

对频率步进毫米波导引头干扰技术研究

项正山

(桂林长海发展有限责任公司,广西 桂林 541001)

摘要: 针对频率步进毫米波精确制导武器如何实施有效对抗问题,在分析频率步进毫米波导引头二维成像工作原理基础上,构建了导引头二维成像场景,对频率步进毫米波导引头成像处理以及多种干扰样式进行了系统全面仿真。仿真结果表明,不论干扰源是否位于导引头天线波束覆盖范围内,采用非相参干扰和相参干扰都可对毫米波导引头实现干扰,非相参干扰能量较为分散,相参干扰能量较为集中。据此,提出了逆增益和有源干扰的复合干扰策略,在实现频率步进毫米波导引头干扰的同时,可同步实现干扰源自身防护。

关键词: 频率步进;毫米波导引头;噪声调频;相参干扰

中图分类号: TN95

文献标识码: A

DOI:10.16157/j.issn.0258-7998.201002

中文引用格式: 项正山. 对频率步进毫米波导引头干扰技术研究[J]. 电子技术应用, 2021, 47(4): 137-144.

英文引用格式: Xiang Zhengshan. Research on jamming technology of frequency-stepping millimeter-wave guided seeker[J]. Application of Electronic Technique, 2021, 47(4): 137-144.

Research on jamming technology of frequency-stepping millimeter-wave guided seeker

Xiang Zhengshan

(Guilin Changhai Development Co., Ltd., Guilin 541001, China)

Abstract: Aiming at the problem of how to implement effective countermeasures against frequency-stepping millimeter-wave precision guided weapons, this paper analyzes the working principle of two-dimensional imaging of frequency-stepping millimeter-wave guided seekers, constructs the two-dimensional imaging scene of frequency-stepping millimeter-wave guided seekers, and carries out systematic and comprehensive simulation on imaging processing of frequency-stepping millimeter-wave guided seekers and various jamming techniques. The simulation results show that no matter whether the jamming source is located in the range of antenna beam coverage of the seeker or not, both incoherent and coherent jamming can jam frequency-stepping millimeter-wave guided seekers. The energy of incoherent jamming is more dispersed, and the energy of coherent jamming is more concentrated. Therefore, a compound jamming strategy of inverse gain and active jamming is proposed in this paper, which can realize jamming of frequency-stepping millimeter-wave guided seeker and simultaneously realize self-protection of the jamming source.

Key word: frequency-stepping; millimeter-wave guided seeker; noise modulation; coherent jamming

0 引言

毫米波器件技术突破和毫米波器件成本逐渐降低,使得毫米波技术得到快速发展与广泛应用,其中,毫米波精确制导是毫米波技术应用的一个重要方向,相对于红外和光学波段,毫米波适应复杂战场环境和恶劣气象条件能力更强;相对于微波波段,毫米波结构尺寸小,易实现超大带宽、系统复杂性低、易于工程实现^[1-2],具有分辨率高和抗有源、无源干扰能力强等优点,安装有毫米波制导的精确制导武器具有全天候的作战能力^[3-4]。

现代电子战中,毫米波电子对抗技术已引起世界各国的重视^[5],毫米波制导对抗包括有源对抗和无源对抗两种手段,无源对抗技术研究相对较多,产品应用也较为成熟^[6]。在频率步进导引头(或雷达)一维成像干扰研究方面,2010年,张宏伟等人^[7]给出了频率步进毫米波

导引头的一维成像定性干扰技术研究,2016年,谭铭等人^[1]开展了频率步进雷达一维成像的干扰技术研究,并给出了干扰效能分析。在频率步进毫米波导引头二维成像干扰方面研究较少,因此,研究对毫米波导引头二维成像干扰技术是十分必要的。

本文系统分析了频率步进毫米波导引头二维成像的工作原理,在构建毫米波导引头对地探测几何模型和二维成像处理模型基础上,基于瞄频非相参干扰和数字射频存储器(Digital Radio Frequency Memory, DRFM)技术相参干扰技术,对频率步进毫米波导引头成像性能进行了仿真,对干扰效果进行了系统全面分析,并提出逆增益和有源干扰的复合干扰策略,此方法可有效规避导引头跟踪干扰强点,实现干扰源自身防护,是频率步进毫米波导引头的一个有效干扰方法。利用DRFM技术产

生的相参干扰能通过雷达的相关处理,获得更高的增益,提高了干扰利用效率^[8-12]。

1 频率步进雷达信号二维成像工作原理

毫米波精确制导武器在对地目标实施精确打击主要包括目标搜索、目标检测(或截获)、目标跟踪和寻的三个步骤。毫米波精确制导武器对地实施精确打击过程示意图如图1所示^[13-14]。

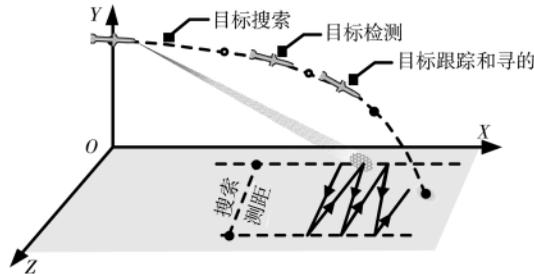


图1 毫米波精确制导武器对地实施精确打击过程示意图

毫米波导引头在建立目标跟踪和寻的之前,导引头通常对给定空域(方位、俯仰、距离等)范围内进行目标搜索。当毫米波导引头检测分辨单元(天线波束、距离波门、速度门等)搜索到目标并且目标回波能量超过导引头设定的检测门限时,称目标被“截获”。

获取一维或二维地面目标成像是毫米波导引头对地目标实施精确打击的前提,利用 Chirp-z 处理步进频率信号可以改善距离分辨性能^[15],因此,在体积、重量等受限条件下,毫米波导引头为实现对地目标的成像,通常采用步进频信号工作方式,步进频发射信号示意图如图2所示。

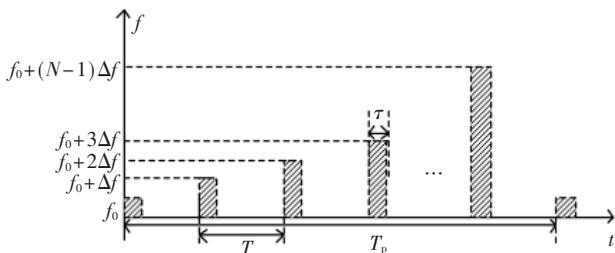


图2 步进频发射信号示意图

导引头一个积累周期内的频率步进信号可表示为:

$$s_i(t) = \sum_{k=0}^{m-1} \sum_{i=0}^{n-1} c_i u(t - kT_p - iT) e^{j(2\pi(f_0 + i\Delta f)t + \theta_i)} \quad (1)$$

$$u(t) = \begin{cases} 1 & kT_p + iT \leq t \leq kT_p + iT + \tau \\ 0 & \text{其他} \end{cases} \quad (2)$$

其中,τ是脉冲宽度,T是脉冲重复周期,T_p是相同频率脉冲重复周期,f₀是基频,Δf是频率步进间隔,n是频率步进数,m是积累周期内相同频率重复次数,θ_i是相对相位,c_i是常数。脉冲宽度τ与频率步进间隔Δf满足τ ≤ 1/Δf^[16]。

导引头信号处理系统框图如图3所示。

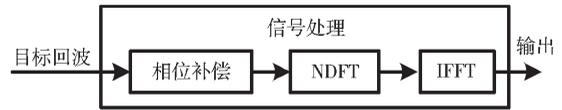


图3 导引头信号处理系统框图

假设地面静止目标距离导引头起始距离为R₀(时间t=0对应的距离),径向速度为v,光速为c,目标的回波信号可表示为:

$$s_{ii}(t) = \sum_{k=0}^{m-1} \sum_{i=0}^{n-1} c_i u(t - kT_p - iT - \tau') \cdot e^{j(2\pi(f_0 + i\Delta f)(t - \tau') + \theta_i)} \quad (3)$$

其中,目标回波延迟时间为:

$$\tau' = 2 \left(\frac{R_0 - vt}{c} \right) \quad (4)$$

回波信号经过下变频后得基带正交信号:

$$X_{ki} = A_i e^{j\psi_{ki}(t)} \quad (5)$$

$$\psi_{ki}(t) = -2\pi f_i \left(\frac{2R_0}{c} - \frac{2vt_{ki}}{c} \right) \quad (6)$$

$$t_{ki} = kT_p + iT + \frac{t_r}{2} + \frac{2R_0}{c} \quad (7)$$

其中,A_i为常数,t_r为一维距离像起始距离对应的时间延迟。

假定采样时刻为t = kT_p + iT + $\frac{\tau}{2}$,则式(6)可以转化为:

$$\psi_{ki}(t) = -2\pi f_i \left(\frac{2R_0}{c} - \frac{2v}{c} \cdot \left(kT_p + iT + \frac{\tau}{2} + \frac{t_r}{2} + \frac{2R_0}{c} \right) \right) \quad (8)$$

同频脉冲回波采样进行处理可得到目标的速度信息,不同频率连续脉冲回波采样可得到目标的距离信息。其中导引头运动引起目标回波相位变化。

$$\phi_{ki}(t) = -2\pi f_i \cdot \frac{2v}{c} \left(kT_p + iT + \frac{\tau}{2} \right) \quad (9)$$

对目标回波信号进行相位补偿:

$$\xi_{ki}(t) = \psi_{ki}(t) - \phi_{ki}(t) = -2\pi f_i \left(\frac{2R_0}{c} - \frac{2v}{c} \cdot \left(\frac{t_r}{2} + \frac{2R_0}{c} \right) \right) \quad (10)$$

补偿后的回波信号为:

$$S_{ki} = A_i e^{\xi_{ki}(t)} \quad (11)$$

由于脉冲载频不同,n个频率对应不同的目标多普勒频率,采用NDFT,将n个载频的速度门都对应到基频上。

定义偏移因子γ_i = $\frac{f_i}{f_0}$,则NDFT公式为:

$$s(i, h) = \sum_{k=0}^{m-1} S_{ki}(k) \cdot e^{-j2\pi \frac{h\gamma_i k}{m}} \quad i=0, 1, \dots, n-1$$

$$h = -\frac{m}{2}, \dots, 0, \dots, \frac{m}{2} - 1 \quad (12)$$

对s(i, h)进行傅里叶反变换:

$$R(k, t) = \sum_{i=0}^{n-1} s(i, h) \cdot e^{j2\pi \frac{h\gamma_i k}{m}} \quad t=0, 1, \dots, n-1 \quad (13)$$

2 毫米波导引头对地探测建模

毫米波导引头为实现对地探测,其在搜索与截获阶段通常采用下斜视方式进行目标区域探测,毫米波导引

头对地探测几何关系如图4所示。

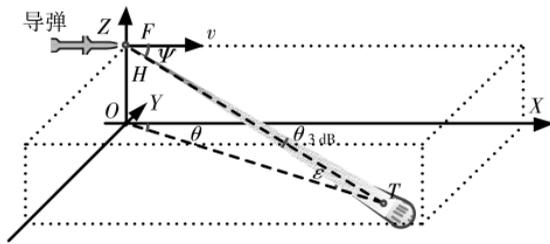


图4 毫米波导引头对地探测几何关系

导弹飞行方向为方位的 0° 角， v 为导弹飞行速度， H 为导弹高度， ψ 为天线轴线与导弹飞行速度方向之间夹角， θ 为天线波束法线方位角， ε 为天线波束俯仰角， R 为目标斜距， θ_{3dB} 为天线主波束宽度。

3 非相参干扰仿真

3.1 仿真条件

毫米波导引头平台仿真条件如下：导弹飞行速度 $v=200$ m/s，导弹飞行高度 $H=200$ m，天线波束方位角 $\theta=20^\circ$ ，天线波束俯仰角 $\varepsilon=8^\circ$ ，导引头距离干扰源距离 $R=2.91$ km，天线波束宽度 $\theta_{3dB}=3.2^\circ$ 。

毫米波导引头工作起始频率 $f_0=35.5$ GHz，频率步进间隔 $\Delta f=5$ MHz，频率步进数 $n=128$ ，脉冲宽度 $\tau=200$ ns，脉冲重复频率PRF=31 kHz，相同频率脉冲重复周期 $T_p=3\ 200$ μ s，积累周期内相同频率重复次数 $m=32$ 。

假设地面存在三个强散射点目标，目标1距离导引头初始距离 $R_0=3\ 002$ ，相对导引头飞行方向夹角 19.05° ；目标2距离导引头初始距离 $R_1=3\ 028$ ，相对导引头飞行方向方位夹角 21.35° ；目标3距离导引头初始距离 $R_2=3\ 052$ ，相对导引头飞行方向方位夹角 20.15° 。

3.2 无干扰导引头二维成像

假设点目标回波强度为1，背景噪声点频为 -20 dB，毫米波引信导引头对地二维成像如图5所示。

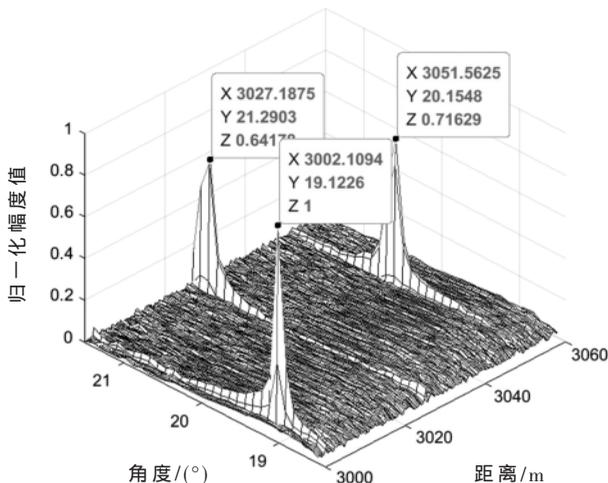
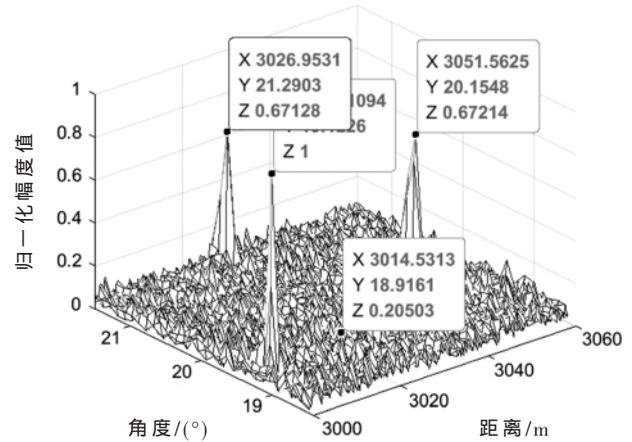


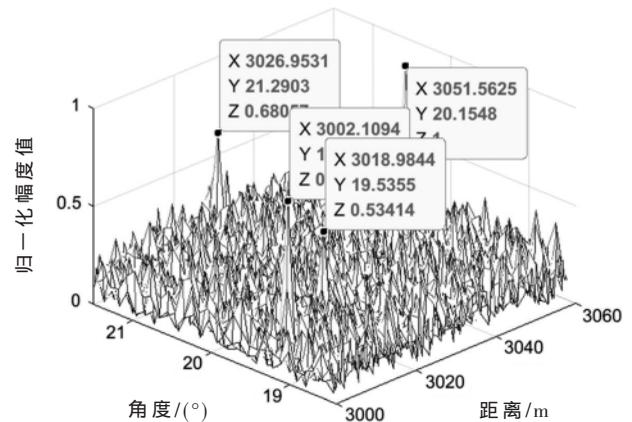
图5 毫米波导引头对地二维成像

3.3 点频瞄准干扰

干扰源根据测频接收机测频结果自产生连续波干扰信号，干信比 J/S 分别取 10 dB和 20 dB，测频最大误差 Δf_{max} 为 2 MHz和 1 MHz时，且最大测频误差小于导引头的接收机带宽一半，即干扰信号能够全部进入导引头接收机，点频瞄准干扰对导引头干扰效果（ $\Delta f_{max}=2$ MHz）和点频瞄准干扰对导引头干扰效果（ $\Delta f_{max}=1$ MHz）分别如图6和图7所示。



(a) 二维成像输出结果(干信比 10 dB)



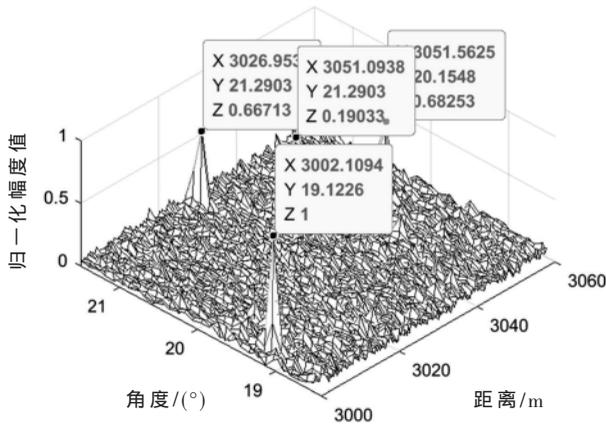
(b) 二维成像输出结果(干信比 20 dB)

图6 点频瞄准干扰对导引头干扰效果($\Delta f_{max}=2$ MHz)

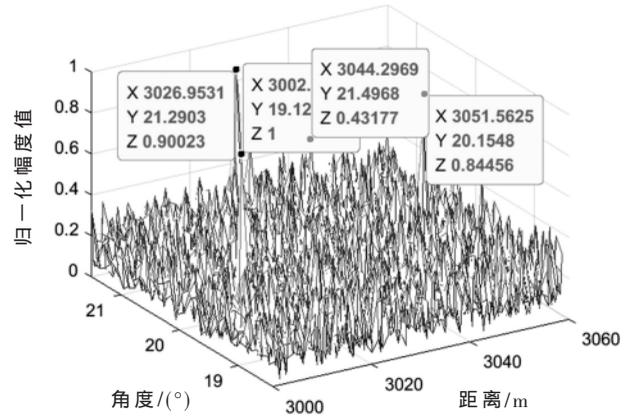
假设测频接收机测频结果不存在误差，依此产生点频连续波干扰信号，干信比 J/S 分别 10 dB和 20 dB，点频瞄准干扰对导引头干扰效果(精准瞄频)如图8所示。

干信比 J/S 分别取 10 dB、 20 dB和 26 dB，测频最大误差为 1 MHz时，且最大测频误差小于导引头的接收机带宽一半，即干扰信号能够全部进入导引头接收机，导引头对地二维成像效果($\Delta f_{max}=1$ MHz)如图9所示。

仿真结果表明，点频瞄准干扰时，干扰信号频率精度能够保证全部进入导引头接收机情况下，干扰信号频率精度与干扰效果关系不大，波束内干扰时，干信比 J/S 为 20 dB左右，点频瞄准干扰产生的随机假目标与导引

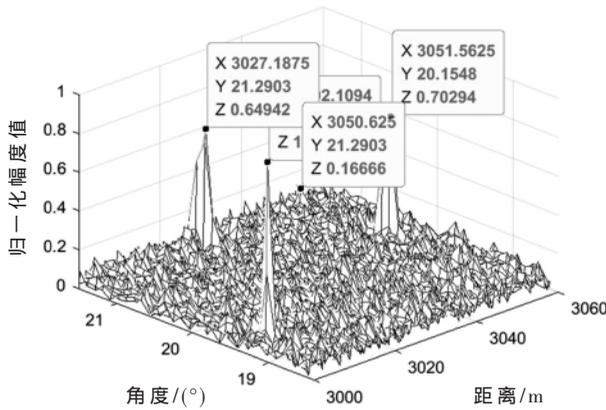


(a) 二维成像输出结果(干信比 10 dB)

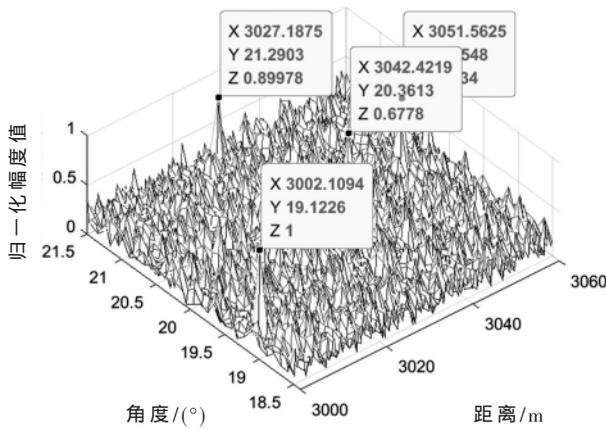


(b) 二维成像输出结果(干信比 20 dB)

图 7 点频瞄准干扰对导引头干扰效果($\Delta f_{\max}=1$ MHz)



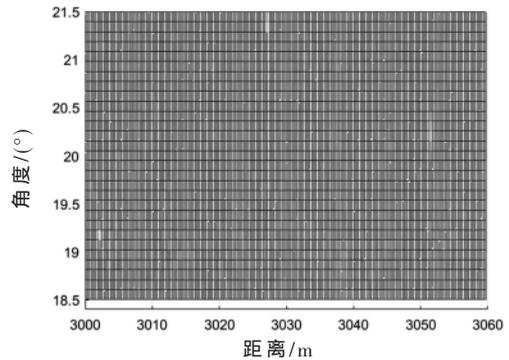
(a) 二维成像输出结果(干信比 10 dB)



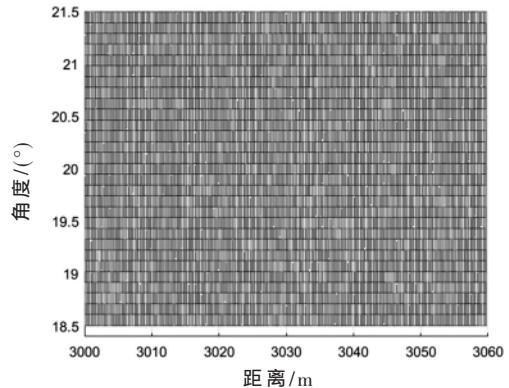
(b) 二维成像输出结果(干信比 20 dB)

图 8 点频瞄准干扰对导引头干扰效果(精准瞄频)

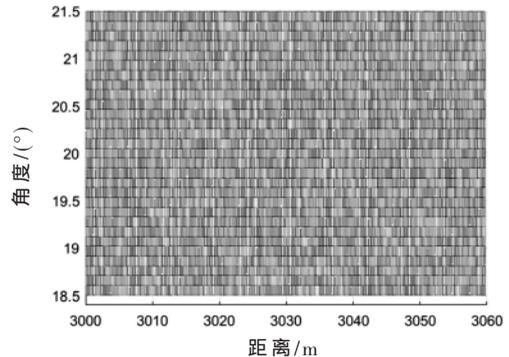
头波束覆盖范围内的目标回波信号强度相当,干信比J/S为26 dB左右,点频瞄准干扰产生的随机假目标覆盖导引头波束覆盖范围内的目标回波信号,波束外干扰时,在目标回波功率一定的情况下,干扰源增加功率倍数与毫米波导引头天线主副瓣增益相同时,波束内干扰与波束外干扰效果相当。



(a) 二维成像输出结果(干信比 10 dB)



(b) 二维成像输出结果(干信比 20 dB)



(c) 二维成像输出结果(干信比 26 dB)

图 9 导引头对地二维成像效果($\Delta f_{\max}=1$ MHz)

3.4 调频噪声干扰

干扰源根据测频接收机测频结果自产生窄带调频干扰信号,测频最大误差 $\Delta f_{\max}=2$ MHz,基带调频噪声信号带宽 $\Delta BW=4$ MHz,且噪声调频信号能够全部进入导引头接收机,干信比 J/S 为10 dB,窄带噪声干扰对导引头干扰效果($\Delta BW=4$ MHz)如图10所示。

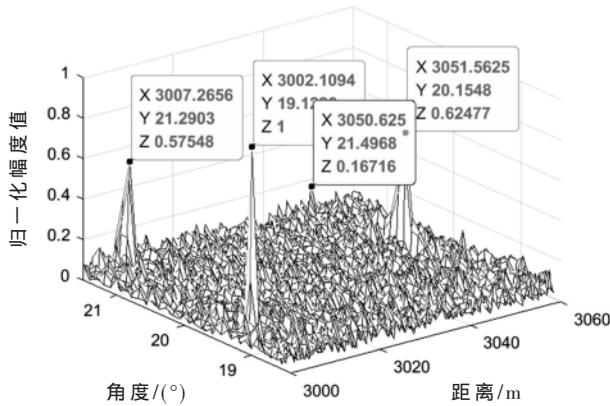


图10 窄带噪声干扰对导引头干扰效果($\Delta BW=4$ MHz)

干扰源根据测频接收机测频结果自产生窄带调频干扰信号,测频最大误差 $\Delta f_{\max}=1$ MHz,基带调频噪声信号带宽 $\Delta BW=2$ MHz,且噪声调频信号能够全部进入导引头接收机,干信比 J/S 为10 dB,窄带噪声干扰对导引头干扰效果($\Delta BW=2$ MHz)如图11所示。

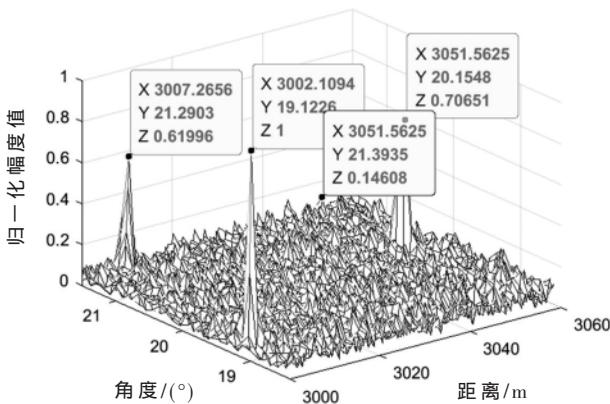


图11 窄带噪声干扰对导引头干扰效果($\Delta BW=2$ MHz)

仿真结果表明,噪声调频干扰时,噪声调频信号能够全部进入导引头接收机情况下,干扰信号带宽与干扰效果关系不大,且噪声调频干扰对导引头干扰效果与点频瞄准干扰对导引头干扰效果相当。

4 相参干扰仿真

4.1 仿真条件

仿真条件同3.1。

4.2 延迟多抽头转发干扰

4.2.1 波束内干扰

假设干扰源相对导引头飞行方向方位夹角 19.05° ,延迟抽头数4,假设导引头接收机接收的单个假目标回

波功率与真实目标回波功率相同,且假目标均分干扰源输出功率,则干信比 J/S 为6 dB。延迟多抽头干扰对导引头干扰效果(波束内干信)如图12所示。

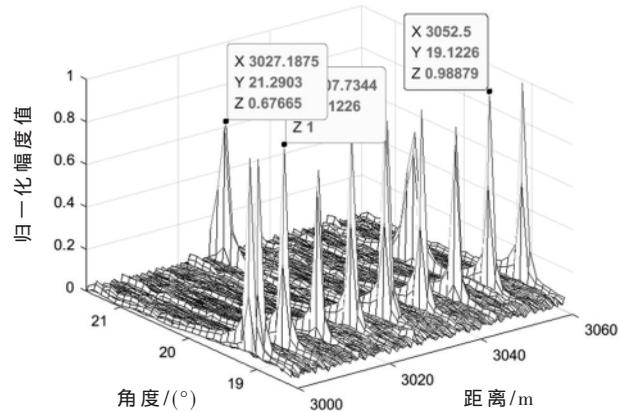


图12 延迟多抽头干扰对导引头干扰效果(波束内干扰)

4.2.2 波束外干扰

假设干扰源相对导引头飞行方向方位夹角分别为 16° 和 25° ,延迟抽头数4,假设导引头接收机接收的单个假目标回波功率与真实目标回波功率相同,且假目标均分干扰源输出功率,干信比 J/S 为6 dB。延迟多抽头干扰对导引头干扰效果(波束外 16° 干信)如图13所示,延迟多抽头干扰对导引头干扰效果(波束外 25° 干信)如图14所示,导引头对地二维成像效果(波束外 25° 干信)如图15所示。

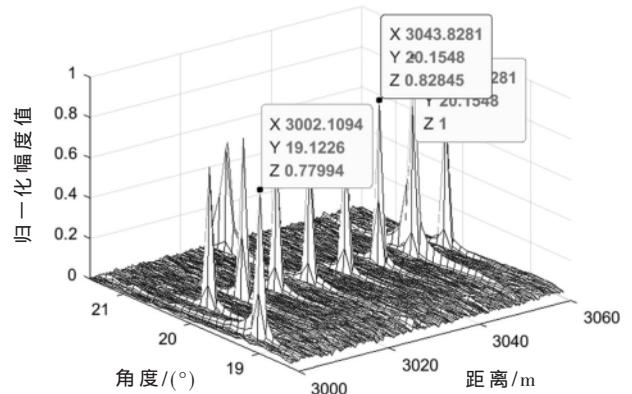


图13 延迟多抽头干扰对导引头干扰效果(波束外 16° 干信)

仿真结果表明,延迟多抽头转发干扰,不论干扰源是否位于导引头天线波束照射的范围内,干扰信号都能够产生较强的距离假目标,导引头波束扫描成像过程中,干扰源能够在导引头波束扫描的覆盖范围内连续产生方位假目标,从而对导引头产生距离+方位假目标的效果。

4.3 延迟多抽头+相位调制转发干扰

根据4.2仿真结果可以,波束内干扰与波束外干扰产生的干扰效果类似,因此,延迟多抽头+相位调制转发干扰只仿真波束内干扰。

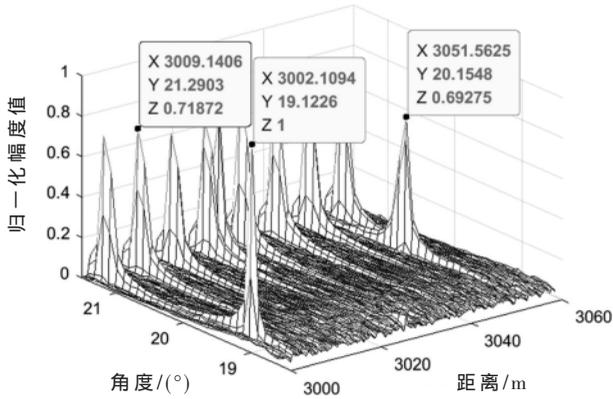


图 14 延迟多抽头干扰对导引头干扰效果(波束外 25°干信)

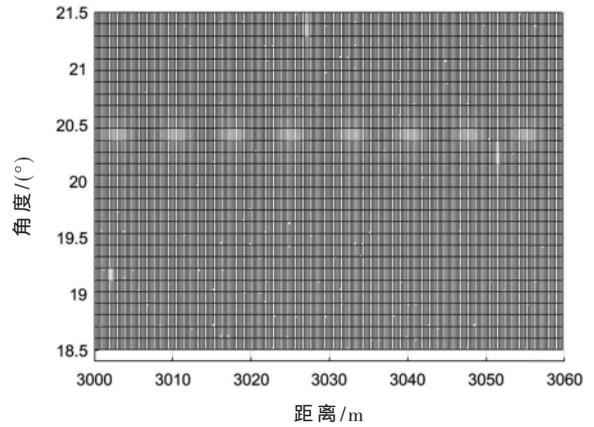


图 17 导引头对地二维成像效果(小距离段掩盖)

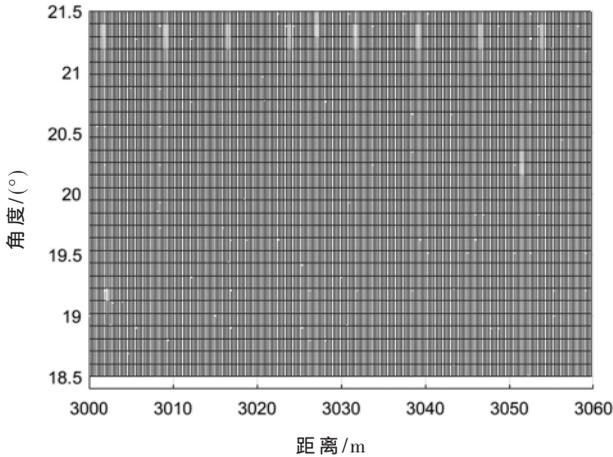


图 15 导引头对地二维成像效果(波束外 25°干信)

假设干扰源相对导引头飞行方向方位夹角 20.5°, 延迟抽头数 4, 假设导引头接收机接收的单个假目标回波功率与真实目标回波功率相同, 且假目标均分干扰源输出功率, 则干信比 J/S 为 6 dB, 同时进行不同距离维度的相位调制, 形成不同距离段的掩盖区域。

小距离段相位调制, 延迟多抽头+相位调制转发干扰对导引头干扰效果(小距离段掩盖)如图 16 所示, 导引头对地二维成像效果(小距离段掩盖)如图 17 所示。

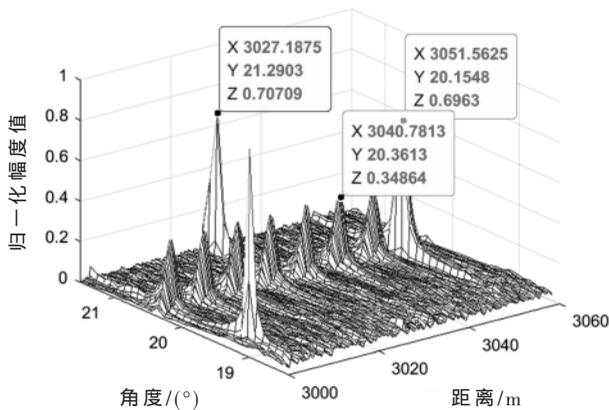


图 16 延迟多抽头+相位调制转发干扰对导引头干扰效果(小距离段掩盖)

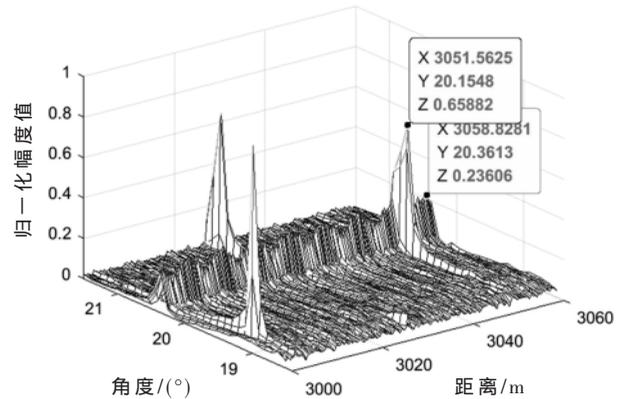


图 18 延迟多抽头+相位调制转发干扰对导引头干扰效果(长距离段掩盖)

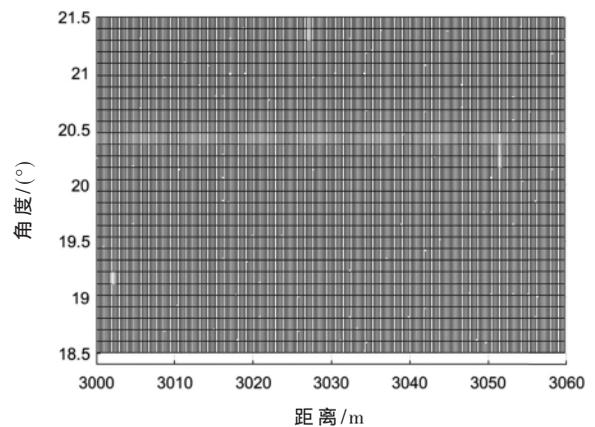


图 19 导引头对地二维成像(长距离段掩盖)

长小距离段相位调制, 延迟多抽头+相位调制转发干扰对导引头干扰效果(长距离段掩盖)如图 18 所示, 导引头对地二维成像效果(长距离段掩盖)如图 19 所示。

假设干扰源相对导引头飞行方向方位夹角 20.5°, 延迟抽头数 4, 假设导引头接收机接收的单个假目标回波功率是真实目标回波功率 2 倍, 且假目标均分干扰源输出功率, 则干信比 J/S 为 12 dB, 同时进行不同距离维度的相位调制, 形成不同距离段的掩盖区域。

小距离段相位调制,延迟多抽头+相位调制转发干扰对导引头干扰效果(小距离段掩盖)如图 20 所示,导引头对地二维成像效果(小距离段掩盖)如图 21 所示。

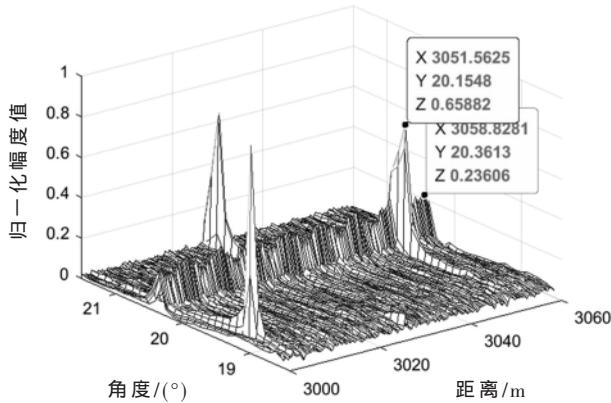


图 20 延迟多抽头+相位调制转发干扰对导引头干扰效果(小距离段掩盖)

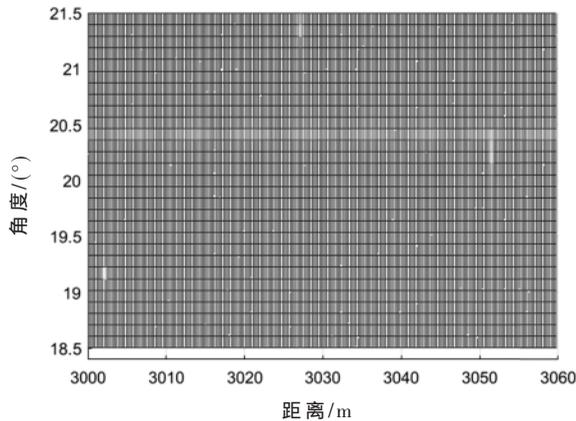


图 21 导引头对地二维成像效果(小距离段掩盖)

长小距离段相位调制,延迟多抽头+相位调制转发干扰对导引头干扰效果(长距离段掩盖)如图 22 所示,导引头对地二维成像效果(长距离段掩盖)如图 23 所示。

仿真结果表明,延迟多抽头转发+相位调制转发干

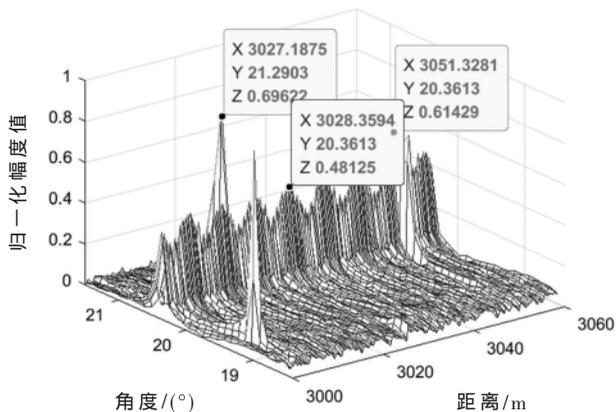


图 22 延迟多抽头+相位调制转发干扰对导引头干扰效果(长距离段掩盖)

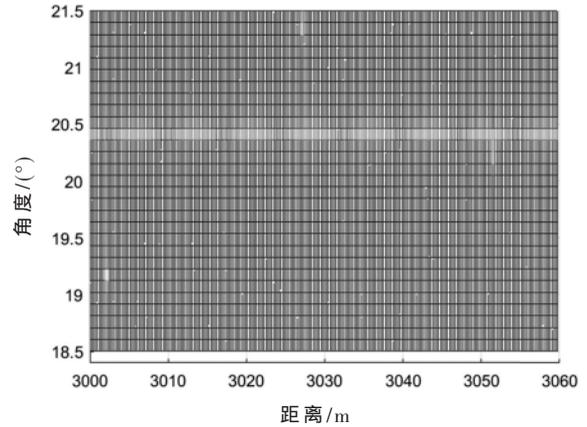


图 23 导引头对地二维成像(长距离段掩盖)

扰,干扰信号都能够产生较强的距离假目标,单个假目标掩盖距离越长,则假目标信号峰值能量越弱,在干扰调制参数不变情况下,假目标功率峰值与干信成正比,且导引头波束扫描成像过程中,干扰源能够在导引头波束扫描的覆盖范围内连续产生方位假目标,从而对导引头产生距离+方位假目标的效果。

5 干扰分析

通过以上干扰仿真,可以得出以下结论:

(1)不论干扰源是否位于导引头波束覆盖范围,非相参干扰和相参干扰都能够对导引头实现干扰,且目标回波功率一定的情况下,分别位于副瓣区、主瓣区的干扰源干扰功率比与导引头天线主副瓣比相当时,同一种干扰样式的干扰效果相同。

(2)点频瞄准和窄带噪声调频干扰获取的干扰效果相当,对导引头形成一种干扰压制的效果,当干信比达到 23 dB 左右时,干扰源可以对导引头波束覆盖范围内的目标实现有效遮盖干扰。

(3)延迟转发干扰和延迟转发+相位调制干扰可获得峰值功率较强的假目标,单个假目标功率峰值随掩护距离增加而减弱,通常干信比 J/S 为 10 dB 左右,假目标峰值功率与目标回波功率相当。

(4)不论是相参干扰还是非相参干扰,需采用逆增益进行干扰,可实现导引头波束扫描过程中不产生强功率假目标,从而保障干扰源的安全。

6 结论

通过理论分析与建模仿真,针对频率步进毫米波导引头,非相参干扰时,可实现导引头波束覆盖范围内成像干扰,干扰能量分散;相参干扰时,合理延迟多抽头及相位调制,产生的假目标功率强度更为集中,与非相参干扰相比,获取同样的假目标功率峰值,其干信比较低,同时逆增益干扰可实现导引头波束扫描过程中,不产生强功率假目标,从而保障干扰源的安全,因此,逆增益和有源干扰的复合干扰策略是对抗频率步进毫米波导引头的一种有效方法。

参考文献

[1] 谭铭,王春阳,李欣,等.对步进频雷达灵巧干扰的建模方法与仿真[J].传感器与微系统,2016,35(7):26-29.

[2] 金胜,朱天林,王海波.步进频雷达成像技术研究进展[J].飞行器测控学报,2013,32(6):490-495.

[3] 刘春生,鲍燕飞,伍波.难以干扰的几种新体制雷达[J].航天电子对抗,2001(2):28-30.

[4] 胡体玲,李兴国.毫米波步进频率单脉冲雷达及其信号处理[J].雷达科学与技术,2006,4(4):193-196.

[5] 刘柳.不断发展的毫米波对抗技术[J].飞机工程,2006(3):11-13,58.

[6] 凌永顺,同武勤,张鑫,等.毫米波对抗技术[J].光电工程,2004,31(7):1-4,41.

[7] 张宏伟,冯振,俞静一,等.对频率步进毫米波导引头的干扰研究[J].电子信息对抗技术,2010,25(4):35-38.

[8] 周政,唐宏,张永顺,等.基于时域采样的灵巧噪声干扰研究[J].现代雷达,2010,32(5):53-55.

[9] 徐晓阳,包亚先,周宏宇.基于卷积调制的灵巧噪声干扰技术[J].现代雷达,2007,29(5):28-31.

[10] 张智,赵健,李帅.针对频率步进雷达的一种灵巧噪声干扰方法[J].舰船电子对抗,2010,33(2):5-8.

[11] 尚志刚,白渭雄,董会旭.对PD雷达进行综合欺骗干扰研究[J].火力与指挥控制,2013,38(1):91-93.

[12] 郭诚,颜振亚.噪声调制灵巧噪声对雷达干扰性能研究与实现[J].现代雷达,2014,36(7):77-80.

[13] 向敬成,张明友.毫米波雷达及应用[M].北京:国防工业出版社,2016.

[14] 张江华,梁培康,刘逸平,等.毫米波导引头系统设计与工程实现[M].北京:国防工业出版社,2016.

[15] 张东坡,刘兴钊.基于NDFT的步进频率雷达信号处理[J].雷达科学与技术,2004,2(5):289-292,314.

[16] 梁潇,袁业术.频率步进雷达信号的二维处理[C].2005年中国电子学会第十一届青年学术年会论文集,2005:709-712.

(收稿日期:2020-10-13)

作者简介:

项正山(1979-),男,硕士,高级工程师,主要研究方向:雷达对抗及信号处理。

(上接第136页)

[5] 习近平.在网络安全和信息化工作座谈会上的讲话[N].人民日报,2016-04-26(002).

[6] 陈师尧,樊燕红,付勇,等.ANT系列分组密码算法[J].密码学报,2019,6(6):748-759.

[7] 邹祎,李浪,贺位位,等.轻量级密码算法LBlock的FPGA优化实现[J].计算机系统应用,2015,24(7):240-243.

[8] HONG D, SUNG J, HONG S, et al. HIGHT: a new block cipher suitable for low-resource device[C]. International Workshop on Cryptographic Hardware and Embedded Systems. Springer, Berlin, Heidelberg, 2006.

[9] BOGDANOV A, KNUDSEN L R, LEANDER G, et al. PRESENT: an ultra-lightweight block cipher[C]. Proceedings of Cryptographic Hardware and Embedded Systems, 2007: 450-466.

[10] SHIBUTANI K, ISOBE T, HIWATARI H, et al. Piccolo: an ultra-lightweight block cipher[C]. Proceeding of the CHES 2011. Nara, Japan. LNCS 6917, 2011: 342-357.

[11] GUO J, PEYRIN T, POSCHMANN A, et al. The LED block cipher[C]. Cryptographic Hardware and Embedded Systems—CHES 2011. Springer Berlin Heidelberg, 2011: 326-341.

[12] WU W L, ZHANG L. LBlock: a lightweight block cipher[C]. Applied Cryptography and Network Security—ACNS 2011. Springer Berlin Heidelberg, 2011: 327-344.

[13] GÉRARD B, GROSSO V, NAYA-PLASENCIA M, et al. Block ciphers that are easier to mask: How far can we

go?[C]. Cryptographic Hardware and Embedded Systems—CHES 2013. Springer Berlin Heidelberg, 2013: 383-399.

[14] 高志权.高性能高安全的密码机研究[J].信息安全与通信保密,2019(11):28-35.

[15] 刘小平,何云斌,董怀国.基于Verilog HDL的有限状态机设计与描述[J].计算机工程与设计,2008(4):958-960.

[16] 孔昕,吴武臣,侯立刚,等.基于Verilog的有限状态机设计与优化[J].微电子学与计算机,2010,27(2):180-183.

[17] 蔡冰清,白国强.SM3杂凑算法的流水线结构硬件实现[J].微电子学与计算机,2015,32(1):15-18.

[18] 李磊,韩文报.FPGA上SHA-1算法的流水线结构实现[J].计算机科学,2011,38(7):58-60.

[19] 何星,张铁军,侯朝焕.流水线结构FFT/IFFT处理器的设计与实现[J].微电子学与计算机,2007(4):141-143,147.

[20] 周雍浩,董婉莹,李斌,等.可重构的SHA-3算法流水线结构优化及实现[J].现代计算机,2020(12):15-20.

(收稿日期:2020-09-23)

作者简介:

王建新(1977-),男,博士,副教授,主要研究方向:电子信息工程。

刘芮安(1997-),通信作者,男,硕士研究生,主要研究方向:密码算法的FPGA设计与实现,E-mail:ryenliu@sina.cn。

肖超恩(1982-),男,博士,讲师,主要研究方向:人工智能。

版权声明

经作者授权，本论文版权和信息网络传播权归属于《电子技术应用》杂志，凡未经本刊书面同意任何机构、组织和个人不得擅自复印、汇编、翻译和进行信息网络传播。未经本刊书面同意，禁止一切互联网论文资源平台非法上传、收录本论文。

截至目前，本论文已经授权被中国期刊全文数据库（CNKI）、万方数据知识服务平台、中文科技期刊数据库（维普网）、DOAJ、美国《乌利希期刊指南》、JST 日本科技技术振兴机构数据库等数据库全文收录。

对于违反上述禁止行为并违法使用本论文的机构、组织和个人，本刊将采取一切必要法律行动来维护正当权益。

特此声明！

《电子技术应用》编辑部

中国电子信息产业集团有限公司第六研究所