

文章编号: 2095-4980(2021)01-0107-05

## 基于双谱的射频指纹提取方法

贾济铖, 齐琳

(哈尔滨工程大学 信息通信工程学院, 黑龙江 哈尔滨 150001)

**摘要:** 研究了基于通信辐射源射频指纹(RFF)的同类型设备分类识别理论, 通过提取通信信号的围线积分双谱值来作为设备个体识别的特征向量, 使用支持向量机(SVM)分类器进行识别。构建辐射源识别系统, 并使用实测信号进行仿真测试。结果显示该方法具有稳定的识别效果, 且在信噪比(SNR)为-22 dB时, 系统可以达到接近90%的分类识别准确度。这说明本文提出的基于双谱的RFF提取方法有效。

**关键词:** 物理层安全; 射频指纹; 围线积分双谱; 个体识别

**中图分类号:** TN918

**文献标志码:** A

**doi:** 10.11805/TKYDA2019291

## RF fingerprint extraction method based on bispectrum

JIA Jicheng, QI Lin

(College of Information and Communication Engineering, Harbin Engineering University, Harbin Helongjiang 150001, China)

**Abstract:** The classification and recognition theories of the same type of equipment based on the Radio Frequency Fingerprint(RFF) of the communication radiation source are studied. The integral bispectrum values of the communication signal are extracted as the feature vector of the device, and the Support Vector Machine(SVM) classifier is used for identification. After constructing a radiation source identification system, the measured signals are used for simulation testing. The simulation results show a stable recognition effect by using the proposed method, and the system can achieve nearly 90% classification recognition accuracy when the Signal to Noise Ratio(SNR) is -22 dB. This result validates the effectiveness of bispectrum-based RF fingerprint extraction method.

**Keywords:** physical layer security; Radio Frequency Fingerprint(RFF); contour integral bispectrum; individual identification

物联网及 5G 的快速发展, 使彼此链接的无线设备越来越多, 同时也带来了一系列监管与安全的难题。辐射源设备的个体识别技术, 即特定辐射源识别(Specific Emitter Identification, SEI)可用于无线设备的身份认证、设备监管等方面<sup>[1-3]</sup>, 可以有效解决安全隐私问题, 增加物联网的安全性。因此, 同类型辐射源设备的准确识别成为当下通信安全与隐私面对的严峻问题。在军用领域中, 辐射源识别更加重要, 该应用可以针对敌方通信网络进行剖析, 并得到一个有价值的分析结果, 可使我方在电磁战场获得更大优势<sup>[4]</sup>。

辐射源设备个体识别的相关研究, 早期主要从设备的开关机瞬态信号进行分析<sup>[5-6]</sup>。然而在实际情况下, 暂态信号特征存在难以识别同厂家、同工作模式的辐射源个体, 并且为了提取暂态信号, 需要极高的采样率进行数字化等问题。因此利用稳态信号特征对辐射源进行个体识别的研究逐渐增多<sup>[7-10]</sup>。2008 年, Suski 等<sup>[9]</sup>从 802.11a 设备的前导信号中提取功率谱密度构成射频指纹(RFF), 并选择频谱相关分类器用于分类。结果表明, 当信噪比(SNR)大于 6 dB 时, 可实现接近 80%的识别精确度。最近, 有一些基于统计学习和深度学习的设备识别方法, 如, 使用深度学习方法检测物理层属性以识别认知无线电, 实验结果表明, 在 7 个 2.4 GHz 商用 ZigBee 设备上, 识别准确率达到 92.29%<sup>[11]</sup>。还有 2 种方法的组合, 如将双谱作为 RFF, 使用卷积神经网络用于设备识别<sup>[12]</sup>。此外, 还有将信号进行希尔伯特-黄变换, 然后使用深度残差网络对变换后的图进行视觉处理, 最终实现近 98%的识别率<sup>[13]</sup>。

收稿日期: 2019-08-14; 修回日期: 2019-11-06

作者简介: 贾济铖(1997-), 男, 在读硕士研究生, 主要研究方向为通信信号处理等。email:jiajicheng@hrbeu.edu.cn

本文对通信辐射源设备稳态信号段的本质特征进行深入研究,采集实际的对讲机通信信号,并提出一种基于信号高阶谱分析的 RFF 提取方法。通过分析辐射源通信信号的双谱特征来区分同类型的设备,即采用围线积分双谱值作为其特征向量,使用支持向量机(SVM)对其进行分类识别。经过对实测信号的仿真测试,在-22 dB 信噪比(SNR)的条件下识别准确率可以达到 90%。该实验结果表明,本文所用方法提取的稳态特征可以很好地将同类型的不同设备区分开来,且分类过程对高斯噪声不敏感。

## 1 基于双谱的辐射源识别方法

### 1.1 辐射源个体识别相关理论

分类过程可以帮助人们对事物的认识更加深刻,其关键在于重新建立一个感知到的模型,并通过此来认识事物的内涵,获得处理该类事物的统一方法。而分类成功与否,在于对象的模型以及分类方法,并尽量去除主观观点。对于一个对象模型,极为重要的一点是提取针对于此的专有特征<sup>[14]</sup>。对于本文研究的辐射源设备分类识别问题,首要工作是根据待识别对象——辐射源信号的本质特点,构建一个基于该特点的分类方法或系统架构。即使同类型辐射源设备为同厂家、同批次生产,也仍会由于制造容差和漂移容差的存在,导致设备彼此之间有一定的硬件差异,这种差异表现为通信信号独一无二的细微特征,该特征通常被称为辐射源的 RFF。根据 RFF 自动识别一个辐射源,被称为辐射源的指纹识别。一般而言,通信辐射源的分类系统主要由信号采集、预处理、特征变换与提取、分类识别 4 部分组成,见图 1<sup>[3]</sup>。

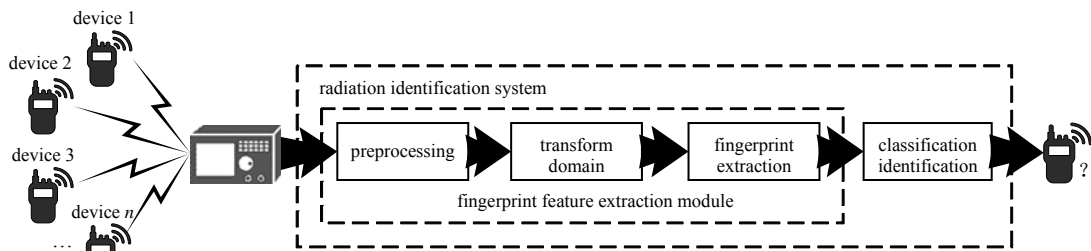


Fig.1 Block diagram of radiation source individual identification system  
图 1 辐射源个体识别系统框图

信号采集装置和预处理模块可以采集到辐射源设备信号,识别及截取有用信号,并去除一定的噪声,获得可以进行特征提取的辐射源射频信号段;特征变换及处理是将信号从时域转换至谱分析域,利于进行下一步的特征提取;指纹特征提取模块将该信号中的细微差异以某种形式提取出,作为辐射源设备的指纹特征;之后将该 RFF 输入分类识别模块进行辐射源设备的识别。如果提取的指纹数据维度过高,可以在分类识别模块之前加入一个数据降维处理模块,提高分类识别的速度及准确度。

### 1.2 基于高阶谱分析的 RFF 提取方法

信号的双谱变换分析,具有相位保持性、尺度变化性、时移不变性的特点,这保证了辐射源信号在经过变换后不会损失过多的有用信息,利于进行辐射源设备的分类识别,且理论上高阶谱分析可以免疫高斯噪声的影响。由于双谱变换得到的双谱图不利于进行分类识别,会耗费大量资源进行二维图像的识别,因此本文使用围线积分双谱方法将二维图像积分为一维函数值,再进行相应的分类识别。

目前研究成熟的围线积分双谱算法有以下 4 种:轴向积分双谱(Axial Integral Bispectrum, AIB)、圆周积分双谱(Circumferentially Integrated Bispectrum, CIB)、径向积分双谱(Radial Integral Bispectrum, RIB)及矩形积分双谱(Square Integral Bispectrum, SIB)。接下来将介绍这 4 种围线积分方法并研究基于此方法的指纹特征提取算法,最后通过实测信号验证该算法的有效性。

首先,信号  $x(t)$  的双谱可表示为:

$$B_x(\omega_1, \omega_2) = \sum_{\tau_1=-\infty}^{\infty} \sum_{\tau_2=-\infty}^{\infty} c_{3x}(\tau_1, \tau_2) e^{-j(\omega_1\tau_1 + \omega_2\tau_2)} \quad (1)$$

式中:  $C_{3x}(\tau_1, \tau_2) = \int_{-\infty}^{+\infty} x^*(t)x(t+\tau_1)x(t+\tau_2)dt = E\{x^*(t)x(t+\tau_1)x(t+\tau_2)\}$  为信号的三阶相关函数;  $\tau_1$  与  $\tau_2$  为相关函数的自变量,代表着 2 个延时;  $\omega_1$  与  $\omega_2$  为双谱二维平面的轴。

1) 轴向积分双谱：轴向积分双谱算法主要是将双谱平面沿  $\omega_1$  或  $\omega_2$  轴进行积分运算，对于信号  $x(t)$ ，假定其双谱为  $B(\omega_1, \omega_2)$ ，定义：

$$AIB(\omega) = \frac{1}{2\pi} \int_{-\infty}^{\infty} B(\omega_1, \omega_2) d\omega_2 = \frac{1}{2\pi} \int_{-\infty}^{\infty} B(\omega_1, \omega_2) d\omega_1 \quad (2)$$

由 Fourier 变换投影可知，轴向积分双谱可以看做信号的三阶相关函数轴切面的傅里叶变换。

2) 圆周积分双谱：圆周积分双谱算法的积分路径为一系列以原点为圆心的同心圆周，将同心圆周上的双谱值进行离散求和即可得到 CIB 值，其具体定义为：

$$CIB(\alpha) = \int B_p(\alpha, \theta) d\theta \quad (3)$$

式中  $B_p(\alpha, \theta)$  为双谱估计的极坐标表示。CIB 保留了一定的相位信息，并且存在尺度伸缩不变性，但积分路径较之其他几种积分方法较为复杂，实际操作中还会因为非均匀采样导致平面点的遗漏和重复计算。

3) 径向积分双谱：径向积分双谱是通过将对双谱平面内，经过原点的直线路径上的双谱值进行离散求和得到。根据积分双谱相位，RIB 定义为：

$$RIB(\alpha) = \arctan\left(\frac{I_i(\alpha)}{I_r(\alpha)}\right) \quad (4)$$

式中： $I_i(\alpha)$  和  $I_r(\alpha)$  分别为双谱积分的同相及正交分量， $I(\alpha) = I_r(\alpha) + jI_i(\alpha) = \int_0^{1/(1+\alpha)} B(f_1, \alpha f_1) df_1$ ， $B(f_1, \alpha f_1)$  为信号的双谱值。径向积分双谱保留了双谱的相位信息，却缺乏信号的尺度信息，因此其对形状相似的信号彼此的识别有着较大的影响。

4) 矩形积分双谱：矩形积分双谱将双谱平面上以双谱原点为中心的系列矩形的各条边作为积分路径进行累加运算，具体的 SIB 积分计算为：

$$SIB(\omega) = \oint_{S_r} B(\omega_1, \omega_2) d\omega_1 d\omega_2 \quad (5)$$

式中  $S_r$  表示矩形积分双谱的积分路径。从 SIB 的计算过程知，SIB 可以充分利用双谱平面中的特征信息，不会出现点的遗漏和重复计算。

计算信号双谱，并经过围线双谱积分即可得到一组一维向量，作为其 RFF 向量进行分类识别处理。

### 1.3 RFF 特征向量的特点

提取的辐射源 RFF 应具备以下特点<sup>[3]</sup>：a) 通用性：对于发送设备，均可以使用该提取方法得到可进行个体识别的 RFF；使用的接收设备应是通用的，即提取的 RFF 不随接收机改变而改变，这是应用 RFF 进行广泛的设备识别的前提；b) 唯一性：不同无线设备发送的射频信号不同，而同一个设备的 RFF 应是独有的、唯一的，这是进行个体识别的重要因素；c) 短时不变性：提取的 RFF 应具有一定的时间稳定性，不应随着时间推移、设备的运行时间及老化等而产生变化，导致识别精确度下降；d) 独立性：从承载数据的稳态信号段提取出的 RFF 应与承载的数字信息无关，只与设备的硬件特征有关。

根据上述提取 RFF 的原则，通过实测数据对本文所提出的基于双谱的 RFF 特征提取方法进行验证，结果表明该方法提取的 RFF 符合上述特征。

## 2 个体识别算法

### 2.1 数据采集

使用对讲机设备进行实测数据的采集和算法的仿真实验验证。为充分验证算法的有效性，待识别设备选用同批次生产的同型号 10 台对讲机，型号为摩托罗拉 A12。为保证接收信号质量，采用示波器进行信号的采集。具体的设备采集参数见表 1。

表 1 实测信号参数

Table 1 Measured signal parameters

modulation	working frequency/MHz	sampling rate/MHz	sampling points
FM	410	24	350 000

每台对讲机采集 50 次开关机状态信号，总计得到 500 个射频信号。为验证算法的泛化性能，采用交叉验证的方法划分训练和测试数据集，其中训练和测试样本的比例为 3:2。

不考虑实际信道中的多径、时延等因素的影响，实际信号采集过程中，采用线缆直接与接收机相连接的方式，但同时加入加性高斯白噪声信道环境条件，测试所提算法的有效性及准确度，以及该算法对高斯噪声的敏感程度。

2.2 分类识别算法

采集到信号后，将其标记为  $\{S_i, i=1,2,3,\dots,10\}$ 。将第  $l$  个对讲机输出信号的第  $k$  个采样信号记为  $x_k^{(l)}(1), x_k^{(l)}(2), x_k^{(l)}(3), \dots, x_k^{(l)}(N)$ ，其中  $N=350\ 000$  为样本点数， $l=1,2,3,\dots,10$  为要区分的设备编号， $k=1,2,3,\dots,50$  为观测到的数据组数。

同类辐射源设备个体识别系统整体框图见图 2。

步骤 1 对示波器采集到的信号  $\{S_i, i=1,2,3,\dots,10\}$  进行预处理，基于变点检测函数 `findchangepts`<sup>[15]</sup> 进行样本信号的起始点检测，截取射出射频信号的稳态段。

步骤 2 在预处理后的  $\{S_i, i=1,2,3,\dots,10\}$  信号上依次加上不同功率的高斯噪声，以达到不同信噪比的研究要求。求取每个样本信号  $x_k^{(l)}(t)$  的双谱，并分别计算其 4 种围线积分双谱值，作为其 RFF 向量。

步骤 3 使用鲁棒主成分分析法(Robust Principal Component Analysis, RPCA)降低 RFF 向量的维度，减少噪声、强相关成分的影响。通过降维可以减小分类过程的负担，增加分类识别的时效性和准确性。

步骤 4 将降维后的 RFF 向量输入到基于高斯核函数的支持向量机进行 3:2 的训练与测试，并进行 5 次交叉实验，计算其平均识别准确率。

步骤 5 对支持向量机输出的预测标签进行观察，绘制混淆矩阵深入分析。

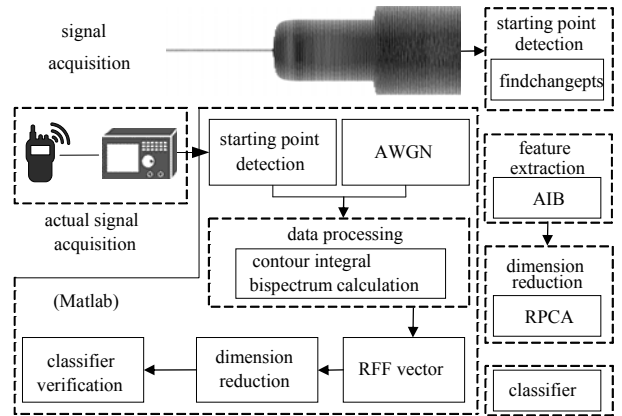


Fig.2 Block diagram of RFF extraction method based on contour integral bispectrum

图 2 基于围线积分双谱的 RFF 提取方法框图

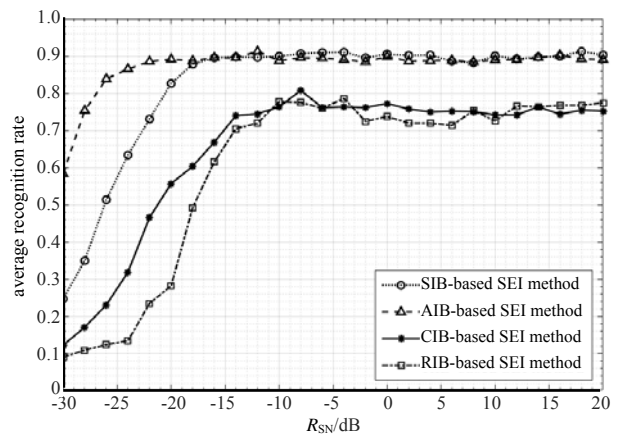


Fig.3 Average recognition rate as a function of signal to noise ratio

图 3 平均识别率随信噪比变化曲线

3 实验与分析

通过对实际采集信号的实验测试，根据步骤 4 得到 4 种围线积分双谱方法平均识别率随信噪比的变化曲线，如图 3 所示。由图 3 可知，基于 AIB 和 SIB 的特征提取方法的识别率明显优于其他 2 种算法，主要是因为这 2 种双谱积分方法在极坐标下进行运算，即使双谱面中离散点的分布在极坐标中不均匀，在实际操作过程中，它们也将被相邻点取代，因此保留了大部分的双谱特征。由图 3 还可看出，当 SNR 高于 -20 dB 时，基于 AIB 和 SIB 的特征提取方法可达近 90% 的分类识别率，这表明双谱特征提取方法受高斯白噪声的影响很小，这也验证了前文的观点，即高阶谱特征可以很大程度地抑制高斯噪声。

根据步骤 5 绘制混淆矩阵进一步分析，以效果最好的基于 AIB 提取方法为例，在 SNR 为 20 dB 下进行，得到图 4 所示的混淆矩阵。其中，矩阵图中数字为设备个数，列摘要为每个预测类的正确和错误分类的观察数，显示为相应预测类的观察数的百分比；行摘要为每个真实类的正确和错误分类的观察数，显示为相应真实类的观察数的百分比。可看出，设备 1,4,7 和 10 很好地被区分出来，其中设备 3 的识别效果最差，并且该方法容易将设备错分为设备 4，这种情况的误分类率达 37.5%，同时也使得设备 4 的识别率达到 100%。

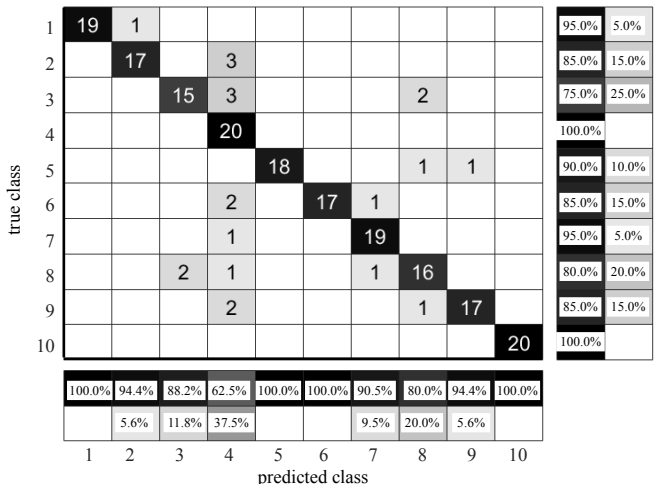


Fig.4 Classification result confusion matrix based on AIB method

图 4 基于 AIB 方法的分类结果混淆矩阵

整体看，该方法可达到 90% 的分类准确度，较之传统的基于功率密度分析方法提升了 10%，且对高斯噪声不敏感，实验结果表明文中的 RFF 提取方法是稳健可行且有效的。

#### 4 结论

本文采用高阶谱分析中的双谱分析进行辐射源设备的分类识别。其中，提取的围线积分双谱值，作为特征向量准确地描述了辐射源信号之间的区别，符合 RFF 应具备的 4 个特点，且对环境中的高斯噪声有较强的抑制能力。对实际信号使用本文的特征提取方法，将得到特征向量输入 SVM 中得到了较好的识别效果，解决了同类辐射源设备的个体识别问题，为后续接下来有关不同类、复杂环境下的辐射源个体识别研究奠定了一定的基础。

#### 参考文献：

- [1] DANEV B,ZANETTI D,CAPKUN S. On physical-layer identification of wireless devices[J]. ACM Computing Surveys, 2012,45(1):1-29.
- [2] REISING D R,TEMPLE M A,JACKSON J A. Authorized and rogue device discrimination using dimensionally reduced RF-DNA fingerprints[J]. IEEE Transactions on Information Forensics and Security, 2015,10(6):1180-1192.
- [3] 俞佳宝,胡爱群,朱长明,等. 无线通信设备的射频指纹提取与识别方法[J]. 密码学报, 2016,3(5):433-446. (YU Jiabao, HU Aiqun,ZHU Changming,et al. RF fingerprinting extraction and identification of wireless communication devices[J]. Journal of Cryptologic Research, 2016,3(5):433-446.)
- [4] 唐哲,雷迎科. 基于最大相关熵的通信辐射源个体识别方法[J]. 通信学报, 2016,37(12):171-175. (TANG Zhe,LEI Yingke. Method of individual communication transmitter identification based on maximum correntropy[J]. Journal on Communications, 2016,37(12):171-175.)
- [5] DANEV B,CAPKUN S. Transient-based identification of wireless sensor nodes[C]// Proceedings of the 8th International Conference on Information Processing in Sensor Networks(IPSAN 2009). Piscataway,US:IEEE, 2009:25-36.
- [6] REHMAN S U,SOWERBY K,COGHILL C. RF fingerprint extraction from the energy envelope of an instantaneous transient signal[C]// Communications Theory Workshop. Piscataway,US:IEEE, 2012:90-95.
- [7] KOHNO T,BROIDO A,CLAFFY K C. Remote physical device fingerprinting[J]. IEEE Transactions on Dependable & Secure Computing, 2005,2(2):93-108.
- [8] TOMKO A A,RIESER C J,BUELL L H. Physical-layer intrusion detection in wireless networks[C]// 2006 IEEE Military Communications Conference(MILCOM 2006). Washington,DC,USA:IEEE, 2007:1-7.
- [9] SUSKI II W C,TEMPLE M A,MENDENHALL M J,et al. Using spectral fingerprints to improve wireless network security[C]// 2008 IEEE Global Telecommunications Conference. New York:IEEE, 2008:2185-2189.
- [10] POLAK A C,GOECKEL D L. Wireless device identification based on RF oscillator imperfections[J]. IEEE Transactions on Information Forensics and Security, 2015,10(12):2492-2501.
- [11] MERCHANT K,REVAY S,STANTCHEV G,et al. Deep learning for RF device fingerprinting in cognitive communication networks[J]. IEEE Journal of Selected Topics in Signal Processing, 2018,12(1):160-167.
- [12] DING L,WANG S,WANG F,et al. Specific emitter identification via convolutional neural networks[J]. IEEE Communications Letters, 2018,22(12):2591-2594.
- [13] PAN Y,YANG S,PENG H,et al. Specific emitter identification based on deep residual networks[J]. IEEE Access, 2019(7): 54425-54434. DOI: 10.1109/ACCESS.2019.2913759.
- [14] 蔡忠伟,李建东. 基于双谱的通信辐射源个体识别[J]. 通信学报, 2007,28(2):75-79. (CAI Zhongwei,LI Jiandong. Study of transmitter individual identification based on bispectra[J]. Journal on Communications, 2007,28(2):75-79.)
- [15] Matlab documentation findchangepts[EB/OL]. (2016-01-01)[2019-06-24]. [https://ww2.mathworks.cn/help/signal/ref/findchangepts.html?SearchHighlight=findchangepts&s\\_tid=doc\\_srchttitle](https://ww2.mathworks.cn/help/signal/ref/findchangepts.html?SearchHighlight=findchangepts&s_tid=doc_srchttitle).