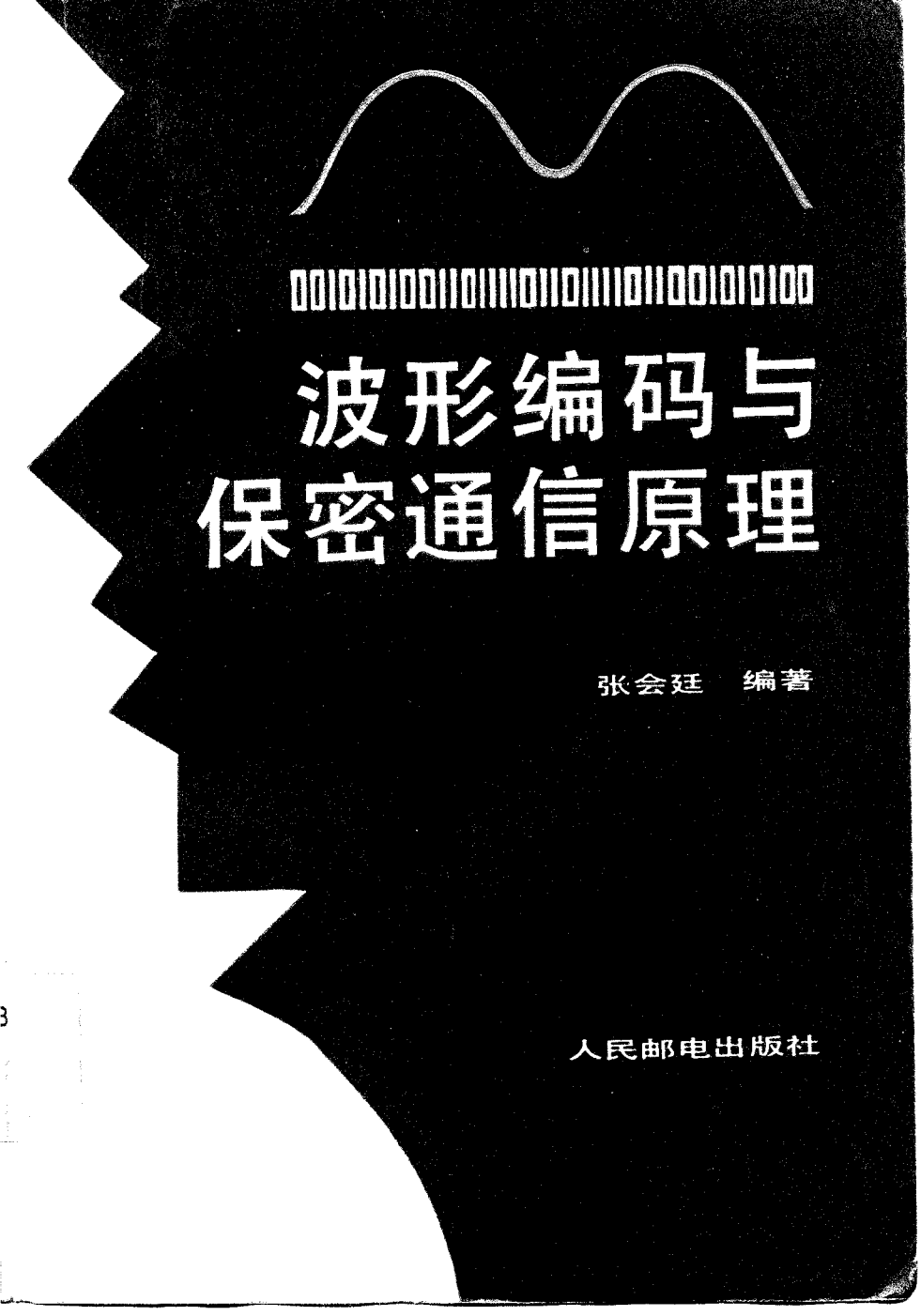

波形编码与保密通信原理

张会廷　编著

人民邮电出版社

内 容 提 要

本书讨论数字保密通信技术领域里的两个重要问题：一是如何把模拟信息高质量、高效率地变换为数字信号，这就是波形编码技术；二是如何使所传递的信息安全保密，不被第三者所窃取，这就是波形保密和密钥对抗技术。从第一章至第九章叙述波形编码的基本概念、特点，介绍各种脉码调制、增量调制和数字码变换的原理、方法，论证各种波形编码的质量指标。从第十章至第十四章介绍波形保密和密钥对抗的基本原理、方法，并叙述了电话、数据、图象数字保密通信网的一般知识。

本书可供从事通信专业的工程技术人员、教师、研究生和高年级学生参考。

波形编码与保密通信原理

张会廷 编著

人民邮电出版社出版

北京东长安街27号

轻工业出版社印刷厂印刷

新华书店北京发行所发行

各地新华书店经售

开本：787×1092 1/32　　1983年10月第一版

印张：12 4/32　页数：194　　1983年10月 北京第一次印刷

字数：265 千字　　印数：1—5,500册

统一书号：15045·总2757-无6247

定价：1.50 元

前　言

在现代通信领域里，发展数字通信系统和数字通信网，是近十多年来的重要方向。电话、图象等模拟信息的数字化传输，具有抗干扰性强、保密性好、利于实现数字时分交换网及进一步发展成为综合业务数字通信网等优点。如何把模拟信息高质量地变换成数字信号，是波形编码技术所要研究的课题。所谓“波形编码”就是对信息的电信号波形进行量化和编码、变成数字信号的过程。本书不仅较系统地叙述了各种脉码调制、增量调制的编码方法，还进一步介绍了第三种波形编码方法—数字码变换。这种新的编码方法一般是先对信息波形进行高速率增量调制，然后再对具有多余度的输出信码序列进行第二次数字编码，将传输所需的数据率压缩，以达到节约数字信号占用信道频带的目的。

本书讨论和比较了各种波形编码的主要质量指标—量化信噪比与抗干扰度。

有些信息要求在传递途中不被第三者所窃取。波形编码、数字保密技术可以很好地解决信息传输过程中的安全保密问题。本书从波形保密和密钥对抗的基本原理到数字加密的一般方法，从密码的基本数学结构到电话、数据、图象数字保密网的一般构成，作了初步介绍。

书中错误及不妥之处请读者指正。

目　录

第一章 概 述

第一节 波形编码通信基本原理

现代通信有模拟与数字通信两种基本方式。打普通电话或用电缆、微波、卫星传输多路载波电话及电视图象等，均属模拟通信；打电报、传数据、通数字电话及数字传真等，均属数字通信。信源产生的信号，也分模拟与数字两种形式，例如电话信号是对讲话声波的模拟；电视信号是对图象或活动景物的模拟。模拟信号的参数随时间而连续变化，其值可以有无限多个；数字信号是离散的脉冲序列，其参数值只有有限多个。例如用二进制脉冲序列$X(1, 0)$时，数字信号只有两个状态，一个状态（有脉冲）表示数字“1”，另一个状态（无脉冲）表示数字“0”。某些数字信号，例如数字电话和数字传真的信号，是为了利用数字信号的抗干扰性强和保密性好而从模拟信号变换来的。由模拟信号变换成数字信号的过程叫“编码”，也叫模—数变换。由数字信号变换为模拟信号的过程叫“解码”，也叫数—模变换。编码的方法分“波形编码”和“参数编码”两大类。本书要讨论的是前一类编码方法。

表示模拟信号的参数随时间而变化的状况的曲线叫做信号波形。例如图1-1就是声音“e”的模拟信号波形。所谓“波形编码”包括把模拟波形离散化及变成数字信号序列的全过程。要把连续的模拟信号离散化，需使它在时间和幅度上都

"量化"。常用的方法是对模拟信号进行等时间间隔的取样，来达到时间上的量化；再将幅度分为若干层，以与取样值最近一层的幅度值代替取样值，来达到幅度上的量化。设取样时间间隔为T_t，取样频率为$\frac{1}{T_t}$。当$\frac{1}{T_t}$大于或等于模拟信号最高频率的两倍时，用时间上离散的取样脉冲序列就可以完全无失真地表达模拟信号。这就是所谓的"取样定理"。但是，用量化取样值来代替原来的模拟取样值，总会引起量化失真。取样时间间隔和量化层间隔越小，量化失真也越小。将量化取样值或仅将其变化或跃变斜率换用二进制（或多进值）脉冲来表示，就达到了"波形编码"的目的。上述"量化"方法的示意图见图1-2。

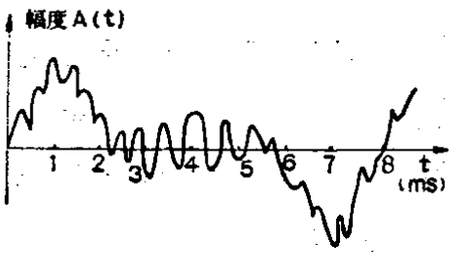

图 1-1　声音"e"的信号波形

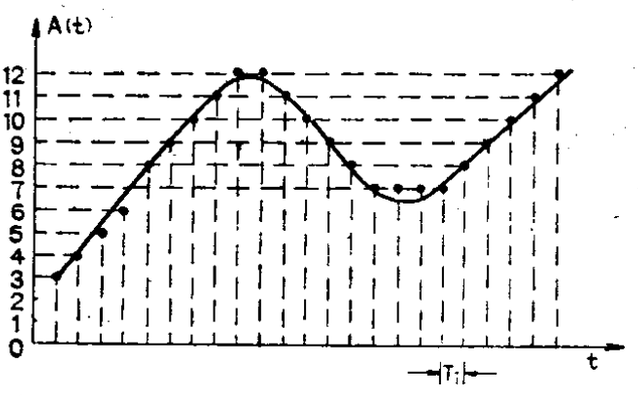

图 1-2　模拟信号在时间和幅度上的量化

现在以图 1-3 所示最简单的波形编码方法为例，来说明波形编码的意义。图中（a）画出了输入到编码器的模拟信号波形 $S(t)$ 和它的量化（幅度分为若干层）近似信号波形 $S(t)$；（b）是定时脉冲序列，其周期为 T_{DM}；（c）是编码器

输出的数字信码序列。在每一个定时脉冲的前沿（或后沿）将$S(t)$与$\hat{S}(t)$进行比较。若$S(t)>\hat{S}(t)$，则编码器输出一个正脉冲，即信码为"1"；若$S(t)\leqslant\hat{S}(t)$，则编码器不输出脉冲，即信码为"0"。当信码为"1"时，编码器中的本地解码器使$\hat{S}(t)$上升一个台阶电压Δu_0（即相邻两层幅度值之差）；当信码为"0"时，则使$\hat{S}(t)$下降一个台阶电压Δu_0。由图中(*a*)及(*c*)可见，信码序列最初一段依次出现9个"1"，$\hat{S}(t)$相应地依次上升9个台阶电压；其次一段连续出现7个"0"，$\hat{S}(t)$相应地连续下降7个台阶电压，这样，$\hat{S}(t)$跟随着$S(t)$的变化而上升或下降，就意味着用量化波形$\hat{S}(t)$代替了模拟波形$S(t)$；而$\hat{S}(t)$的上升与下降对应着"1"与"0"，这意味着把模拟信号$S(t)$变成了二进制（1，0）的数字信号序列。

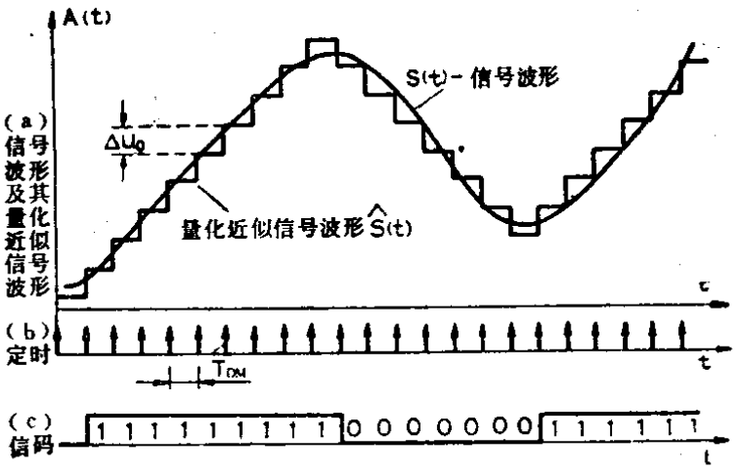

图 1-3　波形编码示意图

波形编码又叫数字化调制。其具体方法有：（一）增量调制（*Delta Modulation*，简称*DM*）及其发展型；（二）脉码调制（*Pulse Code Modulation*，简称*PCM*）及其发展

型；(三)上述两种编码再进行数码变换(*Code Conversion*)。这些方法将在第二、三、四章分别详细叙述。

波形编码数字通信基本原理方框图如图1-4所示，系由模

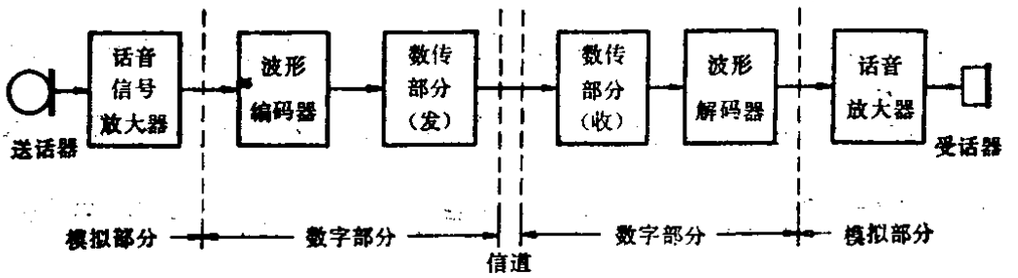

图 1-4　数字通信基本原理方框图

拟、数字、信道(线路)三部分组成。送受话器、话音放大器属于模拟部分；编码及解码器和数传收、发设备属于数字部分；信道就是传输数字信号的有线或无线通路。发端的任务是把话音模拟信号变成数字信号并发送给收端；收端的任务是将收到的、线路传来的数字信号再生解码，还原成话音信号输出。

第二节　波形编码数字通信的特点

波形编码是把模拟信号变换成数字信号来传输与交换，借以提高通信质量，达到通信保密目的的主要方法之一。波形编码数字通信的优点如下：

(一) 高抗干扰性。在模拟信号波形上迭加了干扰电压后，无法消除干扰的影响，所以模拟通信的抗干扰性不强。数字信号的情况就大不相同。例如在二进制脉冲信号上迭加了干扰电压后，虽说也会引起脉冲波形的失真，但只要干扰在允许范围内，就可以使数字信号“再生”，完全消除干扰的影响，所以数字通信的抗干扰性强。数字信号的“再生”原理如图1-5所示。设信码在传输过程中受到干扰，使收到

的波形（信码＋干扰）有失真。在与发定时同步的收定时点上，如果（信码＋干扰）电压大于判决门限电压，就再生“1”码；反之，则再生“0”码。若发送的是“1”码，而接收的（信码＋干扰）电压不低于门限电压，则不产生误码；若发送的是“0”码，接收的（信码＋干扰）电压不高于门限电压，也不产生误码。当干扰电压大到一定程度时，虽会产生误码，不过这时如果略为提高信号电压，就会使误码率很快下降。

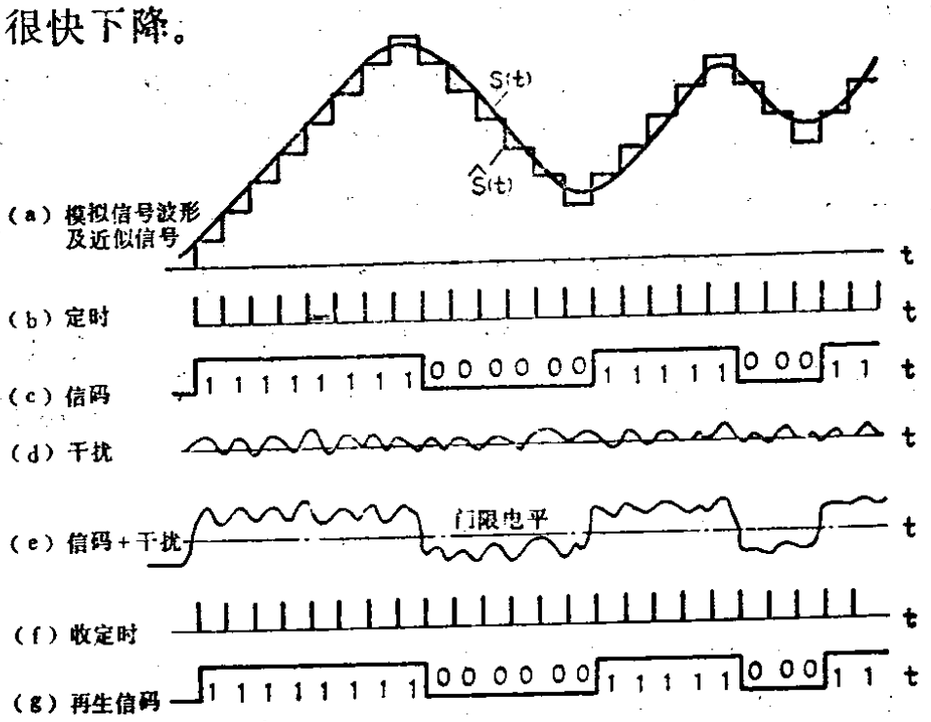

图 1-5　数字信号的再生

波形编码数字信号抗干扰性强有以下具体表现：（1）当接收机输入端信号与干扰电压之比超过一定门限值时，输出信号与干扰电压之比很高。例如用数字信号对高频载波进行振幅键控时，若收信机输入端信号与干扰电压之比在10分贝以上，则输出话音信号与干扰电压之比就可达60 分 贝 以 上（详细计算见第九章）。如果要使调幅模拟接收机的输 出 达到这样高的信号与干扰比，将需要提高接收机输入端信号与

干扰电压比(或者说提高发信机的功率)许多倍。(2)在有许多中继站的模拟通信线路上，各站上的杂音是积累的；而在数字通信线路上，由于各站上数字信号可以“再生”，从而基本上消除了杂音积累。例如有100个中继站的模拟通信线路，要达到两个终端站直通时接收机输出端的信号与噪声比，则需将信号的功率提高约100倍；而有100个再生中继站的数字通信线路，要达到两个终端站直通时接收的误码率(例如1×10^{-7})，则只需将信号功率提高一点几倍即可。

(二) 高保密性。由于对数字信号能够极其方便地加上高度保密的数字密码，故波形编码数字通信有高保密性。加密的一般原理如图1-6所示。令二进制数字信号序列为$X(1,0)$，数字密码产生器输出的二进制密码序列为$Y(1,0)$。$X(1,0)$与$Y(1,0)$在加密运算器内相加(模二加)，得出在线路上传输的密信码$Z(1,0)$。模二运算的规则是：

$$1\oplus1=0;\quad 0\oplus0=0;$$
$$1\oplus0=1;\quad 0\oplus1=1;$$

例如 $X(1,0)=1\ 1\ 1\ 0\ 0\ 1\ 0\ 0\ 0\ 1\ 1\cdots\cdots$

$Y(1,0)=0\ 1\ 0\ 1\ 1\ 1\ 0\ 1\ 1\ 0\ 0\cdots\cdots$

则 $Z(1,0)=1\ 0\ 1\ 1\ 1\ 0\ 0\ 1\ 1\ 1\ 1\cdots\cdots$

接收者知道密钥，也就是知道$Y(1,0)$，对加了密的信码$Z(1,0)$可用$Y(1,0)$去再和它作模二加，还原为$X(1,0)$，即

$Z(1,0)=1\ 0\ 1\ 1\ 1\ 0\ 0\ 1\ 1\ 1\ 1\cdots\cdots$

$Y(1,0)=0\ 1\ 0\ 1\ 1\ 1\ 0\ 1\ 1\ 0\ 0\cdots\cdots$

$Z(1,0)\oplus Y(1,0)=1\ 1\ 1\ 0\ 0\ 1\ 0\ 0\ 0\ 1\ 1\cdots\cdots$

$=X(1,0)$

再经解码即可得到原来信号波形。

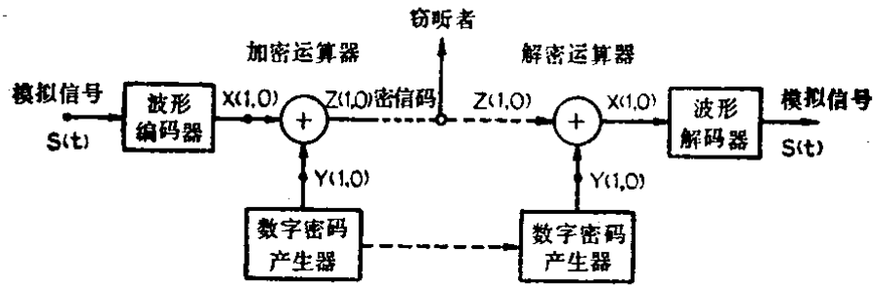

图 1-6　数字保密通信原理图

线路中间的窃密者不知$Y(1,0)$，所以不能解密。波形编码数字通信保密性能好的具体表现有以下几点：（1）可以实现全比特数字加密（每个比特都进行加密运算叫全比特加密），对信息加密量大。例如64千比/秒数字电话，传输每个音节约需 50 到 270 毫秒时间（按汉语统计值），实现全比特加密等于对每个音节进行了约 3.2 千到 1.7 万次可能的“破坏”，这对信号结构的“破坏”是非常彻底的。（2）发信息与否（讲话与否？有图象与否？），窃密者从窃收的密信码$Z(1,0)$中是无法区别的，只能听到或者看到一片白噪声或“雪花”。（3）在破译密码之前，窃密者也无法区别是何种信息（话、报、数据、图象），因为所有信息的数字信号都是1，0序列。（4）密码$Y(1,0)$序列的数目，即密钥量可以做得十分大，使得人工或用专门电子计算机破密都十分困难。

（三）其它优点。除了上述两个主要优点外，波形编码数字通信还有其它一些优点。例如：（1）通话质量和音量稳定。我们知道，普通模拟电话的音量与音质往往受到传输线路远近与衰减大小的影响；而波形编码电话，只要数字信号能再生，则通话质量与音量和传输线路远近及衰减大小无

关，总象在隔壁房间打电话一样清晰。（2）便于实现时分多路复用。随着中、大规模数字集成电路的发展，复用设备可以做得体积小，重量轻。（3）各种信息都数字化之后，便于存储、处理和交换，利于将来建立各种业务综合数字网。（4）能适应发展电子计算机通信网的需要。

另一方面，波形编码要产生量化失真或量化噪声。为使量化信噪比提高或量化失真减小，一般需要加多量化层数，因而需要提高波形编码的比特率，这样就会使信号频谱展宽。结果，一个模拟话路不足以通一路波形编码数字电话；一个模拟电视通路的频带，一般也不够通一路数字电视。本书将讨论不展宽或少展宽占用信道频带的高质量波形编码数字通信的理论。

第三节　波形编码与参数编码的比较

本节将对波形编码与参数编码作概略比较，借以进一步阐明波形编码技术的特点。

参数编码是对话音信号的生成模型参数，例如声道参数和激励参数（有声与无声），进行编码。在发端对模拟信号的信息参数进行分析，并将有用的信息参数编码送到对方；在收端再根据这些参数合成模拟信息。所以这实际是对模拟信号进行分析与合成的通信技术。早在三十年代，贝尔系统就开始研究话音编码器（*Voice Coder*）。当时研究的目的是为了节约使用信道频带。一般一个标准话路占用3100赫信道带宽。从信息论观点来看，频带这么宽的语言信号是含有

多余信息的。图1-7是实测的有声音的元音“ee”的信号线状频谱图。横坐标为频率，纵坐标为幅度。最邻近纵坐标的一条谱线代表声带颤动的频率，即基本频率；其余的谱线代表基本频率的谐频。图上的频谱线有很精细的结构、幅度不同的谐频相当丰富；虚线是频谱的包络。这两者是语言分析与合成的基础。频谱图上几处出现尖锐高峰，是由于整个声道存在谐振特性，而使能量在那里集中的缘故，称之为共振峰。在不发声的辅音里，线谱为零，且存在着噪声成分，故频谱是连续的。

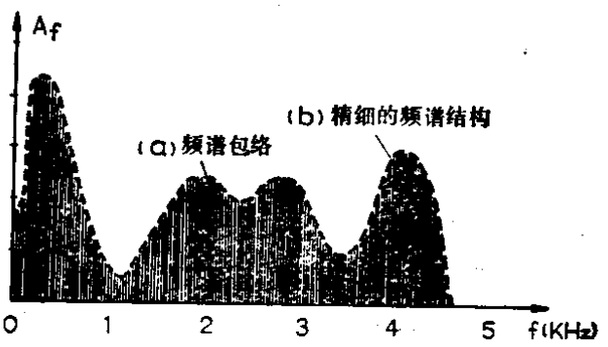

图 1-7　声音频谱图举例

人耳对语音信号的反映有三个基本特点：（1）能作短时间的频率分析；（2）对信号的相位不大灵敏；（3）对信号的周期性（音调）很灵敏。这些都是实现分析与合成通信技术的重要依据。

最早的话音分析-合成法使用频谱分路声码器（或称信道声码器）。它沿频率轴对频谱包络进行分段取样，频段取样数目在300—3400赫话音频带内为10到20段。分段越多，参数取得越精确，合成的话音质量越好。信道声码器的原理方框图如图1-8所示。从送话器来的话音信号接到几个支路，每个支路中有一个带通滤波器，其通带带宽从100赫到400赫不等。经过带通滤波器后的各部分信号，再经整流、低通，得到各频段频谱包络的幅度，用它们来反映整个频谱包络的形状。另有一个支路，专门提取话音信号的基波（代表音调）；还有一个支路，专门检测有声与无声。将这些频率很低、变