

Algorithms of Radio Wiretapping Signal Modulations Recognition

CUI Can^{1,3}, LIU Zuoxue², KONG Deqiang^{1,4}, CUI Kai⁵

1. Company of Postgraduate Management, Institute of Command and Technology of Equipment, Peking, China

2. Department of Information Equipment, Institute of Command and Technology of Equipment, Peking, China

3. Unit 73687 of the PLA, Fuzhou, China

4. Unit 91404 of the PLA, Qinhuangdao, China

5. Department of Information Project, Jiangsu City Ocation College, Lianyungang, China

e-mail: dk217@126.com; lzx626@sohu.com kdq669@126.com; dk217@126.com

Abstract: This paper uses algorithms based on the characteristic parameters to identify AM, LSB, USB, FM, PSK, QPSK six common radio wiretapping signals. Considering the characteristics of wiretapping signals and the researches of A. K. Nandi, this paper improves the original parameters and proposes some new characteristic parameters when analyzing the instantaneous information. And computer simulation is applied to show that improved recognition algorithm needs less calculation and achieves better recognition effects.

Keywords: signal identification; modulation method; characteristic parameters; simulation

语音窃听信号调制识别算法研究

崔灿^{1,3}, 刘作学², 孔德强^{1,4}, 崔凯⁵

1. 装备指挥技术学院研究生管理大队, 北京, 中国, 101416

2. 装备指挥技术学院信息装备系, 北京, 中国, 101416

3. 中国人民解放军73687部队, 福州, 中国, 350101

4. 中国人民解放军91404部队, 秦皇岛, 中国, 066001

5. 江苏城市职业学院信息工程系, 连云港, 中国, 222000

e-mail: dk217@126.com; lzx626@sohu.com kdq669@126.com; dk217@126.com

【摘要】利用基于特征参数的算法对AM、LSB、USB、FM、PSK、QPSK六种常见窃听器信号进行识别, 结合窃听信号的特点, 归纳总结A.K.Nandi等人的研究成果, 在对调制信号的瞬时信息进行分析时, 对原有的参数做了改进, 并且提出了新的特征参数, 对改进的识别算法做了系统分析与仿真实现, 减小了计算量, 达到了较好的效果。

【关键词】信号识别; 调制方式; 特征参数; 仿真

1 引言

如何正确、有效地自动识别不同的调制样式, 在软件无线电、频谱监测、电子对抗、反窃听等方向有着广泛的应用。在反窃听设备中, 调制信号的识别对提升危险信号的等级有着重要的作用。本文利用基于特征参数的决策理论算法对AM、LSB、USB、FM、PSK、QPSK六种常见窃听器信号进行了识别, 针对窃听信号的特点归纳总结A.K.Nandi等人的研究成果, 对原有的参数做了改进, 提出了新的特征参数, 对改进的识别算法做了系统分析与仿真实现。

2 调制识别的算法与仿真

本文中接收机经射频处理后的中频信号为70MHz, 在计算复杂度允许的条件下, 尽可能提高中频信号带宽, 我们选用的带宽为10MHz, 采样频率选为25MHz, 在对10MHz的带宽内的信号分析后, 将感兴趣的信号分离出来, 将分离的信号经下变频后, 对其进行36倍的抽取后得到正交的I、Q路信号, 经过卡尔迪变换后得到信号的瞬时幅度信息 $a(n)$, 瞬时相位信息 $\phi(n)$, 在这里, 相位的主值区间取 $(-\pi \sim +\pi)$ 。在下面的分析和仿真中, 我们假定分析带宽内只有一个语音调制信号, 其他的干扰信号都已被滤去。

2.1 改进的谱对称性P

传统的特征参数P如下：

$$p = \frac{p_l - p_u}{p_l + p_u} \quad (1)$$

式中：

$$p_l = \sum_{i=1}^{f_{cn}} |s(i)| \quad p_u = \sum_{i=1}^{f_{cn}} |s(i + f_{cn} + 1)| \quad (2)$$

式中 $S(i) = FFT(s(n))$, $f_{cn} = (f_c N_s - 1) / f_s$ (f_c 为载频, f_s 为采样频率, N_s 为采样点数)。此时为带通采样信号, 这里的 f_c 取采样滤波后的中频5MHz。因为采样频率为25MHz, 假定我们采样点数取1000, 则对信号 $s(n)$ 做FFT的频率分辨率为 $\Delta f = f_s / N_s$, 即25KHz。因为音频信号主要分布在300Hz—3400Hz, 以此时的频率分辨率不能将信号区分开来。所以只有提高频率分辨率才能将信号识别, 采样频率系统已经确定, 不好改变; 提高傅立叶变换的点数, 会对算法的计算量有很大的影响。在这里我们采取对采样信号抽取的方法来提高频率分辨率的精度, 因为采样频率为25MHz, 所以可分析带宽为12.5MHz, 采样后中频为5MHz, 假定调制后的带宽不超过150KHz, 我们经过计算采用64倍抽取后满足我们的需要, 抽取相当于将可分析带宽分为64个相等的部分, 抽取前信号落在第26个区间, 抽取后相当于将其按区间翻转到第一个区间, 不会改变现有频谱特性, 此时 $f_c = 200$, 并且会使频率分辨率达到0.39KHz, 满足我们对语音信号识别的需要。抽取前后频谱仿真比较如图1所示:

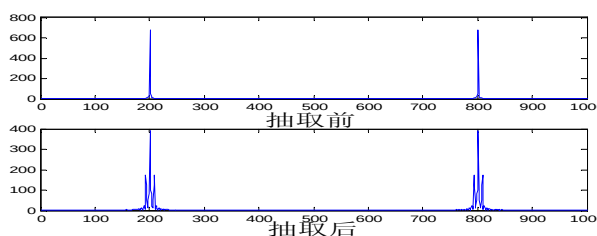


Figure 1. Spectrum before and after decimation
图1. 抽取前后的频谱

图2是在信噪比SNR为从0db到30db变化时六种信号的改进的谱对称性P值, 从图中可以经过改进后不仅能够减小运算量, 而且能有效的把AM、FM、PSK、QPSK信号与USB、LSB区分开来, 而P值自身的符号

可以将USB与LSB区分开来。

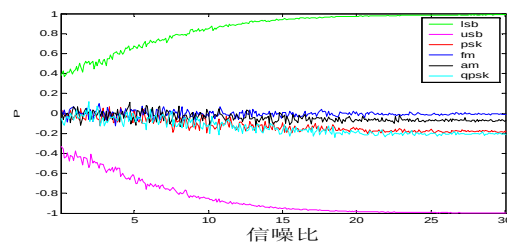


Figure 2. P of six signals
图2. 六种信号的P值

2.2 非弱信号瞬时相位绝对值差分的突变点个数 N_c

我们定义 $q(i)$:

$$q(i) = \|\varphi_o(i)_{(a_n(i) > a_t)} - \varphi_o(i-1)_{(a_n(i) > a_t)}\| \quad (3)$$

$q(i)$ 中的突变点的个数就定义为非弱信号瞬时相位绝对值差分突变点个数 N_c 。式中, $a_n(i)$ 归一化的瞬时幅度值, $a_n(i) = a(i) / m_a$, m_a 为瞬时幅度 $a(i)$ 的平均值, $m_a = \frac{1}{N_s} \sum_{i=1}^{N_s} a(i)$, a_t 是判断弱信号段的一个幅度判决门限电平, 取非弱信号段的信号进行处理主要是为了减小噪声的对判决结果的影响影响。 $\varphi_o(i)$ 为非弱信号的瞬时相位, 对 $\varphi_o(i)$ 取绝对值可以消除信号相位在主值区的边界来回跳变。

在实际中, 当I、Q路信号较弱时, 受到噪声的影响, 会影响到信号瞬时相位的判决。例如, 当I路信号为0.1, Q路信号也为0.1时, 此时信号的瞬时相位应该为第一象限的 $+\pi/4$, 因为此信号比较若弱, 在实际中该信号受到噪声的影响时, 此信号的I路Q路信号的值会有很大的变化, 以至于该信号的瞬时相位也有很大的变化。如图3所示, 该图是50个点的I、Q路均为0.1的信号通过信噪比为5dB的信道后所做的瞬时相位图, 如图所示, 受到噪声干扰的I、Q路所得到的相位可能分布在四个象限的任一个地方, 这种情况下的瞬时相位已经完全不能表示原来信号的相位, 为了解决噪声对弱信号的瞬时相位影响的问题, 我们选取一个非弱信号的判决门限, 将不能表示原信号瞬时相位的弱信号除去。

另外我们在利用I、Q路信号求瞬时相位时, 当所求的信号虽然满足非弱信号的要求, 但是此信号的瞬时相位在主值域的边界 (即 $+\pi$ 和 $-\pi$ 处) 附近时, 加上噪声的影响, 相位将在主值域的边界来回跳变, 出现所谓的乒乓现象。例如, 在没有噪声的情况下, 假

定其中一个采样点的I路信号为-1, Q路信号为0.0314, 则此时的这个采样点的瞬时相位为 0.99π , 但是由于在实际中必会受到噪声的影响, Q路信号可能会变为-0.0314, 则瞬时相位会变为 -0.99π 。显而易见这样会对利用瞬时相位进行识别的准确度带来影响。为此, 我们对信号的瞬时相位取绝对值, 这样, 四种信号的瞬时相位就不会出现在边界点的乒乓现象, AM、FM信号的瞬时相位的绝对值仍然是连续的, PSK信号的瞬时相位的绝对值在码元的值发生变化时也会发生变换, 而QPSK信号的 $+\pi/2$ 和 $-\pi/2$ 会成为 $+\pi/2$ 一个相位点, 所以QPSK的三种码元发生变化时相位会发生变化。取瞬时相位的绝对值后, 既能解决主值域的边界跳变问题, 又能较好的识别信号, 而且计算量小, 简单实用。弱信号以及边界点的跳变对瞬时相位的影响从PSK和QPSK中比较容易看出来, 图4是通过噪声没有经过处理的信号的瞬时相位与通过噪声

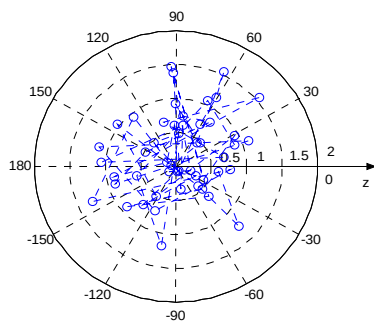


Figure 3. Phase of weak signals
图3. 弱信号的相位图

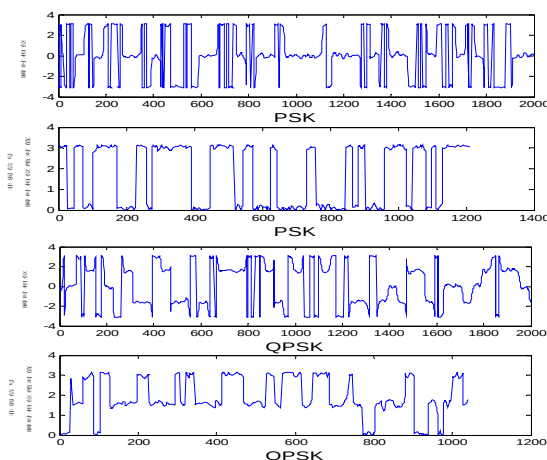


Figure 4. Effect of phase by noise
图4. 噪声对信号相位的影响

的非弱信号的瞬时相位的绝对值的比较, 此时信噪比

的值取10db。从图中可以看出对信号取非弱信号以及取瞬时相位的绝对值比较好的解决了噪声对瞬时相位的影响问题。

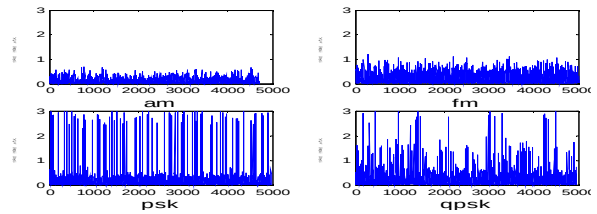


Figure 5. Break points of four signals
图5. 四种信号的突变点

图5为信号在信噪比为5db时的非弱信号瞬时相位绝对值仿真图, 在AM、FM调制时, 音频信号用matlab里的wavrecord录制的音频信号, 采样点数为Ns为360000个, 调频信号的频偏为8000。在QPSK、PSK调制时, 符号率Fd=10000符号/秒, 码元数目取250个。四种信号在抽取后取10000个点进行仿真, 对应的为瞬时相位绝对值差分突变点的仿真图。从仿真图中可以看出, 数字调相存在着明显的非弱信号瞬时相位绝对值差分突变点, 设置合适的门限即可对调相信号PSK、QPSK与AM、FM进行识别。

2.3 改进的零中心非弱信号段瞬时相位非线性分量绝对值的标准偏差 σ_{ap}

传统的零中心非弱信号段瞬时相位非线性分量绝对值的标准偏差 σ_{ap} 为

$$\sigma_{ap} = \left[\frac{1}{c} \left(\sum_{a_n(i) > a_t} \phi_{NL}^2(i) \right) - \left(\frac{1}{c} \sum_{a_n(i) > a_t} |\phi_{NL}(i)| \right)^2 \right]^{1/2} \quad (4)$$

式中, $a_n(i)$ 、 a_t 和在Nc中的意义一样, c是所有采样信号N(i)中经幅度判决门限电平 a_t 判决属于非弱信号的个数。 $\phi(i)$ 是各采样时刻瞬时相位的非线性分量。在载波完全同步时, 有 $\phi_{NL}(i) = \phi(i) - \phi_0$, 式中,

$$\phi_0 = \frac{1}{N_s} \sum_{i=1}^{N_s} \phi(i) \text{ 即瞬时相位的均值, } \phi(i) \text{ 是瞬时相位。}$$

因为PSK信号存在两种瞬时的相位0和 π , 两种瞬时相位的相位差 π , 当采样点足够多时, 0和 π 出现的概率可以看做是一样的, 则其均值为 $\phi = \pi/2$, 瞬时相位与均值的差值为 $\phi_{NL}(i) = \pm\pi/2$, 取绝对值后为 $\phi_{NL}(i) = \pi/2$ 将PSK的 $|\phi_{NL}(i)|$ 代入式(4)中, 因为

$|\phi_{NL}(i)|$ 只有一个值, 所以 $|\phi_{NL}(i)|$ 的标准差为零。而 QPSK 因瞬时相位有四个值, 所以瞬时相位非线性分量绝对值的标准偏差 σ_{ap} 不为零, 且大于零。

下面是我们对这个参数作出的一点改进: 从上一节的分析中我们知道 PSK、QPSK 信号在受到噪声影响时, 其瞬时相位会在主值域的边界来回跳变, 如果不解决这个问题, PSK 的 $\phi_{NL}(i)$ 值会有三种情况, 此时 PSK 信号的零中心非弱信号段瞬时相位非线性分量绝对值的标准偏差 σ_{ap} 就不会为 0, 与 QPSK 信号无法区分开来。为了解决这个问题, 在这里我们仍然是取瞬时相位的绝对值, 这样不仅能解决相位在边界点的跳变问题, 使两种信号区分开来, 而且此种算法计算量小, 容易实现, 只是做了绝对值运算。

下图是在信噪比 SNR 为从 0db 到 30db 变化时 PSK 与 QPSK 的改进的 σ_{ap} 值, 采样的点数为 2000 个点。从图中可以看出仿真结果与分析的结果大体一致, 因为在仿真时取的点数有限, 所以 PSK 的 $\phi_{NL}(i)$ 值与理论分析的结果有差异, 导致 PSK 的 σ_{ap} 没有为零, 但是却更接近于零, 选取合适的判决门限, σ_{ap} 值的大小可以将 PSK 与 QPSK 信号分开来。

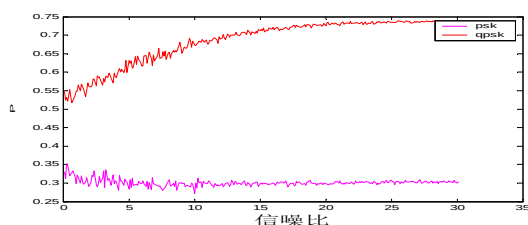


Figure 6. Standard deviation of two signals
图6. 两种信号的标准偏差

2.4 零中心归一化瞬时幅度谱密度的最大值 $\gamma_{\max}$

定义零中心归一化瞬时幅度谱密度的最大值 $\gamma_{\max}$:

$$\gamma_{\max} = \max \left| \text{fft}[a_{cn}(i)]^2 \right| / N_s \quad (5)$$

其中, N_s 为采样点数, $a_{cn}(i)$ 的意义和在 σ_{ap} 中的一样。下图是在信噪比 SNR 为从 0db 到 30db 变化时 FM 与 AM 的 $\gamma_{\max}$ 值, 从图中可以看出仿真结果与分析的结果一致, 选取合适的判决门限, $\gamma_{\max}$ 值的大小可以将 FM 与 AM 信号分开来。

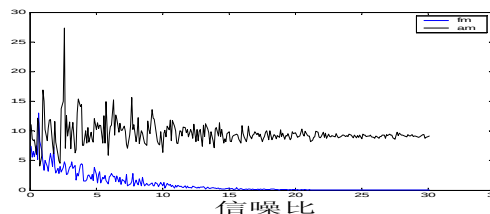


Figure 7. Maximum value of the spectral of two signals
图7. 两种信号的幅度谱密度最大值

2.5 分类识别

经过大量仿真, 设置最佳判决门限, 按照前面参数的顺序建立判决树识别, 依照前面的仿真参数进行 200 次的仿真, 得到在 7db 以上的识别率可以达到 99% 以上, 在 5-7db 之间识别率也可以达到 80% 以上, 证明了改进的算法不仅减小了运算量, 并且达到了较好的识别效果。

3 结束语

本文研究了音频窃听信号的识别算法, 针对语音窃听信号的特点对用于软件无线电识别的参数进行了改进, 并且解决了相位在主值边界跳变对判决影响的问题。本文得出的结论在反无线窃听等方面都将有广泛的应用前景。

致谢

论文是在我的导师刘作学教授的悉心指导下完成的, 孔德强和崔凯对论文的修改、绘图、排版做了大量细致的工作, 在此对他们付出的辛勤工作致以诚挚的谢意。最后, 我要把最诚挚的谢意献给我操劳一生的父母。

References (参考文献)

- [1] Fan Hai-bao Yang Zhi-jun Cao Zhi-gang. Signal modulations recognition of satellite communication[J]. Journal of communication, 2004, 25(1): 140-149.
范海波, 杨志俊, 曹志刚. 卫星通信常用调制方式的自动识别[J]. 通信学报, 2004, 25(1): 140-149.
- [2] SWAMI A, SADLER B M. Hierarchical digital modulation classification using cumulales[J]. IEEE Trans Commun, 2000, 48(3): 416-429.
- [3] Liang Hong, Ho K C. Identification of digital modulation types using the wavelet transform. Proc. IEEE.
- [4] Military Commun. Conf. MILCOM99, New Jersey, October 1999: 427-431.
- [5] Ketterer H, Jondral F, Costa A H. Classification of modulation modes using time-frequency methods. Proc. IEEE ICASSP-99, Phoenix, March 1999. vol. 5: 2471-2474.