

通信电台个体识别中的载波稳定度特征提取技术研究

张旻 王若冰 钟子发

(解放军电子工程学院 309 研究室 合肥 230037)

摘要: 由于电台频率稳定度较高,造成电台个体之间的频率波动特征差别较小,因此需要精确的频率稳定度提取技术,而目前常规信号频率提取方法获取的频率稳定度特征难以达到精度要求。该文重点研究了频率稳定度的有效提取技术,提出了3种有效的提取方法,在详细分析基本原理基础上,进行了仿真实验,比较精确地获取了载波频率稳定度信息,最后利用实际电台进行了验证,结果表明算法的有效性。

关键词: 频率稳定度; 细微特征; 特征提取; 个体识别

中图分类号: TN76

文献标识码: A

文章编号: 1009-5896(2008)10-2529-04

Study on the Techniques on Extracting Carrier Frequency Stability of Individual Communication Transmitter Identification

Zhang Min Wang Ruo-bing Zhong Zi-fa

(Division 309, Electronic Engineering Institute of PLA, Hefei 230037, China)

Abstract: Since the frequency stability of radio transmitter is high, the error of the carrier frequency is very small, and it is hard to obtain the individual stability difference using traditional approaches due to their low frequency extraction precision. In this paper, the stability of carrier frequency is used as the fine-grained characteristics of the individual communication transmitter based on the stability analysis. After that, the techniques of extracting frequency stability are well discussed, three approaches are put forward which can extract the fine-grained feature by some special processing the carrier signals. On the basis of analyzing principles of these methods, simulation and practical signals experiments are carried out, and the experimental results show that these approaches are effective.

Key words: Frequency stability; Fine-grained characteristics; Feature extraction; Individual identification

1 引言

通信电台识别的最终目的是实现通信电台的个体识别,也就是利用通信电台发射的无线电信号来区别通信电台。由于电台发射机的器件离散性和生产制造工艺过程不一致性,从原理上说每一部电台也会有能够唯一反映其个体属性的“指纹”特征,如果我们能从不同电台发射的信号中提取出反映该电台个体属性的“指纹”特征,就可以在截获的众多通信信号中快速地将每个信号对应的电台区分开来,实现通信信号个体属性的识别;电台个体识别在无线电安全通信、军事通信对抗和民用无线电监测等领域具有十分重要的意义,受到了国内外相关研究单位的关注^[1-4]。

电台个体识别关键在于提取电台的细微特征,作为电台的细微特征应能充分代表电台个体的特征,并具有可检测性,即电台指纹特征应能从有限观测数据检测出来。目前国内研究的指纹特征采用的都是暂态 turn-on 特征^[1-4],基于暂态 turn-on 特征的电台识别技术成功应用于阻止非法无线入侵等通信安全领域,而作为军事通信对抗和民用非法无

线电台检测时,由于是针对非合作方电台进行侦察和截获,无法获取暂态 turn-on 电台特征,因此需要寻找新的有效的细微特征进行电台个体识别。

短时电台频率稳定度特征可以作为电台个体有效的细微特征^[5],但由于电台个体的频率稳定度较高,传统的方法例如 FFT 变换,频谱分析、以及时频分析的方法都难以区分个体的频率稳定度特征^[1],因此利用载波稳定度进行电台识别在实际应用中还存在相当大的困难^[5],其原因在于无法有效提取出频率波动特征,本文研究了3种有效的方法提取载波的波动信息,克服了传统的瞬时频率提取方法无法满足识别精度要求的难题,为进一步的电台个体识别打下了基础。

2 载波稳定度特征的提取

尽管电台个体的频率稳定度不同,但它们之间的差别是比较小的,特别是相同型号的通信电台之间的载波频率稳定度之间差别更小,如何精确提取载波频率,达到能够识别电台目的成为解决问题的关键。本文重点研究了以下几种方法,从不同的角度来获取载波频率稳定度信息。

2.1 载波的包络伪调制法

通过对通信信号进行合理抽取,将频率波动信息转换到

伪调制的包络信息中,而包络特征易于提取,从而巧妙地回避了直接计算频率波动难以满足精度的难题。

对标准正弦信号抽样,在满足抽样定理条件的前提下,抽样频率处于某个范围时,无论抽样序列的包络还是抽样序列的周期性都与原始正弦信号比都发生变化,产生了不应有的调制,即伪调制,如图1所示。左图为一标准正弦信号,恒包络;右图为仿真对信号进行抽样,其包络发生了明显变化。原因在于抽样时很难保证每次正好能采到原始信号的峰值点,尤其当抽样频率在 $f_s \in (2f_0, 5f_0)$ 时,导致了伪调制的产生。如果通信信号频率稳定,即便是无法保证每次采样到峰值点,其伪调制的包络信号也具有一定的周期性,图2(a)所示是仿真接收机中频1.4MHz输出的载波经7MHz抽取后的信号包络波形,上层为无干扰的信号,下层为15dB信噪比信号处理的结果。然而如果载波频率发生了波动,则很难获取有规则的包络信号,如同样的载波信号中分别仿真加入一定的相位调制信息,使得载波发生波动,则抽取的信号包络发生了明显的变化,如图2(b)所示,上层无干扰,下层15dB信噪比信号。

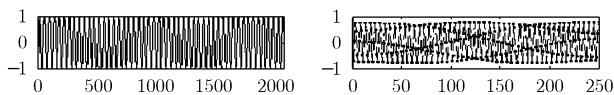


图1 载波的伪调制

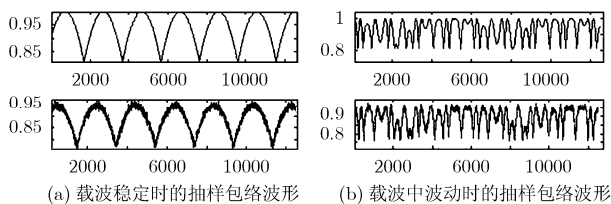


图2 载波抽样后的包络信号

通信电台正弦波振荡器输出的是调相波,使得接收到的信号在频率上发生了相应变化,信号波形会因频率的波动造成信号峰值位置不断波动,这时对该信号均匀抽样时,必然导致伪调制的包络产生。进一步的实验发现对不同电台的载波信号处理,能获取不同的伪调制包络波形,这是由于不同电台频率的波动不同而造成的,而且在电台稳定工作后同一部电台的包络变化基本是一致的,因此可以提取载波伪调制包络信息作为电台的细微特征。

通过采样将电台载波稳定度特征转变到伪调制信号的包络上,包络特征比较容易提取^[6],通过包络特征不同来区分电台稳定度的不同,进一步达到电台识别的目的。但该方法也存在明显的缺点,即对信号的信噪比要求较高,当信号较弱时,信号自身包络畸变较大,会对伪包络特征中包含频率变化的特征造成很大影响。

2.2 “零中频”法

众所周知,发射机振荡器实际的输出信号应该为一个调

幅调相波,其调相信息是机器自身的特性,包含在载波的波动的频率中,可以采用零中频方法提取相位波动信息,如图3所示。

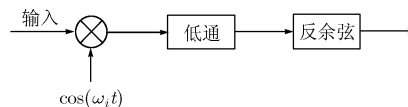


图3 零中频法

假设中频输出信号是 $s_i(t) = 2A(t)\cos(\omega_i t + \varphi(t))$ (1) 经 $\cos \omega_i t$ 混频后得

$$s'(k) = A(k)\cos(\varphi(k)) + A(k)\cos(2\omega_2 k + \varphi(k)) \quad (2)$$

低通滤波器消去高次谐波后获取信号

$$I(k) = A(k)\cos(\varphi(k)) \quad (3)$$

反余弦就能得到瞬时相位调制信息:

$$\varphi(k) = \arccos(I(k)/A(k)) \quad (4)$$

忽略电波传输的变化和接收机的影响, $\varphi(k)$ 就是发射电台的载波波动的相位信息。而实际中接收方只能估计信号的中频为 ω'_i ,即与实际的中频存在误差 $\Delta\omega = \omega_i - \omega'_i$,则混频后变成:

$$s'(k) = A(k)\cos(\Delta\omega + \varphi(k)) + A(k)\cos(2\omega_2 k + \Delta\omega + \varphi(k)) \quad (5)$$

低通滤波器消去高次谐波,得:

$$\begin{aligned} I(k) &= A(k)\cos(\Delta\omega + \varphi(k)) \\ &= A(k)\cos\Delta\omega\cos(\varphi(k)) - A(k)\sin\Delta\omega\sin(\varphi(k)) \quad (6) \end{aligned}$$

当 $\Delta\omega$ 很小,接近零时,由于 $\cos\Delta\omega \approx 1$, $\sin\Delta\omega \approx 0$,则式(6)仍然能近似表示为式(3),但当 $\Delta\omega$ 不接近为零,这时提取的 $\varphi(k)$ 信号在精度处理上会带来一定的影响,用式(4)计算瞬时相位调制信息就会产生一定误差,如图4所示。

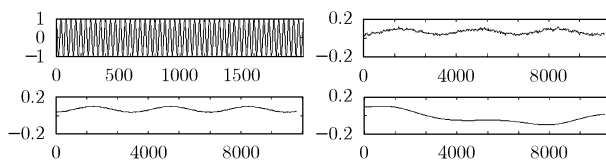


图4 零中频法提取相位波动信息

图4左边的上层是加了单音相位调制的载波波形,下层和右边的上、下层是提取的相位 $\varphi(k)$ 波动信息,左边的下层提取的是无噪声信号提取结果,右边的上层是15dB信噪比的信号提取结果,右边的下层是中频估计与实际存在误差时提取的相位信息结果。从图中可见,零中频方法要求中频频率要准确,如果存在误差,获取的相位特征发生了变化,对进一步识别带来不利影响。因此应用该方法时应能较准确地分析出信号的载波的中心频率。

2.3 多周期“过零点”检测法

如果能精确获取采样信号的零点位置,通过零点的位置分析获取信号的频率信息,从而进一步处理获取信号的频率

稳定度信息, 从而达到提取频率波动的目的。该方法的关键是精确计算出过零点的位置。

采用数学处理方法求取精确过零点位置的方法, 可以提高瞬时频率测量的分辨率。该方法的基本思想是基于正弦函数在零点附近有 $\sin x \approx x$ 的性质, 由此可以对过零的相邻两点建立一直线方程。

如图 5 所示。 $A(X_{m+1}, Y_{m+1})$ 、 $B(X_m, Y_m)$ 、 $C(X_{n+1}, Y_{n+1})$ 和 $D(X_n, Y_n)$ 是采样四点, X_i 和 X_{i+1} 是正弦函数两相邻过零点。可得 A 、 B 两点的直线方程为

$$\frac{Y - Y_m}{X - X_m} = \frac{Y_{m+1} - Y_m}{X_{m+1} - X_m} \tag{7}$$

因此, 精确过零点位置为

$$X = X_m - Y_m \frac{X_{m+1} - X_m}{Y_{m+1} - Y_m} \tag{8}$$

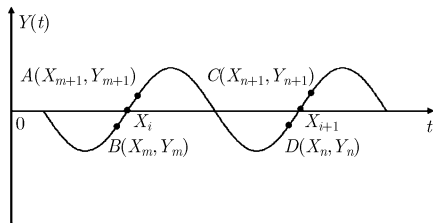


图 5 信号过零点分析图

通过计算相邻两个过零点的间距就能得出该段信号的频率值了, 如图 6 所示。图左边的上层是仿真加了单音相位调制的载波信号, 信号的载波频率为 1.4MHz, 相位波动为频率为 4.5kHz 的正弦信号, 使得载波频率在 1.3995MHz~1.4005MHz 之间波动; 图 6 左边的下层采用过零点法获取的信号频率序列, 准确提取了信号频率特征。

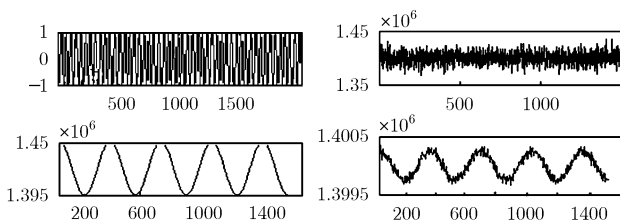


图 6 “过零点”检测法

然而该方法获取频率的精度受信号波形影响较大, 当存在干扰时, 接收信号发生一定的畸形, 直接影响频率精度, 如图 6 右边的上层所示, 它是采用过零点方法计算的结果(在左边的上层信号中加入了白噪声, 信噪比为 15dB 载波信号), 从结果上可以看出, 同左边的下层有很大的差异, 虽然频率在 1.4MHz 附近波动, 但无法处理出波动的单音波形来, 因此算法需要进一步提高精度。

单周期计算时, 误差来源于起始和结束点的零点位置, 假设两点的位置误差 ΔT_1 与 ΔT_2 , 则单个周期测量的最大误差为 $\Delta T = |\Delta T_1| + |\Delta T_2|$ 。如果 N 周期为一组计算, 则仍然

只存在起始和结束点的测量误差, 这使得最大的测量误差与单个周期的相比没有变化, 但单个周期分配到的误差为 $\Delta T / N$, 可见单个多周期过零点方法能减少测量误差 N 倍, 使得测量精度有较大的提高。

对于频率波动的载波信号, 其波动频率的周期远小于信号的载波频率, 采用多周期的过零点测量方法能获取比较精确的载波频率, 并将载波缓慢的波动特征准确提取出来, 如图 6 右边的下层就是采用 500 周期进行计算的结果(载波信号信噪比仍然为 15dB), 对于第 n 个零点的频率 $f(n)$ 采用下式来获得:

$$f(n) = f_s / [(x(n + 500) - x(n)) / 500] \quad (n = 1, 2, \dots, l - 500, \\ l \text{ 是采样点的长度})$$

这样就能获取噪声信号的过零点频率值, 其中包含了频率波动值, 基本与没有加噪的信号提取出的图 6 中左边的下层结果一致, 比原右边的上层信号有了很大的提高, 将频率波动信息基本提取了出来。可见采用多周期的分析方法获取的载波频率准确度有了极大的提高。

实际中由晶体产生的载波信号的波动频率远低于载波频率, 多周期“过零点”检测方法能精确提取信号的“准”瞬时频率, 而瞬时频率的变化能够反映出载波频率的波动特征, 因此是一种比较好的检测载波波动特征的方法。

3 实验与分析

3.1 仿真实验

本文仿真接收机中频 1.4MHz, 带宽 30kHz, 采样频率 7MHz, 5 种不同的相位波动的载波信号, 相位的波动频率在 1.5kHz~10kHz 之间, 造成的载波频率波动范围在 100Hz~3000Hz。每一类载波信号在 10~20dB 信噪比范围波动, 各产生 100 组仿真信号。

3.1.1 3 种方法分形特征提取的结果

(1)采用伪包络调制方法 采用载波伪包络调制方法, 提取包络信息后, 对包络波形提取盒维和信息维特征, 从每类中随机抽取 20 个共 100 个特征样本作出如图 7 的特征分布图。

(2)采用零中频的方法 采用零中频方法, 提取载波的相位调制特征后, 提取其盒维和信息维特征, 其特征分布如图 8 所示。

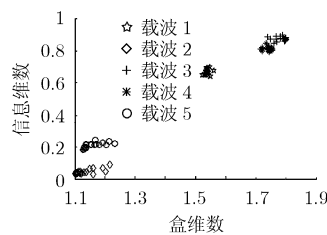


图 7 伪调制法提取载波包络特征分形分布图

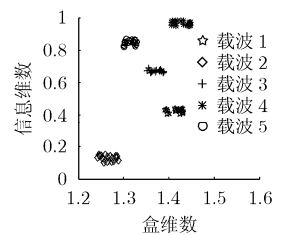


图 8 零中频法提取载波相位特征分形分布图

(3)采用多周期过零点方法 采用多周期过零点方法,直接获得载波频率波动信息后,提取其盒维和信息维特征,其特征分布如图9所示。

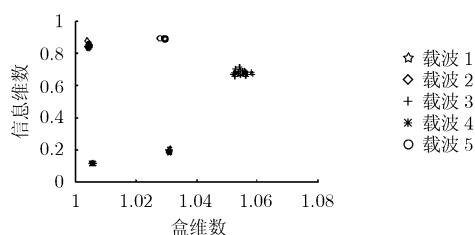


图9 过零点法提取的瞬时频率特征分形分布图

从图7-图9中可以看出,除有少部分相交外,各类的特征分界比较明显。3种方法都能有效地获取仿真信号载波波动信息。

3.1.2 表1是采用3-cross validation的验证方法得到的最近邻分类方法识别的正确率

表1 仿真信号分类识别率(%)

方法	载波1	载波2	载波3	载波4	载波5
伪包络	100	100	94.7	95.9	100
零中频	100	100	100	100	100
过零点	100	100	100	100	100

3.2 实际通信电台实验

选择了3种型号的5部超短波通信电台(分别为900-1, 900-2, 121-1, 121-2和500-1,其中900-1与900-2和121-1与121-2分别为同一厂家生产的同一型号电台)做实验,在相距800m处采用超短波接收机(频率稳定度在 10^{-8} 以上,高于发射机 10^{-6} 频率稳定度)接收,信号的信噪比在10dB以上,接收机的中频为1.4MHz,带宽为30kHz,采样频率为7MHz,共进行3天实验,每天每部电台发射20组信号。要求接收机和发射机都在开机半小时后进行实验,采用同仿真相同算法进行识别,识别结果如表2所示。

表2 5部实际电台产生载波分类识别率(%)

方法	900-1	900-2	121-1	121-2	500-1
伪包络	83.3	81.7	85.0	90.0	100
零中频	88.3	83.3	85.0	88.3	100
过零点	90.0	90.0	95.0	85.0	100

从表2中的数据可以得出结论:3种频率稳定度特征的提取方法基本都能达到对电台的正确识别,而进一步检查误判的结果发现主要是在同型号电台之间的误判,不同型号之

间的没有造成误判,这与同型号电台之间的频率稳定度特征差别较小而不同型号电台之间差别较大的结论是一致的。

4 结束语

尽管不同通信电台的短时频率稳定度有一定的差异,能够作为电台的细微特征,然而其中的差异较小,使得无法通过提取信号瞬时频率特征的方法来获取频率稳定度特征,因此本文重点研究了3种方法进行频率稳定度提取,从仿真的结果得出3种方法都能有效提取频率稳定度特征,理论分析和实际电台实验都表明多周期过零点检测方法比较适合载波波动特征检测,识别率最高;当然3种算法的优劣还需要做深入的研究,并通过实验进一步进行检验,得出更加准确的结论,在实际使用中可以扬长避短,甚至可以综合使用,使得算法能够更加精确的提取频率波动信息,达到对通信电台个体识别的要求,从而使得电台识别不只限于短时暂态turn on特征,为非合作方的电台个体识别打下基础。

参考文献

- [1] Ren Chunhui, Wei Ping, Lou Zhiyou, and Xiao Xianci. Individual communication transmitter identification based on multifractal analysis. *Journal of Electronics(China)*, 2005, 22(4): 409-415.
- [2] Ureten O and Serinken N. Bayesian detection of radio transmitter turn-on transients. *Proc. IEEE EURASIP Workshop Nonlinear Signal and Image Processing*, Antalya, Turkey, 1999: 830-834.
- [3] Jeyanthi Hall, Michel Barbeau, and Evangelos Kranakis. Detection of transient in radio frequency fingerprinting using signal phase. In *Wireless and Optical Communications*, ACTA Press, Banff, Alberta, Canada, July 2003: 13-18.
- [4] Hall J, Barbeau M, and Kranakis E. Enhancing intrusion detection in wireless networks using radio frequency fingerprinting. In *Proceedings of the 3rd IASTED International Conference on Communications, Internet and Information Technology (CIIT)*, St. Thomas, U.S. Virgin Islands, November 2004: 201-206.
- [5] 董晖, 姜秋喜. 基于多脉冲的雷达个体识别技术. *电子对抗*, 2006, (6): 12-18.
- [6] 张旻. 一种有效的瞬时包络特征提取方法研究. *电子工程学院学报*, 2004, 23(4): 12-17.

张旻: 男, 1966年生, 博士, 副教授, 从事通信信号处理、模式识别、计算智能等方向研究。

王若冰: 男, 1979年生, 硕士生, 从事通信信号分析与信息处理方向研究。

钟子发: 男, 1957年生, 教授, 博士生导师, 从事通信信号处理、数据融合等方向研究。