第34卷 第13期 计 算 机 工 程 2008年7月
Vol.34 No.13 Computer Engineering July 2008
·安全技术· 文章编号：1000—3428(2008)13—0163—03 文献标识码：A 中图分类号：TP301.6

抗 RPE-LTP 压缩编码的语音加密算法

周世健[1,2]，齐宏飞[1]，蒋 睿[1]，杨晓辉[1]
(1. 东南大学信息安全研究中心，南京 210096；2. 中国人民解放军 73691 部队，南京 210014)

摘 要：针对 GSM 系统的安全机制不能实现端到端安全通信，提出一种能够穿透 RPE-LTP 压缩编码声码器的新型语音加密算法。该算法不会破坏语音特征，可以抗 RPE-LTP 压缩编码，实现在 GSM 语音通道中的端到端安全通信。选择算法参数的值取 20~25 时可以获得良好的加解密效果，取 20 时可以获得良好的时、频域失真度。

关键词：语音加密；GSM 系统；规则脉冲激励-长期预测压缩编码；端到端安全通信

Voice Encryption Algorithm of Anti-RPE-LTP Compress Coding

ZHOU Shi-jian[1,2], QI Hong-fei[1], JIANG Rui[1], YANG Xiao-hui[1]
(1. Research Center of Information Security, Southeast University, Nanjing 210096; 2. Unit 73691 of PLA, Nanjing 210014)

【Abstract】For the GSM security mechanisms can not achieve end-to-end secure communications, this paper presents a novel voice encryption algorithm, which can penetrate RPE-LTP coding Vocoder. The encryption algorithm does not destroy voice features, has anti-RPE-LTP coding features, and can realize the end-to-end secure communications in the GSM voice channel. It can receive good encryption effects when the algorithm parameter is among 20 and 25, and it can get good distortion on time domain and frequency domain when the parameter is 20.

【Key words】voice encryption; GSM system; RPE-LTP compress coding; end-to-end secure communications

1 概述

现有GSM系统安全机制[1-2]是在假设核心网络部分安全可信的前提下设计的，因此，只考虑了无线信道部分的安全，导致系统不能为用户提供端到端的安全通信。在一些特殊情况下常需要提供端到端的安全语音通信信道。为此，近年出现了一些实现端到端安全语音通信的新产品[3]，主要有德国GMSK公司的Cryptophone、以色列Snapshield公司制造的手机加密模块Snapcell、瑞典CRYPTOAG公司开发的GSM话音加密模块、挪威KONGSBERG公司研制的NSK200 安全电话等。以上产品均是通过对GSM网络数据通道进行加密和传输技术实现GSM语音端到端加密的。其优点是方式灵活、实现技术众多，但也存在着明显的局限性，比如，由于建立连接和运用自动重传机制导致延时过大；GSM数据通道在通过国际网络时存在互用性问题；不支持新的移动增值业务。相比之下，通过传统GSM网络语音通道加密的延迟较小，能与现有网络的各种业务很好地融合，有利于在现有用户中普及。但是这种加密语音技术也存在挑战，由于语音通道中存在采用规则脉冲激励-长期预测(Regular Pulse Excitation- Long Term Prediction, RPE-LTP)压缩编解码的声码器，因此常规的加密技术将失效。

本文根据 RPE-LTP 声码器的编解码原理，提出了一种抗 RPE-LTP 压缩编码的语音加密算法。

2 GSM 语音通信过程

GSM手机的语音通信流程[4]如图 1 所示。话音转化成电信号后，通过A/D变换为数字信号；然后经RPE-LTP编码，成为代表语音的 13 Kb/s的信息流；在进行交织和调制发射间，还必须通过加密模块完成无线信道的加密功能。在接收端进行相应模块的逆操作即可。GSM现有的安全机制主要由图 1 的加密模块部分和相应的鉴权、识别及认证机制共同 实现。

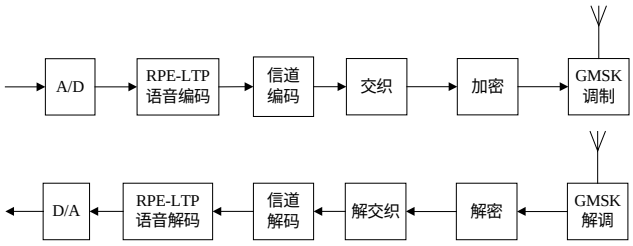


图 1 GSM 手机语音通信流程

3 RPE-LTP 语音编解码算法

RPE-LTP语音编解码[5-6]是语音编解码领域中一个重要的编解码标准，不仅是GSM语音通信，在因特网语音传输、多媒体通信中也得到了广泛的应用。

3.1 编码器原理

RPE-LTP语音编码器原理如图 2 所示。它包括预处理、LPC分析、短时分析滤波、长时预测和规则脉冲激励序列编码 5 个部分。其中，预处理采用 8 kHz采样率对输入模拟语音采样得到原始语音信号$s_0(n)$，去除$s_0(n)$中的直流分量后，采用一阶FIR滤波器进行高频预加重，得到信号$s(n)$。LPC分析将信号的每 160 个样点(20 ms)分为一帧，每帧计算出 8 个对数面积比参数$LAR(i)$, i=1,2,…,8。短时分析滤波产生短时LPC残差信号$d(n)$。利用长时预测对$d(n)$进行处理，进一步去

基金项目：江苏省自然科学基金资助项目(BK2006108)
作者简介：周世健(1979－)，男，硕士研究生，主研方向：信息安全；齐宏飞，硕士研究生；蒋 睿，讲师、博士；杨晓辉，副教授、博士
收稿日期：2007-08-24 **E-mail：**zhoushijian@sohu.com

除冗余，得出长时预测参数和长时残差信号。对经过短时、长时预测后得到的LPC信号进行加权滤波、规则脉冲序列提取和量化编码，得到每帧 260 bit的编码。

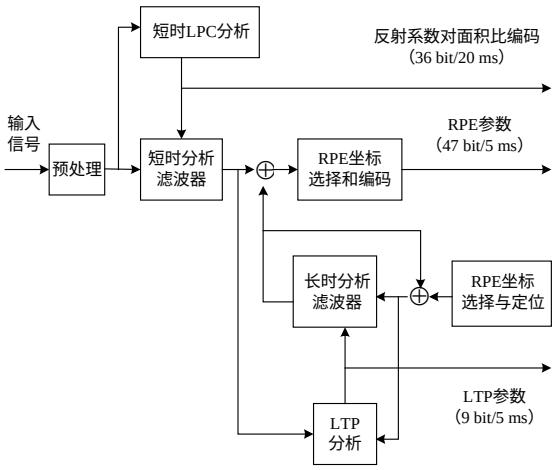


图 2　RPE-LTP 编码器简化框图

3.2　解码器原理

解码器的结构与编码部分的反馈环基本相同，如图 3 所示。用语音码重构短时残差信号，然后依次将其送到短时合成滤波器和去加重滤波器中，得到重构语音信号输出。

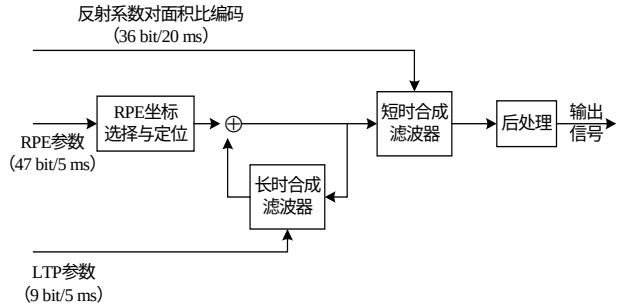


图 3　RPE-LTP 解码器简化框图

4　算法设计

4.1　算法原理

4.1.1　加密原理

令 M 为明文信息，k 为算法密钥，由 k 产生的加密矩阵为 $\boldsymbol{P}_k$，$\boldsymbol{Q}_k$ 为解密矩阵(即 $\boldsymbol{P}_k^{-1}$)，C 为密文，则有：

$$C = \boldsymbol{P}_k(M) \tag{1}$$

$$M = \boldsymbol{P}_k^{-1}(C) = \boldsymbol{Q}_k(C) \tag{2}$$

知道 C 和 k 后，密文接收端就能恢复出原来的明文，但必须满足 $\boldsymbol{P}_k$ 是单值的，即一个密钥 k 对应唯一的一对加解密矩阵 $\boldsymbol{P}_k$ 和 $\boldsymbol{Q}_k$。

4.1.2　加密矩阵评价标准

加密矩阵性能的优劣可由信息剩余可懂度 RI 来评价，其值越大，表示矩阵加密性能越差，反之，则矩阵加密性能越好。设测试所用的明文信息集合有 N 个元素，置换后不可懂的密文信息集合有 G 个元素，则剩余可懂度表示为

$$RI = \frac{N-G}{N} \times 100\% \tag{3}$$

但实际中只能以人耳判断是否可懂，显然这种判定方法主观性很强，难以准确客观地对剩余可懂度作判定。一般可以通过加密矩阵的平均位移、平均间距和最小间距来判定。

(1)平均位移定义为

$$AD = \frac{1}{m}\sum_{i=1}^{m}\left|i-\alpha(i)\right| \tag{4}$$

其中，m 为矩阵内参加置换元素的个数；i 和 $\alpha(i)$ 意义为：对于任意正整数 n，集合{0,1,2,⋯,n-1}的一个置换 α 是一个为每一个整数 $i(0 \le i \le n-1)$ 分配一个唯一的整数的变换，记为 $\alpha(i)$。

加密矩阵的平均位移是一个重要的因素，但是，仅一个大的平均位移还不能确保一个低的信息剩余可懂度，因此，需要引入最小间距和平均间距。

(2)平均间距定义为

$$\Delta h = \left|\alpha(i+1)-\alpha(i)\right|-1 \tag{5}$$

若某一个置换恰为两相邻元素的置换，则平均间距为最小间距，即 $\Delta h = 0$。因此，在平均间距较大的前提下，取相对较大的平均位移会获得一个较大的 RI 值。

4.2　算法描述

本文提出的加解密算法结合了语音信号处理和分组密码加密运算的特点，对 RPE-LTP 压缩编码具有很好的恢复性，其加密强度也可满足特殊需求。本算法针对 RPE-LTP 压缩编解码的特性，对人类的自然语音信号进行变换处理后对其加密，使之成为不可懂的声音信号，同时保证不可懂信号在通过 RPE-LTP 编码器后能被对端的解码器恢复，经解密就能成为原来的语音信号。

算法的主要思路为：在时域把原始语音分解为符合 RPE-LTP 编解码要求的单位帧，根据分组密码的原理，通过选择合适的加密矩阵对分解后的单位帧进行加密，使之成为不可懂语音信号，经 RPE-LTP 编码后送入 GSM 传输信道，在接收端进行逆向解密。

整个算法的流程如图 4 所示。

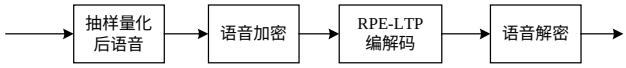


图 4　算法流程

在选择加密矩阵时，根据上文所讨论的加密矩阵原理，若要获得较好的加密效果需要选择较大的 Δh 值和 AD 值。其中，Δh 从根本上决定了加密矩阵的优劣。根据以上分析，可以获得好的加密矩阵。例如，当 n=15 时，Δh 最大为 5；当 n=30 时，Δh 最大为 7。此外，参数 Δt (即原始语音分解的单位帧长)的选择必须满足不破坏原始语音的语音特性，以确保加密后语音能穿透 RPE-LTP 编解码声码器。

5　仿真测试与结果

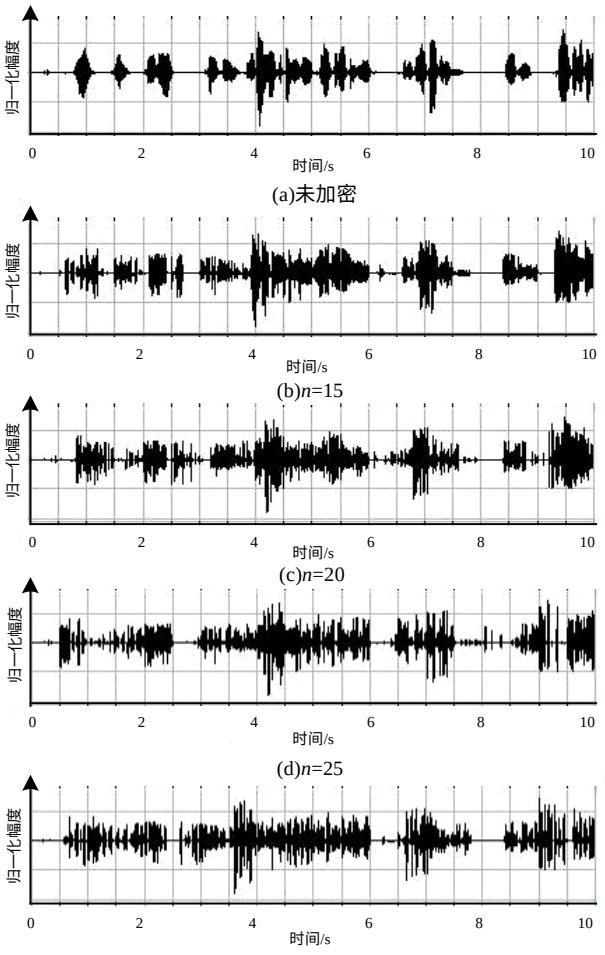
5.1　仿真环境

整个算法测试在 GSM RPE-LTP 声码器仿真平台上进行，平台采用 C 代码编写的声码器仿真程序 toast.exe。在此平台中，文件的输入必须是不包括文件前缀的纯语音码流文件，因此，在处理前需要将.WAV 文件转换为.SND 文件。整个观测平台采用 Systemview 软件。

5.2　仿真结果

5.2.1　不同分组 n 对加密性能的影响

根据算法原理，不同的分组 n 对算法性能有一定的影响：n 越大，算法的加密强度就越大。从图 5 中可以看出，选择 30 作为分组长度的效果比选择 15, 20 和 25 好。虽然理论上 n 的值越大，算法的性能就越好，但考虑整个加密系统的延时等因素，n 必须取一个合适的值。



(a)未加密　(b)n=15　(c)n=20　(d)n=25　(e)n=30

图 5　不同分组加密长度选择仿真波形

5.2.2　算法加密强度比较

本文的算法和其他几种常见的传统加密算法的加密强度比较如表 1 所示。从中可以看出，使用本文算法选取 n=30 时，加密强度最大，这与图 5 的结论相同。

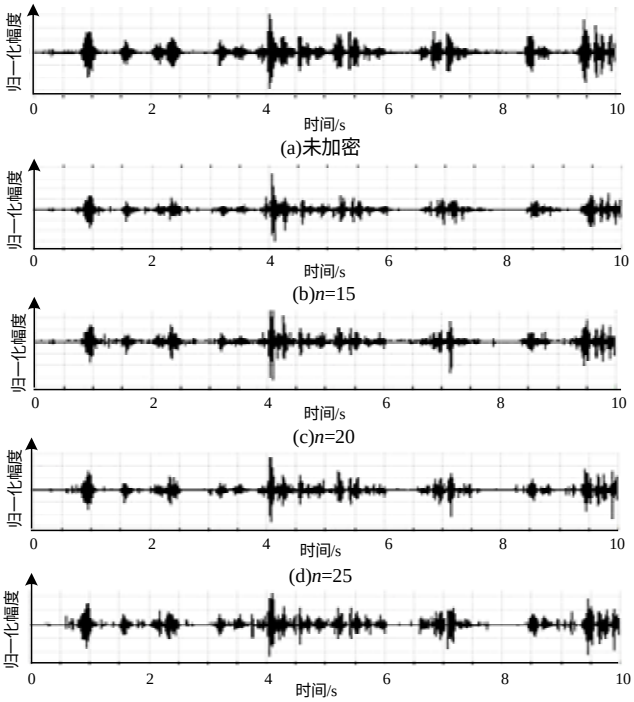
表 1　算法加密强度比较

算法名称		加密强度
DES		7.2×10^{16}
3DES		5×10^{33}
AES		3.4×10^{38}
本文算法	n=30	2.7×10^{32}
	n=25	1.6×10^{25}
	n=20	2.4×10^{18}
	n=15	1.3×10^{12}

由上文可知，算法性能和加密强度是一对矛盾的参数。通过大量仿真试验，分组长度 n 取 20 或 25 可以在这对参数间取得较好的平衡。

5.2.3　时、频域失真度评价

通过仿真发现，经过 GSM RPE-LTP 声码器的语音信号在时域和频域上本来就有一定程度的失真。本文仿真了不同参数的时、频域失真度，图 6 为不同分组 n 时域的失真对比。可以看出，经过本算法加解密的信号其失真度与未加解密的信号区别不大。



(a)未加密　(b)n=15　(c)n=20　(d)n=25　(e)n=30

图 6　时域失真度对比

表 2 是 n=20 时的频域失真度对比值。

表 2　时频域失真度对比值　(%)

测试参数	原始语音	正常 GSM 话音通信语音	使用本算法通过 GSM 仿真平台语音(n=20)
时域失真度	0.000	17.084	20.578
频域失真度	0.000	9.608	12.782

此外从实际的主观听觉感受表明，解密后的语音仅比原语音多了一些噪声，并不影响整体听觉效果。

6　结束语

本文针对现有 GSM 系统安全机制中未考虑端到端加密的缺陷，提出了一种可在传统语音通道中实现端到端安全通信的加密算法，用以解决传统加密算法因 RPE-LTP 压缩编解码而无法在 GSM 系统中运用的问题，具有很好的抗 RPE-LTP 压缩编解码特性。本算法已经利用 DSP 技术在现有 GSM 系统中得到实现，被证明具有很好的实用价值。

参考文献

[1] ETSI. GSM 02.09-1993 Security Aspects[S]. 1993.

[2] ETSI. GSM 03.20.EXT-1993 Security-related Network Functions[S]. 1993.

[3] 梁鸿斌, 曾　勇. GSM 系统中话音加密技术的研究[J]. 通信技术, 2003, (9): 101-103.

[4] Hellwig K, Vary P, Massaloux D, et al. Speech Codec for the European Mobile Radio System[C]//Proc. of IEEE Global Communications Conference. [S. l.]: IEEE Press, 1989: 1065-1069.

[5] ETSI GSM 06.10-1995 GSM Full Rate Speech Transcoding[S]. 1995.

[6] ETSI GSM 06.01-1992 Speech Processing Functions General Description[S]. 1992.