第32卷 第20期 计 算 机 工 程 2006年10月
Vol.32 № 20 Computer Engineering October 2006
·安全技术· 文章编号：1000—3428(2006)20—0153—02 文献标识码：A 中图分类号：TN 91

基于滤波带的非同步加密算法

曾 涯，周 东，罗 勇
(电子科技大学电子通信学院，成都 610054)

摘 要：给出了加密的一般模型，为了解决非同步语音加密的问题，用滤波带分析语音的分解和合成，对李善林提出的同步加密算法进行改进，在语音数据帧不引入冗余数据的情况下，实现非同步加密，相对于李的算法降低了运算开销，在同等条件下，一次性加密算法的时间开销只有原来的20%左右，同时恢复语音效果更好。

关键词：滤波带；加密；非同步；

Asynchronization Encryption Algorithm Based on Filter Banks

ZENG Ya, ZHOU Dong, LUO Yong
(School of Communication, University of Electronic Science and Technology of China, Chengdu 610054)

【Abstract】 The paper presents the general encryption approach. To address the synchronization problem of the voice communication, it uses the filter banks that can analysze and synthesize the voice. And it improves the algorithm proposed by Lee Shanlin. The approach not only reduces the computation cost but also deducts the redundancy data. Moreover, its effect is better than the algorithm proposed by Lee Shanlin as the result of software simulation.

【Key words】 Filter banks; Encryption; Asynchronization

现代通信技术在向大容量、高质量、高效能、高可靠性发展的同时，通信保密与保护信息安全传输尤为重要。相比于模拟加密，数字加密方式实现更简单，而且加密后效果保密性更强。但是，无线设备的数据接口终端，并不完全兼容；模拟－数字－模拟加密方式则适用于所有的无线终端。与数字语音加密方式相比较，模拟－数字－模拟的加密方式特别适合于无线语音通信；同时由于加密算法的开销较小，因此特别适用于实时多媒体通信处理。

李善林提出了一种非同步加密算法[1]，但是运算比较复杂，同时语音恢复的效果不是很理想。通过减少冗余数据，可以对同步算法进行改进，由于减少了对冗余数据多次重复加密的时间开销；在同等条件下，一次性加密算法的时间开销只有原来的20%左右，同时恢复语音效果更好。

1 加密模型

用数字信号处理的方法来实现模拟信号的非同步加密，原始语音信号采样的样本信号 $x(n)$经过映射 T 变换为 $y(n)$。

在讨论异步方法前，一个问题是传统的加密方法为什么一定需要同步。所有的数字信号处理的模拟加密方法，每 N 个样本定义一个分割片 $\overline{x}r$，用 N 个样本的窗 $w(n)$滤波

$$\bar{\mathbf{x}}_r=\begin{bmatrix} x(rN-N+1)\omega(n-1) \\ x(rN-N+2)\omega(n-2) \\ \dots \\ x(rN)\omega(0) \end{bmatrix}=\begin{bmatrix} x_r(0) \\ x_r(1) \\ \dots \\ x_r(n-1) \end{bmatrix} \tag{1}$$

r 是分割片的下标，向量 $\overline{x}r$，$\{\mathbf{x}_r(k),k=0,1,...,N-1\}$，窗函数 $w(n)$在 $n=0,1,2,...,N-1$之外全为 0。$\overline{x}r$ 经过矩阵 T 映射

$$\bar{\mathbf{y}}_r=T\ \bar{\mathbf{x}}_r \tag{2}$$

这里

$$\bar{\mathbf{y}}_r=\begin{bmatrix} y_r(0) \\ y_r(1) \\ \dots \\ y_r(n-1) \end{bmatrix} \tag{3}$$

向量y_r，$\{y_r(k),k=0,1,...,N-1\}$是加密后的语音数据分割片。所有模拟的数字信号加密方法的不同在于$w(n)$和T的选取。所有的加密过程和解密过程需要处理同一语音数据帧，才能得到原来的语音信号，并且实现同步处理。不同步，就是说加密过程和解密过程处理的帧数据不一样，这可能由延迟造成，这也就是需要同步的原因。

现在的问题是在失步的情况下，如何还原得到原始语音帧。一种解决方法就是扩展分割片的长度到 N'，邻接的分割片的数据部分重叠，一个条件就是 $N'>N$。通过引入冗余数据和压缩变换实现同步处理。但是，这种方法会增加计算的复杂度和成本，并且语音的效果不是很理想。下面的方法可以在不增加数据冗余的情况下，解决语音数据帧加密同步的问题。这可以通过滤波带的概念来分析解决这个问题。

2 滤波带

现在的问题就是选择合适的N样本窗函数$w(n)$和加密矩阵T保证加密同步过程，一种可能的解决方法就是用滤波带的方法[2]。滤波带的方法为语音信号的分解和复原提供了一种极佳的解决方案。

一个理想的滤波带有 N－1 理想带通滤波器，$H_k(e^{j\omega}),k=1,2,...,N-1$和一个低通滤波器$H_0(e^{j\omega})$，均匀分布

作者简介：曾 涯(1980－)，男，硕士生，主研方向：通信信号处理，光存储网络；周 东，副教授；罗 勇，硕士

收稿日期：2005-11-14 **E-mail：**ya.zeng@163.com

在整个频谱上，ω 分布在 0 到 2π。分割的滤波器不重叠。所有的滤波器形成一个宽大的全通滤波器。对于第 k 个滤波器，$H_k(e^{j\omega}), k=1,2,...,N-1$，中心在 $\omega_k=\left(\frac{2\pi}{N}\right)k$，带宽 $\frac{2\pi}{N}$，如果原始的语音数据用滤波带，可得到分割子带的频率分量。

$$Y_n(k)=[x(n)*h_k(n)]e^{-j\omega_k n} \tag{4}$$

$h_k(n)$ 是 $H_k(e^{j\omega})$ 的冲激响应，‘ * ’是卷积。由于 $Y_n(k)$ 是频带小于原来的语音信号，因此，可以用更低的采样率下采样得到 $Y_{rR}(k)$，只要满足条件 $R\le N$。这里 $r=1,2,...$。原始语音信号可以从 $Y_{rR}(k)$ 直接得到。首先，插值 $Y_{rR}(k)$ 得到原始序列 $Y_n(k)$，再把各分量相加就得到原始语音。

$$x(n)=\sum_{k=0}^{N-1}Y_n(k)e^{j\omega_k n} \tag{5}$$

式(4)是滤波带分解方程，式(5)是滤波带合成方程。Schafer，Rabiner和portnoff给出滤波带的一种算法实现[3,4]，主要过程如下：

$$Y_n(k)=\sum_{m=-\infty}^{\infty}x(n)h\,(n-m)e^{-j\left(\frac{2\pi}{N}\right)m} \tag{6}$$

$h(n)$是总的系统函数的冲激响应，长度为 N

$$h(n)=\frac{\sin\left(\frac{n\pi}{N}\right)}{\frac{n\pi}{N}} \tag{7}$$

$h(n)$长度为 N，因此，得到近似表达

$$Y_n(k)=\sum_{m=0}^{N-1}x(m)h(n-m)e^{-j(\frac{2\pi}{N}k)n} \tag{8}$$

$$x(n)=\sum_{k=0}^{N-1}Y_n(k)e^{j\left(\frac{2\pi}{N}k\right)n} \tag{9}$$

3 同步分析

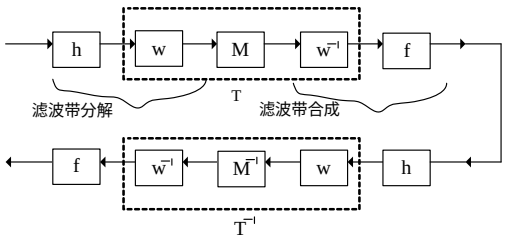


图 1 语音加密流程

图 1 示出了语音加密流程，其中 h 和 f 分别是滤波和插值滤波器，h 等于 f。w 和 w^{-1}分别是傅立叶变换矩阵和逆傅立叶变换矩阵。由于通过滤波带分析，可以实现语音信号的分解和复原，因此实现同步加密的关键问题就是，如何选取频率加密矩阵 M 和解密矩阵 M^{-1}，以及时域矩阵 T 和 T^{-1}最终满足什么条件。当系统完全同步，可以从 $Y_n(k)$ 中恢复得到 $x(n)$；但如果系统处于失步，即假设系统加密处理与解密处理是不同的语音帧。同步形式表示为 $\{Y_n(k),k=1,2,...,N-1\}$；失步形式表示为 $\{Y_{n+s}(k),k=1,2,...,N-1\}$，s 是时间滞后。由于在频域的采样频率一样，由采样理论可知，时间延迟引起的失步并不会改变 $Y_n(k)$ 的形式，因此可以恢复得到原始语音信号 $x(n)$。为了方便实现，降低运算开销，并减少有限长效应对语音信号的影响，而且看到图 1 中的加密过程可以合并为一个映射，加密频域矩阵和两个傅立叶变换矩阵组合到一起。

$$T=WMW^{-1} \tag{10}$$

通过选取合适的参数 T，同步可以不加考虑，从而实现非同步加密，并可省掉两次傅立叶变换的开销。T 需要满足的条件是一定要可逆。现在的问题是找是否存在这样的矩阵。在频域失步将引起相位失真，由于相位失真对声音的效果影响很小，因此可以不管延迟在频域产生的效果。

频率如果为实数，变换到时域就为复数。为了减少运算，并且避免相位失真在不同滤波子带传播。一种比较简单的方法就是选取均匀置换矩阵。一个矩阵满足下面的条件，就是均匀置换矩阵。

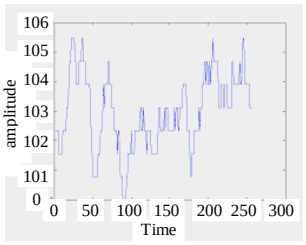
$$T_{\ell,m}=[t_{ij}]\ ,i,j=0,1,...,N-1 \tag{11}$$

$$t_{ij}=\begin{cases}1; & if\ \ j=((\ell\times i+m))_N\\ 0; & \text{其它}\end{cases} \tag{12}$$

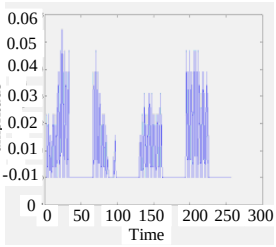
如果 T 为均匀置换矩阵，则 M 也是，反之一样。M 是均匀置换矩阵，T 也是。此外，并不是所有的都 T 可逆，因此需要选择合适的 ℓ，m，才能满足 T 可逆条件，如果不满足这个条件，将不能够恢复语音或恢复后失真会很大。到这里确定了参数 $W,W^{-1},M,M^{-1},T,T^{-1}$。

4 算法仿真

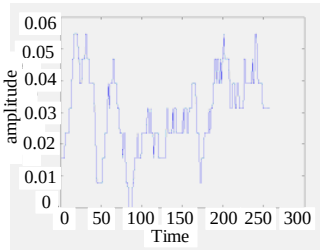
置换矩阵就是每一行，只有唯一的一个 1。这里选取置换矩阵的维数为 32×32，ℓ =7，m=6 进行模拟，加密矩阵 T 可逆。仿真的结果如图 2 所示。



(a) 原始语音



(b)加密后的语音



(c)16 样本点失步的解密语音

图 2 语音时域波形

图 2 的时域波形只是语音信号波形中的一部分。分别为原始语音，加密后语音和 16 样本点的失步解密后语音。对于时域对应的频域，图 2 中原始语音信号的频域和解密后的语音信号频域基本一致，加密后语音信号频域被置乱后，频谱的能量均匀分布（白化处理）。

为了说明本文算法加密的效率，对于同一数据块分别使用本文的算法加密和传统的数据加密算法 DES 进行加密，加密时间的比较结果如表 1 所示，从加密时间看，本文算法加密 4 轮的开销才与 DES 加密开销接近。

表 1 加密时间比较

算　法	DES	文中加密算法			
	一次	1 轮	2 轮	3 轮	4 轮
运行时间	0.203	0.04	0.12	0.21	0.30

5 结束语

通过分析讨论了滤波带在语音分解，合成的应用和语音加密原理，得到一种改进的语音同步加密方法，在相同的加密条件下，并不需要在语音帧中引入冗余的数据，减少加密过程运算的复杂度。

(下转第 162 页)