

一种新的 BOC(n, n) 型信号的精确捕获算法*

陈 适, 张天骐, 周 圣, 易 琛

(重庆邮电大学 信号与信息处理重庆市重点实验室, 重庆 400065)

摘 要: 针对 BOC(n, n) 型信号自相关函数存在三个峰值导致伪码捕获模糊性的问题, 提出了一种新的基于相关函数的精确无模糊的捕获算法。该算法将信号进行频域的多普勒补偿, 通过本地增设 QBOC(n, n) 支路, 利用 BOC(n, n) 信号自相关以及 BOC(n, n) 和 QBOC(n, n) 互相关, 经移位 $\pm T_c/4$ 、取模、求和、平方运算而实现。理论与仿真分析表明, 该算法在不改变自相关主峰宽度的情况下完全消除相关副峰的同时, 显著提高了主峰峰值; 比传统捕获算法的性能好 4.5 dB 左右, 并且捕获精度良好、易于实现。

关键词: BOC(n, n); 自相关; 多普勒补偿; 无模糊; 捕获

中图分类号: TP301.6; TP391.9

文献标志码: A

文章编号: 1001-3695(2013)03-0672-04

doi:10.3969/j.issn.1001-3695.2013.03.006

Novel unambiguous acquisition algorithm of BOC(n, n) signal

CHEN Shi, ZHANG Tian-qi, ZHOU Sheng, YI Chen

(Chongqing Key Laboratory of Signal & Information Processing, Chongqing University of Posts & Telecommunications, Chongqing 400065, China)

Abstract: For the problem of ambiguous acquisition of BOC signal caused by its auto-correlation had three peaks for BOC(n, n), this paper presented a new accurate method which was based on correlation function. Firstly, it made the receiving signal Doppler compensation in frequency domain, and implemented the new algorithm by adding a local quadratic BOC(n, n) signal and using the result of BOC(n, n) signal auto-correlation and BOC(n, n) and QBOC(n, n) cross-correlation, after shifting $\pm T_c/4$, modulus, summation, square. Theory and simulation results show that, the method does not only change the autocorrelation peak width, completely eliminate the related side peaks at the same time, and significantly improve the peak, increases the probability of detection about 4.5 dB than traditional acquisition algorithm, but also the precision of capture are very good and easy to implement.

Key words: BOC(n, n); auto-correlation function; Doppler frequency domain compensation; unambiguous; capture

0 引言

二进制偏移载波(BOC)调制是卫星导航领域中一种新型的信号调制方式,其基本思想是对 BPSK 基带信号使用一种类似于信源编码的处理方法,从而使得其频谱产生适当的偏移。产生方法就是通过在原有 BPSK 调制的基础上,再用一个二进制副载波对 BPSK 信号进行二次扩频,从而把 BPSK 信号的功率谱以载频为中心分裂成对称的两部分,这样在同频带传输的同时保持与传统直扩信号的主瓣能量不重叠,避开了对载频点功率谱的干扰,很好地解决了频谱共存的问题。BOC(1,1)调制信号目前已经被 GPS 的 L1C 和 Galileo 的 E2 + L1A + E1 所采用^[1],但由于副载波的影响,BOC 信号的自相关函数会存在多峰特性,容易导致信号在捕获和跟踪时出现模糊,从而产生误捕获或误跟踪,因此研究该信号的精确无模糊捕获算法具有重要的现实意义。

目前,研究者已提出了一些无模糊的捕获算法。文献[2]提出了 BPSK-like 算法,将副载波调制近似为正弦波调制,从而可以将 BOC 调制信号等效为两个载频不同的 BPSK 调制信

号之和,这样就消除了副载波调制造成的模糊性;但是这种方法并没有体现 BOC 调制捕获精度高、抗多径的优点。文献[3]提出了自相关副峰消除技术(auto-correlation side-peak cancellation technique, ASPECT),通过自相关函数平方与 BOC/PN 互相关函数平方之差达到消除副峰的目的;但是其单峰性不够理想,对副峰消除的不彻底。文献[4]提出了一种 filtered 相关算法,利用 BOC(1,1)信号自相关函数以及 BOC(1,1)信号和偏移的 PN 序列互相关函数之差作为捕获依据,得到的新变量也大致上是单峰的;但是主副峰值比不够大。文献[5]提出了一种三路并行捕获算法,通过在本地增加超前、滞后 BOC(1,1)信号,在模糊位置处通过超前、滞后路消除模糊性,但是这种方法只适用于串行捕获,因此速度较慢。文献[6]提出了一种新的捕获结构,利用 BOC(1,1)信号和偏移的 PN 序列互相关函数通过组合运算,完全消除了副峰,但同时却减少了主峰峰值,并且增加了主瓣的宽度,造成捕获精度不高、性能不好。

本文研究了一种基于相关函数组合合成的处理方法,首先对接收到的信号进行 FFT 处理,并且通过循环移位达到频域内多普勒补偿的目的;然后通过 FFT 求得 BOC(1,1)自相关以及 BOC(1,1)和 QBOC(1,1)的互相关,对互相关结果进行移

收稿日期: 2012-06-25; **修回日期:** 2012-09-07 **基金项目:** 国家自然科学基金资助项目(61071196, 61102131); 国家教育部新世纪优秀人才支持计划项目(NCET-10-0927); 信号与信息处理重庆市市级重点实验室建设项目(CSTC2009CA2003); 重庆市杰出青年基金项目(CSTC2011jjjq40002); 重庆市自然科学基金资助项目(CSTC2009BB2287, CSTC2010BB2398, CSTC2010BB2409, CSTC2010BB2411)

作者简介: 陈适(1989-), 男, 湖南衡阳人, 硕士研究生, 主要研究方向为复杂扩频信号的捕获与跟踪(chenshi.21@163.com); 张天骐(1971-), 男, 四川眉山人, 教授, 博士(后), 主要研究方向为语音信号处理、通信信号的调制解调、盲处理等; 周圣(1986-), 男, 湖南衡阳人, 硕士研究生, 主要研究方向为低信噪比下 TDSCDMA 通信信号的检测与估计; 易琛(1984-), 男, 湖南岳阳人, 硕士研究生, 主要研究方向为抗干扰数字水印及其破解。

位 $\pm T_c/4$ 、取模、求和,再加上自相关结果,取平方得到新的组合相关函数形式。新的相关函数完全去除了副峰、提高了主峰峰值,并且可以维持主瓣的宽度与原BOC(1,1)信号自相关函数主瓣宽度一致。因此,该方法不仅可以提高检测性能,也能体现BOC信号在捕获精度方面的优势。

1 理论分析

1.1 BOC调制信号模型

接收的BOC(1,1)调制信号可以表示为

$$r(t) = Ad(t)c(t)SC(t)\cos((\omega_c + f_d)t + \varphi) + N(t) \quad (1)$$

其中: A 表示信号幅度; $d(t)$ 表示数据; $c(t)$ 表示扩频码; $SC(t)$ 表示副载波; ω_c 表示载波频率; f_d 是传输过程中产生的多普勒频偏; $N(t)$ 表示均值为零、方差为 σ_n^2 的加性高斯白噪声。接收机接内,经过下变频、采样之后可表示为

$$r(n) = Ad(n)c(n)SC(n)\cos(f_d n + \varphi) + N(n) \quad (2)$$

其中:扩频码速率等于副载波速率,即 $R_c = 1/T_c = R_s$ 。图1显示出了BOC(1,1)调制信号调制过程的时域波形,图2显示出了BOC(1,1)和相应BPSK信号的功率谱密度,图3显示出了BOC(1,1)和相应BPSK基带信号的自相关函数波形。

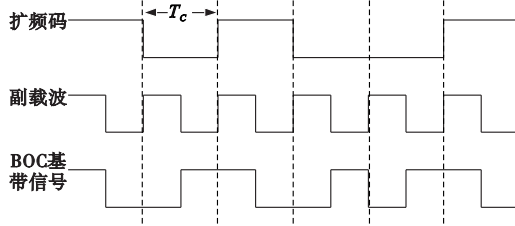


图1 BOC(1,1)调制的时域波形

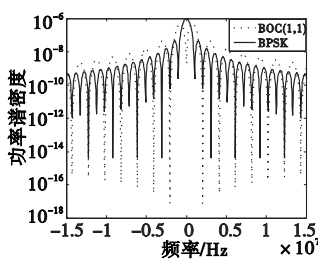


图2 BPSK、BOC(1,1)的功率谱密度

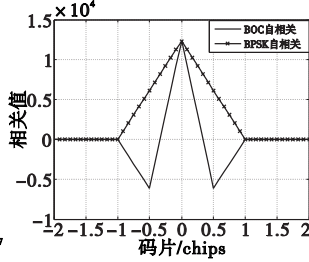


图3 BPSK、BOC(1,1)基带信号自相关函数

由图1可以看到,BOC(1,1)调制基带信号实际上就是每一个PN码片经过一个周期的副载波方波信号的调制。由图2可以看到,与BPSK直接调制信号频谱主瓣就在载频处不同,BOC(1,1)调制信号的频谱主瓣分裂到距离中心频率为 $\pm R_s$ 的两个频点上了。由图3可以看到,与BPSK基带信号自相关只有一个峰相比,BOC(1,1)自相关存在两个副峰,这说明捕获存在模糊性,但同时BOC(1,1)自相关函数的主瓣宽度明显小于BPSK基带信号自相关,这体现了BOC调制信号的捕获精度高的优点。

1.2 多普勒频偏补偿

在传统的捕获算法中,对多普勒频偏的搜索是在时域中按顺序完成的,也就是说,输入信号通过乘以覆盖整个频率不确定性的许多区段中的多普勒频率,随后,这每一个经过频率调节的输入信号与本地码序列进行相关匹配。但这种搜索方法太慢,因此可以进行频域的多普勒频率搜索。其基本原理就是时域复指数相乘等效于频域偏移。

$$f(t) \times e^{j2\pi f_d t} \Leftrightarrow \text{FFT}[f(f - f_d)] \quad (3)$$

对接收到的BOC调制信号的FFT结果进行不同程度的循

环移位,即可完成残余频偏的频域并行搜索。将FFT结果循环左移相当于信号在时域进行负的多普勒频偏补偿,反之循环右移相当于信号在时域进行正的频偏补偿。并且有频偏补偿精度定义:

$$f_{\text{prec}} = f_s/L \quad (4)$$

其中: f_s 为采样频率, L 为信号点数。

采用这种方法只需对接收信号进行一次FFT处理,然后通过不同程度的循环移位即可对整个频偏范围进行搜索。与常用的顺序搜索方法相比,该方法减少了计算量,且容易实现。

1.3 目前常用的合成捕获结构

在BOC(1,1)调制信号的同步方法研究中,提出了很多的无模糊合成捕获结构,针对不同捕获策略,其相应算法实现形式也不尽相同。ASPeCT实现策略是通过降低自相关函数的副峰来提高主副峰值比,降低模糊性。数学表达式为

$$Un = |x_{\text{BOC}}(\tau)|^2 - |x_{\text{BOC/PN}}(\tau)|^2 \quad (5)$$

其中: $x_{\text{BOC}}(\tau)$ 代表BOC自相关函数; $x_{\text{BOC/PN}}(\tau)$ 代表BOC与相应PN码的互相关函数。而对于BOC(1,1)有

$$x_{\text{BOC}}(\tau) = \text{tri}_0(\tau/l) - \frac{1}{2}\text{tri}_{1/2}(\tau/l) - \frac{1}{2}\text{tri}_{-1/2}(\tau/l) \quad (6)$$

$$x_{\text{BOC/PN}}(\tau) = \frac{1}{2}\text{tri}_{-1/2}(\tau/l) - \frac{1}{2}\text{tri}_{1/2}(\tau/l) \quad (7)$$

其中: $\text{tri}_\alpha(\tau/l)$ 表示自变量为 τ 、中心为 α 、底带宽度为 l 、峰值高度为1的三角形函数。将式(6)和(7)代入式(5)可得

$$\begin{aligned} Un &= |x_{\text{BOC}}(\tau)|^2 - |x_{\text{BOC/PN}}(\tau)|^2 = \\ &= (\text{tri}_0(\tau/l) + \frac{1}{2}\text{tri}_{-1/2}(\tau/l) + \frac{1}{2}\text{tri}_{1/2}(\tau/l))^2 - \\ &= (\frac{1}{2}\text{tri}_{-1/2}(\tau/l) + \frac{1}{2}\text{tri}_{1/2}(\tau/l))^2 = \end{aligned}$$

$$\begin{aligned} &= \text{tri}_0^2(\tau/l) \times (\text{tri}_0(\tau/l) + \text{tri}_{-1/2}(\tau/l) + \text{tri}_{1/2}(\tau/l)) = \\ &= \text{tri}_0^2(\tau/l) + \text{tri}_0(\tau/l) \times \text{tri}_{-1/2}(\tau/l) + \text{tri}_0(\tau/l) \times \text{tri}_{1/2}(\tau/l) \end{aligned} \quad (8)$$

显然,该算法主要利用了BOC/PN互相关峰与BOC自相关副峰在位置和峰值上接近,并且在自相关主峰位置,互相关值为零的特性构造而成。由式(8)结果可以看到,主峰峰值是不变的,而副峰则大致上被消除了。

Filtered相关法实现策略是通过提高主峰峰值来提高主副峰值比,降低模糊性。数学表达式为

$$\begin{aligned} \text{Fil} &= |x_{\text{BOC}}(\tau) - 0.5(x_{\text{BOC/PN}}(\tau + T_c/2) - \\ &= x_{\text{BOC/PN}}(\tau - T_c/2))|^2 \end{aligned} \quad (9)$$

其中: $x_{\text{BOC/PN}}(\tau + T_c/2)$ 和 $x_{\text{BOC/PN}}(\tau - T_c/2)$ 分别是本地超前/滞后PN码与BOC信号的互相关, T_c 代表PN码的码片宽度。由式(7)可得

$$x_{\text{BOC/PN}}(\tau - T_c/2) = \frac{1}{2}\text{tri}_{-1}(\tau/l) - \frac{1}{2}\text{tri}_0(\tau/l) \quad (10)$$

$$x_{\text{BOC/PN}}(\tau + T_c/2) = \frac{1}{2}\text{tri}_0(\tau/l) - \frac{1}{2}\text{tri}_1(\tau/l) \quad (11)$$

将式(10)和(11)代入式(9)可得

$$\begin{aligned} \text{Fil} &= |\frac{3}{2}\text{tri}_0(\tau/l) - \frac{1}{2}\text{tri}_{-1/2}(\tau/l) - \frac{1}{2}\text{tri}_{1/2}(\tau/l) - \\ &= \frac{1}{4}\text{tri}_{-1}(\tau/l) - \frac{1}{4}\text{tri}_1(\tau/l)|^2 \end{aligned} \quad (12)$$

该算法主要利用了码相关波形(code correlation waveform, CCRW)的思想^[7]获得。由式(12)结果可以看到,副峰峰值是不变的,并且增加了两个更小的副峰,而主峰峰值增加了50%。

文献[6]提出了一种新的捕获结构,实现策略是完全消除副峰来达到捕获无模糊性。数学表达式为

$$\begin{aligned} x_{\text{proposed}}^2 &= x_{\text{BOC/PN}}^2(\tau - T_c/2) + x_{\text{BOC/PN}}^2(\tau + T_c/2) - \\ &= (x_{\text{BOC/PN}}(\tau - T_c/2) + x_{\text{BOC/PN}}(\tau + T_c/2))^2 \end{aligned} \quad (13)$$

将式(10)和(11)代入式(13)可得

$$\begin{aligned} x^{\text{proposed}} = & \frac{1}{4}(tri_{-1}^2(\tau/l) + tri_0^2(\tau/l) - 2tri_0(\tau/l)tri_{-1}(\tau/l)) + \\ & \frac{1}{4}(tri_1^2(\tau/l) + tri_0^2(\tau/l) - 2tri_0(\tau/l)tri_1(\tau/l)) - \\ & (\frac{1}{2}tri_1(\tau/l) - \frac{1}{2}tri_{-1}(\tau/l))^2 = \\ & \frac{1}{2}tri_0^2(\tau/l) - \frac{1}{2}tri_0(\tau/l)tri_{-1}(\tau/l) - \\ & \frac{1}{2}tri_0(\tau/l)tri_1(\tau/l) - \frac{1}{2}tri_1(\tau/l)tri_{-1}(\tau/l) \end{aligned} \quad (14)$$

该算法同样借助了码相关波形的思想。由 $tri_a(\tau/l)$ 函数的性质可知, $tri_0(\tau/l)tri_{-1}(\tau/l)$ 、 $tri_0(\tau/l)tri_1(\tau/l)$ 、 $tri_1(\tau/l)tri_{-1}(\tau/l)$ 基本上都为零,于是提出的变量 $x^{\text{proposed}} \approx \frac{1}{2}tri_0^2(\tau/l)$, 可看到这是一个完全消除了副峰的相关函数,但与自相关函数主峰峰值为 $tri_0(\tau/l)$ 相比,主峰峰值减少了 $(2-\sqrt{2})/2$ 。

以上三种算法都具有一些局限性,ASPeCT 消除副峰不够彻底,且主峰峰值不变;Filtered 相关法提高了主峰峰值,但副峰峰值不变并增加了两个新的副峰;文献[6]提出的捕获结构可以完全消除副峰,但同时也减少了主峰峰值,并且由于利用的是 BOC/PN 互相关,使得主瓣的宽度与自相关相比也增加了。因此,希望提出一种新的捕获结构,在完全消除副峰的同时也能够增加主峰峰值,并且还能够保持自相关主瓣的宽度。

1.4 新的合成捕获结构

定义本地扩频码经偏移 $\pi/2$ 的方波调制的 BOC 信号为正交 BOC 信号,也就是 QBOC (quadratic BOC)。BOC(1,1) 和 QBOC(1,1) 的互相关函数^[8]为

$$\begin{aligned} x_{\text{BOC/QBOC}}(\tau) = & -\frac{3}{4}tri_{1/4}(\frac{\tau}{l}) + \frac{1}{4}tri_{3/4}(\frac{\tau}{l}) + \\ & \frac{3}{4}tri_{-1/4}(\frac{\tau}{l}) - \frac{1}{4}tri_{-3/4}(\frac{\tau}{l}) \end{aligned} \quad (15)$$

根据 CCRW 思想,提出一种新的捕获结构如下:

$$\begin{aligned} \hat{x}^{\text{proposed}} = & (x_{\text{BOC/PN}}(\tau) + |x_{\text{BOC/QBOC}}(\tau - T_c/4)| + \\ & |x_{\text{BOC/QBOC}}(\tau + T_c/4)| - \\ & |x_{\text{BOC/QBOC}}(\tau - T_c/4) + x_{\text{BOC/QBOC}}(\tau + T_c/4)|)^2 \end{aligned} \quad (16)$$

由式(15)可知:

$$\begin{aligned} x_{\text{BOC/QBOC}}(\tau + T_c/4) = & -\frac{3}{4}tri_{1/2}(\frac{\tau}{l}) + \frac{1}{4}tri_1(\frac{\tau}{l}) + \\ & \frac{3}{4}tri_0(\frac{\tau}{l}) - \frac{1}{4}tri_{-1/2}(\frac{\tau}{l}) \end{aligned} \quad (17)$$

$$\begin{aligned} x_{\text{BOC/QBOC}}(\tau - T_c/4) = & -\frac{3}{4}tri_0(\frac{\tau}{l}) + \frac{1}{4}tri_{1/2}(\frac{\tau}{l}) + \\ & \frac{3}{4}tri_{-1/2}(\frac{\tau}{l}) - \frac{1}{4}tri_{-1}(\frac{\tau}{l}) \end{aligned} \quad (18)$$

将式(6)(17)(18)代入式(16)可得

$$\begin{aligned} \hat{x}^{\text{proposed}} = & (tri_0(\frac{\tau}{l}) - \frac{1}{2}tri_{1/2}(\frac{\tau}{l}) - \frac{1}{2}tri_{-1/2}(\frac{\tau}{l}) + \\ & \frac{3}{2}tri_0(\frac{\tau}{l}) + tri_{1/2}(\frac{\tau}{l}) + \frac{1}{4}tri_1(\frac{\tau}{l}) + \\ & tri_{-1/2}(\frac{\tau}{l}) + \frac{1}{4}tri_{-1}(\frac{\tau}{l}) - \frac{1}{2}tri_{1/2}(\frac{\tau}{l}) - \\ & \frac{1}{2}tri_{-1/2}(\frac{\tau}{l}) - \frac{1}{4}tri_{-1}(\frac{\tau}{l}) - \frac{1}{4}tri_1(\frac{\tau}{l}))^2 = \\ & (\frac{5}{2}tri_0(\frac{\tau}{l}))^2 = \frac{25}{4}tri_0^2(\frac{\tau}{l}) \end{aligned} \quad (19)$$

由式(19)的理论分析结果可以看出,新提出的捕获结构不仅完全消除了副峰,而且使得主峰峰值增加了 150%。

从提出捕获结构在主峰增加、副峰消除方面来比较,本文提出的捕获算法无疑是最好的。从计算复杂度方面来比较,

ASPeCT 需要两次相关、两次平方运算;Filtered 相关法需要两次相关、两次移位、一次数乘、一次平方运算;文献[6]提出的算法需要一次相关、两次移位、三次平方运算;本文提出的算法只需要两次相关、两次移位、一次平方运算。由此可以看出本文算法不仅在性能上是最好的,并且计算复杂度也是最少的。

2 算法总结

2.1 算法框图

图 4 给出了实现上述算法的结构框图。

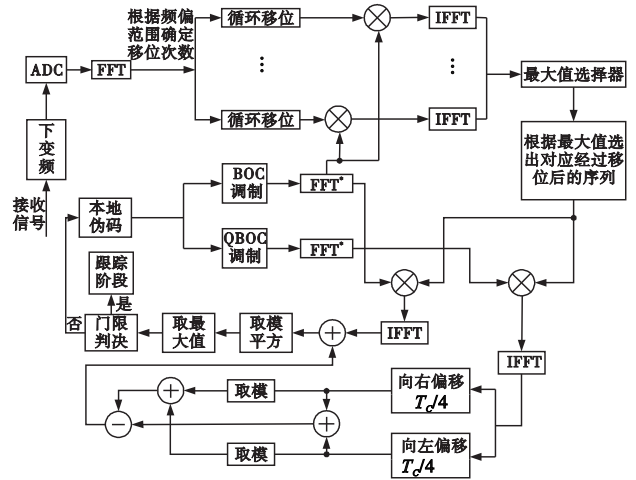


图4 基于FFT的BOC(1,1)信号捕获实现框图

2.2 算法流程

- 将接收的 BOC(1,1) 调制信号经过下变频,以适当的采样频率采样,表示为 r 。
- 生成本地 PN 序列 local-PN,并将 PN 序列进行副载波调制得到 local-BOC 和 local-QBOC 序列。
- 将 r 进行 FFT 处理得到 r' ,然后根据接收信号载波频偏的范围,将 r' 分别进行 k 次循环左移和 k 次循环右移,这样连同 r' 构成了 $2k+1$ 个频偏补偿序列。
- 将 local-BOC 和 local-QBOC 序列也进行 FFT 处理后,取共轭得到 $\text{FFT}\{\text{local_BOC}\}^*$ 和 $\text{FFT}\{\text{local_QBOC}\}^*$ 。
- 将 $2k+1$ 个频偏补偿序列分别与 $\text{FFT}\{\text{local_BOC}\}^*$ 相乘并进行 IFFT 运算,得到 $2k+1$ 个相关结果序列。取每一个相关结果序列中的最大值记为 c_k , $2k+1$ 个 c_k 构成 c 。
- 取出 c 中最大峰值所对应的频偏补偿序列 r'_k ,也就是经过多普勒补偿之后的接收信号的频域形式。
- 将 $\text{FFT}\{\text{local_BOC}\}^*$ 和 $\text{FFT}\{\text{local_QBOC}\}^*$ 与 r'_k 分别相乘,再进行 IFFT 运算,得到相关运算结果 x_{BOC} 和 $x_{\text{BOC/QBOC}}$ 。
- 将得到的相关结果按照本文捕获结构的方式处理之后,得到新的相关函数。
- 选取新的相关函数中的最大值,与门限进行比较。若最大值超过门限值,则认为捕获成功,进入跟踪阶段。
- 若最大值小于门限值,调制本地伪码相位。重复步骤 b) ~ i),直到出现超过门限值的峰值为止。

3 仿真实验及结果分析

3.1 算法原理仿真

为了验证新提出的捕获结构的有效性,使用 MATLAB 进行仿真验证,得到如图 5 所示的仿真图。图 5 中分别代表的是 ASPeCT、Filtered 相关法、文献[6]提出的捕获结构以及本文提出的捕获结构。图 5 中只选取了主峰位置附近的相关包络。

由图 5 可以看到,本文提出的捕获结构可以完全消除副

峰,同时提高主峰峰值,并且还可以保持与自相关相同的主瓣宽度。这样既可以避免捕获的模糊性,也能充分利用BOC调制的优点,并且可以极大地改善检测性能。

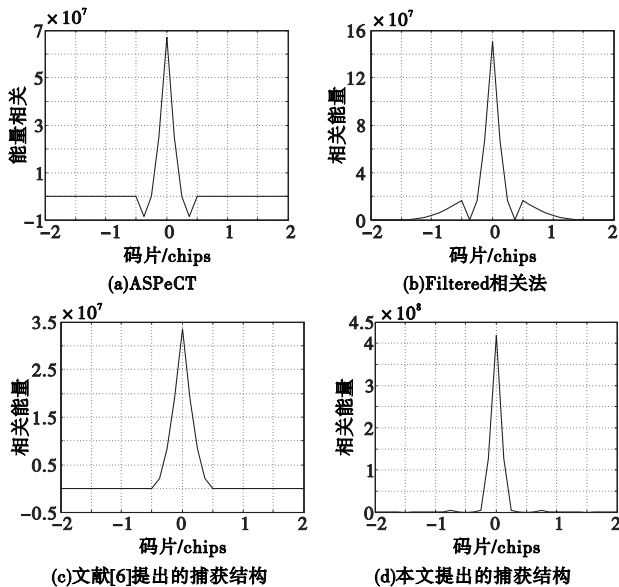


图5 四种算法的相关能量比较

3.2 算法捕获性能仿真

为了进一步验证该算法的捕获性能,使用MATLAB对伪码捕获过程进行仿真。仿真中用的是BOC(1,1)调制信号,信号经过下变频后的多普勒频偏 $f_d = 7.2$ kHz,伪码长度为 $L_{PN} = 1023$ 。假设伪码偏移量为 $\varphi = 250$,采样频率为8.148 MHz。由于采用的是BOC(1,1)调制信号,可知副载波频率为1.023 MHz,那么一个周期的BOC调制基带信号的采样长度(采样点个数)为 $L = 1023 \times 1 \times \frac{8.148 \text{ M}}{1.023 \text{ M}} = 8184$,由式(4)可得频偏补偿

精度 $f_{\text{prec}} = \frac{f_s}{L} = \frac{8.148 \text{ M}}{8184} = 1000 \text{ Hz}$,同样伪码偏移在采样点上

体现出来的偏移量 $\varphi' = \varphi \times \frac{L}{L_{PN}} = 250 \times 8 = 2000$ 。

3.2.1 最佳频偏补偿序列判断

对接收信号 r 做FFT后得到 r' ,将 r' 根据频偏大小范围进行循环左、右移位各 $k = 10$ 次,再分别与 $\text{FFT}\{\text{local_BOC}\}^*$ 通过IFFT运算得到 $2k + 1$ 个相关结果序列,检测每一个相关结果序列中的相关峰值,得到如图6所示的相关峰值。图中编号为负代表循环左移,也就是频偏补偿值为负。仿真中设信噪比为5 dB。由图6可以看到,最大相关峰值出现的位置在-7处,也就是最佳频偏补偿值为 $f_b = -7 \times f_{\text{prec}} = -7 \text{ kHz}$,频偏补偿残差为 $f_{\text{can}} = ||f_b| - f_d| = |7000 - 7200| = 200 \text{ Hz}$,这与仿真中所设置的频偏值大致是一致的,剩余的频偏残差对捕获的相关峰值的影响已经较小,并且可以通过提高采样频率来达到更高的补偿精度。

3.2.2 同步伪码所在位置判断

将最佳多普勒补偿序列 r'_{-3} ,也就是经过多普勒补偿之后的接收信号的频域形式与本地 $\text{FFT}\{\text{local_BOC}\}^*$ 和 $\text{FFT}\{\text{local_QBOC}\}^*$ 相乘,再进行IFFT运算,之后再按照前文所述的步骤进行处理,得到新的相关函数 $K(n)$,如图7所示。仿真中的信噪比为5 dB,图中只取了 $K(n)$ 相关峰值前、后各100个采样点。

由图7可以看到,峰值对应的位置在第2000个采样点处,这与设置的仿真条件是一致的。在信噪比为5 dB时,可以

准确地在伪码偏移位置出现一个主峰且没有副峰。

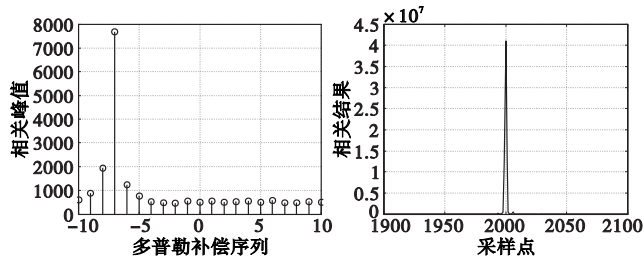


图6 不同多普勒补偿序列对应的峰值

图7 捕获仿真

3.2.3 主峰比例峰值比较

对于得到的相关结果序列 $K(n)$,定义比例峰值 $P_p = \max\{|\text{abs}(K(n))| / \text{ave}\{|\text{abs}(K(n))|\}\}$,其中 ave 表示取平均。在同样情况下,对BOC(1,1)信号进行四种捕获算法的比例峰值仿真,接收信号都已经过频域的多普勒频偏补偿,得到不同信噪比下比例峰值的仿真图,如图8所示。

由图8可以看到,本文提出的捕获结构的主峰比例峰值远远高于其他三种算法,在信噪比为20 dB时,本文算法的主峰比例峰值是专利提出算法的2倍,而主峰比例峰值可作为捕获判定的依据,可知本文算法有着比其他三种算法更好的捕获性能。

3.2.4 检测概率比较

对BOC(1,1)信号进行四种捕获算法的捕获性能仿真,得到不同信噪比下检测概率的仿真图,如图9所示。仿真中所使用的捕获判断依据的方式是:是否在伪码偏移位置出现最大值。

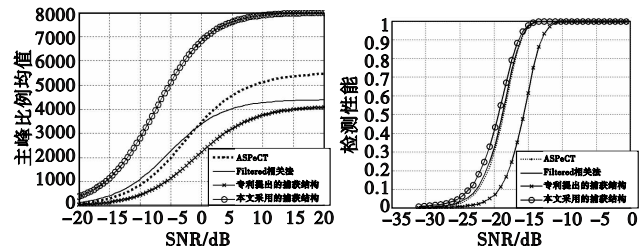


图8 四种算法的比例峰值仿真 图9 四种算法的检测性能仿真

由图9可以看到,本文提出的捕获结构的检测性能要比BOC专利捕获结构的性能好4.5 dB左右。这是因为专利捕获结构的主峰峰值降低了,在噪声的影响下旁瓣可能会超过主峰的值,从而令检测性能较差;而本文算法由于主峰峰值很大,且完全没有副峰,这样受噪声的影响相对较少,这与主峰比例均值的性能也是一致的。

4 结束语

对于BOC(1,1)调制信号捕获的模糊性问题,本文提出了一种频域多普勒补偿与相关函数组合的无模糊捕获算法。对接收信号进行并行的频域多普勒补偿,基于FFT对BOC/local-BOC、BOC/local-QBOC两路相关结果移位 $\pm T_c/4$ 、取模、求和、平方的组合运算,得到的新相关函数消除了原相关函数的副峰,提高了比例峰值和检测概率,并且新相关函数的主瓣宽度保持与BOC(1,1)自相关函数相同的主瓣宽度,可知该算法有着很高的捕获精度。仿真实验结果表明,新的捕获算法的检测概率比传统专利算法提高约4.5 dB左右,并且捕获速度较快,硬件实现简单。虽然文中主要是针对BOC(1,1)信号进行分析,但是可以很容易推广到BOC(n,n)型信号。(下转第681页)

窗口宽度时,应根据所求的模幂的指数 k 的大小,适当选取窗口宽度 ω ,以保证 $t > 2^\omega - 1$ 。在进行大整数的模幂运算时,笔者推荐选取窗口宽度 $\omega = 2, 3, 4$ 。

表1 指数 k_i 在不同的 ω 下的 2^ω 进制长

ω	l_1	l_2	l_3	l_4	l_5
1	433	533	633	733	833
2	217	267	317	367	417
3	145	178	211	245	278
4	109	134	159	184	209
5	87	107	127	147	167
6	73	89	106	123	139

表2 固定基窗口方法在不同的 k, ω 下的运行时间 /s

ω	k_1	k_2	k_3	k_4	k_5
1	26.234 4	26.687 5	27.203 1	27.718 8	28.25
2	21.796 9	22.546 9	23.328 1	24.156 3	24.968 8
3	21.812 5	23.937 5	24.390 6	25.421 9	27.609 4
4	24.125	26.109 4	28.078 1	29.984 4	31.953 1
5	31.546 9	34.812 5	38.00	41.203 1	44.531 3
6	46.50	52.00	57.703 1	63.109 4	68.671 9

表3 平方乘法算法在不同的 k 下的运行时间 /s

k_1	k_2	k_3	k_4	k_5
88.953 1	110.828	130.344	152.813	171.516

表4 固定基窗口方法相对于平方乘法算法的提高程度 /%

ω	k_1	k_2	k_3	k_4	k_5
1	70.507 6	75.919 9	79.129 7	81.860 9	83.529 2
2	75.496 2	79.656	82.102 6	84.192 2	85.442 3
3	75.478 7	78.401 2	81.287 5	83.364	83.902 7
4	72.879	76.441 6	78.458 4	80.378 3	81.370 1
5	64.535 4	68.588 7	70.846 3	73.036 8	74.036 6
6	47.725 3	53.080 5	55.73	58.701 4	59.961 7

3 结束语

模幂运算是公钥密码体制中一个很重要的运算,其运算速度直接影响到公钥密码体制能否有效地实现。本文与其他解决 a) 类模幂问题的算法类似,也采用了预处理技术,将椭圆曲线的定点标量乘的固定基窗口方法应用在模幂运算中,与 SMM 算法进行组合,得到一种新的关于模幂运算的固定基窗口方法,并以牺牲存储空间为代价,获得了较快的运算速度。预存储空间中存放的是固定底数 g 的模幂,当固定窗口宽度

ω , 存储空间大小与指数 k 的二进制长度 t 有关, t 越大,所需的预存储空间越大,相对于二进制的平方乘法算法,运算速度提高越大。为保证较高的运算速度,窗口宽度 ω 不能选得太大,笔者推荐选取窗口宽度 $\omega = 2, 3, 4$ 。

参考文献:

- [1] RIVEST R, SHAMIR A, ALDEMAN L. A method for obtaining digital signatures and public-key cryptosystems[J]. *Communications of the ACM*, 1978, 21(2): 120-126.
- [2] GORDON D M. A survey of fast exponentiation methods[J]. *Journal of Algorithms*, 1998, 27(1): 129-146.
- [3] MENEZES A J, VAN OORSCHOT P C, VANSTONE S A. Handbook of applied cryptography[M]. Boca Raton: CRC Press, 1996.
- [4] BRICKELL E F, GORDON D M, McCURLEY K S, et al. Fast exponentiation with precomputation[C]//Proc of Eurocrypt on Advances in Cryptology. New York: Springer-Verlag, 1993: 200-207.
- [5] De ROOIJ P. Efficient exponentiation using precomputation and vector addition chains[C]//Proc of Eurocrypt on Advances in Cryptology. New York: Springer-Verlag, 1995: 389-399.
- [6] DIMITROV V S, COOKLEV T V. Two algorithms for modular exponentiation using nonstandard arithmetics[J]. *IEICE Trans on Fundamentals*, 1995, E78-A(1): 82-87.
- [7] DIMITROV V S, JULIEN G A, MILLER W C. An algorithm for modular exponentiation[J]. *Information Processing Letters*, 1998, 66(3): 155-159.
- [8] GATHEN J, NOCKER M. Exponentiation using addition chains for finite fields[EB/OL]. (2008-3-18). <http://citeseer.nj.nec.com/vonzurgathe-n00exponentiation.html>.
- [9] KNUTH D E. The art of computer programming[M]. 2nd ed. [S. l.]: Addison-Wesley, 1981.
- [10] KOC C K. Analysis of sliding window techniques for exponentiation[J]. *Computers & Mathematics with Applications*, 1995, 30(10): 17-24.
- [11] CHIOU C W. Parallel implementation of the RSA public-key cryptosystem[J]. *International Journal of Computer Mathematics*, 1993, 48(3): 153-155.
- [12] LOU D C, CHANG C C. An adaptive exponentiation method[J]. *Journal of Systems and Software*, 1998, 42(1): 59-69.
- [13] HANKERSON D, MENEZES A, VANSTONE S. Guide to elliptic curve cryptography[M]. New York: Springer-Verlag, 2004: 104.
- [14] CHEN Y. A new fast RSA algorithm[J]. *Journal of University of Electronic Science and Technology of China*, 1996, 24(2): 223-228.

(上接第 675 页)

参考文献:

- [1] 王先发, 禹化龙, 张碧雄. 我国未来卫星导航信号的优先选择——BOC 调制信号[J]. *中国电子科学研究院学报*, 2009, 4(3): 307-312.
- [2] LOHAN E S. Statistical analysis of BPSK-like techniques for the acquisition of Galileo signals[J]. *AIAA Journal of Aerospace Computing Information and Communication*, 2006, 3(5): 234-243.
- [3] JULIEN O, MACABIAU C, CANNON M E, et al. ASPECT: unambiguous sine-BOC(n, n) acquisition/tracking technique for navigation applications[J]. *IEEE Trans on Aerospace and Electronic Systems*, 2007, 43(1): 150-162.

- [4] NUNES F D, SOUSA F M G, LEITAO J M N. Multipath mitigation technique for BOC signals using gating functions[C]//Proc of the 2nd European Space Agency Workshop on Satellite Navigation User Equipment Technologies. 2004.
- [5] 邢兆栋, 张其善, 杨东凯. GALILEO 接收机中 BOC(1,1) 信号的捕获[J]. *北京航空航天大学学报*, 2006, 32(6): 687-690.
- [6] 陈佳品, 齐佳敏, 陈翔, 等. 二进制偏置载波信号精确同步装置及其同步方法: 中国, 201110108183[P]. 2011-09-14.
- [7] 刘哲, 倪少杰, 牟卫华, 等. CCRW 技术在 MBOC 调制信号下多径抑制性能[J]. *全球定位系统*, 2011, 36(4): 29-33.
- [8] 杨力, 潘成胜, 冯永新, 等. 一种 BOC 调制信号的同步主峰检测新算法[J]. *宇航学报*, 2010, 31(8): 2008-2014.