTP 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。

经过对大量语音信号的 RPE-LTP 编码前后特性分析研究发现,一段语音信号经过编解码后,能量改变的幅度不大。所以,可以利用相邻语音段能量比来进行信息隐藏。如果将相邻段能量比定位越大,越能保证正确解码但是隐藏效果越差。反之亦然。可以在隐藏算法中采用 ABS 技术,对每一段

收稿日期:2006 - 10 - 08;**修订日期**:2006 - 12 - 31 **基金项目**:黑龙江省教育厅科学技术研究资助项目(11511006)

作者简介:陈雪松(1972 -),女(蒙古族),黑龙江肇州人,副教授,博士,主要研究方向:信息安全、语音信息隐藏; 金七顺(1981 -),女(朝鲜族),黑龙江齐齐哈尔人,硕士,主要研究方向:语音信息隐藏; 杨永田(1939 -),男,山东莱州人,教授,博士生导师,主要研究方向:计算机网络及应用、分布式计算机系统、容错计算机系统.

输入的明文进行 RPE-LTP 预编码,分析出编码以后的大致能量比范围,然后实时的调整输入信号能量比。这样可以既获得好的隐藏效果,又能保证解码效果。

2 隐藏算法

具体实现流程如下:

1)将隐藏信息 S 用 Gray 码进行纠错交织编码,形成 $q$bit 的隐藏信息 X:

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

2)将明文语音 P 进行分段,设 P 为 M 个样点的公开语音,分段后表示为:

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

式(2)中,K 表示明文的总长度;L 表示每段样点数;$p(k)$ 表示第 k 段语音。要保证隐藏信息 X 能完全嵌入,必须满足 $q \leqslant L$。在本文 L 取 160。

3)将 p 分成前后 $\frac{L}{2}$ 段,分别计算其能量。

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

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

4)将 x_i 嵌入到 p 的具体过程:

(1)确定一个比较小的 α,文中选择为 1.1。

(2)计算前后 $\frac{L}{2}$ 段的放大增益:

$$\alpha_1 = \begin{cases} \alpha \times E_2/E_1, & x(i) = 1 \text{且} E_1/E_2 < \alpha \\ 1, & \text{其他} \end{cases} \tag{5}$$

$$\alpha_2 = \begin{cases} \alpha \times E_1/E_2, & x(i) = 1 \text{且} E_2/E_1 < \alpha \\ 1, & \text{其他} \end{cases} \tag{6}$$

(3)根据 α_1, α_2 的值将 $x(i)$ 嵌入到明文 p 中:

$$p'(k \times L + j) = \begin{cases} p(k \times L + j) \times \alpha_1, & 0 \leqslant j < L/2 \\ p(k \times L + j) \times \alpha_2, & L/2 \leqslant j \leqslant L \end{cases} \tag{7}$$

将得到的明文 p' 进行编码,得到编码语音 p_c',再对 p_c' 进行解码得到 p_d'。

(4)如果 $x(i) = x(i)'$,则 p' 即为需要的携密语音;如果 $x(i) \neq x(i)'$,则提高 α 值,并转到(2)步。

由于透明性和鲁棒性是一对矛盾,嵌入深度 α 增加,鲁棒性随之提高,但势必导致携密语音 p' 质量的下降,因此这里的 α 值将依据 ABS 算法进行自适应调整。本文开始使 $\alpha = 1.1$。

3 信息提取算法

信息提取算法的流程框图如图 1 所示。

1)将携密明文语音 p' 进行分段,每段长为 L 个采样点,分段后表示为:

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

2)计算前后 $\frac{L}{2}$ 点能量:

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

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

3)进行判断,得出密文信息 X'。判断如下所示:

$$X'(i) = \begin{cases} 1, & E_1' > E_2' \\ 0, & E_2' \geqslant E_1' \end{cases} \tag{11}$$

将 X' 经过解纠错交织之后得到密文信息。

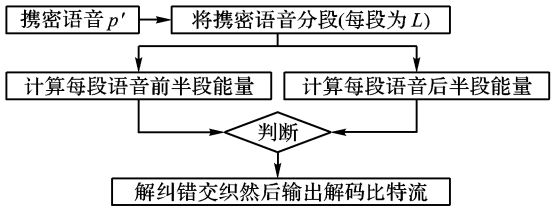
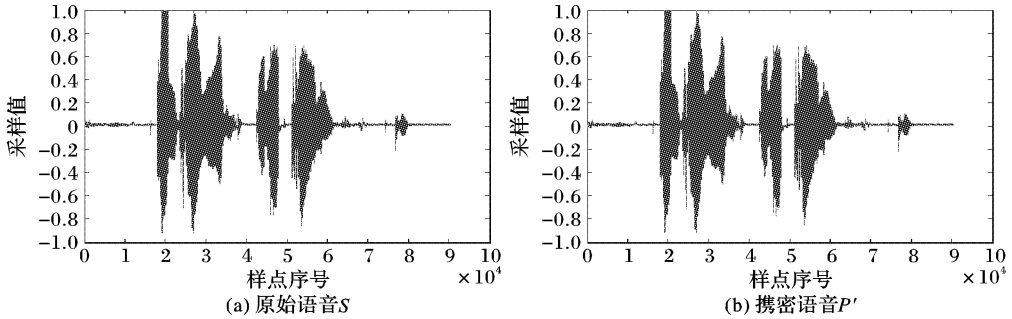


图 1 信息提取算法流程

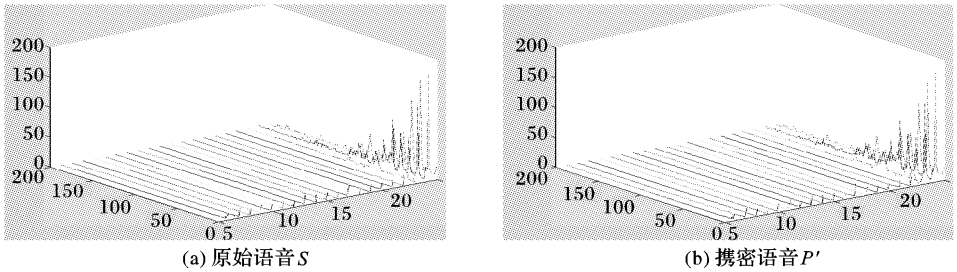
4 仿真分析

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 8kHz 采样,16bits 量化的语音,语音 S 共91 000 个样点。语音段长 L 为 160 个采样点,嵌入深度 α 初始值 1.1。分别在无攻击和多种攻击情况下分析本文算法的性能。



(a) 原始语音 S (b) 携密语音 P'

图 2 原始语音与携密语音之间的波形图



(a) 原始语音 S (b) 携密语音 P'

图 3 原始语音与携密语音之间的频谱图

(下转第 845 页)

计算完成后再进行比较,而算法 2 则是只需在第一张表完成的基础上即可开展比较工作。

3)求解成功时的条件和结果的计算公式。算法 1 求解成功时有 $\alpha^{mj} = y = \beta\alpha^{-i}, 0 \leqslant i,j \leqslant m-1$,结果为 $\log_\alpha\beta = (mj + i) \bmod n$。而算法 2 求解成功时则是 $\alpha^{mj} = y = \beta\alpha^{i}, 1 \leqslant i,j \leqslant m$,结果为 $\log_\alpha\beta = (mj - i) \bmod n$。

4)是否需要求解逆元。算法 1 需要求解逆元,而算法 2 则无需求解任何逆元。

5)表排序与查表时间。算法 1 需对两张表都排序,且查表时间与表的规模直接相关(为 $O(m)$)。而算法 2 由于引入抗冲突的哈希函数,无须排序操作,且查表时间也降为 $O(1)$。

表 1 列出了改进算法与原算法的性能区别。

表 1　改进算法与原算法的性能对比

比较项目	原算法	改进算法
预计算 α^m	采用平方乘算法	采用具有较小海明权重指数的多精度平方乘算法,运算速度提高约 11%
预计算 α^{-1}	采用扩展的 Euclidean 算法, $O(\log\alpha) \approx O(\log m)$ *	无
缓存	需存 α^m 和 α^{-1}	只需存 α^m
表 1 元素计算时间	m 次群乘法	相同
表 2 元素计算时间	m 次群乘法	平均$(m+1)/2$ 次群乘法 * *
表排序	两个表,每个表各 $O(m\log m)$	无
查表时间	$O(m)$	$O(1)$
需存贮的元素数目	$2m$	m

注:* $m = \lceil\sqrt{n}\rceil$,n 为元素 $\alpha \in G$ 的阶。

* * 当查找成功时所需的平均计算时间 $= \sum_{i=1}^{m} i \cdot \left(\frac{1}{m}\right) = \frac{m+1}{2}$ 次群乘法。

6　进一步的改进措施

改进后的小步—大步攻击算法较原算法而言进行了算法实现上的多项优化,但这仅是针对算法本身的优化,两种算法所面对的问题规模仍然是相同的。可以尝试通过降低问题的规模来进一步缩短攻击算法的计算过程。这一点对于比特位较长的素数 p 意义更加明显。

一个较易快速实现的措施就是对将要计算的 $\log_\alpha\beta$ 先进行奇偶筛选,这样可以将问题的规模降低约一半。该措施的有效性和奇偶筛选的实现方法由下面的命题 4 给出。其中 n,α,β 的意义同定义 1,且定义在模 p 的乘群 Z_p^* 上。

命题 4　若 $\beta^{n/2} = 1 \bmod p$,则 $\log_\alpha\beta$ 是偶数,否则是奇数。

证明　设 $x = \log_\alpha\beta \bmod n$,则 $\beta = \alpha^x \bmod p$。有 $(\alpha^{n/2})^2 = \alpha^n = 1 \bmod p$,则 $\alpha^{n/2} = \pm 1 \bmod p$。因 α 的阶为 n,有 $\alpha^{n/2} \neq 1 \bmod p$,故 $\alpha^{n/2} = -1 \bmod p$。从而 $\beta^{n/2} = \alpha^{x\cdot n/2} = (-1)^x \bmod p$。也即 $\beta^{n/2} = 1 \bmod p$ 时 $\log_\alpha\beta$ 是偶数,否则是奇数。

7　结语

本文将改进后的小步—大步攻击算法与原算法的性能进行了对比分析,表明上述改进措施均是正确而行之有效的。如何减少存贮开销,尽量避免或减少求逆元运算,如何有效应用多精度算法,以及通过变换指数表现形式来加速幂运算速度等,都值得在日益广泛应用的密码系统和签名方案的实现过程中加以充分考虑和探讨。

努力提高攻击算法的运算效率只是一个方面的工作,延伸到如何降低算法的输入规模将是一件非常有意义的工作。本文仅讨论了离散对数的奇偶筛选问题,如何预测或确定离散对数中的其他多个特定比特位的数值值得进一步的深入研究。

参考文献:

[1] ALFRED JM, PAUL CVO, SCOTT AV. Handbook of applied cryptography[M]. 胡磊, 王鹏, 译. 北京: 电子工业出版社, 2005. 99 - 101, 459 - 468, 527 - 532.

[2] DOUGLAS RS. Cryptography theory and practice. Second edition [M]. 冯登国, 译. 北京: 电子工业出版社, 2003. 193 - 227.

[3] JOHANNES B, DAMIAN W. Discrete logarithms: recent progress [A]. International Conference on Coding Theory, Cryptography and Related Areas[C]. Berlin: Springer-Verlag, 2000. 42 - 56.

[4] ANDREW O. Discrete logarithms: the past and the future[J]. Designs, Codes, and Cryptography, 2000, 19(2/3): 129 - 145.

[5] CHRIS S. The discrete log problem[D]. PhD. Thesis, University of Toronto, 2002. 7 - 9.

[6] WADE T, LAWRENCE CW. Introduction to cryptography with coding theory[M]. 邹红霞, 许鹏文, 李勇奇, 译. 北京: 人民邮电出版社, 2004. 121 - 122, 127 - 134.

[7] MUIR JA, STINSON DR. On The low hamming weight discrete logarithm problem for nonadjacent representations[J]. AAECC, 2006, 16(6): 461 - 472.

(上接第 842 页)

图 2 是语音信号隐藏秘密信息前后的波形图,图 3 是语音信号隐藏秘密信息前后的频谱图。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。在长度为 4.109s(样点总数约为 9.1×10^4)的语音数据中嵌入了 2964bit 的信息。从图中可以看出秘密信息嵌入后没有引起语音信号质量大的变化。

5　结语

本文基于一般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能量比调整(ABS Energy Ratio Adjust)算法。算法采用了 ABS 技术,在隐藏算法中根据输入明文语音实时的调整相邻段能量比,使得隐藏效果和解码效果都达到最佳值。大量仿真试验结果表明,算法对 GSM 中的 RPE2LTP 编码有很强的鲁棒性。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条件下信息安全传输、数字水印等领域。

参考文献:

[1] 陈力, 谢玉琼. 一种基于分形维数的自适应语音信息隐藏算法[J]. 武汉大学学报, 2003, 49(3): 313 - 317.

[2] 郑见灵, 谭月辉, 焦桂芝, 等. 音频文件中信息隐藏技术研究及其实现[J]. 河北工业科技, 2006, 23(2): 76 - 79.

[3] WU ZJ, YANG W, YANG YX. ABS-based speech information hiding approach[J]. Electronics Letters, 2003, 39(22): 1617 - 1619.

[4] 吴志军, 钮心忻, 杨义先, 等. 语音隐藏的研究及实现[J]. 通信学报, 2002, 23(8): 99 - 104.