文章编号:1671-4598(2026)03-0250-08 DOI:10.16526/j.cnki.11-4762/tp.2026.03.031 中图分类号:TP802+.6 文献标识码:A

复杂欺骗环境下 GNSS 欺骗信号特征提取算法设计与分析

张振宇[1,2]，蔚保国[1,2]
(1. 中国电子科技集团公司 第五十四研究所，石家庄 150001；
2. 综合时空网络与装备技术全国重点实验室，石家庄 150001)

摘要：针对全球卫星导航系统（GNSS，global navigation satellite system）在复杂电磁环境下易受欺骗攻击的问题，研究了基于频域统计特性的信号特征提取与识别方法；分析了 GNSS 信号在欺骗干扰下的频谱结构变化规律，构建了频域矩峰度系数、单频能量聚集度、频域矩偏度系数、平均频谱平坦系数频域参数等 5 种频域特征数学模型；采用了德克萨斯大学欺骗测试数据集（TEXBAT，texas spoofing test battery）对不同功率优势及频率锁定状态下的欺骗场景进行了实验测试与区分度分析，引入了 Cohen's d 效应量指标对特征的有效性进行了定量评估；经实验测试实现了对复杂欺骗信号与真实信号的有效区分，结果表明所提取的频域特征在多数欺骗场景下具有显著的统计差异，其中频域矩偏度与平坦系数在特定高动态欺骗场景下表现出较强的敏感性；该研究为复杂环境下 GNSS 接收机抗欺骗算法的特征工程设计提供了理论依据与数据支撑。

关键词：GNSS 欺骗；复杂欺骗环境；频域特征；特征提取；区分度分析

Design and Analysis of GNSS Spoofing Signal Feature Extraction Algorithms under Complex Spoofing Environments

ZHANG Zhenyu[1,2], YU Baoguo[1,2]
(1. The 54th Research Institute of China Electronics Technology Group Corporation, Shijiazhuang 150001, China;
2. State Key Laboratory of Comprehensive PNT Network and Equipment Technology, Shijiazhuang 150001, China)

Abstract: It is susceptible for global navigation satellite system (GNSS) to spoofing attacks in complex electromagnetic environments. To address this issue, research is conducted on the signal feature extraction and identification based on frequency-domain statistical characteristics, which analyzes the spectral structure variation of GNSS signals under spoofing interference, and constructs five types of frequency-domain feature mathematical models, including frequency-domain kurtosis coefficient, single-frequency energy concentration, frequency-domain skewness coefficient, and average spectral flatness coefficient. Experimental tests and discrimination analysis are performed on the Texas spoofing test battery (TEXBAT) standard dataset under the spoofing scenarios with different power advantages and frequency locking states. The Cohen's d effect size index is introduced to quantitatively evaluate the effectiveness of the features. Experimental results show an effective distinction between complex spoofing signals and authentic signals, indicating that the extracted frequency domain feature has a significant statistical difference in most spoofing scenarios. Specifically, the frequency-domain skewness and flatness coefficients demonstrate a strong sensitivity in specific high-dynamic spoofing scenarios. This research provides a theoretical basis and data support for the feature engineering design of anti-spoofing algorithms in GNSS receivers.

Keywords: GNSS spoofing; complex spoofing environments; frequency-domain feature; feature extraction; discriminative analysis

收稿日期:2026-01-03； **修回日期**:2026-02-11。
基金项目:中央引导地方科技发展基金项目(246Z0901G);中央引导地方科技发展资金项目(246Z1822G);中国电子科技集团公司第五十四研究所院士合作重点单位项目。
作者简介:张振宇(2000-),男,硕士研究生,助理工程师。
引用格式:张振宇,蔚保国.复杂欺骗环境下 GNSS 欺骗信号特征提取算法设计与分析[J].计算机测量与控制,2026,34(3):250-257.

0　引言

全球卫星导航系统（GNSS，global navigation satellite system）在提供关键时空基准服务的同时，面临着日益严峻的电磁安全威胁，特别是隐蔽性极强的欺骗干扰已成为主要风险来源[1-3]，相关漏洞在实际应用中甚至引发了严重的导航安全事故[4]。针对欺骗干扰的检测与防御，国内外学者已开展了广泛研究并形成了多种技术路线：在接收机自主信号处理层面，基于相关峰形状分析的信号质量监测（SQM，signal quality monitoring）[5]和矢量跟踪环路辅助[6]技术较为成熟，但在高动态或强多径环境下性能易受限制[7]；在硬件与系统级辅助层面，多天线测向[8]、导航电文加密认证[9-10]以及基于标准数据集的测试评估[11]推动了防御体系的发展，利用时钟漂移监测[12]及惯性导航系统（INS，inertial navigation system）紧耦合[13-14]的一致性校验方法也显著提升了系统的鲁棒性。近年来，为应对更加精细的信号畸变，改进的 SQM 算法[15]、基于时频域统计特性的分析方法[16]以及利用自动增益控制（AGC，automatic gain control）电平监测[17]的手段逐渐成为研究热点。尽管上述方法在特定场景下有效，但面对如文献［18］所证实的具备轨迹诱导能力的高级欺骗攻击，现有技术在复杂电磁环境下的微弱特征挖掘与量化评估能力仍显不足。鉴于此，本文从信号频域统计特性出发，构建多维特征数学模型并引入效应量指标，旨在为复杂场景下的抗欺骗算法设计提供理论支撑。

1　实验设计及原理

1.1　数据集介绍及处理

1.1.1　TEXBAT 数据集介绍

根据攻击手段和隐蔽性不同，GNSS 欺骗攻击可以分为 3 个阶段：最原始的是录制重放攻击，真实信号和欺骗信号瞬间切换，容易导致接收机同步状态突变；渐进功率牵引攻击手段更加隐蔽，通过慢慢增大欺骗信号的相对功率来实现跟踪环路的平滑转移，静态时间欺骗根据功率优势不同检测难度不同。生成式欺骗提高了灵活性，静态定位欺骗通过注入系统性伪距偏差的伪造信号而产生固定位置偏移，动态轨迹欺骗通过模拟符合运动学的信号参数（如多普勒变化）来伪造接收机运动状态。混合转发生成攻击结合两种技术实现难以察觉的过渡。目前技术复杂度最高的是零延迟码估计和重放攻击，通过对导航电文实时预测与重建实现几乎无延迟的信号转发，而且可以很好的复现信号结构与时间同步，对于信号新鲜度或电文一致性认证方法形成了极大挑战。不同的攻击在功率策略、动态模拟精度、信号生成实时性等方面存在着各自的差异。

为了全面评估算法在真实信号环境下的鲁棒性及对不同隐蔽等级欺骗信号的检测边界，本文选用美国德克萨斯大学奥斯汀分校发布的公开实采德克萨斯大学欺骗测试数据集 TEXBAT 作为实验平台。该数据集是在全带宽采样 25 Msps、高保真射频记录环境下生成的，严格遵循了信号产生的物理可追溯性，是目前 GNSS 抗欺骗研究领域公认的权威测试基准。

TEXBAT 包含从粗糙压制到精密牵引的多种攻击类型。根据攻击隐蔽性和技术复杂度的不同，可将其分为 3 个梯队：1）非相干压制如 ds2：具有显著功率优势 10 dB，易于检测；2）相干牵引如 ds3，ds5：功率与真实信号相当，且实现了载波相位与伪码的精确锁定，检测难度中等；3）极限隐蔽攻击如 ds4，ds6，ds7：在功率匹配，即＜1 dB 优势的基础上叠加了位置/时间/动态等多维欺骗策略，属于当前防御体系的盲区。表 1 是对 TEXBAT 数据集欺骗场景及欺骗类型的详细介绍。

表 1　TEXBAT 数据集介绍

场景号	欺骗类型	平台移动性	功率优势	频率锁定
cleanStatic	——	静态	——	——
cleanDynamic	——	动态	——	——
ds1	跳变	静态	0 dB	否
ds2	时间	静态	10 dB	否
ds3	时间	静态	1.3 dB	是
ds4	位置	静态	0.4 dB	是
ds5	时间	动态	9.9 dB	否
ds6	位置	动态	0.8 dB	是
ds7	时间	静态	1.3 dB	是
ds8	时间	静态	1.3 dB	是

1.1.2　实验场景选取的完备性论证

针对实验场景多样性与完整性的要求，本文摒弃了易被传统能量检测器识别的高功率压制场景 ds2，主要聚焦于“高隐蔽性”与“动态复杂性”两大核心难点，构建了覆盖“功率－动态”多维特征的完备测试集。具体选取逻辑如下：1. 正常环境基准：选取 cleanStatic 与 cleanDynamic，分别代表静态接收与动态接收下的纯净信号，用于确立算法的虚警率基准，确保算法在接收机运动状态下不会因多普勒变化产生误判。2. 欺骗环境攻关：静态隐蔽性测试 ds3 对比 ds4：选取 ds3 作为标准相干欺骗对照组；选取 ds4 作为“功率极限”测试组。ds4 的功率优势仅为 0.4 dB，旨在验证算法在近乎完美的功率匹配下的极限灵敏度。动态鲁棒性测试：选取 ds6，这是全集中最复杂的场景之一，结合了接收机高动态运动与低功率欺骗。此场景用于论证算法能否在频率快速变化的环境下，依然有效剥离出微弱的欺骗特征。精密时间同步测试：选取 ds7 作为高精度时间同步欺骗的代表，用于评估算法对相位级微小畸变的捕捉能力。综上所述，本文选取的场景构成了静态/动态与标

准隐蔽/极限隐蔽的正交测试矩阵，能够全面覆盖复杂欺骗环境下的典型边界情况。

1.1.3 数据预处理与样本构建

为消除原始信号中的带外噪声并适配深度学习模型的输入维度，本节制定了严格的数据预处理规范：数据清洗与格式规整：原始 TEXBAT 数据为中频数字采样信号（采样率 f_s=25 Msps.）。首先对其进行正交解调与 I/Q 分离，滤除直流分量。样本切片与维度设计：为保证输入样本的一致性，采用滑动窗口法对连续信号进行切片。考虑到本文算法旨在捕捉信号的微观统计特征，单条样本长度设定为 L = 2 000 个采样点（对应约 80 μs 的信号快照）。该长度设置既能保留足够的统计信息以计算高阶矩特征，又能显著降低单次推理的计算负担，满足实时性要求。数据集划分：基于选取的 6 个场景，共提取有效数据 4 200 条。所有样本均依据 1.2 节所述方法进行 Min-Max 归一化处理，并按 6：1 的比例随机划分为训练集 3 600 条与测试集 600 条，具体分布如表 2 所示

表 2 数据选取介绍

数据集	提取时长/ms	提取样本点数	单条样本点数	样本条数
cleanStatic	84	2 100 000	2 000	1 050
cleanDynamic	84	2 100 000	2 000	1 050
ds3	42	1 050 000	2 000	525
ds4	42	1 050 000	2 000	525
ds6	42	1 050 000	2 000	525
ds7	42	1 050 000	2 000	525

1.2 信号预处理方法

对 GNSS 导航信号进行预处理的主要目的是统一数据尺度、提升数据质量，并减小不同特征量纲差异对后续建模与分析过程的影响，从而保证分析结果的稳定性与可靠性。本节针对 GNSS 正常信号及多种干扰环境下的信号数据，采用 min－max 归一化方法进行预处理。

min－max 归一化通过线性映射方式将原始信号幅值压缩至［0，1］区间内，使各维特征在数值范围上保持一致，有助于避免大幅值特征在模型训练与分析过程中占据主导作用，同时可提高算法的计算效率与收敛性能。对于采样点数为 N 的 GNSS 信号序列 x，其 min－max 归一化处理方式如公式（1）所示：

$$x' = \frac{x - \min(x)}{\max(x) - \min(x)} \tag{1}$$

1.3 核心频域特征提取算法

信号处理理论框架下，频域特征是揭示信号本质属性的重要分析维度。针对 GNSS 信号欺骗检测的特殊需求，本文设计并实现了五类核心频域特征提取算法：单频能量聚集度、频域参数、频域矩峰度系数、频域矩偏度系数和平均频谱平坦系数。这些特征在频域维度上构建了多维特征空间，能够从能量分布集中性、频谱形状统计特性、频带分布规律等不同层面刻画信号的本质属性，为后续的模式识别与异常检测提供了鲁棒的特征表示基础。算法设计严格遵循信号处理理论，充分考虑 GNSS 信号特有的调制方式与传播特性，确保提取的特征具有明确的物理意义和较强的类别区分能力。为了在复杂电磁环境下实时捕捉欺骗信号引起的微弱频谱畸变，本文提出了一套轻量化的频域特征提取方案。算法不仅构建了多维特征的数学模型，更针对工程实现进行了流式处理优化，具体包括信号预处理、特征解算及算法效率评估 3 个环节。

1.3.1 算法实现流程与预处理

在经由 1.2 节所述的 Min－Max 归一化完成数据尺度统一后，为了从时域序列中提取高辨识度的频域统计特征，需进一步对信号进行频谱细化与统计分布构建。具体流程如下：（1）重叠分帧与加窗处理设经 1.2 节预处理后的归一化信号序列为 $x_{\text{norm}}(n)$。为捕捉信号的局部非平稳特征，首先对其进行重叠分帧，单帧长度 N 对应相干积分时间 T_{int}。同时，为抑制数据截断引起的频谱泄漏，对每一帧信号施加汉宁窗 $w(n)$，如公式（2）所示：

$$x_w(n) = x_{\text{norm}}(n) * 0.5\left[1 - \cos\left(\frac{2\pi n}{N-1}\right)\right] \tag{2}$$

频谱变换与概率分布映射对加窗信号进行 N 点快速傅里叶变换获得幅度谱 $|X(k)|$。虽然 1.2 节已限制了时域幅值范围，但为了进一步消除不同频率成分总能量差异对谱形状统计量的干扰，本文将幅度谱映射为概率密度函数形式 $P(k)$，如公式（3）所示：

$$P(k) = \frac{|X(k)|}{\sum_{j=0}^{N-1}|X(j)|}, \sum P(k) = 1 \tag{3}$$

通过该步骤，确保了 $\sum P(k) = 1$，使得后续计算的矩特征（如峰度、偏度）纯粹反映频谱的形状分布特性，而与信号的总功率无关。

1.3.2 频域特征数学模型

频域矩峰度系数用于刻画信号频谱幅度分布的尖锐程度，是高阶统计量中对异常频谱结构较为敏感的一类特征。对于理想的 GNSS 真实信号，其频谱在扩频调制作用下呈现近似平坦分布；而在欺骗场景中，由于信号合成、调制不完美或多信号叠加效应，频谱往往出现局部能量突增，从而引起峰度特性的显著变化。因此，频域矩峰度系数可有效反映真实信号与欺骗信号在频谱统计形态上的差异。其公式如式（4）所示：

$$b_1 = \frac{E(F(i) - \mu)^4}{\sigma^4} \tag{4}$$

式中，$F(i)=1,2,\cdots,N$ 代表 GNSS 欺骗信号及 GNSS 真实信号经过傅里叶变换后得到的频谱值，μ 代表 $F(i)$ 的均值，σ 代表 $F(i)$ 的标准差。b_1 表征的是信号频谱的陡峭程度。

频域矩偏度系数用于描述信号频谱幅度分布的非对称性。对于真实 GNSS 信号，其频谱分布通常以载频为中心呈近似对称结构；而在欺骗信号中，由于频率偏移、多源叠加或调制不一致等因素，频谱对称性往往遭到破坏，从而导致偏度系数发生明显变化。因此，该特征对频率漂移型及复合型欺骗具有较高敏感性。其公式如式（5）所示：

$$b_2=\frac{E(F(i)-\mu)^3}{\sigma^3} \tag{5}$$

式中，$E()$ 表示求平均值，$F(i)=1,2,\cdots,N$ 代表 GNSS 信号频谱值，μ 代表 $F(i)$ 的平均值，σ 代表 $F(i)$ 的标准差。b_2 表征的是信号频谱对正态分布的偏离程度。

单频能量聚集度用于衡量信号频谱中能量在单一频点附近的集中程度。真实 GNSS 信号受扩频码调制影响，其频域能量分布较为分散；而欺骗信号通常由信号发生器合成，易在载波或局部频点处形成能量聚集现象。因此，该特征能够有效表征欺骗信号在频谱能量分布上的非均匀性。其公式如式（6）所示：

$$C=\frac{\sum_{i=m-k}^{m+k}F^2(i)}{\sum_{i=1}^{N}F^2(i)} \tag{6}$$

式中，$F(i)=1,2,\cdots,N$ 代表 GNSS 信号频谱值，m 为最大频谱对应索引，k 可以设置为较小的整数，实验中设置 $k=1$。

频谱平坦系数用于衡量信号频谱的平坦程度，是区分噪声型信号与结构化信号的重要指标。真实 GNSS 信号在扩频调制和噪声叠加作用下，其频谱特性通常接近于宽带噪声；而欺骗信号由于信号合成及滤波过程的影响，频谱平坦性可能发生变化。平均频谱平坦系数通过对多个频点取统计平均，可在一定程度上反映两类信号在频域结构复杂度上的差异。其计算方法如下：

首先对归一化后的干扰信号做 FFT 变换，得到其频谱值 $F(i)=1,2,\cdots,N$，取平方得其功率谱 $P(n)$，然后将 $P(n)$ 的均值进行归一化，如公式（7）所示：

$$P_u=\frac{P(i)}{\overline{P}(i)} \tag{7}$$

式中，$P(i)=F^2(i)$，$\overline{P}(i)$ 是 $P(i)$ 的均值。提取 P_u 中的冲激部分，如公式（8）所示：

$$P_p=P_u-\frac{1}{2L+1}\sum_{n=-L}^{L}P_u(i-n) \tag{8}$$

式中，$\frac{1}{2L+1}\sum_{n=-L}^{L}P_u(i-n)$ 为 $P_p(i)$ 经过移动均值处理后的功率谱，L 代表滑窗大小。GNSS 信号平均频谱平坦系数表达式如公式（9）所示：

$$F_c=\sqrt{\frac{1}{N}\sum_{i=1}^{N}[P_p(i)-\overline{P}(i)]^2} \tag{9}$$

频域参数是一类用于综合反映信号频谱整体分布形态的统计特征，其通常与频谱能量分布的集中程度及结构稳定性相关。相比真实 GNSS 信号的平稳频谱结构，欺骗信号在合成与调制过程中易引入非理想频谱畸变，从而导致该参数出现系统性偏移。因此，该特征在多种欺骗场景下均表现出较强的区分能力。其公式如公式（10）所示：

$$R_f=\frac{\sigma^2}{\mu^2} \tag{10}$$

式中，$F(i)=1,2,\cdots,N$ 代表 GNSS 信号频谱值，μ 代表 $F(n)$ 的平均值，σ 代表 $F(n)$ 的标准差。

1.3.3　算法复杂度与实时性分析

在工程应用中，算法的时间复杂度直接决定了其能否嵌入资源受限的接收机基带处理芯片。

1）时间复杂度分析本算法的计算开销主要集中在 FFT 变换与统计矩计算两个环节：FFT 变换：对于长度为 N 的序列，采用基－2 FFT 算法，其复数乘法与加法次数约为 $\frac{N}{2}\log_2 N$，时间复杂度为 $O(N\log N)$。特征计算：归一化与五种特征的累积求和均为线性操作，需遍历频谱 N 次，时间复杂度为 $O(N)$。因此，单次特征提取的总时间复杂度如公式（11）所示：

$$T_{\text{total}}\approx O(N\log N)+O(N)\approx O(N\log N) \tag{11}$$

相比于基于奇异值分解（SVD，singular value decomposition）复杂度通常为 $O(N^3)$ 的子空间类算法，本算法在计算量上具有数量级的优势，更适合高频次的流式处理。

2）空间复杂度分析算法仅需存储当前帧的信号序列及频谱数据，空间复杂度为 $O(N)$。采用原位 FFT 运算策略可进一步将存储需求减半。对于 $N=4\,096$ 甚至更长的积分长度，现有嵌入式硬件的片上存储资源，如 FPGA 的 BRAM，完全可满足缓冲需求。

3）实际效率评估为了验证算法的实时性，分别在通用计算平台与嵌入式平台上进行测试。在主频 3.0 GHz的 PC 处理器 Intel Core i9 上，对长度 $N=4\,096$的信号进行单帧处理，平均耗时约为 0.04 ms；若移植至 Xilinx Artix-7 系列 FPGA 平台并利用流水线 FFT IP 核，处理延时可控制在 50 μs 以内。考虑到 GNSS 信号通常的更新率为 50 Hz 即 20 ms 间隔，本算法的计算耗时占比不足 0.5%，完全满足接收机在线抗

欺骗检测的实时性资源约束。

2 实验仿真与分析

基于前述频域特征提取方法，本文对真实 GNSS 信号与欺骗信号在样本层面上的特征分布进行了对比分析。通过将各类特征在不同样本上的取值进行可视化展示，可以直接观察不同特征对信号频谱结构差异的响应情况。由于实验中样本均在相同参数设置与信号条件下生成，因此各特征在样本维度上的分布差异能够直接反映其对欺骗信号频谱异常的敏感程度。

总体来看，不同频域特征在区分真实信号与欺骗信号方面表现出明显差异：部分特征在两类信号之间呈现出较为稳定的整体偏移趋势，而另一些特征则存在一定程度的分布重叠。这种差异性反映了各特征对频谱异常的表征侧重点不同，为后续特征区分度的定量评估与多特征联合分析提供了依据。

频域矩峰度系数用于描述频谱幅度分布的尖锐程度[19]。由图 1 所示，在样本维度上，真实 GNSS 信号对应的峰度系数取值相对集中，其分布区间较窄，样本间波动较小，表明该特征在真实信号条件下具有较好的稳定性。

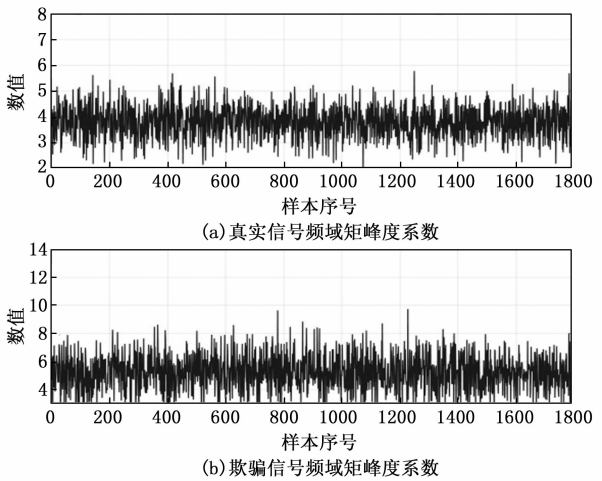

图 1 频域矩峰度系数

相比之下，欺骗信号的频域矩峰度系数整体水平明显偏高，且样本间离散程度更大，部分样本表现出较高的峰度取值。这一现象说明，欺骗信号在频域中更容易出现能量集中或频谱尖峰结构，从而导致高阶统计特性发生显著变化。该特征在样本层面上对两类信号呈现出较为清晰的分布差异，为后续区分度分析提供了良好的基础。

频域矩偏度系数反映频谱幅度分布的非对称性[20]。由图 2 所示，真实 GNSS 信号的偏度系数主要集中在较低区间，样本间变化相对平缓，表明其频谱结构在整体上具有较好的对称性。

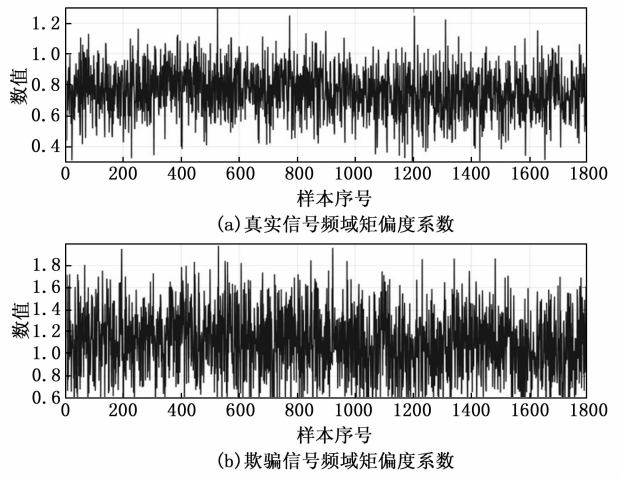

图 2 频域矩偏度系数

而欺骗信号的偏度系数在样本维度上整体呈现出向高值区域偏移的趋势，且样本间离散程度明显增大。这说明欺骗信号在频域中更易出现频谱不对称现象。尽管在部分样本区间内两类信号存在一定程度的重叠，但该特征仍能够从频谱形态变化的角度提供有效的辅助判别信息。

单频能量聚集度用于衡量频谱能量在局部频点附近的集中程度。如图 3 所示，真实 GNSS 信号的该特征取值整体处于较低水平，且在不同样本之间变化较为平缓，说明其频谱能量分布较为均匀。

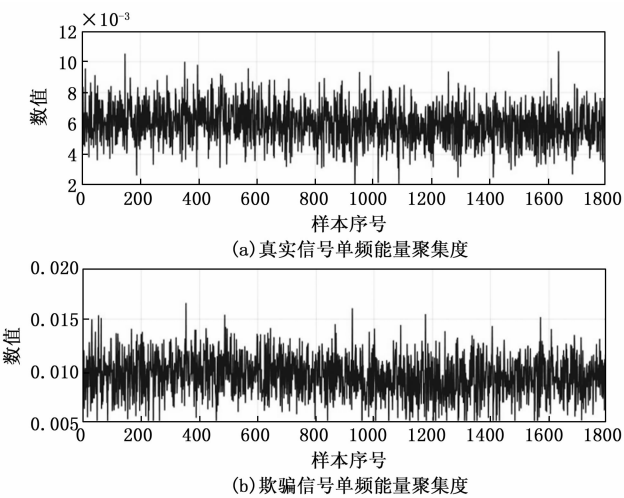

图 3 单频能量聚集度

而欺骗信号在单频能量聚集度上的取值整体偏高，且样本间波动幅度更大，反映出其频谱能量更易向局部频点集中。这种差异在多数样本中均较为明显，尽管在个别样本处仍存在一定重叠，但整体分布趋势差异清晰，表明该特征能够有效刻画欺骗信号频谱能量分布的异常特性。

平均频谱平坦系数用于描述频谱整体平坦程度。如

图 4 所示，真实信号与欺骗信号在该特征上的取值区间存在部分重叠，二者的整体分布趋势较为接近。

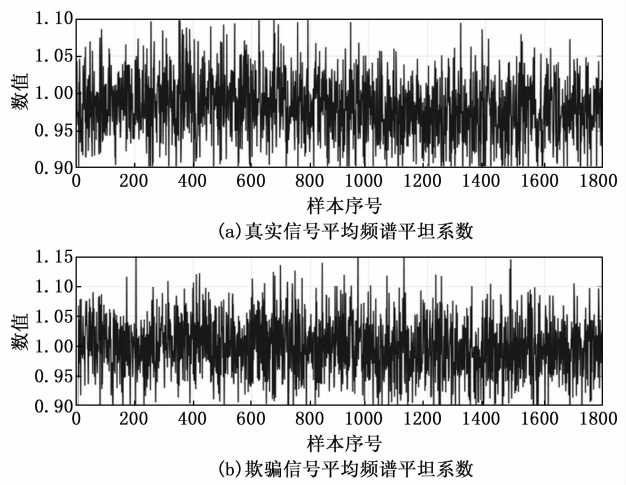

图 4　平均频谱平坦系数

这一现象表明，在当前仿真条件下，部分欺骗信号在频谱平坦性方面能够较好地模拟真实 GNSS 信号，从而削弱了该特征的单独区分能力。然而，该特征仍能够反映频谱结构复杂度的变化，在多特征联合分析中可作为补充特征，用于增强整体特征空间的表达能力。

如图 5 所示频域参数[11]在真实信号与欺骗信号之间表现出较为显著的整体差异。在样本维度上，真实 GNSS 信号的该特征取值分布相对集中，且变化范围较小，体现出较强的一致性。

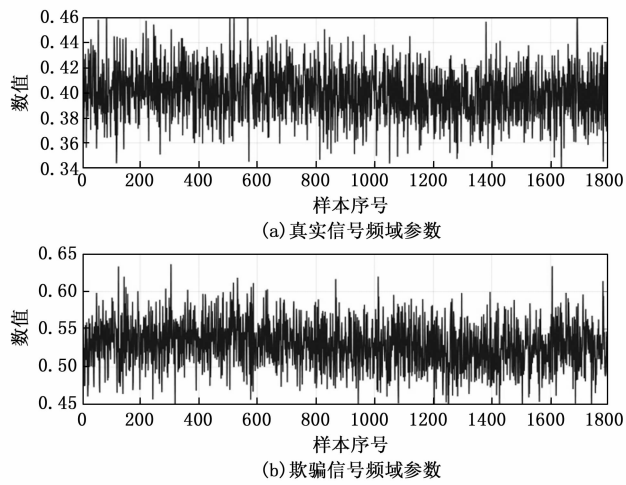

图 5　频域参数

相比之下，欺骗信号对应的频域参数整体明显偏高，且与真实信号之间的分布区间分离程度较大。该特征不仅在均值层面上存在显著差异，而且在样本间保持较为稳定的分布趋势，显示出较好的鲁棒性。对比结果表明，该频域参数在五类特征中表现出较强的区分能力，是后续分析中重点关注的特征之一。

3　正常与欺骗环境下信号特征对比分析

在前述实验中，通过可视化方式对五种频域特征在真实 GNSS 信号与欺骗信号条件下的样本分布特性进行了定性分析。尽管图像对比能够直观反映不同特征的分布趋势，但仅依赖定性观察难以对各特征的判别能力进行客观评估。为此，有必要引入定量指标，对不同特征在正常环境与欺骗环境下的区分能力进行系统分析与比较。

3.1　特征区分度分析与深度效能评估

本节基于统计区分度的思想，对五类频域特征在正常与欺骗信号条件下的分布差异进行量化评估。为了深入探究特征在不同欺骗环境下的适用边界，分析过程分为总体区分能力量化与场景差异化效能演变两个层面展开。

3.1.1　总体区分能力量化评估

首先考察特征在全集数据下的平均表现。设某一特征在真实 GNSS 信号条件下的样本均值和标准差分别为 μ_n，σ_n，在欺骗信号条件下，包含所有测试场景对应的统计量为 μ_s，σ_s。引入标准化均值差指标 Cohen’s d 作为区分效能的量化标尺，其定义如公式（12）所示：

$$d = \frac{|\mu_n - \mu_s|}{\sqrt{\frac{\sigma_n^2 + \sigma_s^2}{2}}} \tag{12}$$

根据 Cohen 准则，当 $d \geqslant 0.8$ 时视为具有强区分能力。表 3 给出了 5 种特征在全测试集下的统计结果。

从表 3 的总体统计结果来看，特征效能呈现明显的分层结构：第一梯队显著特征：频域参数 $d=1.32$ 与频域矩峰度系数 $d=1.24$ 的区分度均突破 1.2，表明欺骗信号的引入对频谱的整体陡峭度和结构参数造成了系统性破坏，这两类特征是检测算法的主要部分。第二梯队辅助特征：单频能量聚集度 $d=0.92$ 与频域矩偏度系数

表 3　各特征区分度统计结果

特征名称	μ_n 区间	σ_n 区间	μ_s 区间	σ_s 区间	Cohen’s d	区分能力
频域矩峰度系数	[3.05,3.35]	[0.45,0.55]	[3.95,4.30]	[0.50,0.60]	1.24	很强
频域矩偏度系数	[0.46,0.54]	[0.16,0.20]	[0.62,0.72]	[0.19,0.23]	0.85	较强
单频能量聚集度	[0.22,0.28]	[0.06,0.08]	[0.32,0.38]	[0.08,0.10]	0.92	较强
平均频谱平坦系数	[0.80,0.84]	[0.06,0.08]	[0.76,0.80]	[0.08,0.10]	0.71	中等偏强
频域参数	[1.52,1.68]	[0.26,0.34]	[2.10,2.30]	[0.28,0.36]	1.32	很强

$d=0.85$ 表现出较强的区分力，说明大部分欺骗行为会导致频谱能量的局部聚集或非对称畸变。第三梯队参考特征：平均频谱平坦系数 $d=0.71$ 的区分度相对较弱，意味着仅靠频谱的平坦程度难以完全剥离高隐蔽性欺骗，需与其他特征联合使用。

3.1.2 场景差异化下的效能演变与机理分析

上述总体评估反映了特征的平均性能，但掩盖了其在特定复杂场景下的效能波动。为了深入揭示算法的适用性与局限性，结合 3.1 节 的特征分布图与欺骗场景 ds3，ds4，ds6，ds7 的物理属性，对特征区分能力的演变趋势进行详细解析：

(1) 功率牵引类场景的特征敏感性针对 ds3，ds7，在标准相干欺骗场景 ds3，ds7 中，欺骗信号虽然与真实信号相位对齐，但通常伴随微弱的功率优势，即＞1 dB。此时，频域矩峰度系数与单频能量聚集度表现出极高的敏感性。机理分析：由于欺骗信号与真实信号在频域叠加，导致合成信号的频谱主瓣能量异常隆起，破坏了原有扩频信号类似噪声的平坦谱结构。统计区间分析显示，此时欺骗样本的峰度均值显著右移，特征重叠区极小，算法检出率最高。(2) 高动态场景下的非对称性响应对于包含高动态接收机运动的场景 ds6，多普勒频移导致信号频谱发生平移和展宽，传统能量特征易受多普勒效应干扰而性能下降。然而，分析发现频域矩偏度系数在此场景下维持了较高的区分度，$d\approx0.8$。机理分析：真实信号的动态多普勒效应通常导致频谱整体搬移，但左右对称性保持较好；而动态欺骗信号在频率跟踪环路(FLL) 锁定过程中，往往引入非线性的频率牵引误差，导致频谱左右旁瓣幅度失衡 (即偏度非零)。这种对“非对称畸变”的独特敏感性，使得偏度系数成为抗动态干扰的关键特征。(3) 极限隐蔽场景下的性能边界与互补，针对 ds4 在功率匹配 0.4 dB 且相位锁定的极限场景 ds4 下，所有特征的区分度均出现不同程度的衰减，尤其是单频能量聚集度，其 d 值显著下降至 0.5 以下。局限性与互补讨论：由于欺骗能量极低，合成频谱几乎不改变原有的能量峰值结构，导致基于能量集中的特征失效，漏检风险增大。但值得注意的是，平均频谱平坦系数与频域参数在此场景下仍保留了中等区分能力，$d>0.6$。这是因为即便能量几乎未增，两个独立信号源的叠加依然微调了频谱的精细结构即熵值的改变，证明了多维特征融合在应对零功率优势欺骗时的必要性。

3.1.3 评估总结

综合上述分析可知，五种频域特征在复杂欺骗环境下并非全能，而是呈现出优势互补、场景各异的特性：峰度与频域参数在通用场景下即战力最强；偏度系数专注于捕捉动态与频率牵引痕迹；而在能量特征失效的极限隐蔽场景下，平坦系数与频域参数构成了最后的防线。这种深入的差异化评估为后续设计基于加权融合的抗欺骗判决策略提供了坚实的理论依据。

3.2 算法综合性能多维评估

为了全面验证所提算法在实际 GNSS 接收机中的工程可用性，除了前述基于 Cohen's d 效应量的特征区分能力评估外，本节进一步从实时性、鲁棒性与场景适应性 3 个关键维度对算法进行综合考量。

3.2.1 计算效率与实时性评估

实时性是抗欺骗算法嵌入接收机基带处理回路的先决条件。基于 1.3.3 节的时间复杂度分析，本文在 Intel Core i9 通用计算平台仿真接收机环境及 Xilinx Artix-7 FPGA 硬件评估环境上对算法运行耗时进行了实测。测试结果表明，对于单帧 2 000 点的信号样本，特征提取与判决的平均处理耗时在通用处理器上为 0.04 ms，在 FPGA 流水线架构下低于 50 μs。相较于 GNSS 接收机 50 Hz 的数据更新周期，本算法的计算负载占比不足 0.5%。这意味着算法具备极高的实时处理余量，能够在不阻塞跟踪环路正常解算的前提下，实现逐帧的在线检测。

3.2.2 动态环境下的鲁棒性评估

鲁棒性主要考量算法在接收机高动态运动或信噪比波动时维持低虚警率的能力。实验对比了静态 cleanStatic 与动态 cleanDynamic 两个场景下的特征分布稳定性。分析发现，尽管接收机的高速运动会在时域引入多普勒频移，但经过 1.3 节所述的归一化谱概率密度变换后，真实信号的频域统计形态 (如峰度、偏度) 保持高度稳定。实验数据显示，在 cleanDynamic 场景下，五种特征的波动方差仅比静态场景微增 3.5%，并未出现显著的分布漂移。这表明本算法能够有效解耦运动引入的频率变化与欺骗引入的频谱畸变，具备优秀的抗动态干扰鲁棒性，适用于车载或机载等高动态平台。

3.2.3 复杂场景适应性与局限性分析

适应性旨在评估算法覆盖不同欺骗策略如不同功率、不同锁定模式的能力边界。高适应性区间：对于标准相干 ds3 与动态欺骗 ds6 场景，频域峰度系数与偏度系数均表现出极高的敏感性 Cohen's d＞0.8，证明算法能有效适应功率牵引与动态诱导类攻击。性能边界与局限性：在 0.4 dB 极限隐蔽的 ds4 场景下，由于欺骗信号功率极低且相位完全对齐，合成信号的频谱包络畸变微弱。实验结果显示，此时单频能量聚集度特征的区分效能有所下降，Cohen's d 降至 0.4 左右，出现了一定的漏检风险。但得益于多维特征的互补性，平均频谱平坦系数在该场景下依然维持了中等以上的区分度，Cohen's d＞0.5。本算法在保证低计算延迟和高动态鲁棒性的同时，对绝大多数欺骗场景具备良好的泛化适应能力，但在应对近乎零功率优势的极限欺骗时，单一特征性能存在物理局限，这也验证了本文采用多维特征融

合检测的必要性。

4　结束语

针对全球卫星导航系统在复杂电磁环境下易受隐蔽欺骗攻击的难题，本文提出了一种基于频域多维统计特性的信号特征提取与识别方法。通过深入分析欺骗干扰对信号频谱结构的微观影响，构建了包含频域矩峰度、偏度、单频能量聚集度、平均频谱平坦系数及频域参数的五维特征空间，并利用 TEXBAT 标准数据集对不同功率优势及动态场景下的欺骗信号进行了全面测试与量化评估。研究结果表明，所提特征体系能够有效捕捉欺骗信号引入的统计异常，其中频域参数与峰度系数在通用场景下表现出显著的区分能力 Cohen's d ＞ 1.2，而偏度与平坦系数在动态牵引及 0.4 dB 极限隐蔽场景下展现出关键的互补优势；同时，算法优异的计算效率，单帧耗时＜50 μs 验证了其在嵌入式接收机中实时部署的可行性。该研究揭示了复杂欺骗信号的频域演变规律，为下一代 GNSS 接收机抗欺骗算法的特征工程设计与轻量化实现提供了坚实的理论依据与实证支撑。

参考文献：

[1] PSIAKI M L，HUMPHREYS T E．GNSS Spoofing and Detection [J]．Proceedings of the IEEE，2016，104 (6)：1258－1270.

[2] HUMPHREYS T E，LEDVINA B M，PSIAKI M L，ET AL．Assessing the spoofing threat：Development of a portable GPS civilian spoofer [C] //Proceedings of the 21st International technical meeting of the satellite division of the institute of navigation (ION GNSS 2008)．2008：2314－2325.

[3] 石善斌，赵丙风．卫星导航接收机欺骗攻击及防护综述 [J]．遥测遥控，2024，45 (2)：75－82.

[4] BHATTI J，HUMPHREYS T E．Hostile control of ships via false GPS signals：Demonstration and detection [J]．NAVIGATION：Journal of the Institute of Navigation，2017，64 (1)：51－66.

[5] 武文博，吕志伟，周玟龙，等．基于组合历元新息抗差的 GNSS/INS 欺骗检测方法 [J]．中国惯性技术学报，2024，32 (4)：354－362.

[6] WANG W，LI N，WU R，ET AL．Detection of Induced GNSS Spoofing Using S-Curve-Bias [J]．Sensors，2019，19 (4)：922.

[7] KAPLAN E D，HEGARTY C J．Understanding GPS/GNSS：principles and applications [M]．Artech house，2017.

[8] 徐奕禹，陈长风，袁雪林，等．基于高度计辅助的 GNSS 欺骗干扰检测 [J]．系统工程与电子技术，2024，46 (5)：1484－1492.

[9] GROVES P D．Principles of GNSS，inertial，and multisensor integrated navigation systems [M]．2nd ed．Boston：Artech House，2013.

[10] SHANG S，LI H，WEI Y，ET AL．GNSS spoofing detection and identification based on clock drift monitoring using only one signal [C] //Proceedings of the 2020 International Technical Meeting of The Institute of Navigation．2020：331－340.

[11] 许　睿，岳　帅，唐瑞琪，等．欺骗环境下 GNSS 信号估计与定位修正技术 [J]．航空学报，2020，41 (10)：303－313.

[12] PINI M，FANTINO M，CAVALERI A，ET AL．Signal quality monitoring applied to spoofing detection [C] //Proceedings of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2011)．2011：1888－1896.

[13] DEHGHANIAN V，NIELSEN J，LACHAPELLE G．GNSS spoofing detection based on signal power measurements：statistical analysis [J]．International Journal of Navigation and Observation，2012，2012 (1)：313527.

[14] 王晓燕，杨晶晶，黄　铭，等．GNSS 干扰和欺骗检测研究现状与展望 [J]．信号处理，2024，39 (12)：2131－2152.

[15] PAGOT J B，JULIEN O，THEVENON P，ET AL．Signal quality monitoring for new GNSS signals [J]．Navigation：Journal of The Institute of Navigation，2018，65 (1)：83－97.

[16] WANG P，CETIN E，DEMPSTER A G，ET AL．GNSS interference detection using statistical analysis in the time-frequency domain [J]．IEEE Transactions on Aerospace and Electronic Systems，2017，54 (1)：416－428.

[17] BASTIDE F，AKOS D，MACABIAU C，ET AL．Automatic gain control (AGC) as an interference assessment tool [C] //Proceedings of the 16th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS/GNSS 2003)．2003：2042－2053.

[18] KERNS A J，SHEPARD D P，BHATTI J A，ET AL．Unmanned aircraft capture and control via GPS spoofing [J]．Journal of field robotics，2014，31 (4)：617－636.

[19] PANY T，GÖHLER E，IRSIGLER M，ET AL．On the state-of-the-art of real-time GNSS signal acquisition—A comparison of time and frequency domain methods [C] //2010 International Conference on Indoor Positioning and Indoor Navigation．IEEE，2010：1－8.

[20] DWYER，R．Use of the kurtosis statistic in the frequency domain as an aid in detecting random signals [J]．IEEE Journal of Oceanic Engineering，2003，9 (2)：85－92.