文章编号:1671-4598(2019)09-0141-05 DOI:10.16526/j.cnki.11—4762/tp.2019.09.031 中图分类号:U675.75 文献标识码:A

基于软件无线电平台的电子侦察系统设计

武 征
(中国人民解放军92941部队94分队,辽宁 葫芦岛 125000)

摘要:软件无线电(SDR)主要是基于一种通用平台进行功能的软件化处理,具有设计自由度高,可快速开发原型系统的优点,目前越来越多的电子设备采用了软件无线电的设计思想,用于设计电子侦察系统也成为了一种新的趋势;文章设计了一套基于PXI总线的小型双通道电子侦察原型硬件系统,采用NI的USRP RIO软件无线电平台,开发扫描侦收与采集软件和数据回放分析软件,应用脉宽与重频估计算法、调制体制/载频/码率联合估计算法以及信号带宽估计算法,可实现对L/S/C频段电磁信号的扫描侦收与数据采集和分析;通过无线试验验证了这些功能可实现;数据分析结果可以看出,对采集信号的载频估计、符号速率估计、信号带宽识别、调制体制识别结果正确,实现了对算法的优化设计,并可以此为基础快速验证电子侦察系统中的参数识别算法性能。

关键词:软件无线电;双通道;电子侦察;原型系统

Design of Electronic Investigation System Based on Software Radio Platform

Wu Zheng
(Unit 92941 of PLA, Huludao 125000, China)

Abstract: The software radio is mainly software processing of functional development Based on a universal platform, has the advantages of high degree of freedom of design and rapid development of the prototype system, at present, more and more electrionic devices adopt the idea of software radio design, the design of electronic detection system has also become a new trend. In this pape, a small dual—channel electronic detection prototype hardware system based on PXI bus is designed. using NI's USRP RIO software radio piatform , development of scanning detection and acquisition software and date playback analysis software, application of pulse width and repetition frequency analysis method, modulation system/carrier/code rate joint estimation algorithm and signal bandwidth estimation algorithm, can realize scanning and data acquisition analysis of L/S/C—band electromagnetic signal. It is verified by wireless experiments that these functions can be realized. As can be seen from the results of the data analysis, The carrier frequency estimation, symbol rate estimation, signal bandwidth recognition and modulation results of the collecteded signal are correct, the optimization design of the algorithm is realized, and the performance of parameter recognition algorithm in electronic investigation system can be verified quickly on the basis of this mentod.

Keywords: software defined radio; two—channels; electronic reconnaissance; prototype system

0 引言

电子侦察系统在现代电子战中扮演着十分重要的角色,是获取敌方目标、通信等情报的主要技术手段,可为针对敌方目标实施电磁干扰或者精确打击提供重要依据。近几年来,随着软件无线电(SDR)技术的迅猛发展及其在无线通信系统应用上取得的巨大成功,采用软件无线电的思想设计电子侦察系统也成为了一种新的思路。

NI的软件无线电平台结合了先进的射频收发仪和LabVIEW图形化开发环境,可用于快速开发无线系统。本文采用的USRP RIO软件无线电平台用途十分广泛,不仅可用于无线通信系统的快速开发,还可用于动态频谱接入、认知无线电、频谱感知、波束成形、雷达系统原型设计等多个领域[1-2]。目前国内外已有多所知名大学和研究机构利用基于USRP + LabVIEW的软件无线电平台进行系统开发,如加州大学伯克利分校Milos等设计的一种协作式MIMO[3]、韩国国家交通大学Yooho Shin等人设计的IEEE 802.11p收发仪[4]、东南大学阳析等设计的基于NI平台的大规模MIMO 5G原型验证系统[5]、北京邮电大学谢轩设计的远程人脸识别系统[6]以及张骞等设计的实时无线电频谱Web发布系统[7]等。

本文旨在利用USRP RIO软件无线电平台实现现代电子战中电子侦察原型系统的设计,可实现频谱扫描、实时频谱显示、单通道驻守、数据采集、数据回放和参数分析等电子侦察系统常用的功能,并可以此为基础快速验证电子侦察系统中的参数识别算法性能。

1 电子侦察原型系统硬件设计

1.1 系统硬件组成

本文设计的小型双通道电子侦察原型系统的硬件组成如图1所示,主要由PXI机箱、PXI嵌入式控制器模块、数据交互模块、USRP RIO软件无线电平台以及接收天线组成,其中PXI嵌入式控制器模块采用数字信号处理器可完成若干调制格式和介入模式的解调和编码,同时也可完

收稿日期:2019-01-06; **修回日期**:2019-04-11。

作者简介:武 征(1969-),男,辽宁昌图人,机电控制专业硕研,高级工程师,主要从事测控靶标总体技术方向的研究。

成产生上变频，转换成模拟波形进行放大和带通滤波。控制器模块和数据交互模块是以板卡形式插入 PXI 机箱的插槽中的，USRP RIO 通过 PCIe 高速线缆连接到数据交互模块。PXI 嵌入式控制器模块内嵌 Windows 操作系统，可运行 LabVIEW 软件开发环境和上位机控制软件；USRP RIO 实现了对射频信号的侦收和基带数据采集功能，并通过数据交互模块与上位机控制软件进行基带数据的传递。

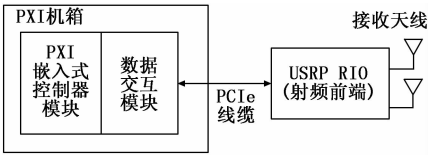

图 1 电子侦察系统原型硬件组成

1.2 USRP RIO 软件无线电平台

NI 的 USRP RIO 软件无线电平台提供了集成的硬件和软件解决方案，可快速构建高性能无线通信系统。每台 USRP RIO 都有两个射频收发信道（RF0 和 RF1），且每个信道都是 I、Q 两路数据采集，USRP RIO 内部还使用了一片 Xilinx Kintex－7 系列芯片进行信号处理。USRP RIO 的体积只有不到 1U 空间的一半大小，其硬件实物图及内部架构分别如图 2 和图 3 所示。从图 3 可以看出，USRP RIO 的内部架构主要由信号处理电路、总线控制电路、存储器、模数与数模转换电路和两个射频通道组成。

图 2 USRP RIO 软件无线电平台硬件实物图

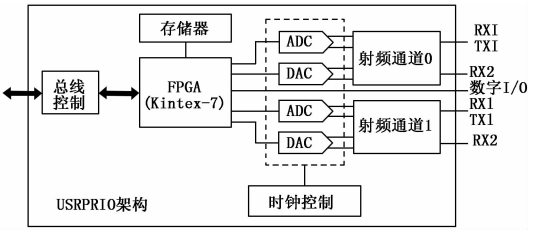

图 3 USRP RIO 软件无线电平台内部架构

USRP RIO 的内部数据处理过程及数据流向如图 4 所示[5]，在接收端，天线接收信号后进行正交下变频，通过 ADC 进行采样获得 I、Q 两路基带数据，然后在 FPGA 内部实现 I/Q 平衡、频率偏移与分数抽取，然后对信号进行处理（可自定义），并通过 DMA FIFO 上传数据到上位机软件进行处理与显示；在发射端，上位机将基带数据通过 DMA FIFO 下传到 FPGA 内部的信号处理模块（可自定义），对数据完成处理之后再进行分数内插、频率偏移、I/Q 平衡等处理，然后转换成 I、Q 两路基带调制信号，通过 DAC 进行数模变换，最后再将基带信号上变频到射频，并通过天线发射出去。收发本振分别采用不同的锁相环（PLL）进行控制，通过上位机可配置为中心频点在 1.2～6 GHz 的射频信号。

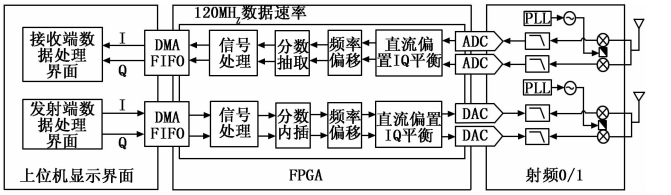

图 4 USRP RIO 内部数据处理过程及数据流向

本文采用了 USRP 2943R 软件无线电平台进行设计，其主要性能参数如表 1 所示。

表 1 USRP 2943R 主要指标参数

发射信道		接收信道	
信道个数	2	信道个数	2
频率范围	1.2 GHz～6 GHz	频率范围	1.2GHz～ 6GHz
频率步进	＜1 kHz	频率步进	＜1kHz
最大输出功率	1.2～3.5 GHz，17～20 dBm	增益范围	0 dB～37.5 dB
	3.5～6 GHz，7～15 dBm	增益步进	0.5 dB
增益范围	0 dB～31.5 dB	最大输入功率	－15 dBm
增益步进	0.5 dB	噪声系数	5～7 dB
实时带宽	120 MHz	实时带宽	120 MHz
I/Q 最大采样率	200 MS/s	I/Q 最大采样率	200 MS/s
DAC：分辨率	16 bit	ADC：分辨率	14 bit
DAC：SFDR	80 dB	ADC：SFDR	88 dB

2 电子侦察原型系统功能及软件设计

2.1 系统功能描述

小型双通道电子侦察原型系统主要实现了对 L/S/C（1.2～6 GHz）频段内电磁信号的侦察、接收、采集与分析功能，可实现一路扫描侦察和一路驻守采集。扫描通道实现了在可配置的起始频率与截止频率之间的频段内对电磁信号进行扫频侦收，并将扫描频段内的全频谱信息显示在上位机软件界面上。操作人员可依据全频谱信息设置采集通道的接收本振，实现对感兴趣信号的采集功能。该软件还可对采集到的信号数据进行回放，并进行数据分析与参数识别，还可用于引导干扰设备产生干扰信号。

2.2 系统软件设计

电子侦察原型系统采用 LabVIEW 开发环境进行软件设计，主要由两部分组成：扫描侦收与采集软件和数据回放分析软件，软件界面设计如图 5 所示，分为扫描侦收与采集控制界面（图 5 左）和数据回放与分析界面（图 5 右）两个组成部分。

软件总功能及各部分软件的功能如图 6 所示。扫描侦收与采集软件主要实现对硬件设备工作参数的配置、系统工作状态指示、实时频谱显示以及信号数据采集控制；数

图 5　小型双通道电子侦察系统上位机软件界面设计

据回放与分析软件主要实现对信号采集数据的回放、频谱分析以及参数识别。

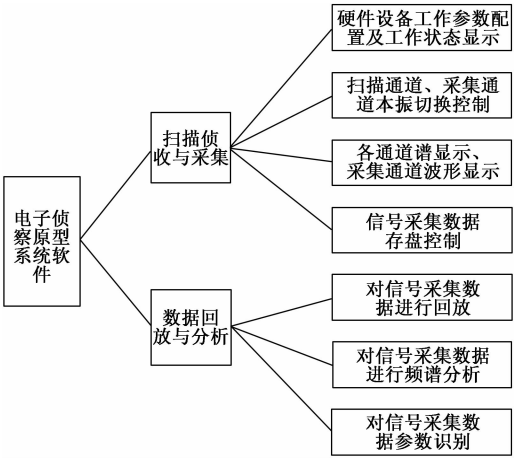

图 6　电子侦察原型系统软件设计

通过扫描侦收与采集软件主控界面可设置扫描通道起始频率和截止频率、采集通道本振、采样率、采样点数、参考电平、数据记录控制以及数据文件存储路径等多个参数，同时可显示全频段频谱图、扫描通道瞬时功率谱、采集通道功率谱、采集通道波形数据以及系统工作状态指示等内容。由于 USRP RIO 可支持 1.2～6 GHz 共 4.8 GHz 的频段，瞬时处理带宽最大为 120 MHz，需要通过扫频的方式以实现全频段频谱分析。本方案中设计扫频步进与采样率相同，为 100 MSps，每 5 ms 切换一次本振，按照 100 MHz 扫频步进计算，扫描整个频段需要 240 ms 的时间。操作人员可以根据全频段频谱图将采集通道本振设置成感兴趣的频点，在采集通道功率谱和采集通道 IQ 数据显示部分观察感兴趣信号的频谱和时域波形，如图 7 所示，同时可以打开数据记录按钮将数据存储到硬盘上。

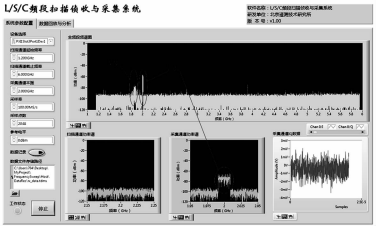

图 7　扫描侦察与采集软件主控界面显示效果

数据回放与分析软件可对信号采集数据进行回放和分析，识别其时域参数、频域参数以及调制参数，同时显示某一段数据的幅度谱、平方谱以及时频谱等频域信息，针对实际采集的一段脉冲信号进行分析的结果如图 8 所示。该信号由信号源产生，脉宽设置为 20 μs，重频设置为 40 μs，采集通道本振与实际信号源输出频率相差 10 MHz，识别结果分别为脉宽 20.06 μs，重频 40 μs，载频 10.00 MHz，信号调制体制识别结果为单频信号，参数估计结果正确。

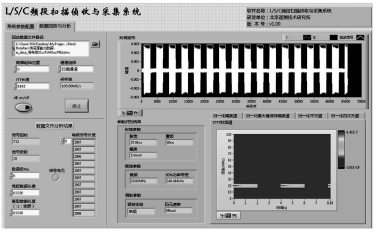

图 8　针对实际采集的信号分析结果显示

3　参数识别算法设计

本文设计的小型双通道电子侦察原型系统可对信号的脉冲宽度（脉宽）、重复频率（重频）、调制体制、载频、码率、带宽进行估计，其中脉宽和重频主要适应雷达脉冲信号，调制体制、载频、码率主要适应几种典型的数字调制信号。

3.1　脉宽与重频估计算法

脉宽与重频识别算法设计如图 9 所示，主要由信号检测、检波、脉冲前后沿统计、脉宽重频计算和平均值统计五个部分。信号检测主要通过时域和频域手段结合的方式，在确定信号有无的同时输出检波结果，然后根据检波信号检测所有上升沿和下降沿的位置，相邻上升沿之间的时间间隔为重频，相邻上升沿与下降沿之间的时间间隔为脉宽，将测量结果中相差很小的结果认为是一个值，统计一组数据中多次测量结果中出现次数最多的测量值，作为脉宽和重频结果的估计值。

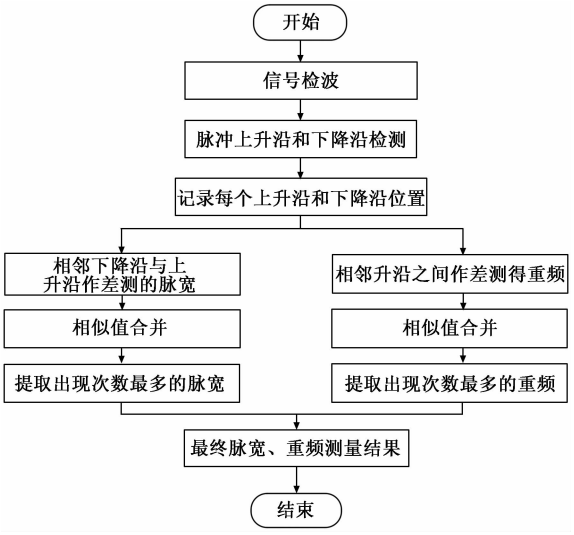

图 9　脉宽与重频估计算法

3.2　调制体制、载频与码率联合估计算法

调制体制、载频与码率联合估计算法实现了对单频信号和 BPSK、QPSK/OQPSK、8PSK、MSK/GMSK 几种常

用数字通信调制信号的分类和参数识别功能。根据相关文献分析[8-9]，这几种数字调制信号的频谱分别具有如表 2 所示的特征（不考虑零频处的频谱），可用于进行分类。

表 2 不同信号类型频谱特征

信号类型	幅度谱特征	平方谱特征	四次方谱特征
单频信号	单根谱峰	——	——
BPSK 调制信号	无明显谱峰	两倍载频处有单根谱峰	零频附近有明显单根谱峰，为符号速率
QPSK/OQPSK 调制信号	无明显谱峰	无明显谱峰	零频附近有明显单根谱峰，为符号速率；四倍载频处有明显单根谱峰
8PSK 调制信号	无明显谱峰	无明显谱峰	无明显谱峰
MSK/GMSK 调制信号	无明显谱峰	二倍载频附近由两根明显谱峰	——

基于表 2 的分析，本文设计并实现了一种基于频谱－平方谱－四次方谱联合分析的调制体制识别与载频、码率估计算法，实现流程如图 10 所示，具体算法步骤如下：

Step 1：对采样信号通过过零检测法粗略估计信号载频，同时计算信号的归一化幅度谱、归一化平方谱和归一化四次方谱；

Step 2：根据载频粗估结果计算一倍载频（fc）、二倍载频（$2fc$）和四倍载频（$4fc$）的频谱位置，并以此提取幅度谱 $fc\pm fc/2$ 范围内的频谱（Spectrum1）、提取平方谱 $2fc\pm fc/2$ 范围内的频谱（Spectrum2）、提取四次方谱 $4fc\pm fc/2$ 范围内频谱（Spectrum3）和 $0\sim fc$ 范围内的频谱（Spectrum4）；

Step 3：统计 Spectrum1～Spectrum3 和归一化平方谱中的过门限谱峰个数，分别为 N1、N2、N3、N4，同时依据下面的决策表进行调制方式的判决以及载频和码率的估计。

表 3 调制识别与载频、码率估计决策表

N1	N2	N3	N4	调制体制识别结果	载频估计结果	码率估计结果
1	1	1	1	单频	谱峰频率	——
＞2	1	1	1	BPSK	Spectrum2 谱峰频率/2	Spectrum4 谱峰频率
＞2	＞2	1	＞2	QPSK、OQPSK	Spectrum3 谱峰频率/4	Spectrum4 谱峰频率
＞2	＞2	＞2	＞2	8PSK	过零检测粗估频率结果	Spectrum4 谱峰频率
＞2	2	2	2	MSK、GMSK	Spectrum2 两谱峰频率之和/2	Spectrum2 两谱峰频率差值

3.3 信号带宽估计算法

信号带宽估计采用能量集中法，其软件实现流程如图 11 所示，实现步骤如下：

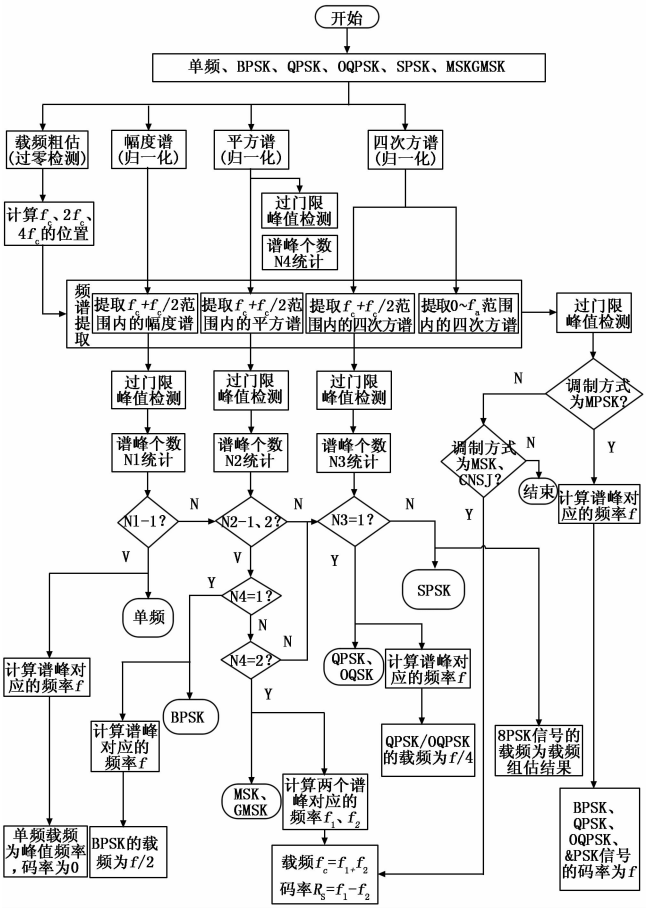

图 10 基于频谱－平方谱－四次方谱联合分析的调制体制识别与载频、码率估计算法

Step 1：对采样信号进行载频估计（参考前面载频估计的算法）和频谱变换，获得信号的幅度谱以及载频在幅度谱上的位置。

Step 2：对幅度谱上所有的点求平方和 S，作为接收带宽内的信号能量；

Step 3：设载频在幅度谱上的位置为 I，以 I 为中心向两边扩展，设扩展参数为 i，计算幅度谱在（$I-i$，$I+i$）范围内的点的平方和 P，作为搜索带宽内的信号能量；

Step 4：计算比值 P/S，若 $P/S\geqslant 90\%$，则进行 Step 5，提取信号带宽估计值；若 $P/S<90\%$，则令 $i=i+1$，若 $i=I$，则进行 Step6；若 $i<I$，重复 Step 3；

Step 5：信号带宽为（$I-i$，$I+i$）范围内的带宽，设幅度谱的频率分辨率为 Δf，则信号带宽为 $2i\Delta f$，带宽估计完成，该带宽估计结果置信度高；

Step 6：信号带宽为 $2I\Delta f$，带宽估计完成，但该带宽估计结果置信度低。

4 电子侦察原型系统无线测试试验

4.1 无线测试试验环境搭建

为了验证本文设计的电子侦察原型系统的基本功能，本文采用了无线试验环境，主要试验设备如表 4 所示。

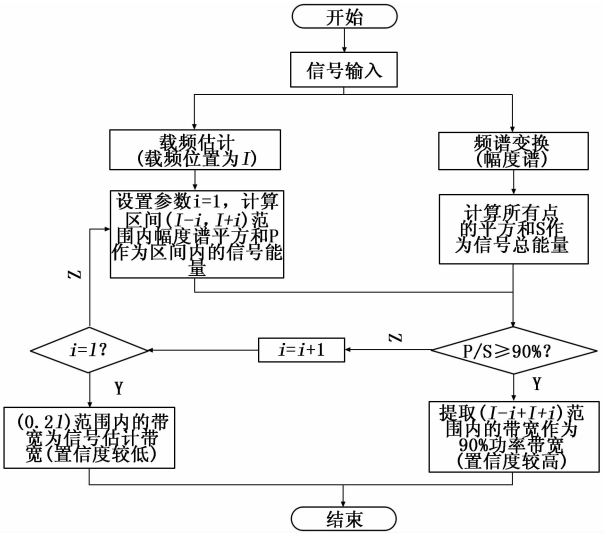

图 11　带宽估计算法软件设计流程

表 4　无线测试试验环境主要设备列表

序号	设备名称	数量
1	PXI 主控机箱	1
2	USRP RIO	2
3	PCIe 连接线	2
4	天线	4

无线测试试验设备连接图如图 12 所示，采用两台 USRP RIO 软件无线电设备，一台作为数字通信原型系统，可模拟典型的通信系统，包括 BPSK、QPSK、OQPSK、8PSK、MSK 和 GMSK 调制以及 OFDM 通信系统，另外一台作为电子侦察原型系统，对通信系统的信号进行侦察采集和参数识别。

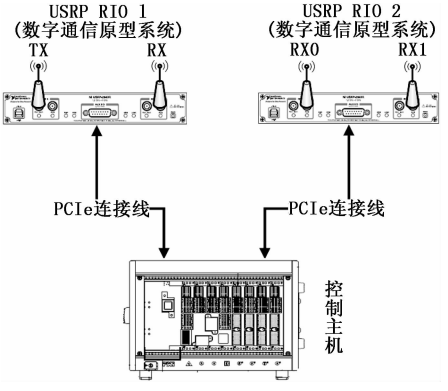

图 12　无线测试试验环境设备连接图

4.2　无线测试数据分析结果

试验过程中分别测试了侦收采集不同调制体制的信号，对其中一次的部分采集数据回放及分析结果如图 13 所示。本次测试中通信原型系统的输出信号配置为 QPSK 调制信号，载频配置为 5 MHz，符号速率配置为 2.5 MBaud，通过数据分析软件的分析结果可以看出，对采集信号的载频估计结果为 5.00 MHz，符号速率估计结果为 2.5 MBaud，信号带宽为 2.49 MHz，调制体制为 QPSK/OQPSK，识别结果正确。

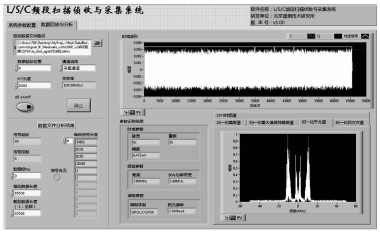

图 13　无线测试试验中针对某配置下数字通信系统的信号分析结果

5　结论

本文基于 NI 的 USRP RIO 软件无线电平台设计了一种小型双通道电子侦察原型系统，是将软件无线电与电子侦察系统结合设计的新理念。该侦察系统可实现对 1.2～6 GHz L/S/C 频段信号的扫描侦收、实时频谱显示、信号采集、信号回放和参数估计等基本功能，并通过无线试验验证了这些功能。

该侦察系统同时采用了 NI 的 LabVIEW 图形化开发环境，可以对软件界面与实际程序进行同步设计，具有很高的设计自由度。不仅如此，以该系统为基础，结合 LabVIEW 开发环境中提供的信号分析工具，可以快速设计并不断加入新的参数识别算法，实现对已有算法的优化设计与快速验证，提升系统性能，极大地缩短了软件开发周期。

参考文献：

[1] National Instruments. USRP RIO Software Defined Radio [EB/OL]. http://www.ni.com.

[2] National Instruments. Overview of the NI USRP RIO Software Defined Radio [EB/OL]. http://www.ni.com/white-paper/52119/en/.

[3] National Instruments. 基于软件无线电的下一代通信系统设计 [EB/OL]. http://www.ni.com.

[4] Nikookhoy Shahin, Nickolas J. LaSorte. 802.11 g channel characterization utilizing labview and NI-USRP [A]. 2013 IEEE International Instrumentation and Measurement Technology Conference (I2MTC) [C]. 2013.

[5] 阳　析. 基于 NI 平台的 Massive MIMO 5G 原型验证系统 [EB/OL]. http://www.ni.com.

[6] 谢　轩. 基于 LabVIEW 和 NI USRP 的远程人脸识别系统设计与实现 [J]. 国外电子测量技术，2016，35 (2)：35-41.

[7] 张　骞，黄　铭，杨晶晶，等. 基于 LabVIEW 和 USRP 的实时无线电频谱 Web 发布系统研究 [J]. 中国无线电，2012，12：62-63.

[8] 刘少林. MPSK 信号调制方式识别与参数估计 [D]. 北京：北京邮电大学，2015.

[9] 赵晓迪. 基于谱分析的通信信号调制识别与参数估计研究 [D]. 成都：西南交通大学，2010.

[10] 韦　平，邵　啸，赵东杰. 基于软件无线电的中频频谱检测方法的优化，兵工自动化，自动测量与控制，2008，27 (10).