ISSN: 2688-8645

Design and FPGA Implementation of Configurable Interference Waveforms for Embedded SDR Systems

Su Liu, Anjin Peng *

School of Electronic Information, Southwest Minzu University, Chengdu, Sichuan, 610225, China

* Corresponding author: Anjin Peng

Abstract

With the continuous evolution of wireless communication systems in terms of architectures, operating frequency bands, and network structures, the communication environment has become increasingly complex and exhibits diversified characteristics. In communication system testing, electromagnetic environment simulation, and countermeasure scenario research, higher requirements have been put forward for the flexibility of jamming signals regarding waveform types, parameter configuration, and transmission modes. However, traditional communication jamming equipment generally suffers from large volume, fixed functionality, and limited waveform types, making it difficult to adapt to rapidly changing application requirements. To address the above issues, this paper designs and implements a configurable jamming waveform generation platform based on an SDR system, focusing on the digital generation methods of various typical jamming waveforms on embedded FPGA platforms. The system utilizes the Zynq-7020 SoC as the signal processing core, combined with the AD9361 integrated RF transceiver chip, to construct a highly integrated baseband processing and RF transmission platform. Parameterized generation and modulation of various jamming waveforms—including single-tone, multi-tone, sweeping-frequency, and broadband noise—are implemented in the Programmable Logic side, with waveform parameter configuration and system operation control completed through the Processing System. Experimental results demonstrate that under limited volume and power consumption conditions, the system can stably generate multiple jamming signal forms, and its RF output spectral characteristics remain consistent with theoretical analysis results, verifying the feasibility and effectiveness of the proposed jamming waveform FPGA implementation method and system architecture.

Keywords

Communication Jamming Signals; Software-defined Radio; FPGA Signal Processing; AD9361.

1. Introduction

In modern wireless communication and information systems, the efficient utilization and management of electromagnetic spectrum resources have become one of the key issues. With the development of communication technology toward broadband, multi-carrier, and digital modulation, communication signals exhibit highly flexible and dynamically changing characteristics in spectral structure and parameter configuration. While this development trend improves communication system performance, it also poses new technical requirements for communication system testing, electromagnetic environment assessment, and related countermeasure research. As one of the important means for studying and verifying communication system robustness[1], the configurability of communication jamming signals in

ISSN: 2688-8645

terms of spectrum coverage, temporal characteristics, and waveform structure is particularly crucial.

Traditional communication jamming equipment usually relies on dedicated hardware or analog circuit implementations[2], featuring relatively fixed structures that make it difficult to support multiple jamming waveform forms on the same platform. Although such equipment has certain advantages in power output and stability, it has obvious deficiencies in system volume, functional scalability, and waveform reconstruction capabilities, which is not conducive to application in miniaturized, distributed, or rapid deployment scenarios. Software-defined radio technology, by migrating signal generation, modulation, and control functions to the digital domain as much as possible, enables the same hardware platform to support multiple communication systems and signal forms through software or logic reconfiguration[3], providing an effective technical approach for the flexible implementation of multi-waveform jamming signals.

Based on the above background, this paper designs and implements a configurable jamming waveform generation platform based on an SDR system, employing the Zynq-7020 SoC and AD9361 RF transceiver chip to build an embedded signal processing platform, with a focus on the digital implementation methods of various typical jamming waveforms in FPGA[4]. The main contributions of this paper include system overall architecture design, signal processing core board implementation, and FPGA implementation and experimental verification of typical jamming waveforms[5], providing a reference for the engineering implementation of configurable jamming waveforms in embedded SDR platforms.

2. System Architecture Design

This chapter describes the overall architecture of the designed system. It first introduces the overall composition of the system and the functions of each functional module; subsequently, combined with the heterogeneous architecture characteristics of the Zynq SoC, it presents the division of control functions and signal processing functions within the system; on this basis, it further analyzes the RF transceiver and baseband signal link structure, and outlines the overall workflow of the system.

2.1. Overview of Miniature Communication Jammer System Architecture

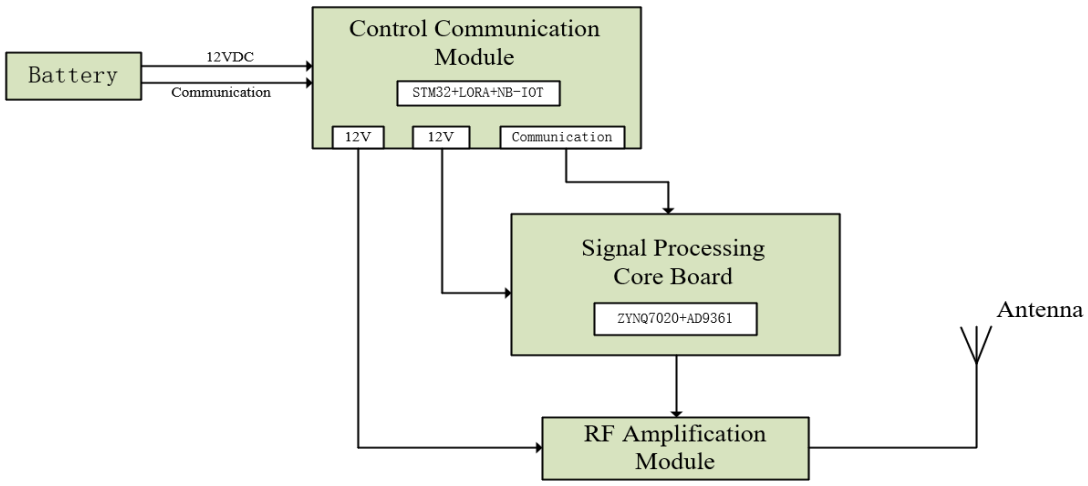


Figure 1. Overall architecture block diagram of the miniature communication jammer

The jamming waveform generation platform designed in this paper takes "configurability, multi-waveform, and miniaturization" as the overall design objectives, adopting a software-

ISSN: 2688-8645

defined radio architecture to implement the generation, modulation, and control functions of communication jamming signals in the digital domain as much as possible. The overall system consists of a signal processing core board, an RF power amplification module, and a battery power supply module with control communication module. The system architecture block diagram is shown in Figure 1.

Among these, the battery power supply module provides stable DC power for the system and implements multi-channel voltage output and power consumption control through the power management unit. The control communication module is responsible for receiving jamming task commands, managing device status[6], and obtaining positioning information, providing a communication foundation for remote scheduling and centralized management of the system[7]. The RF power amplification module amplifies the RF signal output from the core board to meet practical jamming distance and coverage requirements. The signal processing core board serves as the functional core of the entire system, undertaking key tasks such as baseband jamming signal generation, parameter configuration, and RF transmission control[8, 9].It should be pointed out that the system designed in this paper does not involve reconnaissance, demodulation, or high-precision analysis functions of communication signals, but rather serves as a controlled execution platform that generates and transmits specified jamming waveforms according to preset or issued parameters, thereby reducing system complexity while meeting functional requirements and improving engineering feasibility.

2.2. Signal Processing and Control Architecture Based on Zynq SoC

The Zynq-7020 SoC employs a heterogeneous architecture with tight integration between the Processing System and Programmable Logic, providing an excellent foundation for the rational division of control and signal processing functions in the communication jamming system. In this design, system functions are allocated following the principle of "control in PS, signal processing in PL," as shown in Figure 2.

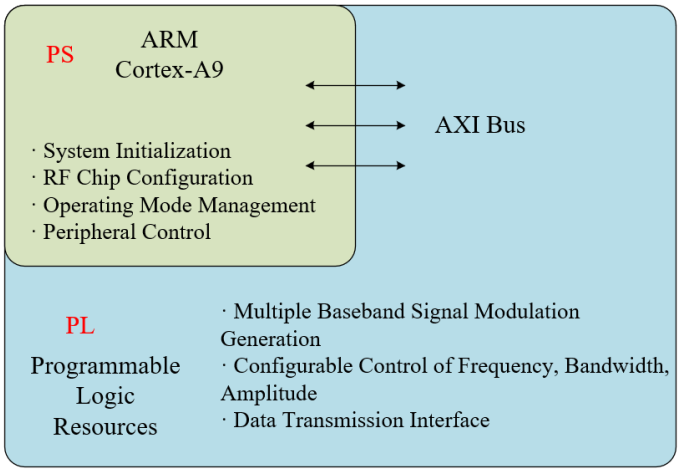


Figure 2. Functional division schematic of Zynq PS-PL

As shown in the figure, the PS side integrates a dual-core ARM Cortex-A9 processor, mainly responsible for system initialization, RF chip configuration, operating mode management, and peripheral control tasks. Given that the AD9361 RF transceiver chip has a large number of registers and a relatively complex configuration process, the PS side performs software configuration through the SPI interface, facilitating online parameter adjustment and system debugging, thereby improving development efficiency[10,11]. The PL side is employed to realize real-time generation and modulation of jamming baseband signals. Leveraging the parallel processing capability of FPGA, it can efficiently implement various jamming waveforms—including single-tone, multi-tone, sweeping-frequency, and broadband noise—

ISSN: 2688-8645

while supporting dynamic configurable control of key parameters. The digital baseband signals generated by the PL side are transmitted to the AD9361 through a high-speed interface to achieve RF signal transmission[12].

This PS-PL collaborative working mode enables the system to guarantee real-time signal processing performance while maintaining system flexibility and engineering maintainability, conforming to the functional reconfigurability requirements of embedded SDR platforms.

2.3. RF Transceiver and Baseband Signal Link Structure

Regarding the RF signal link, this paper employs the AD9361 as the core RF frontend device to realize the conversion from digital baseband signals to RF signals. The AD9361 integrates digital-to-analog converters, up-converters, local oscillator synthesis, and RF transmission chains internally, covering an operating frequency range from 47 MHz to 6 GHz, satisfying the jamming requirements for common communication systems.

In the system, digital baseband signals generated by the PL side are output in I/Q format and transmitted to the AD9361 via the LVDS interface. The basic workflow of the transmission chain is as follows: the baseband processing module inputs I/Q baseband digital signals to the chip through a parallel interface. The signals are processed by the chip's internal programmable polyphase FIR filters and multi-stage interpolation filters, then converted to analog baseband signals by the DAC. Subsequently[13], after filtering through Butterworth LPF and single-pole LPF, amplification and filtering by the TIA, up-conversion to the target RF frequency band by the quadrature mixer, and final RF amplification, the signals are output to the antenna port. The transmission chain structure is shown in Figure 3.

Figure 3. AD9361 transmission chain flowchart

Compared to high-end RF devices using high-speed JESD204B interfaces, this solution offers significant advantages in interface complexity, power consumption, and hardware design difficulty, making it more suitable for miniaturized system implementation. Through software configuration, the system can flexibly adjust carrier frequency, transmission bandwidth, and output power, working synergistically with PL-side jamming waveform parameters to achieve multi-mode, multi-band communication jamming signal transmission.

2.4. System Workflow

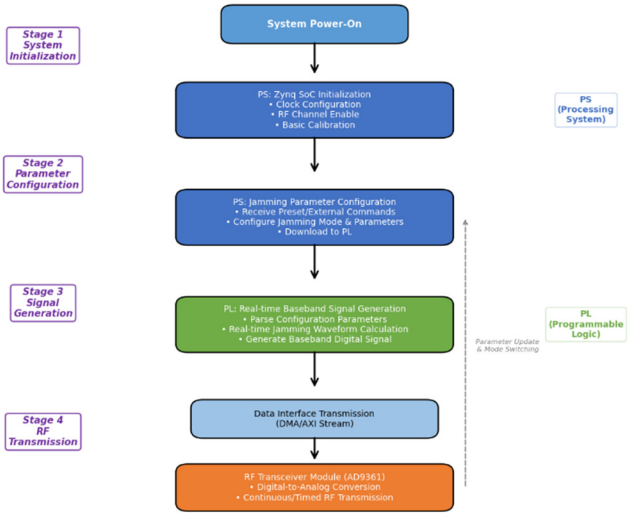


Figure 4. System workflow diagram

ISSN: 2688-8645

The overall system workflow can be summarized into four stages: "system initialization—parameter configuration—jamming signal generation—RF transmission," with the operation flow shown in Figure 4.

After system power-on, the PS side first completes the initialization configuration of the Zynq SoC and AD9361, including clock configuration, RF channel enablement, and basic calibration operations. Subsequently, according to presets or external commands, the PS side transmits jamming mode and parameter information to the PL side. The PL side generates corresponding jamming baseband signals in real-time based on configuration parameters and sends them through the data interface to the RF transceiver module, achieving continuous or timed transmission of jamming signals[14]. This workflow supports rapid switching of jamming waveforms and parameters, providing a unified system framework for subsequent multi-waveform jamming experiments and functional extensions.

3. FPGA Implementation of Jamming Signals

This chapter focuses on the digital generation methods of jamming signals and their FPGA implementation structures. First, the overall implementation approach for digital jamming signal generation is presented. Subsequently, several representative typical jamming signals are selected, and their FPGA implementation methods are explained to provide a foundation for subsequent experimental verification and performance evaluation.

3.1. Overall Approach to Digital Jamming Signal Generation

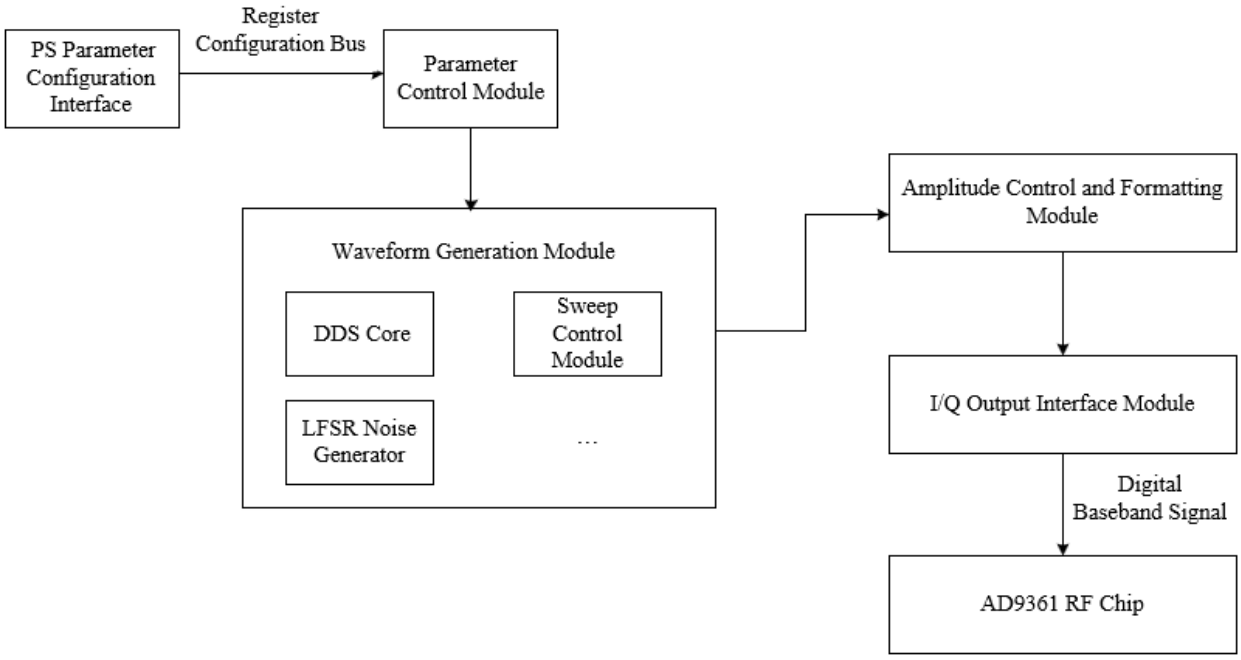


Figure 5. Overall structure block diagram of jamming signal FPGA implementation

In this waveform generation platform, the baseband generation and modulation functions of jamming signals are primarily implemented by the Programmable Logic side of the Zynq-7020. The system adopts a design philosophy of "parameterized waveform generation," where the jamming signal type and its key parameters are controlled through a unified configuration interface, while the specific waveform generation logic is implemented in a modular manner within the PL. In terms of overall structure[15], different jamming modes maintain consistency at the data interface and control channel levels, with differences existing only within the waveform generation modules. This design approach improves FPGA resource reuse efficiency

ISSN: 2688-8645

on one hand, and on the other hand, provides a good structural foundation for subsequent expansion of jamming waveforms.

The jamming signal processing chain on the PL side mainly includes:

(1) Waveform Generation Module: Generates corresponding baseband I/Q signals according to configuration parameters;

(2) Parameter Control Module: Receives control commands from the PS side and completes register configuration;

(3) Amplitude Control and Data Formatting Module: Performs amplitude adjustment and data alignment on the generated digital signals;

(4) I/Q Output Interface Module: Feeds baseband signals to the RF transceiver chip for digital-to-analog conversion and RF transmission.

The overall structure block diagram of the jamming signal FPGA implementation is shown in Figure 5.

3.2. Implementation of Typical Jamming Signals

Based on the aforementioned architecture, this paper implements various jamming signal forms in FPGA. Different types of jamming signals exhibit distinct characteristics in spectral features, implementation complexity, and applicable scenarios. Considering space limitations and representativeness, this paper selects single-tone interference, multi-tone interference, sweeping-frequency interference, and broadband noise interference as typical examples to illustrate their FPGA implementation methods. These signal forms cover the main technical paths commonly encountered in communication jamming, adequately demonstrating the implementation capabilities and flexibility of the designed system.

3.2.1. Single-Tone Jamming Signal Implementation

Single-tone interference is a typical narrowband jamming form with energy concentrated at a single frequency, suitable for suppressing fixed-carrier-frequency communication signals[16]. Its baseband mathematical model can be expressed as:

$$s(t) = A\cos(2\pi f_0 t + \phi) \tag{1}$$

where A represents the signal amplitude, f_0 is the interference frequency, and ϕ is the initial phase.

In FPGA, single-tone signals are typically implemented using the Direct Digital Synthesis method. The core idea of DDS is to generate discrete phase sequences through a phase accumulator, then calculate the corresponding I/Q components using sine/cosine lookup tables or CORDIC algorithms. The output of the phase accumulator can be expressed as:

$$f_{n+1} = f_n + \Delta f \tag{2}$$

where Δf represents the phase increment word, which directly determines the frequency of the output signal.

In this design, the single-tone jamming module mainly consists of a phase accumulator, a sine/cosine generation module, and an amplitude control module, as shown in Figure 6. By configuring the phase increment word and amplitude parameters, flexible control over interference frequency and output power can be achieved. This method offers advantages such as high frequency resolution, stable structure, and low implementation cost, making it suitable for fixed-frequency suppression jamming tasks.

3.2.2. Multi-Tone Jamming Implementation

Based on the single-tone interference structure, multi-tone (comb spectrum) jamming signals can be formed by generating multiple narrowband interference components with different frequencies in parallel and superimposing their outputs. Such jamming signals manifest as multiple discrete spectral lines in the frequency domain[17], with the spectral coverage range

ISSN: 2688-8645

flexibly adjustable according to parameter configuration. Mathematically, the multi-tone interference signal can be represented as the linear superposition of multiple single-tone signals:

$$j(t) = \sum_{n=0}^{L-1} A_n \sin\left[2\pi\left(f_j + n\Delta f\right)t + \varphi_n\right] \tag{3}$$

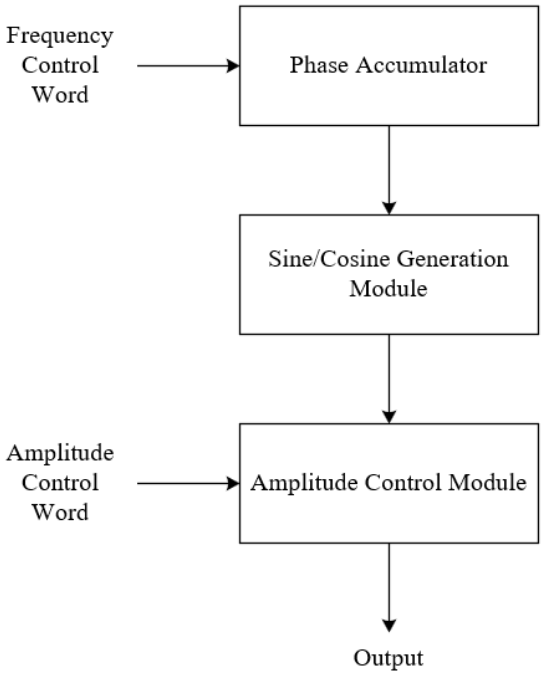


Figure 6. Structure diagram of DDS single-tone jamming signal implementation

where L is the number of tones, Δf is the frequency interval between adjacent tones, and A_n and φ_n are the amplitude and initial phase of the n -th tone, respectively.

In FPGA implementation, multi-tone interference is achieved by instantiating multiple DDS modules in parallel. Each DDS module is independently configured with phase increment words and amplitude parameters, and their outputs are accumulated in the time domain to form the composite interference signal. Due to the inherent parallel processing capabilities of FPGA, multi-tone interference implementation does not introduce significant timing bottlenecks, and the expansion of tone count is limited only by available logic resources[18]. Compared to single-tone interference, multi-tone interference can simultaneously form multiple jamming points within the target communication bandwidth, possessing stronger suppression capabilities against communication systems employing frequency division multiplexing, multi-carrier, or frequency-hopping mechanisms. In engineering applications, by properly configuring the number of tones, frequency intervals, and amplitude distribution, a balance between jamming effectiveness and system resource overhead can be achieved, demonstrating the flexibility of the parameterized jamming signal generation architecture proposed in this paper.

3.2.3. Sweeping-Frequency Jamming Signal Implementation

Sweeping-frequency interference suppresses communication systems with unknown or changing carrier frequencies by continuously varying the interference signal frequency within a certain range, enabling the jamming energy to cover a wide frequency band temporally[19]. The instantaneous frequency can be expressed as:

$$f(t) = f_{\text{start}} + kt \tag{4}$$

Where f_{start} is the starting frequency and k is the sweep rate.

ISSN: 2688-8645

In FPGA, sweeping-frequency interference can be achieved by periodically updating the DDS phase increment word. Within each control period T_{step}, the system accumulates the phase increment word[20], thereby forming a continuously varying output frequency in the time domain. The control structure is shown in Figure 7.

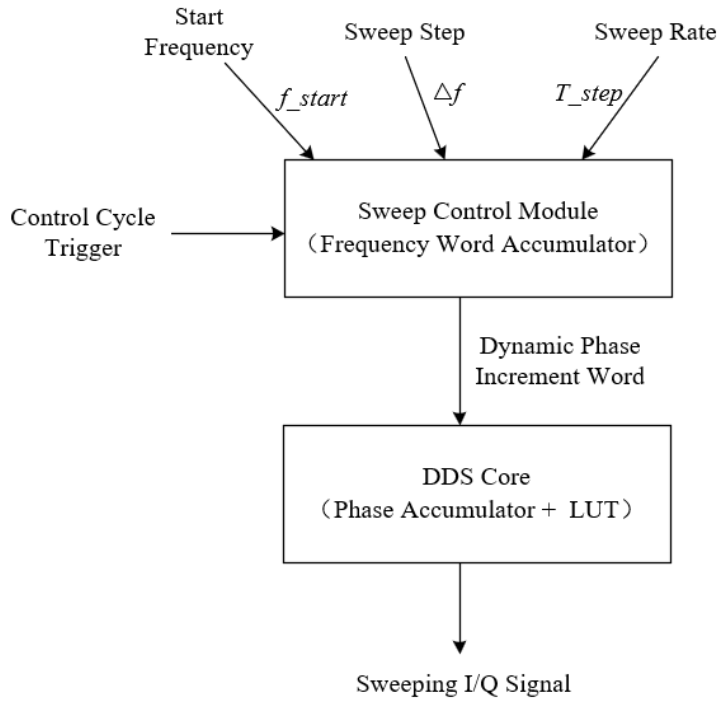


Figure 7. DDS control structure diagram for sweeping-frequency interference

By properly configuring the sweep step size and update rate, the sweep bandwidth and sweep period can be flexibly adjusted. This method features simple implementation and low hardware resource overhead, making it suitable for application in miniature embedded jamming systems.

3.2.4. Broadband Noise Jamming Signal Implementation

Broadband noise interference degrades the signal-to-noise ratio of communication systems by injecting random signals within a wide frequency band, thereby disrupting their normal demodulation performance. Ideally, noise interference can be approximated as a zero-mean, Gaussian-distributed random process.

In FPGA, noise signals are typically generated using Linear Feedback Shift Registers (LFSR) to produce pseudo-random sequences. By selecting appropriate feedback polynomials, pseudo-random sequences with long periods and good statistical properties can be obtained. The generated pseudo-random data, after amplitude normalization and digital filtering processing, are output as I/Q baseband signals to form band-limited noise interference[21,22]. The implementation structure is shown in Figure 8.

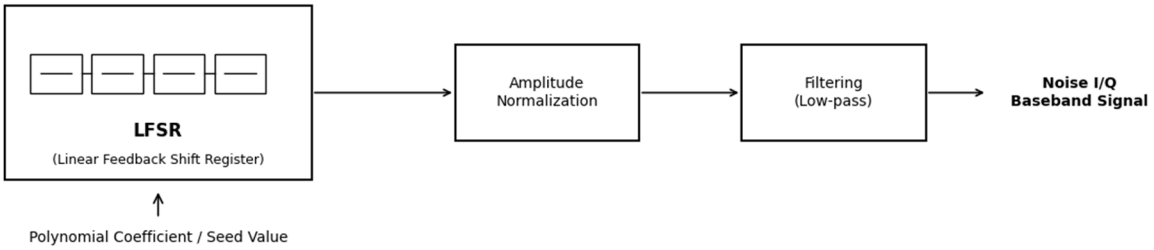


Figure 8. Structure diagram of LFSR noise jamming signal implementation

ISSN: 2688-8645

Compared to deterministic jamming signals, noise interference features simple implementation structure and low resource utilization in FPGA, possessing strong universal jamming capabilities against different communication protocols, and can therefore serve as a basic jamming mode in the system.

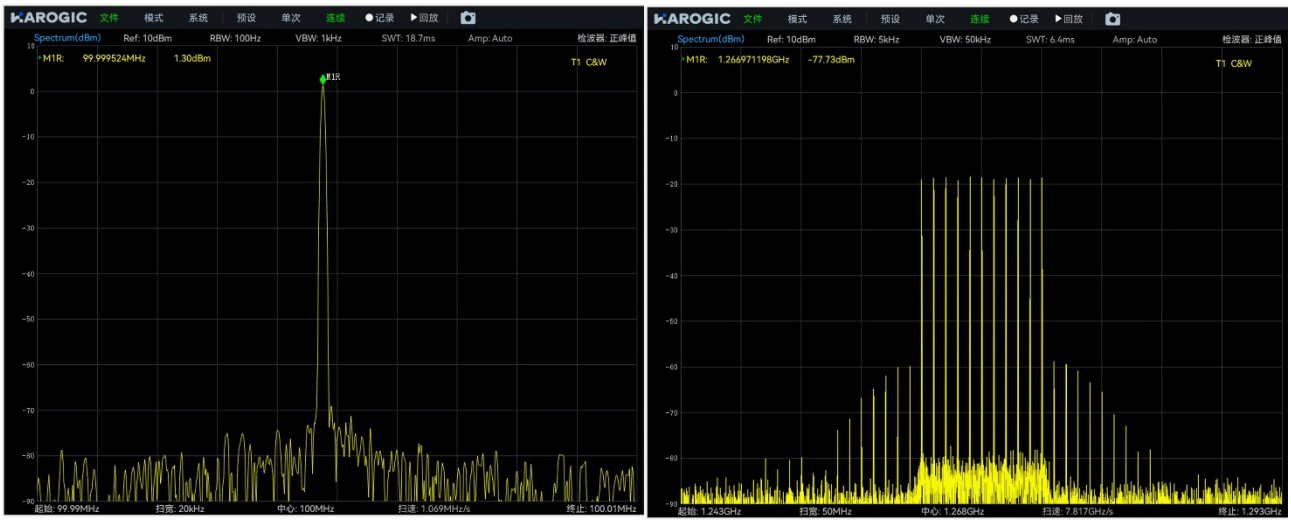
4. Results and Analysis

This chapter verifies the generation and transmission performance of jamming waveforms in the designed system through spectrum testing experiments. The experiments focus on the frequency domain distribution characteristics of RF output signals under different jamming modes to verify the correctness and stability of the FPGA-side waveform generation structure and RF transmission link.

The experimental platform consists of the jamming signal generation platform designed in this paper, an RF power amplification module, and a spectrum analyzer. By configuring the jamming mode, carrier frequency, bandwidth, and related parameters, the frequency domain characteristics of the output RF signals were observed and recorded using the spectrum analyzer. Testing focused on the consistency between spectral morphology and theoretical expectations under different jamming modes.

For single-tone jamming signals, with the interference frequency set to 100 MHz, the spectral results shown in Figure 9(a) demonstrate that the jamming signal forms a clear, stable spectral line at the set carrier frequency, consistent with the configured parameters without significant frequency deviation or spurious components.

For multi-tone jamming signals, with the interference frequency set to 1.268 GHz and the number of tones set to 11, the spectrum in Figure 9(b) presents 11 discrete spectral lines with similar amplitudes and consistent frequency intervals, with the distribution range matching the configured multi-tone frequency set.



（a）Single-tone interference （b）Multitone interference

Figure 9. Test results for single-tone and multi-tone interference

For sweeping-frequency jamming signals, with the initial frequency set to 800 MHz, cutoff frequency at 1200 MHz, and step size of 2 MHz, Figure 10(c) shows that the interference energy is continuously distributed within the set frequency range. The sweep start and stop frequencies are consistent with the system configuration parameters, without obvious frequency breaks or jumping phenomena.

ISSN: 2688-8645

For broadband noise interference, with the interference frequency at 1 GHz and bandwidth at 1 MHz, Figure 10(d) shows uniform distribution of noise energy within the target frequency band, without obvious spectral line structures, consistent with the theoretical characteristics of broadband noise interference.

（c）Frequency sweep interference （d）Noise interference

Figure 10. Test results for sweeping-frequency and noise interference

This chapter verifies the typical jamming signal generation capability of the designed embedded jamming waveform generation platform through spectrum testing experiments. The experimental results indicate that the system can stably generate various jamming signals including single-tone, multi-tone, sweeping-frequency, and broadband noise, with frequency domain characteristics consistent with theoretical analysis, and all parameters can be flexibly adjusted through configuration. These results validate the feasibility and effectiveness in engineering applications of the system architecture and FPGA implementation scheme proposed in this paper.

5. Conclusion

Focusing on the implementation requirements of jamming waveforms in embedded SDR platforms, this paper has designed and implemented a configurable jamming signal generation system based on the Zynq SoC and integrated RF transceiver chips. The system adopts the software-defined radio design philosophy, deploying the digital generation and modulation functions of jamming signals on the FPGA side, and achieving flexible configuration of waveform types and parameters through the processing system. Regarding FPGA implementation, parameterized generation of various typical jamming waveforms—including single-tone, multi-tone, sweeping-frequency, and broadband noise—has been completed, with switching and expansion among multiple jamming modes realized under a unified architecture.

Experimental test results demonstrate that the system can output RF spectral characteristics consistent with theoretical expectations under different operating modes, verifying the feasibility and effectiveness of the proposed jamming waveform FPGA implementation method and system architecture. The research work presented in this paper can provide references for jamming waveform design, electromagnetic environment simulation testing, and related engineering applications in embedded SDR systems. Future work may further investigate jamming signal performance evaluation, system integration optimization, and functional expansion based on this foundation.

ISSN: 2688-8645

References

[1] Zhao G Q: *Principle of Radar Countermeasure* (Xidian University Press, China 2005), p.15-28.

[2] Ma F: Analysis of Anti-jamming Capability of Spread Spectrum Communication, *Journal of Yulin University*, Vol. 17 (2007) No.11, p.25-27.

[3] Jiang N A, Zeng X W: *Spread Spectrum Communication and Its Multiple Access Technology* (Xidian University Press, China 2004), p.88-102.

[4] Ge H L, Song Y F: Application and Design of Distributed Communication Jamming Equipment, *Radio Engineering*, Vol. 34 (2004) No.4, p.29-35.

[5] Yang X N, Lou C Y, Xu J L: *Software Defined Radio: Principle and Application* (Publishing House of Electronics Industry, China 2001), p.42-56.

[6] Zhang P H, Zhang C R, Zhao Y, et al: Design of Software Radio Platform Based on ZYNQ-7000 FPGA and AD9361, *Experimental Technology and Management*, Vol. 36 (2019) No.8, p.85-93.

[7] Cao X T: *Design of Wireless Transceiver System Based on AD9361* (M.S., Xidian University, China 2016), p.20-35.

[8] Yan X D: *Design and Implementation of Wireless Transceiver Based on AD936x* (M.S., Xidian University, China 2018), p.18-32.

[9] Hou X S, Wang X, Zhang X, et al: Design and Implementation of False Target Signal Simulator Based on ZYNQ and AD9361, *Electronic Design Engineering*, Vol. 31 (2023) No.12, p.87-91.

[10] Liu J J, Zheng P, Zhao Z K: Implementation of Miniaturized Radar Reconnaissance and Jamming Based on ADRV9009, *Electronic Information Countermeasures Technology*, Vol. 37 (2022) No.5, p.14-18.

[11] Cui Y: *Research on GPS Jamming Key Technologies Based on LEO Satellite Platform* (M.S., University of Electronic Science and Technology of China, China 2024), p.22-38.

[12] Ma Y C: *Hardware Design and Implementation of UAV Link Suppression and Navigation Spoofing Platform* (M.S., University of Electronic Science and Technology of China, China 2023), p.28-40.

[13] Guo L: Software Generation Method of Communication Jamming Signals, *Radio Communications Technology*, Vol. 31 (2005) No.4, p.40-41.

[14] Zhang S B: *Design and Implementation of Communication Jamming Signal Simulator Based on FPGA* (M.S., Xidian University, China 2021), p.15-45.

[15] Huang Z W, Chen Q: *FPGA System Design and Implementation* (Publishing House of Electronics Industry, China 2005), p.65-78.

[16] Xu G H, Cheng Y X: *Embedded System Development and Application Based on FPGA* (Publishing House of Electronics Industry, China 2006), p.112-125.

[17] Wang R: *Intermediate Frequency Simulation of Radar Deception Jamming Signal Based on FPGA* (M.S., Beihang University, China 2014), p.30-42.

[18] Li S W, Qu J W: Research on Multi-waveform Radar Jamming Generation Technology, *Aerospace Electronic Countermeasures*, Vol. 27 (2011) No.4, p.56-58.

[19] Luo Y J, Yang T F: Design of Radar Jamming Signal Simulator Based on AD9361, *Experimental Technology and Management*, Vol. 37 (2020) No.7, p.105-109.

[20] Quaglia R, Camarchia V, Jiang T, et al: K-Band GaAs MMIC Doherty Power Amplifier for Microwave Radio With Optimized Driver, *IEEE Transactions on Microwave Theory and Techniques*, Vol. 62 (2014) No.11, p.2518-2525.

[21] Zhang C G: *Jamming Methods and Simulation for Digital Communication Systems* (M.S., Xidian University, China 2007), p.15-45.

[22] Feng X P, Li P: *Principles of Communication Countermeasures* (Xidian University Press, China 2009), p.155.