

五、结 论

文中所给出带声软障板的线列阵公式经实验证明是正确的,同时所采用的串、并联水听器实现幅度束控的简便方法是行之有效的,这为大型稀疏圆柱基阵垂直旁瓣的抑制提供了可行的理论依据。

参加本实验工作的主要人员有宋明凯、李先荣、宋兰英、刘崇仪等同志;宋明凯同志对本文做了审阅,并提出宝贵意见,在此一并表示感谢。

参 考 文 献

- [1] 耿成德,声学及电子工程,2(1989),7—10.
- [2] AD 764, 529, R.P. RADLINKI.

模拟置乱语音剩余可懂度的测试研究

张 知 易

(机电部第三十研究所)

1989年6月22日收到

对话音模拟保密通信而言,由于置乱技术的局限性和语音信号的多余度,至使置乱后的保密话音,仍具有一定程度的剩余可懂度。本文描述使用平衡数字串估价剩余可懂度的实验研究。结果表明,四位数字串集合是剩余可懂度测试估价的理想信息之一,而且采用加权校正计分公式 $RI_{dr} = \sum_{i=1}^4 W_i (IR_i - P_{i..})$ 来计算数字串剩余可懂度是可靠、实用的。

一、引 言

言语保密通信要同时完成传递信息和改变被传信号“面目”的任务。实践表明,对语音信号实施数字式加密 (Digitally enciphering) 和模拟置乱 (Analogically scrambling) 都可以达到这种目的。

数字式加密把信息码与密码逐比特“加密”,窃听者不可能通过直觉从加密后的信号中得到任何可懂的信息。他能听到的只是一片噪声。模拟置乱则不同。由于置乱技术复杂程度受到很大局限,以及语音信号本身的多余度,置乱后仍保留一定的“原始”信息,或具有一定的剩余可懂度 (Residual Intelligibility), 窃听者就有可能从保密信号中直接感知部分信息^[1-4]。虽然模拟置乱有这样的弱点,但它的简易和不要求宽带传输等优点使它仍具有较强的生命

力^[4]。模拟话密机的研制者还在竭力用增加技术复杂性的办法来提高保密度,例如 FFT 办法,但要做到完全消除剩余可懂度也不是轻而易举的事。

因此,以定量的办法判断模拟置乱方式的脆弱性或测定其保密度,从而对其使用范围和使用风险做出估价就很有必要了。定量判断的方法之一就是主观测试保密信号的“剩余可懂度”。

剩余可懂度 RI 的定义如下: 设测试所用的明文信息集合有 M 个元素, 测听后不可懂的密文信息集合有 C 个元素, 定义

$$RI = \frac{M - C}{M} \times 100\% \quad (1)$$

称 RI 为百分数剩余可懂度。在没有特别说明时,就叫它“剩余可懂度”。

用一般的可懂度测试法在这里将是不适用的。虽然曾有人谈到用声图来客观测量剩余可

懂度,但由于它要建立在多种客观条件和无异于模式识别那样的高难技术基础之上,而且结果并不令人满意,所以目前仍宜于用主观评价法。也就是在规定的明文信息集合的激励下,由一批经过必要训练的人员来倾听模拟话密机输出的声音,确认他听懂了的信息成份,再根据明密信息核对,统计得到剩余可懂度的估价^[1]。事实将证明,方法虽然是主观的,得到的结果却是反映客观实际的。

显然,剩余可懂度的测试结果与发音人、听音人、被测系统特征以及测试用的信息材料和规定的测听、估算方法有关^[2-3]。鉴于模拟置乱话密机对即使缺少多余度的数码也是很难发挥保密作用的,因此,我们选用十个数字的组合来做为测试的信息材料。

本文将报告几种典型模拟置乱密话用四位数字串估价剩余可懂度的研究结果,并对这些结果进行初步的分析和讨论。由于这一研究在国内还是刚刚开始,国外的现成资料不但很少,而且也不能直接搬来用于对汉语的测试,所以当前的研究结果是个探索性的试验结果。

本文所讨论的测试方法,其基本点是:主观统计测试;用小字库(十个数目字);用短语音(四个数字一组);合适的数字处理。测试对象主要是目前广泛使用着的模拟置乱器,对FFT这类新型变换置乱体制没有做针对性的研究。

二、测试材料的结构

由0,1……9十个数字构成的四位数数字串,广泛用于通信(如报文)和编码(如汉字编码)等场合。因此,选用50个四位字串做为测试材料,每十个一组,一共五组。每组中十个数字的出现率是均等的,即每个数字出现四次,而且随机出现在不同串的不同位置上。另外,两个数字的邻接(包括同一个数字的重复)机会也大致均等,最多两次,最少一次。而且,每一组中不出现两个数字同样邻接的情形。这种伪随机的字串结构,是为便于比较不同测试系统的保密性能而设计的,也为分析提供了方便。

十个数字按通信呼叫方式发音,0,1,2,7,9分别读做: *dòng*(0), *yāo*(1), *liàng*(2), *guǎi*(7), *gōu*(9) 其他读音照常。

三、实验及结果

1. 实验系统

本研究共对三类置乱体制的六种方式进行了剩余可懂度的估价测试。第一类体制是时间分段置乱(简称TSP)加倒频(一种方式);第二类是频带分段置乱(FSP)体制(两种方式);第三类是时间频率分段置乱(TFSP)体制(三种方式)。测试估价均在实验室内进行,从发端输出直接获取保密信号。

2. 实验方法

对每个被测系统,各使用两张发音表,它们是由前述集合中组号和字串序号都任意选择派生成的。每张表均由操标准普通话的男、女发音人发音。置乱采用有限个最佳密钥。每个字串的发音均连呼三遍。每次发音间隔(包括停顿)、男声约4秒,女声约3.5秒。为使测试接近实用保密通信情况,要求每次发音经历不同的密钥状态。

置乱话音经高保真度录音机录制后,再在评听室内由八名中学三年级以上的优秀学生用双耳机收听。他们听力正常,平常操普通话,在测试前经过几天试听明、密信号的训练。

回答采用完整记录的方式,即每听完一个四位数字串的三次读音后,写出这个串确认的每位数字来,即使难以确认,也要写出听到的最好猜测。

3. 计分方法与实验结果

用如下校正公式计算数字串剩余可懂度

$$RI_{di} = \sum_{i=1}^4 W_i(I_{Ri} - P_{ri}) \quad (2)$$

其中, $I_{Ri}(i=1,2,3,4)$ 分别是测试集合M中,记录字串的一位、两位、三位和四位正确答案,用式(1)求得的正确回答率, $P_{ri}(i=1,2,3,4)$ 是分别对一位、二位、三位、四位猜测回答正确的贡献,显然 $P_{r1}=0.1$, $P_{r2}=0.01$, $P_{r3}=$

$0.001, P_{i1} = 0.0001^{[1]}$ 。 $W_i (i = 1, 2, 3, 4)$ 是加权系数, 它是考虑各种数位正确接收的情况下, 猜对其余位对破译的贡献。显然 $W_1 = 0.001$, $W_2 = 0.01$, $W_3 = 0.1$, $W_4 = 1$ 。

根据实测数据, 用式(2)计算几种模拟置乱装置的 RI_{di} 值如表 1 所示。是分别平均男、女声发音得到的, 从上至下是按置乱技术复杂程度递增方式排列的。

表 1 典型模拟置乱装置数字串剩余可懂度

置乱装置	男声(%)	女声(%)	平均(%)
TSP + 倒频	29.6	26.8	28.2
FSP1	11.2	8.8	10.3
FSP2	5.90	5.5	5.7
TFSP1	1.47	0.91	1.12
TFSP2	0.91	0.66	0.79
TFSP3	0.57	0.08	0.32

四、讨 论

如前所述, 置乱语音存在剩余可懂度, 主要有两方面的基础。一是语音信号本身声学方面的特征, 二是实现置乱技术只能达到有限程度的复杂。宏观地看来, 语音信号是一个各态历

经性非平稳随机过程。但微观地看, 它却是一个准平稳的物理过程。长和短(时间域)或宽与窄(频率域)的分割, 都不足以改变语音信号的本来“面目”, 置乱后的时间波形及语谱图(见图 1)都还留下未变的痕迹(在 TSP 系统的语图中特别明显)^[1], 这些痕迹无疑是感知可懂信息的重要线索。也是窃密者进行非实时破译的着眼点。

从表 1 的结果看来, 女声的剩余可懂度得分普遍较男声低。一般说, 这不是置乱器固有的特征。可能的原因有三。第一个原因是男声速度比女声慢半秒左右(如前述)。发音速度慢, 意味着一个音的持续时间较长, 特征稳定的片段增多。对稳定片段的置乱效果是不好的, 特别是时间置乱, 几个稳定波形段的前后位置倒换不大能改变明话波形的实质。第二个原因是女声的基频高于男声, 在同样的分带带宽情况下, 女声落入的谐波数较少, 因而随着语音的变化, 其谐波“滑出”或“滑入”子带引起的变化就大一些, 可懂度受的影响也大, 剩余可懂度也降低。第三个原因, 女声发音能量一般低于男声, 即使在有电平指示的情况下, 也难以控制得和男声一样, 因此, 女声在置乱与测试系统中实

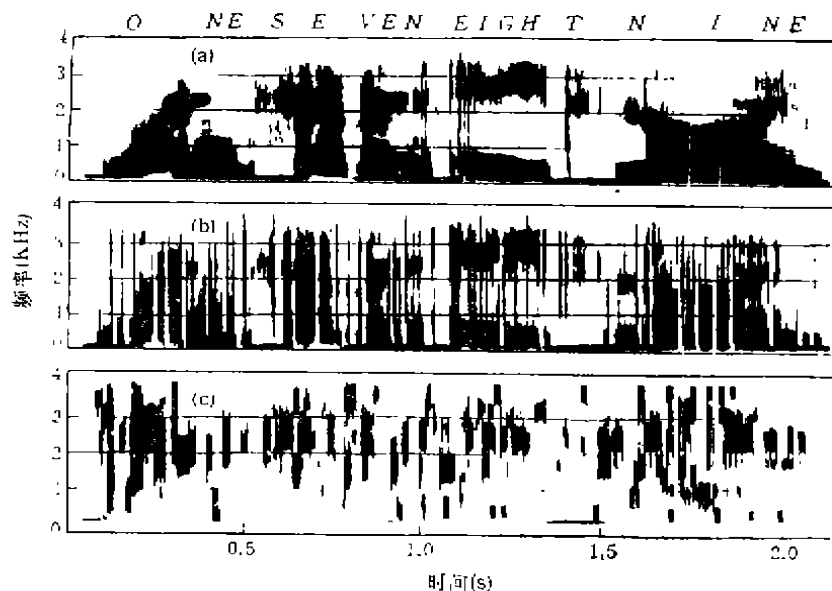


图 1 英语数字串“1789”的(a)原始语音, (b) TSP, (c) TFSP 系统的语图(见参考文献[1])

际的信噪比可能低于男声,可懂度和剩余可懂度均降低。初步试验表明,第一个原因是主要的。在用其他信息材料及男女声相同发音速度的实验研究中,这一现象就基本消除了。

对四位数字串语音,听者听辨的难度不是等同的。从分位核对的结果看,头尾两位数字较之中间两位容易听辨一些。这从表②给出的三个二维置乱装置按位统计所得的结果可以看到。

表 2 数字置乱信号按位统计的正确回答率

置乱装置	第一位	第二位	第三位	第四位
TSP	0.27	0.24	0.24	0.25
TFSP1	0.26	0.17	0.22	0.34
TFSP2	0.31	0.18	0.21	0.30

这些结果还告诉我们,剩余可懂度越低的装置,这一特性越明显。之所以如此,原因不难从分析发音的过程特征找到。对中间位置的数字,完全处于发音过程的连续状态,它们持续时间一般较头、尾位短,置乱段(时间或频率段)受上下文影响的概率较高,感知判断的难度也就增加。或许还有听音者的心理原因,他(她)们往往对头、尾音更加精力集中,而对中间两位读音注意不够。但如将这两位得分予以加权平均的话,可能在一定程度上代表了停顿较短的连续语言剩余可懂度的估价水平^[1]。

研究中还对每个数字的回答进行了表 3 所示的混淆矩阵的计算。对角线的结果表明,模拟置乱装置的可懂度,依赖于个别数字的特征。最明显的是数字“4”、“7”、“5”和“3”的发音,误识率普遍较低。这很可能是由于音调及能量信息起了重要的作用。我们知道,数字“4”的读音是由低能量的声母 *s* 和低能量的韵母 *i* 结合而成的,总的能量较其它数字发音的能量都低,自然很容易从置乱的字串发音中分辨出来。数字“3”的读音是由低能量、长持续的 *s* 和高能量、长持续的 *an* 音结合而成的。能量由低至高变化;持续时间较长,从而相同特征段相邻的机会(即不受上下文影响的概率)增多,也就比较易于使数字“3”和其它数字的读音区分开来了。至

于数字“5”和“7”的误识率最低,而且数字“2”的误识率也不高。这主要应归因于它们都是发音为第三声(“2”发音为 *liǎng*; “7”发音为 *guǎi*)的字,音调即降又升这一特征所包含的信息量可能比其他单音调的更多。在一个有限时间长度的置乱段内,其音调的这种非单调性没有造成彻底破坏时,灵敏的人耳一旦捕获到尚存的这一特征线索,并结合其他的线索,便必然较多地感知和区分出他们。

表 3 一种二维置乱器的数字混淆矩阵«男声»

		听 者 的 回 答									
置乱器输入		0	1	2	3	4	5	6	7	8	9
	0	0.12	0.04	0.11	0.03	0.21	0.09	0.18	0.13	0.05	0.03
	1	0.04	0.21	0.02	0.17	0.02	0.07	0.06	0.03	0.16	0.21
	2	0.02	0.02	0.21	0.01	0.01	0.34	0.04	0.33	0.01	0.03
	3	0.04	0.18	0.02	0.38	0.03	0.03	0.02	0.02	0.15	0.14
	4	0.05	0.01	0.12	0.02	0.39	0.10	0.12	0.11	0.06	0.02
	5	0.01	0.02	0.22	0.02	0.02	0.23	0.06	0.33	0.00	0.03
	6	0.09	0.03	0.14	0.03	0.18	0.14	0.23	0.09	0.06	0.02
	7	0.01	0.01	0.12	0.01	0.03	0.33	0.03	0.44	0.02	0.01
	8	0.04	0.16	0.03	0.18	0.06	0.05	0.04	0.04	0.16	0.25
	9	0.06	0.12	0.02	0.21	0.05	0.02	0.02	0.03	0.27	0.21

实验中发现,对所有测试装置和大多数测试队员来说,将一个数字混淆为另一个数字的现象几乎是不变的。而且这种混淆多发生在具有相同音调读音的数字之间。例如:第三声读音的数字“2”、“5”和“7”之间混淆最为严重;其次是第四声读音的数字“6”误识为“4”,第一声读音的“9”误识为“8”,“8”误识为“3”,以及它们之间的反方向混淆等等。但不同音调读音的数字间,特别是第三声和第一、四声的数字读音间却很少发生混淆。例如数字“5”和“8”、“0”之间;“7”和“0”、“1”、“9”之间,几乎不发生误识。这无疑应归功于它们之中的韵母包含较长时间的稳定发音过程;较大差异的频谱特征破坏未尽。残存的频谱特征还足以在它们之间做出区分。这也说明,听者在倾听置乱语音时,音调信息成了他们用于下判断的主要信息。而音调特征在模拟置乱处理中,也是最难“摧毁”的。

五、结 束 语

本研究结果告诉我们：首先，模拟置乱，特别是分段置乱，只能实现语音特征的宏观变化，微观地看并没有造成重大的变化，残存的音调、能量、频谱特征等还为辨识置乱信号中的有用信息提供了重要线索。其次，用十个数字组成的中小规模的字串集合来主观评价置乱装置的剩余可懂度，得到的结果是比较可靠和有效的。

实验证明，置乱技术的任何改进，都会灵敏地反映出数字串剩余可懂度的降低。

参 考 文 献

- [1] Jayant N. S. et al, *B. S. T. J.*, Part1, 62-1 (1983), 25—47.
- [2] Miller, G. A. G. A. Heise, and W. Lichten, *J. Exp. Psychol.* 41, (1951), 329—335.
- [3] 阿姆斯特塔 B. L. 著，“可靠性数学”，科学出版社 (1978)，3—41.

一种近似测量换能器效率及其等效电参数的简易方法

林书玉 张福成 周光平 钱建平

(陕西师范大学声学研究所) (七〇五所西安分部)

1989年4月1日收到

本文提出了一种近似测量换能器效率的简易方法。在换能器负载对其共振频率影响不大的情况，利用换能器的等效电路，根据换能器效率的定义，推出了只依赖于频率及谐振时换能器两端电压与电流之间相位角的效率表达式，把测量阻抗的要求变成了测量相位角的要求，与导纳圆法比较，所用仪器简单，测量迅速，克服了导纳圆法中逐点测量及逼近的麻烦，为迅速分析换能器的性能提供了一条简单的测量途径。

一、引 言

在分析换能器的性能时，换能器的等效电路是非常重要的，换能器的大部分性能参数都是根据等效电路中的概念定义的，并且换能器的许多分析及测量方法也都是由分析研究等效电路而得出的，例如导纳圆图法^[1]，M曲线法等。导纳圆图法是一种普遍采用的方法，它能给出换能器的绝大部分性能参数。但是导纳圆图法也存在一定的局限性。第一，所用仪器较复杂。第二，测试步骤较烦，需要测量换能器谐振频率附近许多频率点的导纳值，并且为了提高测量精度，所取频率间隔要小，同时每改变一

次频率均需重新平衡导纳电桥。第三，有时导纳圆并非规则的几何圆，从畸变的导纳圆中得到换能器的性能参数比较困难，且容易产生较大的误差。鉴于这些原因，目前在分析换能器的某一性能时我们已很少采用导纳圆方法。

本文提出了一种利用相位角的概念来测量换能器效率的方法，在一定的近似条件下，结合换能器低频电容的测量，可以获得换能器等效电路中的各个参数值及换能器的有关性能参数，方法简单，测量迅速，而且不需要很复杂的测量仪器。