doi:10.11887/j.cn.202402018 http://journal.nudt.edu.cn

面向数字射频存储的雷达欺骗干扰检测方法

张顺生[1*],陈 爽[1],王文钦[2]

(1. 电子科技大学 电子科学技术研究院,四川 成都 611731;2. 电子科技大学 信息与通信工程学院,四川 成都 611731)

摘 要:基于数字射频存储(digital radio frequency memory,DRFM)技术的转发式欺骗干扰与真实雷达回波高度相干,这导致雷达难以分辨真假目标。针对该问题,提出一种基于Hough变换的DRFM欺骗干扰检测方法。建立基于线性调频的干扰信号模型,分析其谐波分量的频谱特性,采用短时傅里叶变换和二维恒虚警率检测器对干扰信号进行特征提取,并利用Hough变换完成欺骗干扰检测。所提方法是基于DRFM欺骗干扰本身的特征,不依赖于先验信息与应用场景,计算复杂度低,且在低信噪比条件下具有良好的检测性能。计算机仿真实验验证了方法的有效性。

关键词:干扰检测;有源欺骗干扰;数字射频存储;Hough变换

中图分类号:TN974 **文献标志码**:A **开放科学(资源服务)标识码(OSID)**:

文章编号:1001-2486(2024)02-174-08

Radar deception jamming detection method with digital radio frequency memory

ZHANG Shunsheng[1*], *CHEN Shuang*[1], *WANG Wenqin*[2]

(1. Research Institute of Electronic Science and Technology, University of Electronic Science and Technology of China, Chengdu 611731, China;
2. School of Information and Communication Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China)

Abstract: The transponder deception jamming with DRFM(digital radio frequency memory) is highly coherent with real radar echoes, which makes it difficult for radar to distinguish real radar echoes and jamming. To address this issue, a DRFM-based deception jamming detection method based on Hough transform was proposed. The jamming signal model based on linear frequency modulation was established and the spectrum of the jamming harmonics was analyzed subsequently. Then, the short-time Fourier transform and two-dimensional constant false alarm rate detector were used to extract the features of the jamming signal. The Hough transform was used to complete deception jamming detection. The proposed method is based on the characteristics of DRFM deception jamming itself, and does not depend on prior information and application scenario. Moreover, it has low computational complexity and good detection performance under the condition of low signal-to-noise. The effectiveness of the proposed method is verified through simulations.

Keywords: jamming detection; active deceptive jamming; digital radio frequency memory; Hough transform

近几十年来,随着数字射频存储(digital radio frequency memory,DRFM)技术的出现和发展,干扰机能够产生与雷达发射信号高度相干的有源欺骗信号,这些调制方式多样、参数多变的干扰使得雷达难以正常工作。为了抑制这类干扰信号对雷达产生的影响,人们提出了许多抗干扰技术,但无论是基于信号本身的抗干扰手段[1],还是基于雷达组网的抗干扰方法[2],都无疑会占用大量的雷达资源。如何在敌我双方博弈的过程中,快速检测到干扰信号的存在与否,已成为一个值得关注的课题。

针对DRFM转发式干扰,文献[3]指出DRFM对截获的雷达信号进行存储时,采样量化会导致所产生的干扰信号具有一定的谐波分量,在此基础上提出了基于高阶统计量的DRFM欺骗干扰识别算法,开创了利用DRFM干扰机模数转换器(analog to digital converter, ADC)相位量化的谐波效应进行干扰识别的先河。文献[4]在前人的研究基础上,理论推导了DRFM干扰机在相位量化和时延离散后产生的拖引欺骗干扰频谱的数学形式,并提出了基于信号锥理论和自适应相参估计的干扰检测方法,为干扰信号的谐波寄生特性提供了理论依据。文献[5]具体分析了DRFM干扰机在相位量化后产生距离-速度同步拖引干扰的谐波效应,提出了利用信号检测理论与凸优化理论实现该情形下的欺骗干扰检测。文

收稿日期:2022-05-11

*第一作者:张顺生(1980—),男,安徽安庆人,研究员,博士,博士生导师,E-mail:zhangss@uestc.edu.cn

献[6]利用近似熵和运动切近似熵进行干扰识别,在检测到干扰的同时也可以侦测出干扰出现的时刻,但只能针对连续波信号进行检测。文献[7]提取了干扰信号奇异值的统计直方图的方差、峰度、偏度、能量和熵作为特征构建特征向量,并利用支持向量机作为分类器对干扰进行检测。文献[8]提出利用分数阶傅里叶变换测量调频参数,并根据干扰机量化位数匹配调频参数的方法检测 DRFM 干扰。

不过,上述提到的大多数文献采用二元检测器检测,或者是直接对原始信号及其频谱进行操作,这些方法对于高信噪比的单载波雷达信号比较适用,但已无法应对低信噪比的复杂场景。故本文在分析 DRFM 欺骗信号与实际回波的时频域特征的基础上,使用二维恒虚警率(constant false alarm rate, CFAR)检测器进行特征提取,并利用 Hough 变换进行干扰检测,解决了复杂电磁环境下基于 DRFM 有源欺骗干扰信号的检测问题。

1　基于 DRFM 的欺骗干扰信号模型

脉冲压缩技术解决了常规脉冲雷达作用距离和距离分辨率的矛盾,使得脉冲线性调频(linear frequency modulation, LFM)信号在脉冲压缩体制雷达中广泛应用。故而,本文后续的分析均以脉冲 LFM 信号为例,设雷达的中心频率为 f_c,脉冲重复周期为 T_r,雷达发射信号的带宽为 B,脉宽为 τ,发射信号的调频斜率可以表示为 $\mu = B/\tau$,则雷达发射信号可以表示为:

$$s(t) = [p(t) * \sum_{n=-\infty}^{\infty} \delta(t - nT_r)] \cdot e^{j\pi\mu t^2} \cdot e^{j2\pi f_c t} \tag{1}$$

$$p(t) = \begin{cases} 1, & -\frac{\tau}{2} \leqslant t \leqslant \frac{\tau}{2} \\ 0, & \text{其他} \end{cases} \tag{2}$$

忽略时延函数离散化的影响[9],DRFM 接收机在截获雷达信号后,会先将信号转换到接收机中频,以便后续的调制工作。设 DRFM 接收机中频为 f_0,则 DRFM 接收机内部接收到的信号可表示为:

$$x(t) = s(t) \cdot e^{j2\pi f_0 t} \cdot e^{-j2\pi f_c t} \tag{3}$$

一般情况下,被截获的雷达信号的信息主要被携带在信号的相位中,故在进行信号存储时只对相位进行量化。假设干扰机接收端采样量化时采用 $N = 2^M$ 量化,M 为量化位数,根据文献[9]的推导,量化后的信号可以表示为:

$$y(t) = \sum_{m=-\infty}^{\infty} \sin c(m + \frac{1}{N}) \cdot e^{j(Nm+1)\cdot(2\pi f_0 t + \pi\mu t^2)} \tag{4}$$

经过相位量化后的信号由 DRFM 系统进行调制,加入虚假的多普勒频移,经由上变频恢复载波信息后,由发射机发射出去。

$$\hat{y}(t) = y[t - c(t)] \cdot e^{j2\pi f_j t} \cdot e^{j2\pi(f_c - f_0)t} \cdot p(t) \tag{5}$$

式中,f_j 为虚假的多普勒频移,$c(t)$ 为时延函数表示接收信号与发射信号之间的延时量。在理想状况下 $c(t) = at$ 为线性函数,但在实际的 DRFM 系统中,$c(t)$ 通常被量化为一个分段连续的时间函数,用阶梯函数逼近。由于在雷达的一个相关处理间隔内 $c(t)$ 往往远小于 T_r,故可以忽略时延量化对干扰信号频谱的影响[10],后续推导将时延函数看成是时间的连续函数即取 $c(t) = at$。这样可以得到 DRFM 干扰机转发干扰信号模型:

$$\hat{y}(t) \approx \sum_{n=-\infty}^{\infty} p(t - nT_r) \cdot e^{j2\pi(f_c - f_0 + f_j)t} \cdot \sum_{m=-\infty}^{\infty} \sin c\left(m + \frac{1}{N}\right) \cdot e^{j(Nm+1)[2\pi f_0(1-a)t + \pi\mu(1-a)^2 t^2]} \tag{6}$$

那么雷达接收机在下变频后接收到 DRFM 干扰机转发欺骗干扰 LFM 信号:

$$z(t) = \hat{y}(t) \cdot e^{-j2\pi f_c t} = p(t) \cdot e^{j2\pi(-f_0 + f_j)t} \cdot \sum_{m=-\infty}^{\infty} \sin c(m + \frac{1}{N}) \cdot e^{j(Nm+1)[2\pi f_0(1-a)t + \pi\mu(1-a)^2 t^2]} \tag{7}$$

为了确定量化信号的频谱特性,对式(7)的主项 $f_1(t) = e^{j(Nm+1)[\pi\mu(1-a)^2 t^2]}$ 进行分数阶傅里叶变换:

$$F_1(f) = \sqrt{\frac{1 + j\tan\alpha}{1 + k(m)\tan\alpha}} e^{j\frac{\pi f^2 [k(m) - \tan\alpha]}{1 + k(m)\tan\alpha}},$$
$$k(m) = (Nm + 1)\mu(1 - a) \tag{8}$$

根据傅里叶变换的频域特性可知,$f_2(t) = e^{j(Nm+1)[2\pi f_0(1-a)t]} \cdot e^{j2\pi(-f_0 + f_j)t}$ 与 $f_1(t)$ 的乘积的频谱是对 $F_1(f)$ 的频移,在 $\alpha = \pi/2$ 时有:

$$\begin{cases} Z(f) = P(f) * \sum_{m=-\infty}^{\infty} \sin c(m + \frac{1}{N}) \cdot F_1(f) * \delta[g(f)] \\ g(f) = f - (Nm + 1)(1 - a)f_0 - f_j + f \end{cases} \tag{9}$$

其中,$P(f) = \frac{\tau}{T_r} \sin c(\pi\tau f) \sum_{k=-\infty}^{\infty} \delta\left(f - \frac{k}{T_r}\right)$ 为 $p(t)$ 的频谱,从式(9)不难看出,干扰信号 $z(t)$ 的频谱是由多个不同项的和组成的[11-12]。对于采样时间有限的 LFM 信号,信号能量主要集中在支撑区间内,而在支撑区间以外信号的频谱幅度很小,信

号能量可以忽略不计，其形状分布接近矩形[13]，故而可以忽略不同 m 值之间的频谱影响，单独分析不同 m 值下的谐波的特性。

$Z(f)$ 在 $m=0$ 时的分量与真实回波处于相同的频段，起主要的欺骗作用，故称 $Z(f)$ 在 $m=0$ 时的分量为主项。除主项外，干扰频谱还存在 $m\neq 0$ 的谐波分量，即干扰伪项，从式(8)可以看出，随着 m 的增大其幅度项 $|F_1(f)|$ 会减小，而伪项的带宽则会增加，伪项的强度主要由 $|F_1(f)|$ 决定，但会经过 $\mathrm{sinc}(m+1/N)$ 的衰减，正是这些有着一定规律的谐波分量，为区分真假信号提供了可能。

2　基于 Hough 变换的欺骗干扰检测方法

2.1　数据预处理与 CFAR 检测

对于 DRFM 干扰机[14]产生的 LFM 欺骗干扰信号，其主项与真实回波相似且处于同一频段，经过脉冲压缩后，依旧可以达到欺骗的效果[15]。从上文的分析可知，经过 DRFM 干扰机产生的干扰信号存在着干扰伪项，但伪项都会经过 sinc 衰减，衰减后的伪项幅值较低。在频域上，无噪声时很容易区分干扰信号和回波信号，但能量最高的伪项也要比主项低 7 dB，在信噪比为负的情况下，伪项在频域很容易被随机噪声完全淹没。且频谱特征单一，很难进行特征提取和噪声抑制。为了能够更好地对干扰进行识别，本文提出基于 Hough 变换的 DRFM 欺骗干扰的 CFAR 检测[16]，先对信号进行短时傅里叶变换，尽可能保留信号的特征；然后利用二维单元平均－恒定虚警率(cell averaging-constant false alarm rate，CA-CFAR)检测降低随机噪声对伪项的影响，保留伪项的特征；最后利用 Hough 变换对基于 DRFM 的干扰信号进行识别。

图 1 为 $M=2$ 时在无噪声情况下 DRFM 干扰机产生欺骗信号的频谱(干扰信号为 LFM 信号，带宽 10 MHz，脉宽 50 μs，采样率 1 GHz)。从图 1 中不难看出，虽然伪项特征明显，但是能量较低，很容易出现低信噪比下检测失效的问题。并且，若想在频域得到明显的伪项特性所需的采样率很高，这在实际场景下并不适用。故想要提高低干噪比条件下的检测效率，可以从噪声和干扰伪项的特征差异入手。一般而言，噪声为随机分布，很难捕捉其规律性，而从第 1 节的分析可知，DRFM 伪项为线性调频信号，图 2 为无噪声时真实雷达回波与 DRFM 干扰信号时频域对比，从图中也可以清晰地看到伪项的调频信息。故可以将降噪问题转化为噪声环境中的信号检测问题，利用雷达信号检测的手段对伪项进行特征提取。

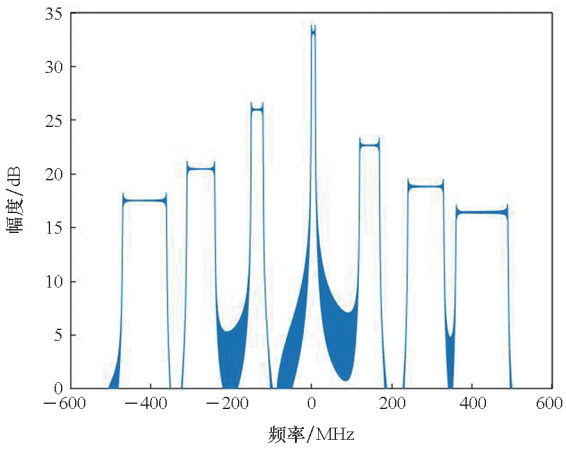
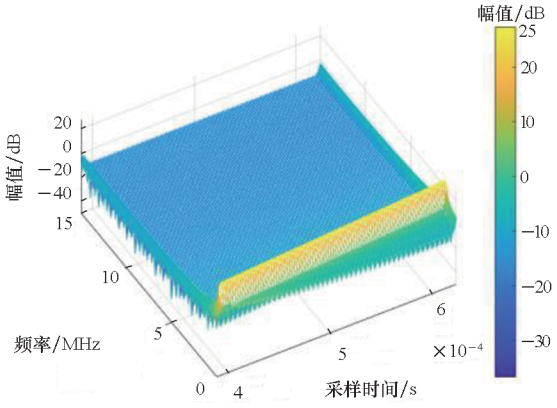


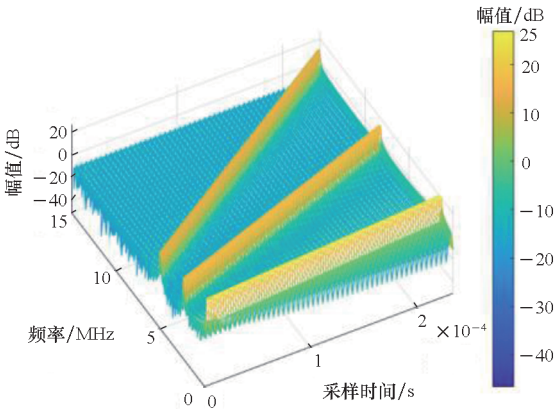
图 1　无噪声时 DRFM 干扰频谱

Fig. 1　DRFM interference spectrum in the absence of noise



(a) 雷达真实回波的时频图

(a) Time-frequency plot of real radar echo



(b) DRFM 欺骗信号的时频图

(b) Time-frequency plot of DRFM spoofing signal

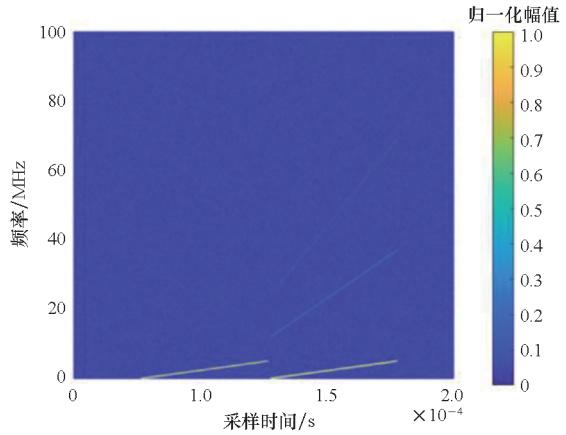
图 2　无噪声时真实雷达回波与 DRFM 干扰信号时频域对比

Fig. 2　Time-frequency domain comparison between real radar echo and DRFM jamming signal in the absence of noise

为降低后续检测的计算复杂度，可先对信号进行脉冲压缩，得到距离信息后，对信号进行裁剪，只保留脉冲到达时间前后一段时间的数据作为待检

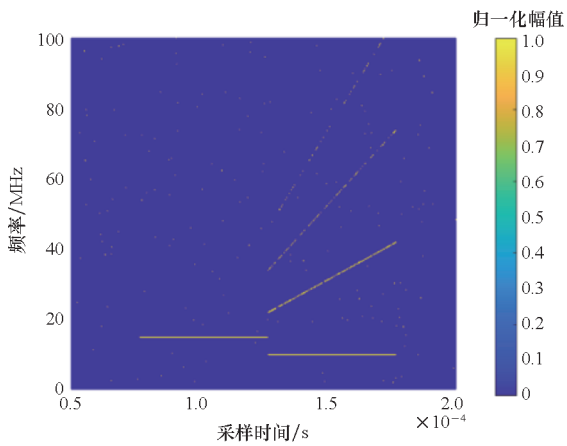
信号。由于主项的功率远高于伪项,为了避免检测时主项对结果造成影响,在预处理环节还需利用发射信号的信息,对待检信号进行去调频操作。去调频后,主项在时频域表示为一条斜率为零的直线段。后续的检测中,可通过斜率滤除主项。

对待检信号经过短时傅里叶变换后会得到一张时频图[17],在无噪声时,调频特征明显,但是在加噪情况下,调频特征容易受噪声影响,此时若直接进行检测,很难检测到真实的伪项信息,且原始待检矩阵未经过量化与边缘化处理,会带来极高的时间复杂度,无法满足实时检测的要求。考虑线性调频信号的时间连续性和调频特性,这里采用二维 CFAR 对调频特征进行提取,既能尽可能多地捕捉到有效信息,又能一定程度上抑制随机噪声的影响。图 3 为 $SNR = -5$ dB 时预处理前后的时频图对比,可以看到,经过预处理后调频特征变得清晰,且主项及回波的干扰斜率归零,便于后续分辨主项与伪项。



(a) 预处理前的待检矩阵

(a) Matrix to be detected before preprocessing



(b) 预处理后的待检矩阵

(b) Preprocessed matrix to be detected

图 3　$SNR = -5$ dB 时预处理前后对比

Fig. 3　Comparison before and after preprocessing when $SNR = -5$ dB

2.2　Hough 变换与干扰检测

虽然经过二维 CFAR 检测可以大面积剔除时频图中的随机噪声,但是一部分伪项的信息也会被当作噪声剔除。同时,为了保留伪项不能设置过低的虚警概率,也会导致部分能量较高的噪声被保留下来,最终得到的是伪项信息残缺的时频图。在这种情况下,很难用传统的信号处理手段对干扰进行检测。根据第 1 节的推导可知,DRFM 伪项在时频图上应该呈现出斜率为调频率的一条线段,虽然经过 CRAR 后会有部分的特征信息缺失,但依旧会保留其相关性,而被保留下来的噪声信息为随机分布的斑点,不具有相关特征。故此,如能在时频图像中检测到除主项外的直线段的存在,便可判定该信号存在伪项,视为 DRFM 干扰信号。

Hough 变换是一种特征提取技术,被广泛应用于图像处理、计算机视觉等领域。它把图像中一个特征点变换到变换空间中的一条直线或曲线,然后通过投票算法检测具有特定形状的物体。

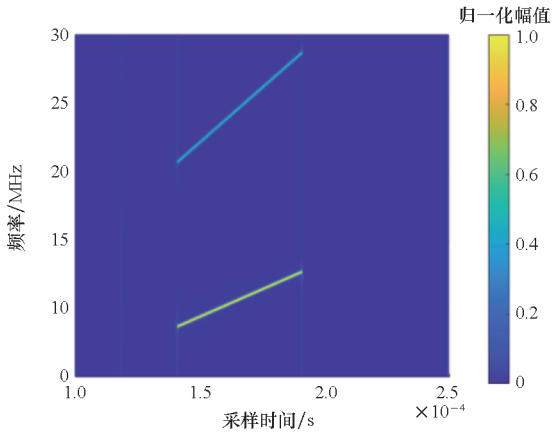
对于笛卡尔空间中的任意一点(x_0, y_0),在极坐标下过该点的直线簇可表示为:

$$r = x_0\cos\theta + y_0\sin\theta \tag{10}$$

式中,r 是从原点到直线的距离,θ 是向量 $\boldsymbol{r}$ 与 x 轴的夹角。任意一对(r_1, θ_1)可视为参数空间(r, θ)中的一个点,过任意一点的直线簇的参数在参数空间形成一条曲线,而当笛卡尔空间中有多个点可以构成一条直线的时候,在参数空间中就会有多条曲线相交于一点,利用该点的参数(r_0, θ_0)便可确定笛卡尔空间中的直线方程。而所谓的投票算法便是寻找图像中的直线参数的方法。在得到参数空间的参数后需建立一个 Hough 矩阵即一个累加器,Hough 矩阵的维数即为参数维数。对于直线检测的问题,其维度为 2,先对 Hough 矩阵置零,再将参数空间的点累加到 Hough 矩阵,这样在判断直线问题时,只需要寻找到累加器中超过阈值 q 的(r, θ)参数对便可确定直线方程。

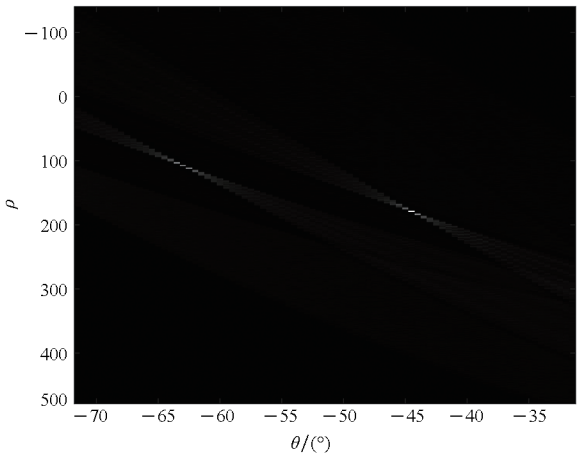
上述即 Hough 变换的原理,在传统的图像检测时,由于图像中的信息相对复杂,需对图像先进行边缘检测,找出边缘点,绘制边缘轮廓矩阵,根据边缘点确定参数空间中的参数。但对于干扰检测问题,时频特征本就比较单一,并且在上一小节,已经对原始数据进行了预处理,通过 CFAR 检测实现了待检矩阵的边缘化,这里可以直接对待检矩阵进行 Hough 变换。由于预处理环节对待检信号已进行了去调频操作,此处便可通过控制检测线段的 θ 值,剔除主项。如图 4(a)为经过本

文方法预处理的一个待检矩阵，图 4（b）为图 4（a）所示矩阵 Hough 变换后 Hough 空间示意图，图 4（b）Hough 坐标系下的两个亮点即对应图 4（a）中的两条直线。



（a）笛卡尔坐标系下的待检矩阵

（a）Matrix to be detected in the Cartesian coordinate system



（b）Hough 坐标系下检测结果

（b）Detection results in Hough coordinate system

图 4　笛卡尔坐标系与 Hough 坐标系关系对照图

Fig. 4　Comparison diagram of the relationship between Cartesian coordinate system and Hough coordinate system

本文所述基于 Hough 变换的欺骗干扰检测方法的流程如图 5 所示，可总结为如下步骤：

1）预处理：利用发射信号信息及脉冲压缩得到的距离信息，对原始信号进行信号裁剪和去调频操作。

2）特征提取：对待检信号进行短时傅里叶变换，并利用 CFAR 检测器提取调频信息，实现待检矩阵的边缘化处理。

3）干扰检测：利用 Hough 变换剔除雷达回波与干扰主项，实现对欺骗干扰的检测。

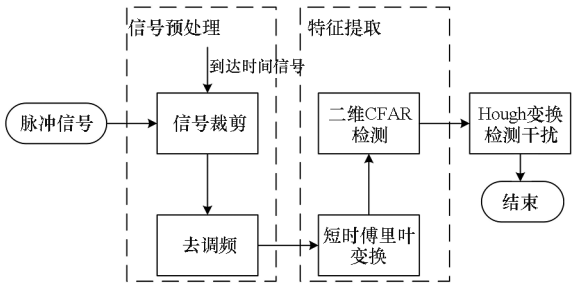


图 5　基于 Hough 变换的欺骗干扰检测方法流程图

Fig. 5　Flow chart of detection of DRFM deception jamming based on Hough transform

3　仿真实验

仿真实验条件设置如下：根据目前典型 DRFM 干扰机结构，可设置 DRFM 量化位数[18] $M=2$（M 值较低，但在实际机载系统的小型化 DRFM 中很常见），DRFM 中频 $f_0=30$ MHz，信号带宽 $B=50$ MHz，采样率 $f_s=150$ MHz。假设检测环境在中频段同一波门中有一到两个未知 LFM 信号分量，可能为真实的雷达回波，也可能为 DRFM 干扰机生成的干扰信号，环境噪声为服从 $n\sim N(0,\sigma^2)$ 分布的零均值复高斯白噪声。设置二维 CFAR 的虚警概率 $P_f=0.000\ 5$，定义信噪比 $SNR=|s(t)|^2/|n(t)|^2$，干噪比 $JNR=|j(t)|^2/|n(t)|^2$，干扰信号强度为目标回波强度的 1.5 倍。

图 6 为量化位数 $M=2$ 且波门中同时存在雷达真实回波和干扰信号时，在 SNR 从 −15 dB 到 10 dB，每个信噪比下进行 10 000 次仿真得到的干扰检测性能曲线。从图 6 中可以看到，随着 SNR 的增大，环境噪声对于干扰谐波的影响不断减小，能够提取到的有效特征增多，检测概率不断

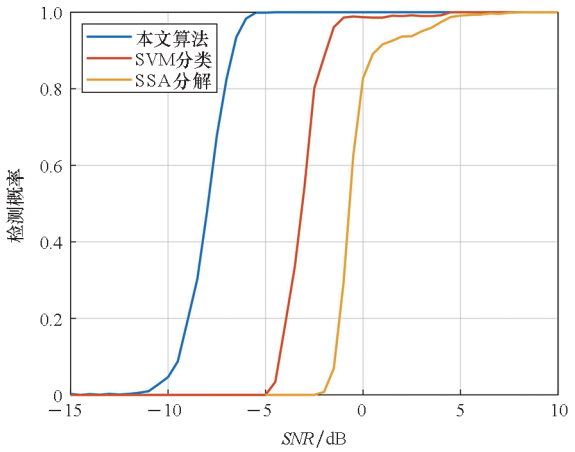


图 6　$M=2$ 时检测性能对比

Fig. 6　Comparison of detection performance when $M=2$

增加,最终趋于稳定。对比其他方法[19],本文方法在负信噪比时仍能保持很好的效果,能够在较为恶劣的情况下对 DRFM 干扰进行有效识别。

图 7 为不同干信比条件下检测性能的对比。从图 7 中可以看到,随着干信比的增加,检测性能也有所提升。仿真结果表明,本文方法在干信比为 0 dB,信噪比为 -5 dB 时,检测概率依旧可以达到 84.65%,实现在低信噪比低干信比情况下的干扰检测。

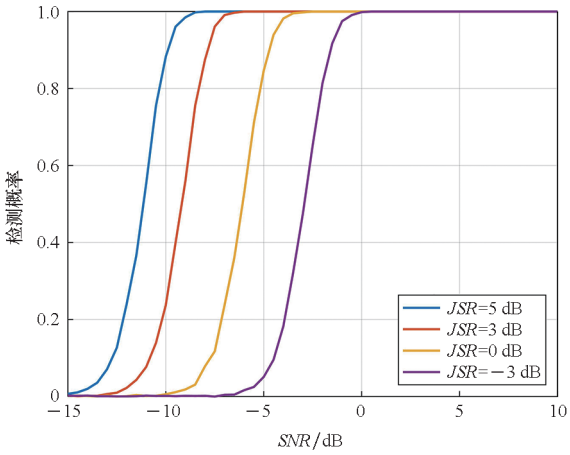


图 7　不同干信比下检测性能对比

Fig. 7　Comparison of detection performance under different *JSR*

雷达信号有多种,除 LFM 脉冲信号外,常用的还有简单脉冲信号和相位调制脉冲信号等。图 8为不同调制类型信号的检测性能对比。仿真表明:针对不同的雷达信号,本文方法在 -6 dB 信噪比时均能达到 86% 以上的检测概率,而且对不同调制类型干扰信号的检测性能差别不大。

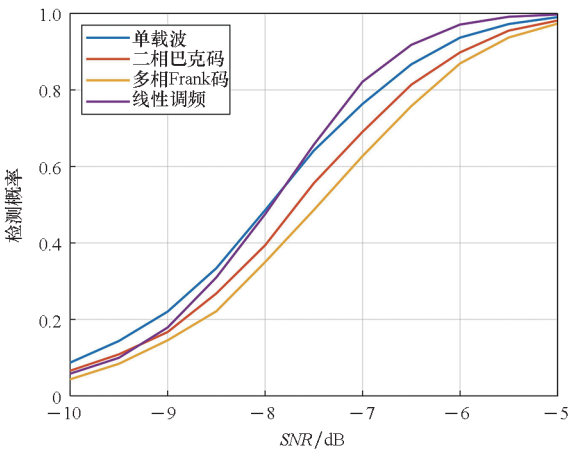


图 8　不同调制类型信号的检测性能对比

Fig. 8　Comparison of detection performance of different modulation types of signals

在进行检测时,由于 Hough 变换时按照累加器的计数来衡量图像中是否存在直线,当图像中处于直线段上的检测点过少时或干扰信息过多时,都会影响检测的效果。图 9 为 Hough 矩阵累加器不同阈值 q 下的检测性能对比。可以看到,合适的累加器阈值能够得到更好的检测性能。q 值过大,会使得低信噪比时的检测性能降低,在高信噪比也会存在一定程度的漏检,甚至可能完全检测不到干扰谐波;q 值过小,不仅会降低检测性能,还会造成一定的虚警,在图像中表现为较低信噪比下 $q=40$ 时,检测概率不为零,这时并非真的检测到干扰,而是将环境噪声误认为干扰伪项导致的虚警。q 值的设置主要与信噪比、量化位数以及 Hough 变换待检矩阵维度有关,后续研究时,可以适当改进原始算法,在各种参数未知的情况下,通过预估检测主项及环境参数,自适应调节 Hough 变换累加器的阈值 q,动态确定检测线段的长度和概率,以提高检测性能。

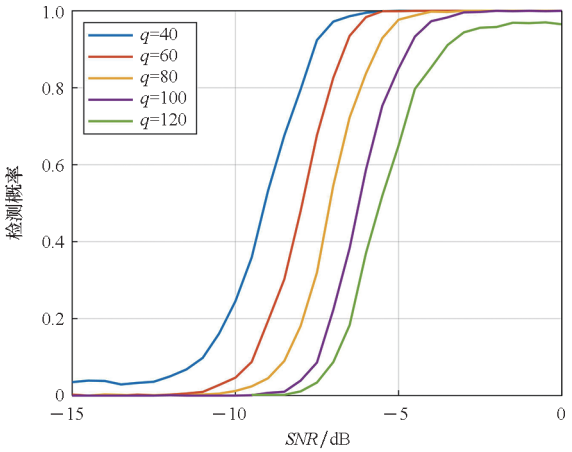


图 9　$M=2$ 时不同阈值下的检测性能对比

Fig. 9　Comparison of detection performance under different thresholds when $M=2$

在针对雷达有源干扰一类问题时,不少学者提出了基于能量和二元检测[20-21]的识别方法,也取得了一定的成果[22]。但这类检测都存在一个比较大的弊端,即适用情况受限,大多以波门内只存在一个雷达回波信号作为对比,针对波门内同时出现雷达回波和欺骗干扰的情况进行检测,无法满足其他情况下的干扰检测。图 10 为波门内存在不同类型回波时的检测性能仿真情况,从仿真结果可以看到,本文方法在不同场景下,依旧可以保持良好的检测性能。

图 11 为 *SNR* 在 -25 dB 到 15 dB 时在不同量化位数 M 下的检测性能对比。从图 11 中可以看到,由于量化位数的增加,根据式(9)的分析可知,DRFM 伪项的带宽也会成倍增长,相应的伪项

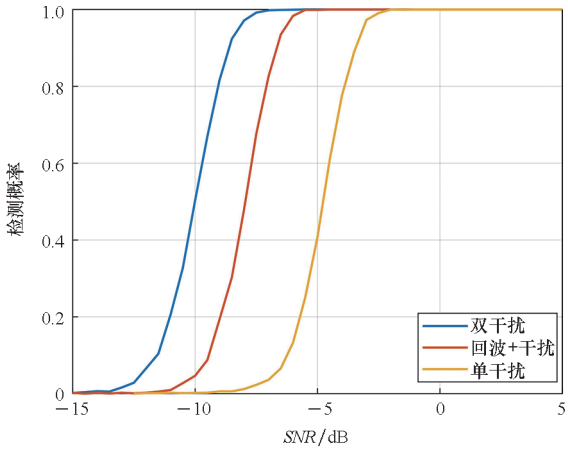


图 10 $M=2$ 时针对波门内不同情况的检测性能分析

Fig. 10 Analysis of detection performance for different situations in the wave gate when $M=2$

的功率也会下降,伪项受噪声的影响会更大,易造成伪项的时频特征难以提取,从而造成检测性能的下降。

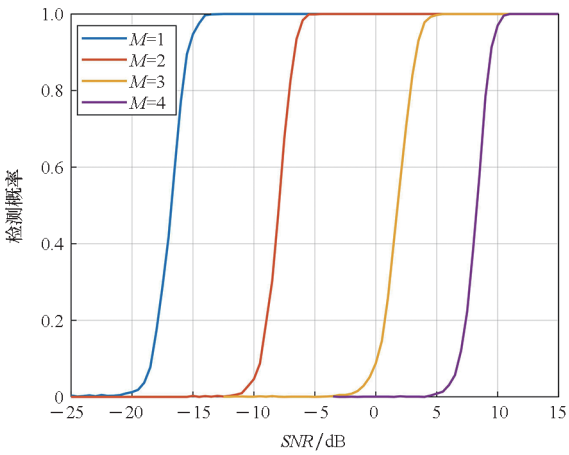


图 11 不同 M 时检测性能对比

Fig. 11 Comparison of detection performance under different M

4 结论

针对传统能量检测器和二元干扰检测器仅适用于干扰及回波同时存在的情况,以及“停 - 发模式”检测无法满足实时性等问题,本文分析了基于 DRFM 干扰的谐波特征,利用短时傅里叶变换和二维 CFAR 检测对谐波特征进行提取,最后利用 Hough 变换进行干扰检测。仿真实验表明:本文方法能够在低信噪比的情况下,针对波门中可能出现的如同时存在干扰和真实回波、仅存在一个欺骗干扰、同时存在一个以上的干扰等情况,做出正确的应答,在更贴近真实的应用环境下有效实现干扰检测。

参考文献(References)

[1] LAN L, LIAO G S, XU J W, et al. Mainlobe deceptive jammer suppression using element-pulse coding with MIMO radar[J]. Signal Processing, 2021, 182: 107955.

[2] XIA D P, ZHANG L, WU T, et al. A mainlobe interference suppression algorithm based on bistatic airborne radar cooperation[C]//Proceedings of the IEEE Radar Conference (RadarConf), 2019: 1 - 6.

[3] HILL P C J, TRUFFERT V. Statistical processing techniques for detecting DRFM repeat-jam radar signals [C]//IEE Colloquium on Signal Processing Techniques for Electronic Warfare, 1992.

[4] GRECO M, GINI F, FARINA A. Radar detection and classification of jamming signals belonging to a cone class[J]. IEEE Transactions on Signal Processing, 2008, 56(5): 1984 - 1993.

[5] 孙闽红, 唐斌. 距离 - 速度同步拖引欺骗干扰的频谱特征分析[J]. 系统工程与电子技术, 2009, 31(1): 83 - 85.
SUN M H, TANG B. Analysis of the frequency spectrum of a simultaneous range-gate-pull-off and velocity-gate-pull-off jamming signal[J]. Systems Engineering and Electronics, 2009, 31(1): 83 - 85. (in Chinese)

[6] YANG X W, LU D W, ZHANG J, et al. Radar jamming detection based on approximate entropy and moving-cut approximate entropy[C]// Proceedings of IET International Conference on Information Science and Control Engineering, 2012.

[7] 定少浒, 汤建龙. 基于 SSA 的 DRFM 速度欺骗干扰识别[J]. 雷达科学与技术, 2020, 18(1): 44 - 50.
DING S H, TANG J L. DRFM velocity deception jamming recognition based on singular spectrum analysis[J]. Radar Science and Technology, 2020, 18(1): 44 - 50. (in Chinese)

[8] 卢云龙, 李明, 闫琰. 利用调频率匹配的 DRFM 欺骗干扰检测方法[J]. 西安电子科技大学学报, 2014, 41(5): 67 - 73, 134.
LU Y L, LI M, YAN Y. Method for detecting DRFM deception jamming based on LFM rate matching[J]. Journal of Xidian University, 2014, 41(5): 67 - 73, 134. (in Chinese)

[9] GRECO M, GINI F, FARINA A. Radar detection and classification of jamming signals belonging to a cone class[J]. IEEE Transactions on Signal Processing, 2008, 56(5): 1984 - 1993.

[10] 陈杨, 石晶, 刘丛浩. 基于改进霍夫变换的车道线识别算法[J]. 汽车实用技术, 2021, 46(6): 42 - 44.
CHEN Y, SHI J, LIU C H. Lane recognition algorithm based on improved hough transform [J]. Automobile Applied Technology, 2021, 46(6): 42 - 44. (in Chinese)

[11] BERGER S D. The spectrum of a digital radio frequency memory linear range gate stealer electronic attack signal[C]// Proceedings of the IEEE Radar Conference, 2001.

[12] BERGER S D. Digital radio frequency memory linear range gate stealer spectrum[J]. IEEE Transactions on Aerospace Electronic Systems, 2003, 39(2): 725 - 735.

[13] 徐会法, 刘锋. 线性调频信号分数阶频谱特征分析[J]. 信号处理, 2010, 26(12): 1896 - 1901.

XU H F, LIU F. Spectrum characteristic analysis of linear frequency-modulated signal in the fractional Fourier domain[J]. Journal of Signal Processing, 2010, 26(12): 1896 – 1901. (in Chinese)

[14] JIANG J, LIU F, HU C. Design and realization of FPGA-based DRFM with high instantaneous bandwidth [C]// Proceedings of the IEEE 15th International Conference on Electronic Measurement & Instruments, 2021: 233 – 239.

[15] ZHAO Y J, TIAN B, WANG C Y, et al. Research on main-lobe deceptive jamming against FDA-MIMO radar[J]. IET Radar, Sonar & Navigation, 2021, 15(6): 641 – 654.

[16] BANDIERA F, FARINA A, ORLANDO D, et al. Detection algorithms to discriminate between radar targets and ECM signals[J]. IEEE Transactions on Signal Processing, 2010, 58(12): 5984 – 5993.

[17] GAO J N, WANG M, CHEN L B, et al. DRFM jamming mode identification leveraging deep neural networks[C]// Proceedings of the International Conference on Control, Automation and Information Sciences, 2021: 444 – 449.

[18] NOURI M, MIVEHCHY M. Velocity deception jamming discrimination using quantization effect[J]. Analog Integrated Circuits and Signal Processing, 2019, 100: 193 – 198.

[19] LU Y L, LI S Y. CFAR detection of DRFM deception jamming based on singular spectrum analysis [C]// Proceedings of the IEEE International Conference on Signal Processing, Communications and Computing, 2017: 1 – 6.

[20] QU Q Z, WEI S J, LIU S, et al. JRNet: jamming recognition networks for radar compound suppression jamming signals[J]. IEEE Transactions on Vehicular Technology, 2020, 69(12): 15035 – 15045.

[21] 曹兰英, 罗美方, 吴健. 基于信息论的脉冲压缩雷达 DRFM 干扰检测技术[J]. 太赫兹科学与电子信息学报, 2018, 16(3): 431 – 435.
CAO L Y, LUO M F, WU J. Detection of DRFM jamming for pulse compression radar based on information theory[J]. Journal of Terahertz Science and Electronic Information Technology, 2018, 16(3): 431 – 435. (in Chinese)

[22] 王奇伟, 孙闽红, 简志华, 等. 基于多模态小样本学习的雷达欺骗干扰识别[J]. 杭州电子科技大学学报(自然科学版), 2022, 18(1): 28 – 33, 102.
WANG Q W, SUN M H, JIAN Z H, et al. Deception jamming recognition based on multimodal and few-shot learning[J]. Journal of Hangzhou Dianzi University (Natural Sciences), 2022, 18(1): 28 – 33, 102. (in Chinese)

(编辑: 梁慧, 杨琴)