

## 基于奇异谱分析的抗数字射频存储距离波门拖引干扰

卢云龙\* 李明 陈洪猛 王泽玉 左磊

(西安电子科技大学雷达信号处理国家重点实验室 西安 710071)

**摘要:** 针对基于数字射频存储(DRFM)技术的转发式欺骗干扰难以检测和抑制问题, 该文根据 DRFM 的延时量化会导致干扰信号产生细微的中心频率频移及谐波分量寄生的特性, 提出一种基于奇异谱分析(SSA)的抗距离波门拖引干扰方法。该方法首先提取干扰信号谐波分量与目标回波经 SSA 分解后奇异值能量的分布差异特征, 实现对有源欺骗干扰的检测, 然后依据干扰中心频率频移特性, 通过划分合适的奇异值子空间重构目标信号, 实现对欺骗干扰的抑制。该方法不需要估计噪声参数, 在干扰检测阶段具有恒虚警特性。Monte Carlo 仿真结果验证了该方法的有效性。

**关键词:** 抗干扰; 距离波门拖引干扰; 奇异谱分析; 延时量化

**中图分类号:** TN974

**文献标识码:** A

**文章编号:** 1009-5896(2016)03-0600-07

**DOI:** 10.11999/JEIT150550

## Countering DRFM Range Gate Pull-off Jamming Based on Singular Spectrum Analysis

LU Yunlong Li Ming CHEN Hongmeng WANG Zeyu ZUO Lei

(National Laboratory of Radar Signal Processing, Xidian University, Xi'an 710071, China)

**Abstract:** Countering the active deception jamming which is repeated by a Digital Radio Frequency Memory (DRFM) has been a challenging problem. Utilizing the characteristics that the Range Gate Pull Off (RGPO) jamming has a slightly different center frequency from the input radar signal and evenly spaced harmonics, a novel anti-jamming approach is proposed based on Singular Spectrum Analysis (SSA). First, the singular values energy distribution diversity between jamming harmonics and target echo, which are pretreated through SSA decomposition, is extracted for jamming detection. Then according to the center frequency diversity, a suitable subspace of singular values is divided for recovering the target echo, which means the jamming is mitigated simultaneously. The proposed approach does not need to estimate noise parameter, and has the precious property of a Constant False-Alarm Rate (CFAR) in the jamming detection stage. The validity of the proposed method is evaluated using experimental data via Monte Carlo simulation.

**Key words:** Anti-jamming; Range Gate Pull Off (RGPO) jamming; Singular Spectrum Analysis (SSA); Time delay quantization

### 1 引言

有源欺骗干扰严重降低雷达对目标的检测性能。其中基于数字射频存储(DRFM)技术的干扰机对截获的雷达脉冲信号进行采样和存储, 精确复制雷达信号脉内特征, 通过特定的调制规律转发截获的雷达信号, 产生具有距离欺骗、速度欺骗及角度欺骗等特性的转发式干扰, 达到需要的欺骗目的。

因干扰机转发的欺骗信号与雷达发射信号高度相干, 从而进入雷达接收机的干扰信号能够获得与真实目标回波相当的处理增益, 使得雷达难以鉴别及抑制干扰<sup>[1,2]</sup>。

对抗欺骗式干扰的前提是检测雷达系统是否受到了干扰, 然后再采取相应的对抗措施。从干扰机角度出发, 文献[3,4]利用 DRFM 相位量化特性, 基于自适应相干估计子与广义极大似然比检测, 提出一种针对 DRFM 转发式欺骗干扰信号的检测方法。该方法只考虑了距离/速度波门内只有目标或干扰的情形, 而实际环境中干扰与目标往往伴随进入雷达接收机, 同时在高相位量化位数条件下, 该方法性能急剧下降甚至失效。文献[5]通过研究线性调制干扰信号的频谱分布特性, 提出基于调频率参数匹

收稿日期: 2015-05-11; 改回日期: 2015-09-11; 网络出版: 2015-11-18

\*通信作者: 卢云龙 yllu@stu.xidian.edu.cn

基金项目: 国家自然科学基金(61271297, 61272281, 61301284), 博士学科点科研专项基金(20110203110001)

Foundation Items: The National Natural Science Foundation of China (61271297, 61272281, 61301284), The Specialized Research Fund for the Doctoral Program of Higher Education (20110203110001)

配的干扰检测方法，但在高相位量化位数时同样存在方法失效的问题。文献[6]分析了距离-速度同步拖引干扰信号的频谱特性，提取出其在频域的细微特征，但并没有给出具体的干扰识别方法。在已知干扰信号存在的前提下，文献[7]设计自适应滤波器从时频解耦后的信号中估计干扰信号，通过干扰信号对消实现干扰抑制，并没有涉及干扰的检测问题。在信号发射端，文献[8,9]基于脉冲分集理论，在脉冲重复期间改变或调整发射信号或其参数，可以有效对抗转发式干扰，但其对发射波形有很高的要求，会增加系统的复杂度。有学者引入极化信息处理、空时自适应信号处理等理论，对于在复杂环境中分离干扰、提取目标信息和提高雷达抗干扰性能等方面，提供了很好的思路和方法。比如文献[10,11]给出了目标与干扰在极化雷达中的数学模型，利用两者在极化散射矩阵上的差异，实现对抗有源欺骗干扰。文献[12,13]提出空时自适应广义旁瓣相消的抗干扰方法，但其需要足够多的训练样本来估计干扰信号。有学者提出通过构建干扰信号的2维分布信息矩阵，将图像处理中的纹理特征引入到对干扰信号的识别算法中，该方法能有效识别欺骗干扰类型，但其没有给出干扰的抑制方法<sup>[14]</sup>。

文献[15,16]指出，DRFM 延时量化会导致干扰信号产生细微的中心频率频移及谐波分量的寄生，而该特性在分析干扰信号特征时往往被忽略<sup>[3-5]</sup>。本文利用干扰机的延时量化特性，在信号处理层面提出了一种基于奇异谱分析的抗距离波门拖引干扰方法。该方法包括干扰的检测和干扰的抑制两部分。由于干扰信号谐波分量的寄生，导致干扰经 SSA 分解后其奇异值分布与信号的奇异值分布存在差异，通过提取真实目标和干扰信号在变换域奇异值的能量分布特性差异，构造特征参数集，实现干扰信号的恒虚警检测。干扰信号相对目标回波存在细微的中心频率频移，因此通过划分合适的奇异值子空间，SSA 算法能够有效重构目标信号，实现干扰的抑制。

## 2 干扰特性分析

不失一般性，以脉冲多普勒(PD)雷达为例，令雷达发射信号为

$$s(t) = \sum_{n=-\infty}^{\infty} p_{\tau}(t - nT_r) e^{j2\pi f_0 t},$$

$$p_{\tau}(t) = \begin{cases} 1, & -\tau/2 < t < \tau/2 \\ 0, & \text{其他} \end{cases} \quad (1)$$

式中  $p_{\tau}$  是脉冲周期为  $T_r$ ，脉宽为  $\tau$  的基带脉冲串， $f_0$  为雷达发射频率。

干扰机接收信号的时域表达式为

$$x(t) = p(t) e^{j2\pi f_t t}, p(t) = p_{\tau}(t) \otimes \sum_{n=-\infty}^{\infty} \delta(t - nT_r) \quad (2)$$

式中  $\otimes$  表示卷积运算，其中  $f_t = f_0 + f_d$ ， $f_d$  为目标多普勒频率。

DRFM 距离欺骗干扰为干扰机对接收到的信号加以延时调制并转发，其时域表达式为

$$y(t) = x(t - c(t))$$

$$= \left( p_{\tau}(t) \otimes \sum_{n=-\infty}^{\infty} \delta(t - nT_r - c(t)) \right) e^{j2\pi f_t (t - c(t))} \quad (3)$$

受波门拖引速度限制，欺骗目标在一个 PD 雷达的相关处理间隔内的移动距离不会超过一个脉冲宽度。相比于  $T_r$ ，式(3)中的  $c(t)$  一般很小，用  $\delta(t - nT_r)$  近似表示  $\delta(t - nT_r - c(t))$  可得

$$y(t) \approx \left( p_{\tau}(t) \otimes \sum_{n=-\infty}^{\infty} \delta(t - nT_r) \right) e^{j2\pi f_t (t - c(t))}$$

$$= p(t) \cdot e^{j2\pi f_t t} \cdot e^{-j2\pi f_t c(t)} \quad (4)$$

则在雷达距离门内同时存在目标回波和干扰的情形下，雷达接收信号可表示为

$$z(t) = A_1 p(t) e^{j2\pi f_t t} + A_2 p(t) e^{j2\pi f_t t} e^{-j2\pi f_t c(t)} + n(t) \quad (5)$$

式(5)右边第1项为目标回波，第2项为欺骗干扰， $n(t)$  为高斯白噪声， $A_1, A_2$  表示幅度，通常有  $A_1 < A_2$ 。

通过式(5)可以看出，除了幅度大小差异外，目标信号与干扰信号的唯一差异在于  $e^{-j2\pi f_t c(t)}$ 。以线性拖引为例，理想的 DRFM 时延调制函数  $c(t) = \alpha t$ ，其中  $\alpha$  为拖引率。由于干扰机的数字化特性，真实的时延函数  $c(t) = \beta \sum_{n=-\infty}^{\infty} n p_{T_c}(t - nT_c - T_c/2)$ ， $\beta, T_c$  分别为时延分辨率和时延更新周期<sup>[15]</sup>。这使得干扰机系统在产生距离欺骗干扰信号时，只能在离散的时间间隔上(DRFM 时延更新周期  $T_c$ )对接收脉冲以离散的步长(DRFM 时延分辨率  $\beta$ )加以时延，这一离散特性使得干扰信号产生细微的中心频率频移和谐波分量的寄生。这里不讨论 ADC 量化产生的谐波影响。

设  $b(t) = e^{-j2\pi f_t c(t)}$ ，将时延函数  $c(t)$  代入可得

$$b(t) = \sum_{n=-\infty}^{\infty} p_{T_c}(t - nT_c - T_c/2) e^{-j2\pi f_t \beta n}$$

$$= p_{T_c}(t - T_c/2) \otimes \left( e^{-j2\pi f_t \beta t / T_c} \sum_{n=-\infty}^{\infty} \delta(t - nT_c) \right) \quad (6)$$

令  $f_c = 1/T_c$ ，引用文献[15]的结论，有  $b(t)$  的频谱  $B(f)$ ：

$$B(f) = e^{-j\pi f / f_c} \frac{\sin(\pi f / f_c)}{\pi f / f_c} \left( \sum_{n=-\infty}^{\infty} \delta(f + \beta f_t f_c - n f_c) \right) \quad (7)$$

容易得到干扰信号频谱：

$$Y(f) = P(f) \otimes B(f - f_i) \\ = \left( \frac{\tau}{T_r} \sum_{m=-\infty}^{\infty} \frac{\sin(m\pi\tau f_r)}{m\pi\tau f_r} \right) \delta(f - mf_r) \otimes B(f - f_i) \quad (8)$$

式中  $P(f)$  为脉冲串  $p(t)$  的频谱, 不考虑  $P(f)$  的频谱延拓及幅度调制, 由前面分析可知, 干扰信号与目标信号在频域的差异在于  $B(f)$ 。从式(7), 式(8)可以得出, 相对于目标信号中心谱线  $f_i$ , 干扰频谱是由间隔为  $f_c$ , 中心在  $f_i - \beta f_i f_c$  处且幅度被中心频率在 0 Hz 的 sinc 函数加权的谱线组成。干扰信号的中心谱线为主分量, 其余谱线为谐波分量。干扰信号中心频率的频移及谐波分量的寄生分别为该类干扰的识别及抑制提供了理论依据。

### 3 基于奇异谱分析的抗干扰方法

当雷达受到 DRFM 距离波门拖引干扰时, 由于干扰信号功率大于目标信号功率, 接收机 AGC 会有一个上跳沿。但是, AGC 的突变有可能是由于目标的强机动等使得 RCS 产生很大变化引起的, 不能只通过 AGC 的突变来判断是否存在干扰。如果在一个雷达距离单元内存在两个或两个以上的目标时, 也会造成多个谱峰, 不能通过谱峰数量来识别干扰。由第 2 节的分析可知, DRFM 转发产生的欺骗干扰信号, 因其与雷达发射信号高度相干而难以用常规方法直接进行干扰检测及对抗。而 DRFM 的延时量化特性会导致干扰回波信号产生细微的中心频率频移和谐波分量的寄生, 因此在距离波门内同时存在目标回波与干扰回波的情形下, 雷达回波可视为多分量信号的叠加。对于多分量信号, 本文引入基于 SSA 的时间序列分析方法, 通过在变换域提取干扰信号与真实目标回波的特征差异, 实现干扰的检测, 再通过划分合适的子空间, 利用 SSA 算法重构目标信号, 在信号处理层面实现对抗有源欺骗干扰。

#### 3.1 SSA 算法原理

奇异谱分析是近年来广泛应用的一种时间序列分析方法<sup>[17-19]</sup>, 包括分解和重构两部分。该算法主要取决于两个因素: 分解过程中窗口长度选择, 重构过程中奇异值及其奇异向量的划分。

假设有长度为  $N$  的 1 维信号  $x = [x_1, x_2, \dots, x_N] \in \mathbb{R}^N$ , SSA 算法分以下几个步骤实现。

步骤 1 定义一个窗长  $L \in \mathbb{Z}$  满足  $L \in [1, N/2]$ , 对信号进行延迟坐标相空间重构, 构造信号  $x$  的迹矩阵(trajjectory matrix)  $\mathbf{X}$ :

$$\mathbf{X} = \begin{bmatrix} x_1 & x_2 & \cdots & x_K \\ x_2 & x_3 & \cdots & x_{K+1} \\ \vdots & \vdots & \ddots & \vdots \\ x_L & x_{L+1} & \cdots & x_N \end{bmatrix} = [\mathbf{X}_1, \mathbf{X}_2, \dots, \mathbf{X}_i] \quad (9)$$

其中  $\mathbf{X}_i = [x_i, x_{i+1}, \dots, x_{i+L-1}]^T \in \mathbb{R}^L, i = 1, 2, \dots, K$ , 这里  $K = N - L + 1$ 。可以看出矩阵  $\mathbf{X}$  为 Hankel 矩阵, 即矩阵元素  $a_{i,j}$  在  $i + j = \text{const}$  时都相等。

步骤 2 对矩阵  $\mathbf{Y} = \mathbf{X}\mathbf{X}^T$  进行 SVD 分解, 令矩阵  $\mathbf{Y}$  的特征值及其对应的特征向量分别为  $(\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_L)$  和  $(\mathbf{U}_1, \mathbf{U}_2, \dots, \mathbf{U}_L)$ , 则迹矩阵  $\mathbf{X}$  的奇异值分解可表示为

$$\mathbf{X} = \mathbf{P}_1 + \mathbf{P}_2 + \dots + \mathbf{P}_L \quad (10)$$

其中  $\mathbf{P}_i$  为基本矩阵(elementary matrix),  $\mathbf{P}_i = \sqrt{\lambda_i} \mathbf{U}_i \mathbf{V}_i^T, \mathbf{V}_i = \mathbf{X}^T \mathbf{U}_i / \sqrt{\lambda_i}$ 。  $\sqrt{\lambda_i}$  为迹矩阵  $\mathbf{X}$  的第  $i$  个奇异值,  $\mathbf{U}_i, \mathbf{V}_i$  分别为对应奇异值的左、右奇异向量。

步骤 3 将式(10)中的  $L$  个基本矩阵  $\mathbf{P}_i$  划分为  $M$  个互不相交的子集  $I_1, I_2, \dots, I_M, \sum |I_m| = L, m \in [1, M]$ , 这里  $M$  取决于具体的应用。令子集  $I = [i_1, i_2, \dots, i_p]$ , 则对应该子集的矩阵  $\mathbf{P}_I = \mathbf{P}_{i_1} + \mathbf{P}_{i_2} + \dots + \mathbf{P}_{i_p}$ , 最终迹矩阵  $\mathbf{X}$  可表示为

$$\mathbf{X} = \mathbf{P}_{I_1} + \mathbf{P}_{I_2} + \mathbf{P}_{I_m} + \dots + \mathbf{P}_{I_M} \quad (11)$$

步骤 4 为了得到原始时间序列中的源信号, 通过平均  $\mathbf{P}_{I_m}$  中的阵元实现, 这些阵元处在相同的反对角线上, 即阵元  $a_{ij}^{I_m}$  的下标  $i, j$  的和为常数。设  $z_m = [z_{m_1}, z_{m_2}, \dots, z_{m_N}] \in \mathbb{R}^N$  为从矩阵  $\mathbf{P}_{I_m}$  重构的长度为  $N$  的 1 维信号, 通过矩阵对角元素  $a_{j,n-j+1}$  的平均, 可以得到

$$z_m(n) = \begin{cases} \frac{1}{2} \sum_{j=1}^n a_{j,n-j+1}, & 1 \leq n \leq L \\ \frac{1}{L} \sum_{j=1}^L a_{j,n-j+1}, & L < n < K \\ \frac{1}{N-n+1} \sum_{j=n-K+1}^L a_{j,n-j+1}, & K \leq n \leq N \end{cases} \quad (12)$$

则原始信号可重构为

$$x = z_1 + z_2 + \dots + z_M = \sum_{m=1}^M z_m \quad (13)$$

可以看出, SSA 算法先分解信号协方差矩阵, 再通过分析奇异值的差异组合不同的基本矩阵, 即选取感兴趣奇异值子空间来重构所需信号分量, 丢弃掉不需要的信号分量或噪声。

#### 3.2 干扰的检测及抑制

奇异值是矩阵的固有特征, 具有非常好的稳定性。对于点目标回波, 其为单分量信号, 经 SSA 分解后只有一个非零奇异值。而对于干扰信号而言, 由于谐波分量的寄生导致其为多分量信号, 经 SSA 分解后除一个较大的奇异值外, 还有部分对应于谐波分量的非零奇异值。当雷达距离波门内同时存在目标回波与干扰信号时, 干扰信号相对于目标信号

有细微的中心频率频移的特性使得干扰主分量与目标频率相互分离<sup>[20]</sup>，因此雷达回波经 SSA 分解后，有两个较大的奇异值，分别对应干扰信号主分量和目标信号，以及部分对应于干扰谐波分量的较小奇异值。

雷达接收信号经 SSA 分解后，利用奇异值分布的差异，构建合适的检验统计量，可以有效识别出干扰信号。设雷达接收回波序列  $F = F^{(1)} + F^{(2)} + F_n$ ， $F^{(1)}$  对应目标回波， $F^{(2)}$  对应欺骗干扰序列， $F_n$  为高斯白噪声序列，令其经 SSA 分解后的奇异值为  $\lambda_i$ ，且  $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_L$ 。目标回波分量和干扰主分量对应的奇异值远远大于谐波分量对应的奇异值，因此干扰谐波分量对应的奇异值将落于集合  $\phi = \{\lambda_i | i = 3, 4, \dots, q\}$  中， $q$  为谐波分量个数。对于目标回波，落于集合  $\phi = \{\lambda_i | i = 3, 4, \dots, q\}$  中的奇异值对应为部分噪声分量。在一定信噪比范围内，干扰信号落在集合  $\phi$  中的奇异值要大于目标信号落在集中  $\phi$  中的奇异值，利用干扰信号奇异值分布的这一特性，本文通过设计具有恒虚警特性的检验统计量，实现干扰的检测。根据雷达接收信号中是否含有欺骗干扰，雷达回波有两种假设：

$$\left. \begin{aligned} H_0: z(n) &= s(n) + w(n) \\ H_1: z(n) &= s(n) + j(n) + w(n) \end{aligned} \right\} \quad (14)$$

其中  $s(n)$  为目标信号， $j(n)$  为欺骗干扰， $w(n)$  为高斯白噪声。 $H_0$  表示雷达没有受到欺骗干扰， $H_1$  表示距离波门内同时存在目标信号与干扰信号。奇异值的大小与信号能量有关，直接利用落于集合  $\phi$  中的奇异值能量作为判决准则，检测门限将依赖于噪声方差大小。考虑提取奇异值的能量分布特性，设计不依赖于噪声参数的干扰检测统计量  $\xi$ ：

$$\xi = \frac{\sum_{i=3}^q \lambda_i}{\text{mean}\{\lambda_i | i = q+1, q+2, \dots, L\}} \quad (15)$$

参数  $q > 0$  且为整数，可以由奇异值的微分确定。事实上，参数  $q$  将奇异值划分为  $\Omega_1, \Omega_2$  两个集合，其中  $\Omega_1$  为谐波分量对应的奇异值， $\Omega_2$  为噪声对应的奇异值，因此统计量  $\xi$  表征两个集合奇异值能量比值的统计特性。令单位方差高斯白噪声  $n(t)$  的检验统计量为  $\xi|_n$ ，设  $h(t) = \alpha \cdot n(t)$ ，其中  $\alpha$  参数调整噪声  $h(t)$  的方差。根据第 3.1 小节中 SSA 算法，可得

$$\left. \begin{aligned} Y_n &= X_n X_n^T = X_n X_n^T = U \Lambda_n U \\ Y_h &= X_h X_h^T = \alpha^2 (X_n X_n^T) = \alpha^2 U \Lambda_n U \end{aligned} \right\} \quad (16)$$

进一步有式(17)关系：

$$\lambda_h = \text{diag}(\alpha^2 \Lambda_n) = \alpha^2 \text{diag}(\Lambda_n) = \alpha^2 \lambda_n \quad (17)$$

将式(17)代入式(15)可得

$$\begin{aligned} \xi|_h &= \frac{\sum_{i=1}^q \lambda_h(i)}{\text{mean}\{\lambda_h(i) | i = q+1, \dots, L\}} \\ &= \frac{\alpha^2 \sum_{i=1}^q \lambda_n(i)}{\alpha^2 \text{mean}\{\lambda_n(i) | i = q+1, \dots, L\}} = \xi|_n \quad (18) \end{aligned}$$

统计量  $\xi$  与噪声方差无关，具有恒虚警特性，因此可以利用单位方差高斯白噪声作为训练样本。令检测门限为  $\lambda_0$ ，给定虚警概率  $P_f$ ，则有

$$\int_{\lambda_0} p(\xi | H_0) d\xi = 1 - P_f \quad (19)$$

式(14)的干扰检测问题可由式(20)解决：

$$\xi|_z \begin{cases} > \lambda_0 \\ < \lambda_0 \end{cases} \begin{matrix} H_1 \\ H_0 \end{matrix} \quad (20)$$

在特征提取过程中，观测信号  $z(n)$  经过了一系列的变换处理，因而很难去求得式(19)中  $p(\xi | H_0)$  的闭式表达式。检验统计量  $\xi$  只与信号分解后的奇异值的分布集中程度有关，而与信号本身强度无关，因此本文采用 Monte Carlo 方法，利用单位方差的高斯白噪声训练样本来确定判决区域。集合  $\Theta = \{\xi_i, i = 1, 2, \dots, Q\}$  表示  $H_0$  假设下的训练样本， $Q$  为训练噪声样本数，并且  $QP_f \gg 1$ ，有

$$\frac{\text{num}(\xi_i < \lambda_0)}{Q} = \frac{QP_f}{Q} = P_f \quad (21)$$

式中  $\text{num}(\xi_i < \lambda_0)$  表示在集合  $\Theta$  中  $\xi_i < \lambda_0$  的个数。由式(21)得到在虚警概率  $P_f$  下的干扰检测门限  $\lambda_0$ 。

干扰机要成功地干扰敌方雷达系统，一般会发射比回波信号功率大得多的干扰信号。DRFM 转发的欺骗干扰与雷达发射信号高度相干，能获得与目标信号相近的处理增益，这会使得雷达接收波门内同时出现一个较强的干扰信号和一个较弱的目标信号，而雷达的跟踪波门会被较强的干扰信号捕获，导致雷达给出错误的距离信息，因此，雷达要成功地进行反干扰，需要分析干扰信号和目标回波信号特征的异同之处，然后滤除干扰信号，使得雷达跟踪波门能正确跟踪上真实的目标。由前面分析可知，不同的奇异值对应不同的信号分量，而雷达回波的主要信息对应于较大的第 1 第 2 奇异值分量。在基于 SSA 方法检测到干扰信号的前提下，利用干扰信号功率一般要比目标回波功率大的先验信息，在一定的干信比范围内，可以认为最大奇异值对应于干扰信号主分量信息，第 2 个奇异值对应于目标回波信息。因此选取第 2 个奇异值为目标信号的子空间，结合其对应的奇异向量，利用 SSA 算法重构目标信号，实现干扰的抑制。

这里不考虑谐波对应的奇异值超过目标的极端情况。首先这需要很高的干信比，对干扰机发射功

率要求很高, 比较难达到。其次, 信号能量的激变容易导致敌方探测到战场的异常。图 1 为抗干扰算法流程图。

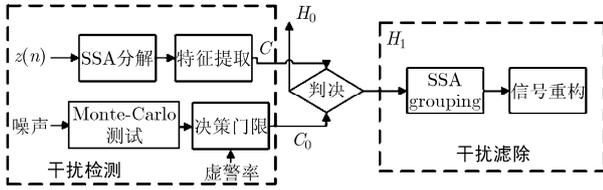


图 1 抗干扰算法流程图

#### 4 实验结果与分析

仿真实验参数如下: 雷达工作于 X 波段, 中心频率为 9.655 GHz。雷达发射信号为脉冲宽度为 1  $\mu$ s, 脉冲重复频率为 10 kHz 的单载波脉冲信号。雷达相干处理间隔(CPI)为 102.4 ms, 样本数为 1024。设有一点目标初始位置位于雷达 30 km 处, 该目标上的自卫式干扰机对雷达系统施加距离欺骗干扰。干扰机的参数设置同文献[11], 令 DRFM 的时延分辨率为 4.44 ns, 更新周期为 4.5 ms, 拖引率  $\alpha=1 \times 10^{-6}$ 。定义信噪比为  $SNR = |s(t)|^2 / |n(t)|^2$ , 干信比为  $JSR = |j(t)|^2 / |s(t)|^2$ ,  $j(t)$  为干扰信号, 强度一般为目标信号  $s(t)$  的 1.3~1.5 倍。 $n(t)$  为服从  $n \sim N(0, \sigma_n^2)$  分布的零均值复高斯白噪声。

图 2 给出了仅有目标信号情形下雷达回波经 SSA 分解后其所有奇异值按幅值降序排列后的分布, 图 3 为雷达回波中同时存在目标信号与干扰信号时的奇异值分布, 其中 SNR 为 5 dB, JSR 为 3.52 dB, SSA 分解窗长为 256。从图 2 中可以看出, 第 1 个奇异值  $\lambda_1 = 789.7$  远大于次大奇异值  $\lambda_2 = 49.9$ , 其对应着目标信号信息, 而其余奇异值则对应着噪声信息。而在图 3 中, 前两个奇异值  $\lambda_1 = 1158.9, \lambda_2 = 741.1$  明显大于其他奇异值。前面已分析, 在距离波门内新出现一个目标也会导致信号分解后有两个较大奇异值的产生, 因此不能将前两个奇异值的差异作为鉴别干扰存在的依据。图 4 为部分奇异值  $\phi = \{\lambda_i | i = 3, 4, \dots, q\}$  的分布, 这里  $q$  可以由奇异值的微分得到, 确

保干扰谐波分量对应的奇异值将落于集合  $\phi$  中, 试验中取  $q = 22$ 。从图 4 中可以看出, 当只有目标信号时, 该区间的奇异值相对较小, 对应着噪声信息。当欺骗干扰存在时, 该区间的奇异值明显要大于没有干扰时的奇异值分布, 其对应着干扰谐波分量信息。通过提取雷达回波中有无干扰时奇异值的能量分布差异, 可以有效实现欺骗干扰的检测。图 5 给出了在虚警率  $P_f = 0.001$ , 1000 次 Monte Carlo 试验下不同窗长  $L$  对应的欺骗干扰检测曲线。可以看出 SSA 的分解窗长影响对干扰的检测性能,  $L = 500$  对应的检测性能要优于  $L = 100$  的检测性能。窗长  $L$  越大, 每个数据段包含的信息越多, SSA 分解效果越好, 但大的窗长计算量明显增加。因此在应用中, 需要权衡干扰检测实时性与干扰检测性能之间的关系。

在检测到欺骗干扰的前提下, 利用干扰信号的功率比目标信号的功率要大的先验信息, 能够得到干扰主分量对应着最大的奇异值, 而第 2 个奇异值表征目标信号分量, 其余奇异值包含着干扰谐波分量及噪声信息。通过信号所在的奇异值子空间重构目标信号, 提取真实目标信号分量, 抑制欺骗干扰。图 6 给出了 SNR 为 5 dB, JSR 为 3.52 dB,  $L = 300$  条件下欺骗干扰抑制前后雷达回波信号的频谱。可以看出该方法保留了真实目标的信息, 不仅有效地抑制了干扰, 还有一定的降噪效果。引入雷达抗干扰改善因子来衡量该文所提方法的抗干扰性能, 即雷达采用抗干扰措施时系统输出的信干比与未采用抗干扰措施时系统输出的信干比的比值。实际场景中, 在施加有源欺骗干扰时, 一般信噪比较高, 本文分析在 SNR 为 5 dB, 不同干信比条件下的抗干扰改善因子。图 7 给出了干信比从 3~15 dB 时, 不同窗长条件下对应的抗干扰性能曲线。从图 7 中可以看出, 不同的 SSA 分解窗长对干扰的抑制性能影响比较明显, 较大的分解窗长因其每个数据段包含的信息量大, 导致其有比较理想的干扰抑制性能, 但同时需要较大的运算量, 因此在实际应用中需要折中考虑干扰抑制性能与运算效率问题。

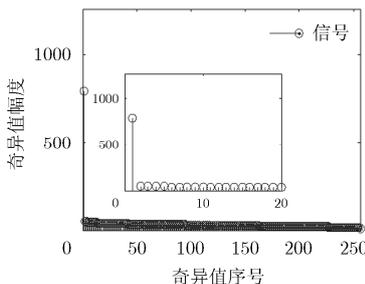


图 2 没干扰时的奇异值分布

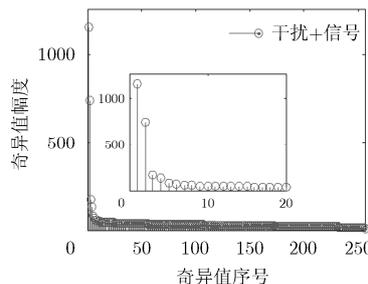


图 3 有干扰时的奇异值分布

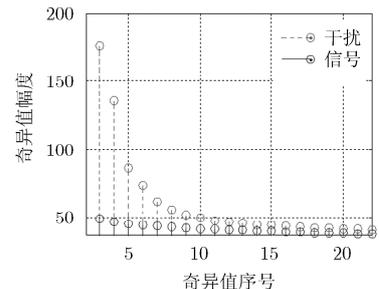


图 4 部分奇异值分布对比

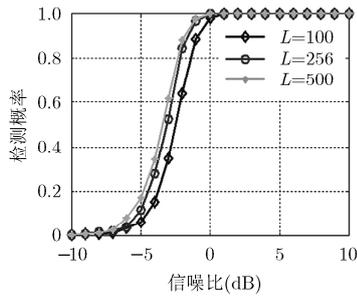


图5 干扰检测性能曲线

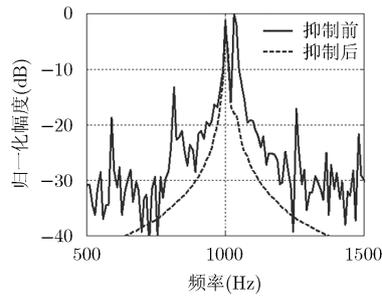


图6 干扰抑制前后频谱

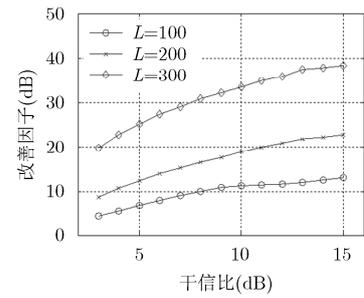


图7 干扰抑制性能曲线

## 5 结束语

有源欺骗干扰因其与雷达发射信号高度相干而难以检测及抑制，本文利用 DRFM 转发式欺骗干扰经延时量化后导致中心频谱频移和谐波分量寄生的细微特性，提出了一种基于时间序列分析方法的抗干扰策略。利用干扰信号在 SSA 变换域的奇异值分布特性，该方法能在信号处理层面有效地检测并且抑制干扰。在干扰检测阶段，由于该方法不依赖于环境噪声参数，具有恒虚警特性。本文方法能有效对抗距离欺骗干扰，在后继工作中，应该考虑联合欺骗干扰的运动特性、微动特性等多维特征对抗其他复杂的欺骗干扰。

## 参考文献

- [1] 刘维建, 谢文冲, 王永良. 部分均匀环境中存在干扰时机载雷达广义似然比检测[J]. 电子与信息学报, 2013, 35(8): 1820-1826. doi: 10.3724/SP.J.1146.2012.01492.  
LIU Weijian, XIE Wencong, and WANG Yongliang. Generalized likelihood ratio test for airborne radar with jamming in partially homogeneous environments[J]. *Journal of Electronics & Information Technology*, 2013, 35(8): 1820-1826. doi: 10.3724/SP.J.1146.2012.01492.
- [2] 李迎春, 王国宏, 关成斌, 等. 速度拖引干扰和杂波背景下脉冲多普勒雷达目标跟踪算法[J]. 电子与信息学报, 2015, 37(4): 989-994. doi: 10.11999/JEIT140856.  
LI Yingchun, WANG Guohong, GUAN Chengbin, et al. Algorithm for target tracking with pulse Doppler radar in the presence of velocity gate pull off jamming and clutter environment[J]. *Journal of Electronics & Information Technology*, 2015, 37(4): 989-994. doi: 10.11999/JEIT140856.
- [3] 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.
- [4] GRECO M, GINI F, and 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] 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.  
LU Yunlong, LI Ming, and YAN Yan. Method for detecting DRFM deception jamming based on LFM rate matching[J]. *Journal of Xidian University*, 2014, 41(5): 67-73.
- [6] 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 Minhong and TANG Bin. 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.
- [7] 卢刚, 唐斌, 罗双才. LFM 雷达中 DRFM 假目标自适应抵消方法[J]. 系统工程与电子技术, 2011, 33(8): 1760-1764.  
LU Gang, TANG Bin, and LUO Shuangcai. Adaptive cancellation of DRFM false targets for LFM radar[J]. *Systems Engineering and Electronics*, 2011, 33(8): 1760-1764.
- [8] AKHTAR J. Orthogonal block coded ECCM schemes against repeat radar jammers[J]. *IEEE Transactions on Aerospace and Electronic Systems*, 2009, 45(3): 725-735.
- [9] ZHANG Jindong, ZHU Daiyin, and ZHANG Gong. New antivelocity deception jamming technique using pulses with adaptive initial phase[J]. *IEEE Transactions on Aerospace and Electronic Systems*, 2013, 49(2): 1290-1300.
- [10] 施龙飞, 王雪松, 肖顺平. 转发式假目标干扰的极化鉴别[J]. 中国科学 F 辑, 2009, 39(4): 468-475.  
SHI Longfei, WANG Xuesong, and XIAO Shunping. Repeater jamming detection based on polarimetric informations[J]. *China Science F*, 2009, 39(4): 468-475.
- [11] 李永祯, 胡万秋, 陈思伟, 等. 有源转发式干扰的全极化单脉冲雷达抑制方法研究[J]. 电子与信息学报, 2015, 37(2): 276-282. doi: 10.11999/JEIT140146.  
LI Yongzhen, HU Wanqiu, CHEN Siwei, et al. Active repeater jamming suppression using polarimetric monopulse radar[J]. *Journal of Electronics & Information Technology*, 2015, 37(2): 276-282. doi: 10.11999/JEIT140146.
- [12] 吴亿锋, 王彤, 吴建新, 等. 基于广义旁瓣相消的机载雷达抗密集转发式干扰方法[J]. 电子与信息学报, 2014, 36(5): 1049-1054. doi: 10.3724/SP.J.1146.2013.01040.

- WU Yifeng, WANG Tong, WU Jianxin, *et al.* A method to suppress dense repeater jamming for airborne radar based on generalized sidelobe canceller[J]. *Journal of Electronics & Information Technology*, 2014, 36(5): 1049–1054. doi: 10.3724/SP.J.1146.2013.01040.
- [13] 同亚龙, 王彤, 代保全, 等. 一种抗密集欺骗式干扰的机载雷达动目标检测方法[J]. *电子与信息学报*, 2015, 37(3): 658–664. doi: 10.11999/JEIT140679.
- TONG Yalong, WANG Tong, DAI Baoquan, *et al.* A moving target detection method to suppress dense deception jamming for airborne radar[J]. *Journal of Electronics & Information Technology*, 2015, 37(3): 658–664. doi: 10.11999/JEIT140679.
- [14] TIAN Xiao and TANG Bin. Spectrum texture features based radar deception jamming recognition using joint frequency-slow time processing[J]. *Journal of Computational Information Systems*, 2013, 9(13): 5181–5188.
- [15] BERGER S D. Digital radio frequency memory linear range gate stealer spectrum[J]. *IEEE Transactions on Aerospace and Electronic Systems*, 2003, 39(2): 725–735.
- [16] 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, Atlanta, 2001: 27–30.
- [17] JAIME Z, REN Jinchang, WANG Zheng, *et al.* Singular spectrum analysis for effective feature extraction in hyperspectral imaging[J]. *IEEE Geoscience and Remote Sensing Letters*, 2014, 11(11): 1886–1890.
- [18] 陈希信, 黄银河. 基于矩阵奇异值分解的高频雷达瞬态干扰抑制[J]. *电子与信息学报*, 2005, 27(12): 1879–1882.
- CHEN Xixin and HUANG Yinhe. A SVD-based approach of suppressing transient interference in high-frequency radar[J]. *Journal of Electronics & Information Technology*, 2005, 27(12): 1879–1882.
- [19] KRISHNA E H, SIVANI K, and REDDY K A. On the use of singular spectrum analysis for OFDM channel estimation[C]. International Conference on Electronics and Communication System (ICECS), Coimbatore, 2014: 1–4.
- [20] CLEMENTE C and SORAGHAN J. Application of the singular spectrum analysis for extraction of micro-doppler signature of helicopters[C]. IET International Conference on Radar Systems (Radar 2012), Glasgow, 2012: 1–5.
- 卢云龙: 男, 1986 年生, 博士生, 研究方向为抗干扰、雷达目标检测.
- 李明: 男, 1965 年生, 博士, 教授, 博士生导师, 从事雷达图像处理与分析、宽带信号处理与微弱目标检测、高速并行信号处理、高性能 DSP 应用系统设计、雷达抗干扰技术等.
- 陈洪猛: 男, 1986 年生, 博士, 研究方向为雷达成像、目标检测.
- 王泽玉: 女, 1990 年生, 博士, 研究方向为微弱目标检测.
- 左 磊: 男, 1984 年生, 博士, 研究方向为时频分析与合成、雷达海杂波抑制、目标检测.