sensors

MDPI

Article

Machine-Learning-Assisted Cyclostationary Spectral Analysis for Joint Signal Classification and Jammer Detection at the Physical Layer of Cognitive Radio

Tassadaq Nawaz * and Ali Alzahrani

Department of Computer Engineering, King Faisal University, Al-Ahsa 31982, Saudi Arabia; aalzahrani@kfu.edu.sa

* Correspondence: tnawaz@kfu.edu.sa

Abstract: Cognitive radio technology was introduced as a possible solution for spectrum scarcity by exploiting dynamic spectrum access. In the last two decades, most researchers focused on enabling cognitive radios for managing the spectrum. However, due to their intelligent nature, cognitive radios can scan the radio frequency environment and change their transmission parameters accordingly on-the-fly. Such capabilities make it suitable for the design of both advanced jamming and anti-jamming systems. In this context, our work presents a novel, robust algorithm for spectrum characterisation in wideband radios. The proposed algorithm considers that a wideband spectrum is sensed by a cognitive radio terminal. The wideband is constituted of different narrowband signals that could either be licit signals or signals jammed by stealthy jammers. Cyclostationary feature detection is adopted to measure the spectral correlation density function of each narrowband signal. Then, cyclic and angular frequency profiles are obtained from the spectral correlation density function, concatenated, and used as the feature sets for the artificial neural network, which characterise each narrowband signal as a licit signal with a particular modulation scheme or a signal jammed by a specific stealthy jammer. The algorithm is tested under both multi-tone and modulated stealthy jamming attacks. Results show that the classification accuracy of our novel algorithm is superior when compared with recently proposed signal classifications and jamming detection algorithms. The applications of the algorithm can be found in both commercial and military communication systems.

Keywords: cognitive radios; signals classifications; stealthy jammer; cyclostationary spectral analysis; artificial neural networks

check for updates

Citation: Nawaz, T.; Alzahrani, A. Machine-Learning-Assisted Cyclostationary Spectral Analysis for Joint Signal Classification and Jammer Detection at the Physical Layer of Cognitive Radio. *Sensors* **2023**, *23*, 7144. https://doi.org/10.3390/s23167144

Academic Editor: Dimitrie Popescu

Received: 20 June 2023
Revised: 20 July 2023
Accepted: 3 August 2023
Published: 12 August 2023

Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

Cognitive Radio (CR) emerged as a result of recent breakthroughs in Software Defined Radios (SDR) and Machine Learning (ML), as well as neuroscience findings [1,2]. Due to Dynamic Spectrum Access (DSA) capability, CR technology has the potential to address the problems of the wireless spectrum shortage and inefficient spectrum utilisation [3,4]. In both TV white space (TVWS) CR networks [5–9] and 5G technology [10], DSA plays a vital role.

In CR networks, the Secondary Users (SUs) can use the radio spectrum with different intentions, which means the licit user uses the radio spectrum in a manner to remain compliant with the security needs of licensed Primary Users (PUs) and avoid interfering with other users, whereas malicious users transmit signals with the motive of interfering with or jamming the communications of the targeted radio system. Due to their broadcast nature, radio communications are susceptible to external attacks launched by malicious users. The physical layer (PHY-layer) is particularly exposed to radio frequency (RF) jamming attacks. RF jamming and anti-jamming are well-known in conventional radio communication systems. However, significant advances have been made in the last two

decades in CR technology that allow the design and deployment of advanced intelligent jamming [11] and anti-jamming [12,13] systems.

The need for measurable communications security in the Internet-of-Things (IoT) and Cyber-Physical Systems (CPSs) frameworks [14–16] has recently necessitated the establishment of an appropriate paradigm. SHIELD, which comprises the methods and techniques for designing secure embedded systems [17], is an important step taken in this direction. TVWS research [18] has also tackled the problem of illegitimate user detection.

CR networks allow the devices to sense the neighbouring radio environments, decide about the occupation of channels, and reconfigure the transmission parameters to achieve the required quality of service. Spectrum sensing is embedded in modern anti-jamming systems and plays a key role in the detection and identification of interfering and jamming entities [19]. Furthermore, it is used to record a history of the malicious user's activities to design more efficient anti-jamming strategies, e.g., in frequency hopping spread spectrum (FHSS) systems it can be used to change the hopping sequence in order to avoid the bands jammed by malicious users [20].

A number of sensing methods were introduced over the last decade, which include energy detector (ED) [21], cyclostationary feature detector (CFD) [22], and matched filter detector (MFD) [23]. ED has a reasonably simple implementation and does not need any prior information about the signal. It is also included in the IEEE 802.22 standard for spectrum sensing. However, the detection performance of ED is significantly degraded in low signal-to-noise (SNR) radio environments. The MFD is the optimal detector but needs thorough prior information on the PU signal. Therefore, a receiver with a dedicated architecture is needed for the PU signal, which makes it impossible to consider in most practical sensing scenarios. On the other hand, in most practical scenarios, CR devices need to detect low-power signals; therefore, a new sensing technique—namely, CFD—is presented in the literature. The CFD technique has the capability to distinguish licit signals from noise and interference in low SNR conditions with high accuracy, which are attained at the expanse of high computational complexity. CFD relies on the cyclostationary features of modulated communication signals, such as modulation rate and carrier frequency, to distinguish between signals. The CFD sensing methods compute the spectral correlation function (SCF) [24–26] of signals, since noise is a stationary process and has no spectral components at harmonics that make it suitable to be used in low SNR environments. SCF has been employed as a reliable method for signal categorisation [27–29] since it produces a unique pattern for each signal. Therefore, it can also be used as a reliable tool to distinguish between legitimate signals and jamming waveforms. In [30], the authors compared the most widely used sensing methods in terms of accuracy and computational complexity. Methods for determining the most likely signal to which the observed feature set belongs are required by feature-based classification algorithms. Choosing the appropriate ML algorithm for signals classification is not the only challenge to overcome to obtain targeted classification accuracy; feature extractions and selection techniques are also important because they have a big impact on classification accuracy. Therefore, a reliable CFD detector is used for feature extraction in this work. In previous works, refs. [31,32] performed cyclostationary spectral analysis on the wideband spectrum resulting in high computational complexity; in order to reduce the overhead, this work exploits the sparse nature of WB, which is a valid assumption in the context of CR, and performed CFD analysis for the NB signal in each occupied sub-band in the WB spectrum. Further, a computationally efficient algorithm strip spectral correlation algorithm (SSCA) [33] is used to compute the SCF, as compared with the FFT accumulation method (FAM) [33] used in previous work. Further, a large dataset is collected using different carrier frequencies, jamming powers, and SNRs as compared with the jammer's fixed power in [31,32]; here, varying jamming power can be considered as a mobile jammer scenario. In this work, a novel, single artificial neural network is proposed to detect and identify both multi-tone and pulse-modulated jammer attacks as well as to classify the legitimate signals with comparable accuracy to the work in [31,32].

While CR has emerged as a solution for DSA/OSA, its capacity to sense and explore a wide variety of frequencies and opportunistic applications has posed severe issues to network security. These features enable attackers to carry out more sophisticated attacks, for example, the primary user emulation (PUE) attacks [34], in which a hostile user impersonates a primary user. Furthermore, attackers can monitor the spectrum and use smart jamming to disrupt it [35,36]. Jamming attacks are Anomalous Spectrum Utilisation Attacks (ASUAs) that cause abnormal spectrum usage and disrupt the DSA/OSA in CR networks.

Our work considers stealthy jamming attacks. Such jammers are equipped with CR-spectrum sensing capability; therefore, they only transmit a jamming signal when activity is sensed over the channel and stop once the legitimate transmission stops. Such jammers are difficult to detect using common sensing techniques like ED at the physical layer. The majority of studies that investigate RF jamming assumed additive white Gaussian noise (AWGN) jamming [37,38].

However, the authors showed in [39,40] that modulation-based jamming attacks can result in optimum jamming in power-constrained conditions. We consider two different types of stealthy jammers: (i) the jammer is equipped with ED capabilities and uses a high-power multi-tone to jam various bands in WB radios; (ii) the jammer is equipped with a feature detector, able to identify the modulation schemes of a legitimate signal, and uses an optimum pulsed jamming strategy against the target signal. Hence, a reliable jammer detection algorithm is required to design a suitable anti-jamming system to counter such jamming attacks.

This article focuses on designing a reliable algorithm for the joint classification of legitimate signals and jammer detection in WB CRs. The main contributions of the article are the following:

1. Classify received licit signals into their corresponding modulation schemes using CFD and artificial neural network;
2. Detect both multi-tone and modulated pulsed stealthy jammers using the CFD and the same trained artificial neural network classifier as above.

We consider a WB spectrum that is constituted of many sub-bands, and each of the sub-bands is used by a narrowband (NB) signal or free. The occupied sub-bands are either used by a licit signal or jammed by the stealthy jammer. The algorithm's first step is to perform cyclostationary spectral analysis on received NB signals and compute the corresponding SCF. Then, angular frequency profile (f) and cycle frequency profile (α) are obtained from the SCF of the signal. These two profiles are combined and used to train an artificial neural network, which then characterise various NB signals in a WB spectrum. Further, the algorithm is tested with an independent signal set at various SNRs. The algorithm has shown significantly high classification performances in the literature in comparison to the proposed techniques [41]. Moreover, it achieved very high jammer detection rates.

The article is structured as follows. Sections 2 and 3 give the system model and proposed algorithm, respectively. Results are illustrated in Section 4. Finally, the conclusions are drawn in Section 5 with some future directions.

2. System Model and Problem Formulation

A number of transmitters (Tx_l), k s.t. $l \in \{0, 1, 2 \dots M-1\}$, are present in the vicinity of CR terminal. The CR terminal sensed a WB spectrum and, therefore, received a signal that can be represented by the expression

$$z(t) = \sum_{l=0}^{M-1} h_l(t) * S_l(t) + v(t) \quad (1)$$

where $S_l(t)$ shows the signal transmitted by the l-th transmitter, $h_l(t)$ is the radio channel between the l-th transmitter and receiver, $*$ represents convolution operator, and $v(t)$ denotes the AWGN with zero mean and power spectral density of σ_v^2. We considered that the

received NB signal's power is degraded over the square of the distance; therefore, the free space path loss model (FSPL) is used to compute the received power at the receiver terminal. Further, it is considered that the channel ($h_l(t)$) is the slow, flat, Rayleigh fading channel in the observation process. It is assumed that transmitters can generate the signals with different modulation schemes, such as binary amplitude shift keying (BASK), binary phase shift keying (BPSK), quadrature amplitude modulation (QAM), quadrature phase shift keying (QPSK), pulse amplitude modulation (PAM), binary frequency shift keying (BFSK), or any other modulation scheme, as depicted in Figure 1. It shows that a receiver node scans a WB spectrum constituting multiple NB transmitted signals while a multi-tone jammer (upper panel) and modulated pulsed jammer (lower panel) try to jam multiple signals at the receiver terminal. The transmitters generate the signals using the following model:

$$S_l(t)_{MPSK} = \sum_{n=-\infty}^{\infty} Ap(t - nT_s)e^{(j2\pi(m_n-1)/M + j2\pi f_c)} \quad (2)$$

where A is amplitude, $T_s = 1/Rs$ is the symbol period and Rs is the symbol rate, $M = 2, 4$ are the number of unique phases, m_n is the n-th transmitted symbol, f_c is the carrier frequency, and $p(t)$ is the Root Raised Cosine Pulse Shape (RCC) filter with a roll-off factor of $\beta = 0.5$.

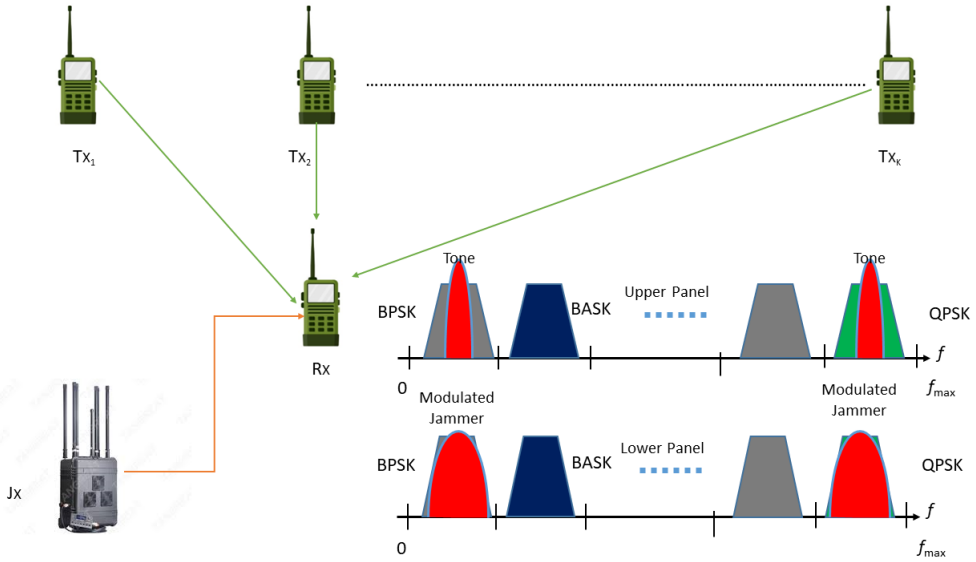

Figure 1. Cognitive radio terminal (Rx) senses a wideband spectrum composed of various narrowband transmitted signals. The multi-tone and modulated pulsed stealthy jammers try to jam different signals at the receiver node.

For our system model, two types of stealthy jammers are considered with different CR sensing capabilities:

1. Jammer is equipped with ED sensing technique and uses multi-tone as the jamming strategy to jam multiple NB signals in the observed WB signal. A tone with sufficiently higher power than the licit signal can jam any of the occupied SBs as shown in Figure 1.
2. Jammer is equipped with a feature detector; hence, it is able to recognise the modulation schemes of transmitted signals and, therefore, uses the optimal pulsed (modulated) jamming schemes against the target signals, as shown in Figure 1.

The pulsed jamming attacks are particularly effective in power-constrained environments, and optimal jamming schemes against modulated target signals are given in [40]. We assumed that both types of jammers are able to transmit powerful RF signals to cause interference at any communication frequency in the WB spectrum. Indeed, the received signal strength (RSS) related to the jamming signal depends on the distance between the

jammer and the receiver terminal. Therefore, in order to simulate this scenario, the jammer-to-signal ratio (JSR) is fixed to 0 dB and the jammer terminal is moved towards receiver terminal from 15 m to 3 m with a step size of 3 m. In second scenario, the distance between the jammer and receiver terminals is fixed to 12 m and the JSR is changed between 0 dB and 7 dB. The dataset is collected for three broad jamming scenarios:

- No jamming: jammer is not transmitting
- Tone jamming: jammer employs multi-tone to jam the NB signals in WB spectrum
- Pulsed jamming: jammer employs pulsed jamming to jam the NB signals in WB spectrum. We used the MatLab environment to simulate the system model according to the specifications provided above.

3. Proposed Algorithm

This section first introduces cyclostationary spectral analysis and artificial neural networks; then, our newly proposed algorithm is presented.

3.1. Cyclostationary Spectral Analysis

The received signal $z(t)$ is considered cyclostationary if its mean and autocorrelation function are periodic with period T_0,

$$M_z(t+T_0) = M_z(t), \qquad R_z(t+T_0,\tau) = R_z(t,\tau). \tag{3}$$

Fourier series components can be used to represent the autocorrelation of a cyclostationary signal $z(t)$.

$$R_z(t,\tau) = E[z(t+\tau/2)z^*(t+\tau/2)] \tag{4}$$

$$R_z(t,\tau) = \sum_{\alpha} R_z^{\alpha}(\tau)e^{j2\pi\alpha t} \tag{5}$$

Here, $E[.]$ is the expectation operator and $\alpha = \frac{b}{T_0}$, where b is an integer. $R_z^{\alpha}(\tau)$ is the cyclic autocorrelation function (CAF) of the received signal $z(t)$ and given by the equation

$$R_z(\tau) = \lim_{T\to\infty} \frac{1}{T} \int_{\frac{-T}{2}}^{\frac{T}{2}} R_z(t,\tau)e^{-j2\pi\alpha t}dt \tag{6}$$

as $R_z(\tau)$ is periodic with period T_0; therefore, (5) can be given by

$$R_z(\tau) = \frac{1}{T_0} \int_{\frac{-T_0}{2}}^{\frac{T_0}{2}} R_z(t,\tau)e^{-j2\pi\alpha t}dt \tag{7}$$

The SCF is obtained by computing the Fourier Transform of the CAF (6) and given by

$$S_z(f) = \int_{-\infty}^{\infty} R_z^{\alpha}(\tau)e^{-j2\pi f\tau}d\tau \tag{8}$$

where $S_z(f)$ is the SCF of received signal $z(t)$, f and α represent the angular and cyclic frequencies, respectively.

The key advantage of using SCF is that its computation is not affected by noise, since noise is a stationary process and its spectral component has no correlation. This allows accurate computation of SCF even at very low SNRs. Moreover, modulated communications signals such as FSK, MSK, QAM, AM, PAM, QPSK, and BPSK with overlapped PSDs have unique SCF patterns. Since higher-order QAM and PSK modulation show the same second-order statistics, our experiments only considered BPSK and QPSK modulation schemes. Higher-order statistics [42] is needed for such signals that will be considered in the future to differentiate between higher-order QAM and PSK. The SCF of BPSK and QPSK signals is shown in Figure 2a,b. These panels show the spectral correlation densities of received NB signals as a function of both angular and cyclic frequencies. Since SCF estimation generates

a large amount of data, it is not feasible to use it as a feature set for a classifier; therefore, two profiles—namely, f-profile and α-profile, given in Equations (9) and (10)—are obtained from SCF. The α-profile of NB BPSK and QPSK signal is depicted in Figure 2c,d. These profiles are combined to form an input feature vector that is then fed to an ANN-based classifier.

$$I(\alpha) = max_f[S_z^\alpha] \tag{9}$$

$$I(f) = max_\alpha[S_z^\alpha] \tag{10}$$

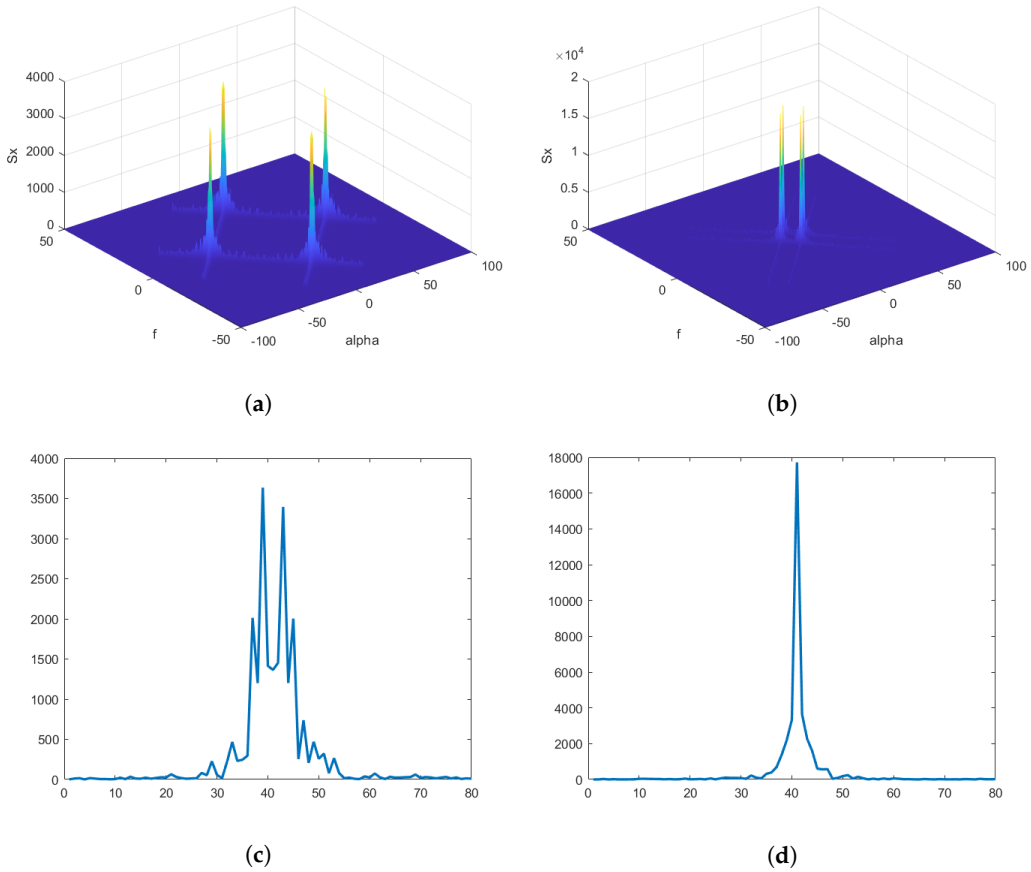

Figure 2. (**a**) SCF of BPSK signal. (**b**) SCF of QPSK signal. (**c**)Alpha profile of BPSK signal. (**d**) Alpha profile of QPSK signal.

3.2. Artificial Neural Network and Proposed Algorithm

The proposed algorithm embeds an Artificial Neural Network (ANN) for spectrum characterisation because of its efficient use in pattern recognition problems. Further, it has the potential to generalise to any carrier frequency, signal-to-noise ratio, symbol rate, and frequency offset, which makes it suitable for the problem under consideration. The system is designed to characterise the spectrum under two stealthy jamming attacks, namely, multi-tone and modulated pulsed jamming attacks. First, a dedicated ANN is used as a classifier for each jamming attack. For multi-tone jamming attack, an ANN classifies received NB signals as BPKS, QPSK, BPSK plus Tone Jammer (BPSK-TJammed), and QPSK plus Tone Jammer (QPSK-TJammed). Similarly, for modulated pulsed jamming attacks, an ANN is used to characterise the signals as QPSK, BPSK, BPSK plus Pulsed Jammer (BPSK-PJammed), and QPSK plus Pulsed Jammer (QPSK-PJammed). ANN, like every supervised machine learning algorithm, operates in two stages: training (offline) and testing (online). The f and α profiles obtained from the SCF of each NB signal are concatenated and fed as a feature vector to ANN. Accordingly, both dedicated ANNs have 100 inputs associated with

both the profiles, a hidden layer with ten neurons whose transfer function is a hyperbolic tangent sigmoid, and an output layer that contained four neurons associated with four signal classes, as discussed above. Each output value is between 0 and 1, and the class with the maximum value is treated as the signal type. The scale conjugate gradient back-propagation [43] algorithm is used to train ANN. For both dedicated ANN architectures, 100 trains are run, with weights being randomly initialised for each run. Each network architecture is trained (70%), validated (15%), and tested (15%) using a dataset of 40,000 signals. Over 98% (average) true positive classification was achieved with a single hidden layer for the four signal classes. Such classification accuracy indicates that an increase in the number of hidden layers will significantly increase the training time but not improve classification accuracy. As a result, the ANN architecture with a single hidden layer that consisted of 10 neurons and performed the best among the 100 trains was chosen for the classification of signals. Figure 3 depicts the ANN used in this work.

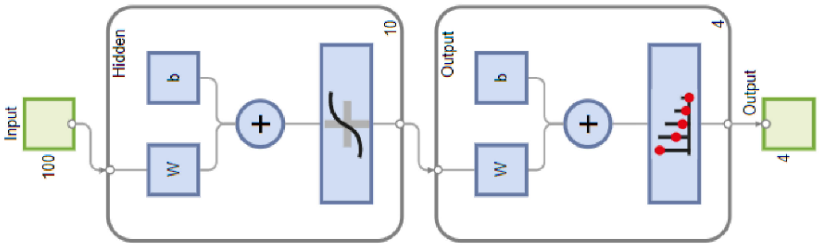

Figure 3. Proposed artificial neural network with ten neurons in hidden layer.

Further, a single ANN is designed to classify the signals under both multi-tone and modulated pulsed stealthy jamming attacks. The ANN is aimed at classifying the signals as BPSK, QPSK, BPSK-TJammed, QPSK-TJammed, BPSK-PJammed, and QPSK-PJammed. The ANN is trained (70%), validated (15%), and tested (15%) using a dataset of 80,000 signals. For the classification of the above six classes of signals, the ANN with a single hidden layer that contained 18 neurons and demonstrated the best results among the 100 trains was chosen. The results are reported in Section 4. The block diagram of the proposed algorithm is depicted in Figure 4 and the pseudo-code of the algorithm is outlined in Algorithm 1. The CR terminal senses a WB spectrum that consists of many NB signals. Then, the SCF of each NB signal is computed according to the procedure detailed in Section 3.1, and f- and α-profiles are subsequently extracted from SCF. The f- and α-profiles of the respective NB signals are concatenated and given as input features to train the ANN. Then, the ANN is also tested for the independent signal set; it classifies the signal in occupied sub-bands as a legitimate signal with a corresponding modulation scheme or NB signal jammed by a particular type of jammer.

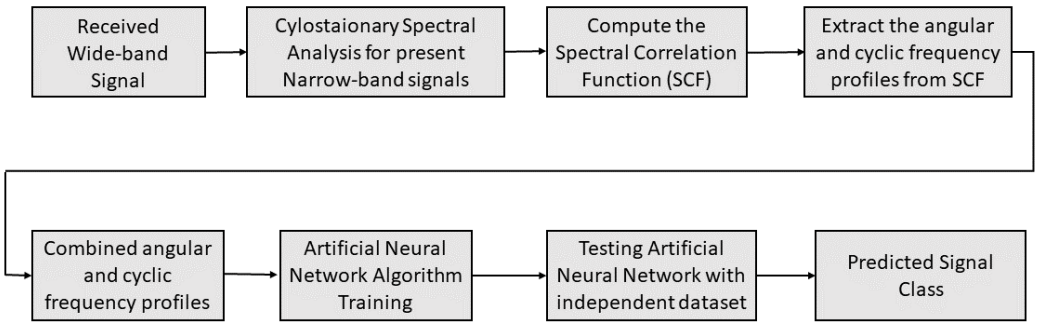

Figure 4. Proposed algorithm for joint signal classification and stealthy jammer detection.

Algorithm 1 Pseudo-code for proposed algorithm

function *Joint Signal Classification and Stealthy Jammer Detection*
Input:
    Train → Train ANN with Labelled data set
    Test → Independent data set
Output:
    Predicted → Signal class
Procedure:
    Initialise all SB states to "free"
    Receive the WB signal
    Divide WB into j SBs
    for $j = 1$ *to* J, **do**
        Compute the SCF of each NB signal
        Obtain the α and f-profiles from SCF
        Feed the concatenated α and f frequency profiles for SB_j to previously trained ANN
        Decision ← Signal class
    end for
end function

4. Simulation Results and Discussion

A WB signal of 50 MHZ, which is occupied by K NB signals, is considered to be sensed by a CR terminal. For our simulations in the MatLab environment, it is assumed that NB signals are generated by QPSK and BPSK modulation schemes. Two types of stealthy jamming attacks, namely, multi-tone and modulated pulsed, are considered against these signals. The WB spectrum is considered to be affected by Rayleigh fading and AWGN. The sampling rate is set to 100 MHz. It is assumed that detection is already performed and the CR node has knowledge of occupied SBs. The signal characterisation is performed at $\alpha = 2f_c$, where AWGN has no correlation. The designed algorithm is further tested with the independent dataset and the classification results are given by confusion matrices.

4.1. Dedicated ANN Architecture for the Stealthy Jamming Attacks

A dedicated ANN architecture, for each type of jamming attack, is designed according to the process detailed in Section 3. The ANN is trained using a dataset of 40,000 signals at various carrier frequencies and SNRs; hence, the system performance is independent of carrier frequencies and SNRs.

The overall performance of the ANN classifier in the presence of a multi-tone stealthy jamming attack is shown in the form of a test confusion matrix in Figure 5 that shows a classification rate of approximately 99% is achieved. The tested signals are 15% (6000) of the total signals used to train ANN. Figure 5 shows that the algorithm successfully identified the un-jammed legitimate signals, QPSK as QPSK and BPSK as BPSK, with 99% and 98% accuracy, respectively. For both jammed signals, BPSK-TJammed and QPSK-TJammed, the classification accuracy is approximately 99.7% and 99.8%. After training and testing the ANN with 40,000 samples, the ANN is further tested using an independent signal set. The system's performance is specifically evaluated online for 1000 independent signals that are generated using various carrier frequencies and SNRs (-9 to 6 dB). The confusion matrices in Tables 1–6 give the classification rate for the four classes of signals. The proposed algorithm, which is based on cyclic spectral analysis and ANN, performs well in most of the system configurations, even at low SNRs. It can be observed in Table 1 that at -9 dB, the ANN classified BPSK and QPSK to their corresponding classes with a rate of 97.7% and 96.7%, while for 98.7% and 99.2%, the algorithm correctly classified the jammed signals (BPSK-Jammed and QPSK-Jammed). Table 1 shows that for all four classes of signals, a classification rate of approximately 99% is achieved. Further, it is possible to infer from confusion matrices (Tables 2–7) that no classification errors (100% accuracy) are observed at and above -3 dB.

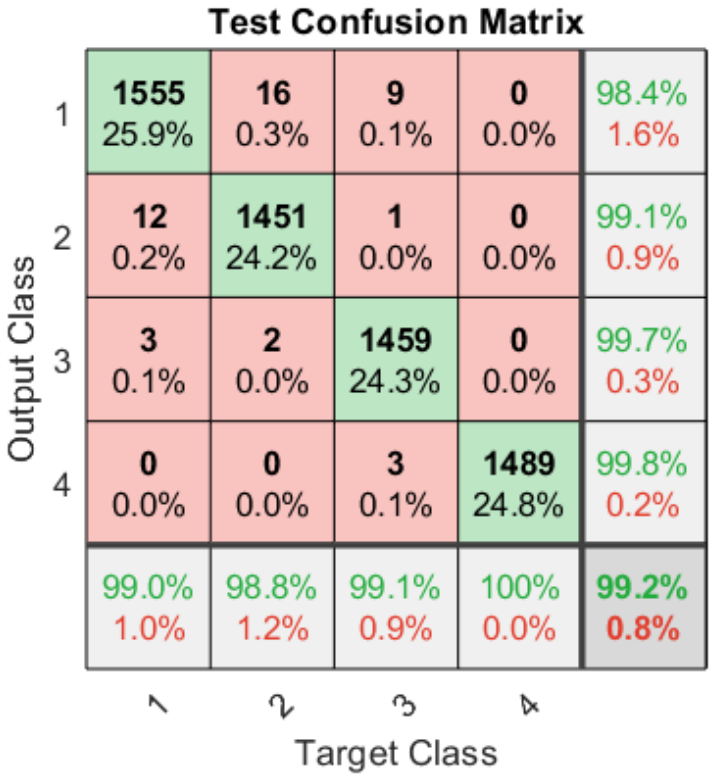

Figure 5. Test confusion matrix of the dedicated ANN with four output classes: BPSK, QPSK, BPSK-TJammed, and QPSK-TJammed.

Table 1. Confusion matrix of the proposed ANN at −9 dB in presence of Tone jamming.

Signal Class	BPSK	QPSK	BPSK-TJammed	QPSK-TJammed
BPSK	977	21	2	0
QPSK	33	967	0	0
BPSK-TJammed	2	3	987	8
QPSK-TJammed	0	0	8	992

Table 2. Confusion matrix of the proposed ANN at −6 dB in presence of Tone jamming.

Signal Class	BPSK	QPSK	BPSK-TJammed	QPSK-TJammed
BPSK	990	10	0	0
QPSK	13	985	0	3
BPSK-TJammed	0	0	992	8
QPSK-TJammed	0	0	2	998

Table 3. Confusion matrix of the proposed ANN at −3 dB in presence of Tone jamming.

Signal Class	BPSK	QPSK	BPSK-TJammed	QPSK-TJammed
BPSK	1000	0	0	0
QPSK	0	1000	0	0
BPSK-TJammed	0	0	1000	0
QPSK-TJammed	0	0	0	1000

Table 4. Confusion matrix of the proposed ANN at 0 dB in presence of Tone jamming.

Signal Class	BPSK	QPSK	BPSK-TJammed	QPSK-TJammed
BPSK	1000	0	0	0
QPSK	0	1000	0	0
BPSK-TJammed	0	0	1000	0
QPSK-TJammed	0	0	0	1000

Table 5. Confusion matrix of the proposed ANN at 3 dB in presence of Tone jamming.

Signal Class	BPSK	QPSK	BPSK-TJammed	QPSK-TJammed
BPSK	1000	0	0	0
QPSK	0	1000	0	0
BPSK-TJammed	0	0	1000	0
QPSK-TJammed	0	0	0	1000

Table 6. Confusion matrix of the proposed ANN at 6 dB in presence of Tone jamming.

Signal Class	BPSK	QPSK	BPSK-TJammed	QPSK-TJammed
BPSK	1000	0	0	0
QPSK	0	1000	0	0
BPSK-TJammed	0	0	1000	0
QPSK-TJammed	0	0	0	1000

Similarly, a dedicated ANN is trained for a total 40,000 signals set at different SNRs and carrier frequencies to classify the signals in the presence of modulated pulsed jamming attacks. ANN classifies the signals into four classes, namely, BPSK, QPSK, BPSK-PJammed, and QPSK-PJammed. The optimal jamming strategies for such a jammer are given in Table 1. The test confusion matrix for signal classification under modulated pulsed stealthy jamming attack is given in Figure 6 and the results show that the proposed ANN correctly classifies all signals with an overall classification of 99.5%. Moreover, the ANN is further tested for an independent signal set and test confusion matrices for various SNRs are shown in Tables 7–12. Table 7 shows that at -9 dB, for all four types of signals—BPSK, QPSK, BPSK-PJammed, and QPSK-Jammed—the classification rate is approximately 99%. Tables 9–12 show that a classification rate of 100% is achieved at and above -3 dB, which makes this algorithm suitable to not only classify the legitimate signals but also detect jamming attacks at low SNRs.

Table 7. Confusion matrix of the proposed ANN at -9 dB in presence of Pulsed jamming.

Signal Class	BPSK	QPSK	BPSK-PJammed	QPSK-PJammed
BPSK	990	5	3	2
QPSK	3	988	2	7
BPSK-PJammed	0	0	992	8
QPSK-PJammed	0	0	5	995

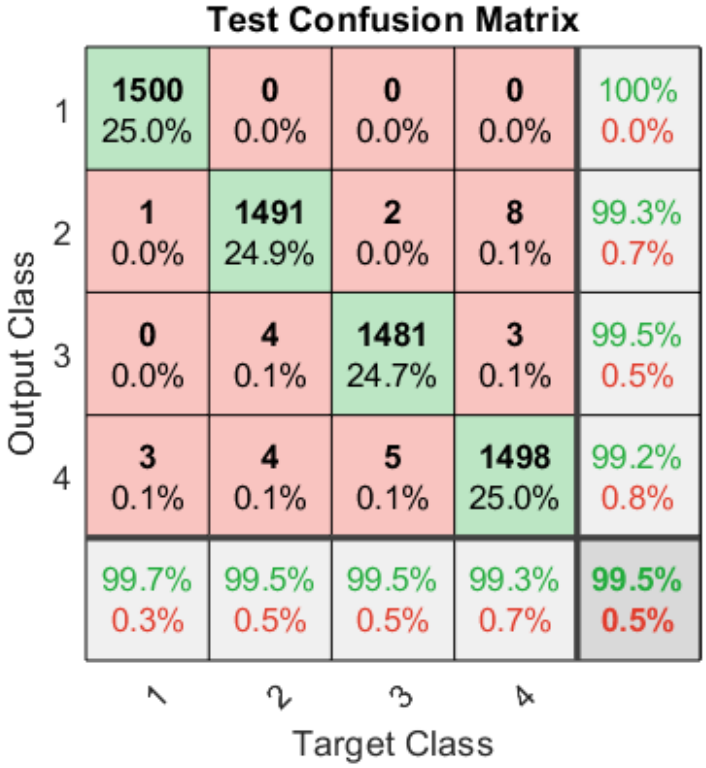

Figure 6. Test confusion matrix of the dedicated ANN with four output classes: BPSK, QPSK, BPSK-PJammed, and QPSK-PJammed.

Table 8. Confusion matrix of the proposed ANN at −6 dB in presence of Pulsed jamming.

Signal Class	BPSK	QPSK	BPSK-PJammed	QPSK-PJammed
BPSK	990	10	0	0
QPSK	13	985	0	3
BPSK-PJammed	0	0	992	8
QPSK-PJammed	0	0	2	998

Table 9. Confusion matrix of the proposed ANN at −3 dB in presence of Pulsed jamming.

Signal Class	BPSK	QPSK	BPSK-PJammed	QPSK-PJammed
BPSK	1000	0	0	0
QPSK	0	1000	0	0
BPSK-PJammed	0	0	1000	0
QPSK-PJammed	0	0	0	1000

Table 10. Confusion matrix of the proposed ANN at 0 dB in presence of Pulsed jamming.

Signal Class	BPSK	QPSK	BPSK-PJammed	QPSK-PJammed
BPSK	1000	0	0	0
QPSK	0	1000	0	0
BPSK-PJammed	0	0	1000	0
QPSK-PJammed	0	0	0	1000

Table 11. Confusion matrix of the proposed ANN at 3 dB in presence of Pulsed jamming.

Signal Class	BPSK	QPSK	BPSK-PJammed	QPSK-PJammed
BPSK	1000	0	0	0
QPSK	0	1000	0	0
BPSK-PJammed	0	0	1000	0
QPSK-PJammed	0	0	0	1000

Table 12. Confusion matrix of the proposed ANN at 6 dB in presence of Pulsed jamming.

Signal Class	BPSK	QPSK	BPSK-PJammed	QPSK-PJammed
BPSK	1000	0	0	0
QPSK	0	1000	0	0
BPSK-PJammed	0	0	1000	0
QPSK-PJammed	0	0	0	1000

4.2. A Single ANN Architecture for Both Stealthy Jamming Attacks

A single ANN is designed to characterise the spectrum in the presence of both multi-tone and modulated pulsed jamming attacks. The ANN is trained with 80,000 signals set at different SNRs and carrier frequencies for six classes of signals, which are BPSK, QPSK, BPSK-Modulated Pulse Jammed (BPSK-PJ), QPSK-Modulated Pulse Jammed (QPSK-PJ), BPSK-Tone Jammed (BPSK-TJ), and QPSK-Tone Jammed (QPSK-TJ). The ANN classifies the signals with a total classification rate of 98.5%, as presented in Figure 7. The true positive for six classes are 99%, 98%, 98%, 97%, 99%, and 99% consecutively, which shows that the proposed algorithm not only classifies the legitimate signals with a very high rate but also detects both multi-tone and modulated pulsed stealthy jamming attacks with very high accuracy. Further, this single ANN gives comparable performance to dedicated ANN architectures (Figures 5 and 6) that used a dedicated neural network to detect one particular type of jamming attack.

Moreover, the ANN is also tested for independent signals from the one used in the previous confusion matrix computation. For testing, 1000 samples, for each class of signals, are tested at SNRs in the range of −9 dB–6 dB. The resultant confusion matrices for each SNR are shown in Tables 13–18. The results show that at −9 dB, the classification rates for un-jammed signals, BPSK and QPSK, are 96.8% and 91.4%, while for four jammed signals—BPSK-PJ, QPSK-PJ, BPSK-TJ, and QPSK-TJ—they are 90.7%, 95.4%, 93.3%, and 96%, respectively. Classification performance is reduced compared with dedicated ANN architecture, for example, the classification rate at −9 dB is approximately 93% compared with 98% with dedicated ANN (Tables 2 and 8) architecture. Similarly, the detection rate of the jammer is also reduced to 93% compared with 99% with dedicated ANN for each jamming attack. However, the performance of the algorithm is increased at −6 dB and classified the first four classes (BPSK, QPSK, BPSK-PJ, and QPSK-PJ) with a rate of approximately 98%, whereas the last two classes of signals (BPSK-TJ and QPSK-TJ) are classified with a rate of 99.5%. A similar trend is observed at −6 dB and a classification rate in dedicated ANN is approximately 100%, whereas it is 97% for single ANN architecture.

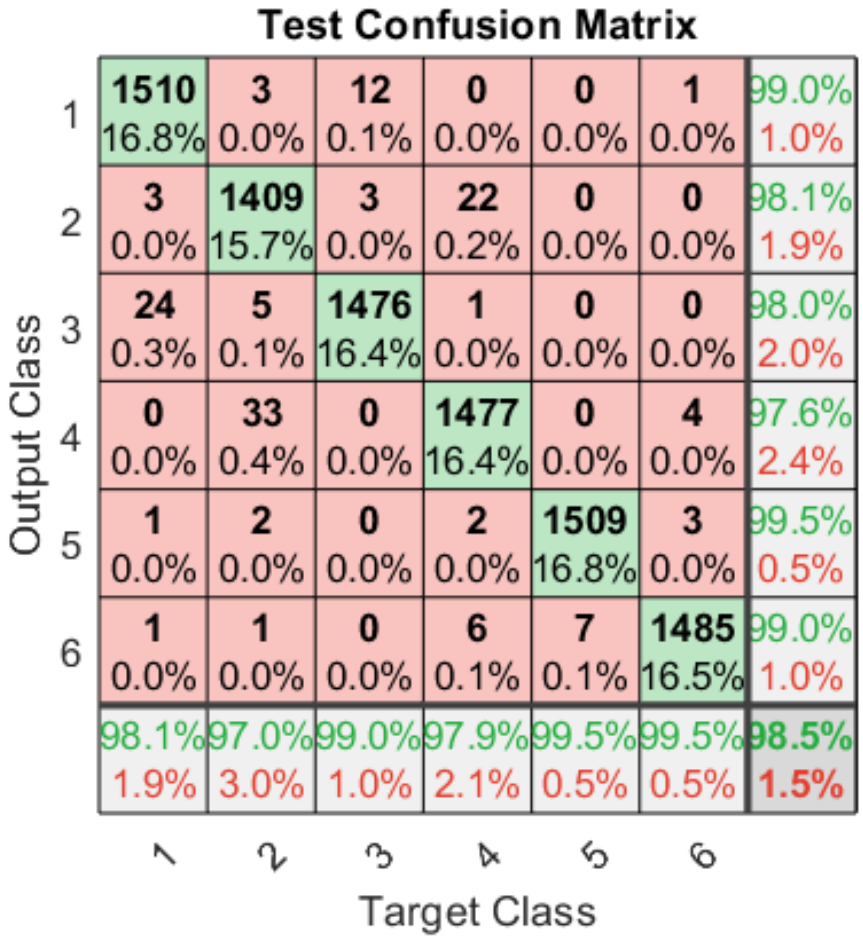

Figure 7. Confusion matrix of the single ANN architecture with six output classes: BPSK, QPSK, BPSK-PJammed, QPSK-PJammed, BPSK-TJammed, and QPSK-TJammed.

A total classification rate of approximately 100% is achieved at −3 dB, which means ANN is able to correctly classify all the signals without any errors. This performance is comparable to dedicated ANN architecture; therefore, it can be inferred from the results that a single ANN architecture can be selected to detect both types of stealthy jamming attacks as well as to classify legitimate signals to their corresponding modulation schemes. The jammer detection rate achieved by the algorithm at different SNRs is plotted in Figure 8. It can be noticed from the figure that a very high jammer detection rate of 0.97 is achieved at low SNR of −6 dB, whereas a jammer detection rate of 1 is attained at −3 dB. Moreover, it can be seen that a very low miss-classification rate of legitimate signals as a jammer is obtained. Further, to evaluate the robustness of the algorithm, the overall signal correct classification rate ordained at various SNRs is given in Figure 9. The figure shows that a classification rate of 0.975 is achieved at −6 dB and increased to 1 at −3 dB. The algorithm achieved such high performances because the SCF of different types of signals results in highly distinct patterns; therefore, corresponding α profiles of signals can be used as a feature set (refer to Section 3.1). Further, an ANN-based classifier is shown to be a robust tool to recognise such patterns of various signals at low SNRs.

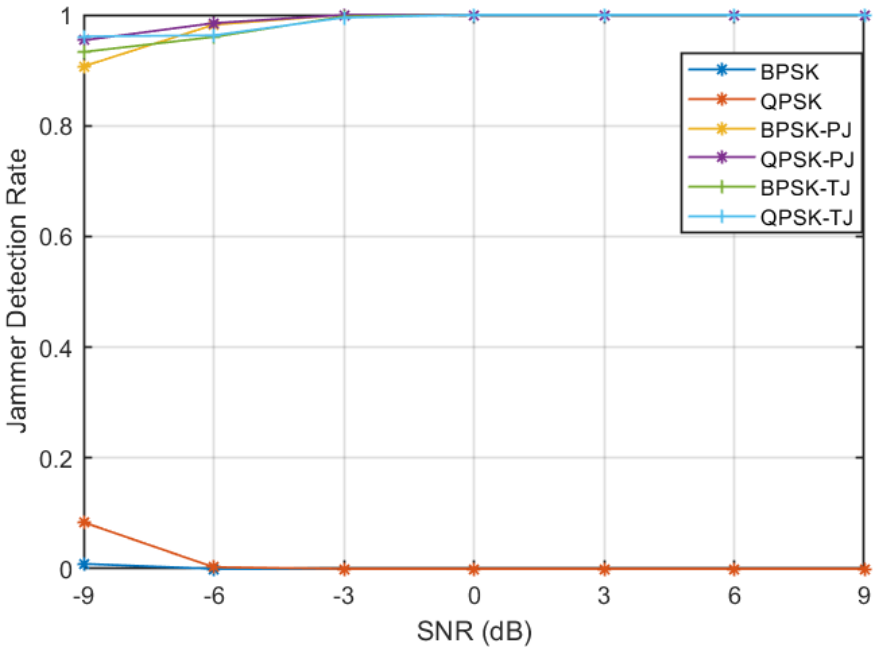

Figure 8. Jammer detection rate at various SNRs.

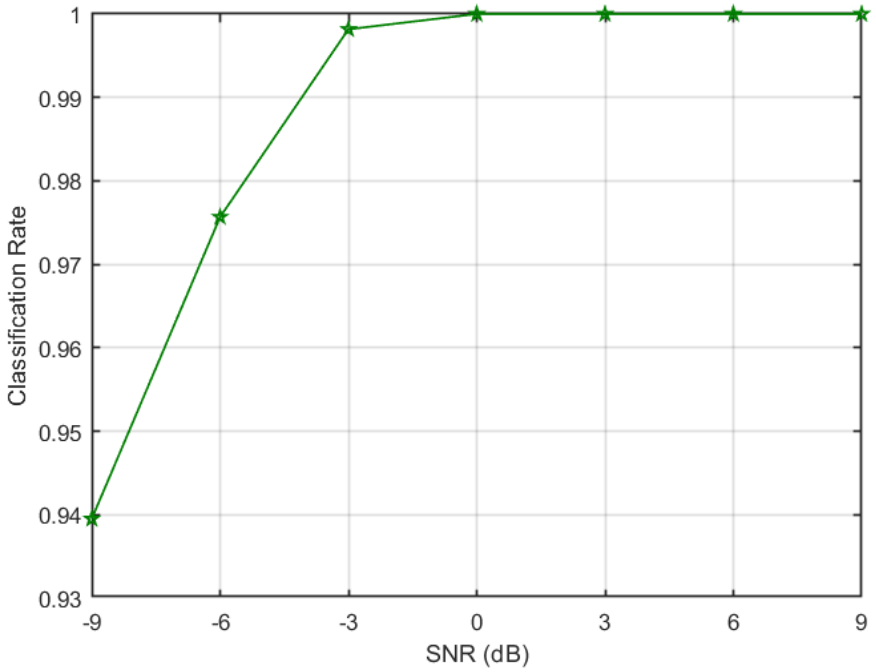

Figure 9. Signal's classification rate at various SNRs.

Table 13. Confusion matrix of the proposed ANN at -9 dB in presence of Tone and Pulsed jamming.

Signal Class	BPSK	QPSK	BPSK-PJ	QPSK-PJ	BPSK-TJ	QPSK-TJ
BPSK	968	23	9	0	0	0
QPSK	2	914	15	1	1	67
BPSK-PJ	9	7	907	1	71	5
QPSK-PJ	0	0	2	954	1	43
BPSK-TJ	0	0	48	5	933	14
QPSK-TJ	0	3	0	23	13	961

Table 14. Confusion matrix of the proposed ANN at −6 dB in presence of Tone and Pulsed jamming.

Signal Class	BPSK	QPSK	BPSK-PJ	QPSK-PJ	BPSK-TJ	QPSK-TJ
BPSK	980	20	0	0	0	0
QPSK	13	984	3	0	0	0
BPSK-PJ	0	1	982	10	7	0
QPSK-PJ	0	0	0	985	1	14
BPSK-TJ	0	0	35	5	960	0
QPSK-TJ	0	9	0	25	3	963

Table 15. Confusion matrix of the proposed ANN at −3 dB in presence of Tone and Pulsed jamming.

Signal Class	BPSK	QPSK	BPSK-PJ	QPSK-PJ	BPSK-TJ	QPSK-TJ
BPSK	999	1	0	0	0	0
QPSK	2	998	0	0	0	0
BPSK-PJ	0	0	1000	0	0	0
QPSK-PJ	0	0	0	1000	0	0
BPSK-TJ	0	0	0	3	997	0
QPSK-TJ	0	0	0	5	0	995

Table 16. Confusion matrix of the proposed ANN at 0 dB in presence of Tone and Pulsed jamming.

Signal Class	BPSK	QPSK	BPSK-PJ	QPSK-PJ	BPSK-TJ	QPSK-TJ
BPSK	1000	0	0	0	0	0
QPSK	0	1000	0	0	0	0
BPSK-PJ	0	0	1000	0	0	0
QPSK-PJ	0	0	0	1000	0	0
BPSK-TJ	0	0	0	0	1000	0
QPSK-TJ	0	0	0	0	0	1000

Table 17. Confusion matrix of the proposed ANN at 3 dB in presence of Tone and Pulsed jamming.

Signal Class	BPSK	QPSK	BPSK-PJ	QPSK-PJ	BPSK-TJ	QPSK-TJ
BPSK	1000	0	0	0	0	0
QPSK	0	1000	0	0	0	0
BPSK-PJ	0	0	1000	0	0	0
QPSK-PJ	0	0	0	1000	0	0
BPSK-TJ	0	0	0	0	1000	0
QPSK-TJ	0	0	0	0	0	1000

Table 18. Confusion matrix of the proposed ANN at 6 dB in presence of Tone and Pulsed jamming.

Signal Class	BPSK	QPSK	BPSK-PJ	QPSK-PJ	BPSK-TJ	QPSK-TJ
BPSK	1000	0	0	0	0	0
QPSK	0	1000	0	0	0	0
BPSK-PJ	0	0	1000	0	0	0
QPSK-PJ	0	0	0	1000	0	0
BPSK-TJ	0	0	0	0	1000	0
QPSK-TJ	0	0	0	0	0	1000

Further, our proposed algorithm achieved significantly high accuracy when compared with most recent techniques for signal classifications that require 10–20 dB SNR for comparable classification performances [44–48]. For example, in [49], the authors presented an algorithm based on instantaneous statistical characteristics and a Support Vector Machine (SVM) capable of classifying modulated signals 2ASK, 4ASK, 2FSK, and 2PSK with a classification rate of 0.95 at 5 dB and can only attain error-free classification at approximately 14 dB. On the other hand, our proposed algorithm achieved a classification rate of 0.975 even at -6 dB, showing a significant performance gain due to the use of expert features that are extracted from signals using cyclostationary spectral analysis. On the other hand, our proposed algorithm achieved a classification rate of 0.975 even at -6 dB, resulting a significant performance gain due to the use of expert features that are extracted from signals using cyclostationary spectral analysis. In [45], the jammer detection algorithm uses the centre frequencies, the peak amplitude of the PSD, and bandwidths of the NB signals as the feature set for the naive Bayes Classifier (NBC). The result shows that at 5 dB the algorithm is able to classify the un-jammed signals (BPSK and QPSK) and jammed signals (BPSK-Jammed and QPSK-Jammed) at a rate of 0.82 and 0.69 (without compression), respectively. Similarly, a classification rate of 0.88 and 0.79 is achieved at 10 dB. It can be observed from the results shown in Table 15 that our proposed technique outperformed the algorithm in [45] and achieved a classification rate of 0.98 for un-jammed and 0.97 at -6 dB. Further, our designed algorithm achieved error-free classification even at -3 dB. Further, it can be noticed that the newly proposed single ANN architecture yields approximately the same accuracy when validated over a large dataset of 80,000 samples, in comparison to our previous work in [31,32], which used a dedicated ANN architecture to detect each type of jamming attack. Such validations show that a single ANN-based algorithm is highly reliable and robust.

5. Conclusions

In this article, a novel algorithm is presented for joint signal classification and stealthy jammer detection in WB radios. The WB is composed of numerous NB signals that could be either licit signals or jammed by a stealthy jammer. The jammers embed energy detection and feature detection capabilities of CR and use multi-tone and modulated pulsed jamming signals to jam the licit NB signals. The received NB signals in WB are fed to the CFD module that computes the corresponding SCF. The features related to α and f profiles are obtained from SCF; then, they are concatenated and provided as input features to the ANN that classifies the signals either as legitimate signals with corresponding modulation schemes or jammers with a particular jamming attack (multi-tone and modulated pulsed). The performances of both the ANN-based classifiers, dedicated networks and single network, are evaluated at different SNRs and classification results are given by confusion matrices. The results showed that our newly proposed algorithm performed well at low SNRs (-6–0 dB) and, even with single ANN architecture, a classification accuracy of 0.98 is achieved at -6 dB. Further, the designed algorithm showed superior performances when compared with recently proposed signal classifications and jammer detection algorithms.

Future work will include the development of an autonomous system capable of dynamically accessing the WB spectrum in a CR environment for applications like defence against more sophisticated jamming attacks. Another interesting future research direction could be exploring deep learning for signal classification that does not need expert features.

Author Contributions: Conceptualization, T.N. and A.A.; methodology, T.N.; software, T.N.; validation, T.N. and A.A.; formal analysis, T.N.; investigation, T.N. and A.A; resources, T.N. and A.A.; data curation, T.N. and A.A; writing—original draft preparation, T.N.; writing—review and editing, T.N. and A.A; visualization, T.N. and A.A.; supervision, T.N.; project administration, T.N. and A.A.; funding acquisition, T.N. and A.A. All authors have read and agreed to the published version of the manuscript.

Funding: This work has been carried out under the financial support of grant GRANT3475 of the Deanship of Scientific Research (DSR), Vice Presidency of Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data used to support the findings of this study are available from the corresponding author upon request.

Acknowledgments: The authors gratefully recognise the Deanship of Scientific Research (DSR) at King Faisal University for financial assistance provided through grant GRANT3475.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Nasser, A.; Al Haj Hassan, H.; Abou Chaaya, J.; Mansour, A.; Yao, K.C. Spectrum Sensing for Cognitive Radio: Recent Advances and Future Challenge. *Sensors* **2021**, *21*, 2408. [CrossRef]
2. Haykin, S. Cognitive dynamic systems: Radar, control, and radio [point of view]. *Proc. IEEE* **2012**, *100*, 2095–2103. [CrossRef]
3. Arjoune, Y.; Kaabouch, N. A Comprehensive Survey on Spectrum Sensing in Cognitive Radio Networks: Recent Advances, New Challenges, and Future Research Directions. *Sensors* **2019**, *19*, 126. [CrossRef] [PubMed]
4. Haykin, S. Cognitive radio: Brain-empowered wireless communications. *IEEE J. Sel. Areas Commun.* **2005**, *23*, 201–220. [CrossRef]
5. Holland, O.; Ping, S.; Aijaz, A.; Chareau, J.M.; Chawdhry, P.; Gao, Y.; Qin, Z.; Kokkinen, H. To white space or not to white space: That is the trial within the Ofcom TV white spaces pilot. In Proceedings of the 2015 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN), Stockholm, Sweden, 29 September–2 October 2015; pp. 11–22.
6. Qin, Z.; Gao, Y.; Parini, C.G. Data-assisted low complexity compressive spectrum sensing on real-time signals under sub-Nyquist rate. *IEEE Trans. Wirel. Commun.* **2015**, *15*, 1174–1185. [CrossRef]
7. Qin, Z.; Gao, Y.; Plumbley, M.D.; Parini, C.G. Wideband spectrum sensing on real-time signals at sub-Nyquist sampling rates in single and cooperative multiple nodes. *IEEE Trans. Signal Process.* **2015**, *64*, 3106–3117. [CrossRef]
8. Ma, Y.; Gao, Y.; Liang, Y.C.; Cui, S. Reliable and efficient sub-Nyquist wideband spectrum sensing in cooperative cognitive radio networks. *IEEE J. Sel. Areas Commun.* **2016**, *34*, 2750–2762. [CrossRef]
9. Martin, J.H.; Dooley, L.S.; Wong, K.C.P. New dynamic spectrum access algorithm for TV white space cognitive radio networks. *IET Commun.* **2016**, *10*, 2591–2597. [CrossRef]
10. Lin, S.; Kong, L.; Gao, Q.; Khan, M.K.; Zhong, Z.; Jin, X.; Zeng, P. Advanced dynamic channel access strategy in spectrum sharing 5G systems. *IEEE Wirel. Commun.* **2017**, *24*, 74–80. [CrossRef]
11. Dabcevic, K.; Betancourt, A.; Marcenaro, L.; Regazzoni, C.S. Intelligent cognitive radio jamming—A game-theoretical approach. *EURASIP J. Adv. Signal Process.* **2014**, *2014*, 171. [CrossRef]
12. Dabcevic, K.; Mughal, M.O.; Marcenaro, L.; Regazzoni, C.S. Cognitive Radio as the Facilitator for Advanced Communications Electronic Warfare Solutions. *J. Signal Process. Syst.* **2015**, *83*, 29–44. [CrossRef]
13. Krayani, A.; William, N.J.; Marcenaro, L.; Regazzoni, C. Jammer Detection in Vehicular V2X Networks. In Proceedings of the 2022 Microwave Mediterranean Symposium (MMS), Pizzo Calabro, Italy, 11–12 May 2022; pp. 1–5. [CrossRef]
14. Barb, G.; Alexa, F.; Otesteanu, M. Dynamic Spectrum Sharing for Future LTE-NR Networks. *Sensors* **2021**, *21*, 4215. [CrossRef] [PubMed]
15. Moon, B. Dynamic Spectrum Access for Internet of Things Service in Cognitive Radio-Enabled LPWANs. *Sensors* **2017**, *17*, 2818. [CrossRef] [PubMed]
16. Lin, R.; Qiu, H.; Jiang, W.; Jiang, Z.; Li, Z.; Wang, J. Deep Reinforcement Learning for Physical Layer Security Enhancement in Energy Harvesting Based Cognitive Radio Networks. *Sensors* **2023**, *23*, 807. [CrossRef]

17. Gao, Y.; Qin, Z.; Feng, Z.; Zhang, Q.; Holland, O.; Dohler, M. Scalable and reliable IoT enabled by dynamic spectrum management for M2M in LTE-A. *IEEE Internet Things J.* **2016**, *3*, 1135–1145. [CrossRef]
18. Fiaschetti, A.; Noll, J.; Azzoni, P.; Uribeetxeberria, R. *Measurable and Composable Security, Privacy, and Dependability for Cyberphysical Systems: The SHIELD Methodology*; CRC Press: Boca Raton, FL, USA, 2017.
19. Mohammadi, J.; Stańczak, S.; Zheng, M. Joint spectrum sensing and jamming detection with correlated channels in cognitive radio networks. In Proceedings of the 2015 IEEE International Conference on Communication Workshop (ICCW), London, UK, 8–12 June 2015; pp. 889–894.
20. Rahman, M.J.A.; Krunz, M.; Erwin, R. Interference mitigation using spectrum sensing and dynamic frequency hopping. In Proceedings of the 2012 IEEE International Conference on Communications (ICC), Ottawa, ON, Canada, 10–15 June 2012; pp. 4421–4425.
21. Chin, W.L.; Li, J.M.; Chen, H.H. Low-complexity energy detection for spectrum sensing with random arrivals of primary users. *IEEE Trans. Veh. Technol.* **2015**, *65*, 947–952. [CrossRef]
22. Kozłowski, S. Implementation and verification of cyclostationary feature detector for DVB-T signals. *IET Signal Process.* **2016**, *10*, 162–167. [CrossRef]
23. Zhang, X.; Gao, F.; Chai, R.; Jiang, T. Matched filter based spectrum sensing when primary user has multiple power levels. *China Commun.* **2015**, *12*, 21–31. [CrossRef]
24. Gardner, W.; Spooner, C. The cumulant theory of cyclostationary time-series. I. Foundation. *IEEE Trans. Signal Process.* **1994**, *42*, 3387–3408. [CrossRef]
25. Roberts, R.S.; Brown, W.A.; Loomis, H.H. Computationally efficient algorithms for cyclic spectral analysis. *IEEE Signal Process. Mag.* **1991**, *8*, 38–49. [CrossRef]
26. Spooner, C.; Gardner, W. The cumulant theory of cyclostationary time-series. II. Development and applications. *IEEE Trans. Signal Process.* **1994**, *42*, 3409–3429. [CrossRef]
27. Wu, Z.; Like, E.; Chakravarthy, V. Reliable modulation classification at low SNR using spectral correlation. In Proceedings of the 2007 4th IEEE Consumer Communications and Networking Conference, Las Vegas, NV, USA, 11–13 January 2007; pp. 1134–1138.
28. Al-Habashna, A.; Dobre, O.A.; Venkatesan, R.; Popescu, D.C. Second-Order Cyclostationarity of Mobile WiMAX and LTE OFDM Signals and Application to Spectrum Awareness in Cognitive Radio Systems. *IEEE J. Sel. Top. Signal Process.* **2012**, *6*, 26–42. [CrossRef]
29. Like, E.; Chakravarthy, V.; Husnay, R.; Wu, Z. Modulation recognition in multipath fading channels using cyclic spectral analysis. In Proceedings of the IEEE GLOBECOM 2008—2008 IEEE Global Telecommunications Conference, New Orleans, LA, USA, 30 November–4 December 2008; pp. 1–6.
30. Yucek, T.; Arslan, H. A survey of spectrum sensing algorithms for cognitive radio applications. *IEEE Commun. Surv. Tutor.* **2009**, *11*, 116–130. [CrossRef]
31. Nawaz, T.; Campo, D.; Mughal, M.O.; Marcenaro, L.; Regazzoni, C.S. Jammer Detection Algorithm for Wide-band Radios using Spectral Correlation and Neural Networks. In Proceedings of the 13th International Conference on Wireless Communications and Mobile Computing, Valencia, Spain, 26–30 June 2017; Volume 1, pp. 890–897.
32. Nawaz, T.; Marcenaro, L.; Regazzoni, C.S. Stealthy jammer detection algorithm for wide-band radios: A physical layer approach. In Proceedings of the 2017 IEEE 13th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Rome, Italy, 9–11 October 2017; pp. 79–83. [CrossRef]
33. Alfaqawi, M.I.; Chebil, J.; Habaebi, M.H.; Datla, D. Wireless distributed computing for cyclostationary feature detection. *Digit. Commun. Netw.* **2016**, *2*, 47–56. [CrossRef]
34. Chen, R.; Park, J.M.; Reed, J.H. Defense against Primary User Emulation Attacks in Cognitive Radio Networks. *IEEE J. Sel. Areas Commun.* **2008**, *26*, 25–37. [CrossRef]
35. Wang, L.; Wyglinski, A.M. A combined approach for distinguishing different types of jamming attacks against wireless networks. In Proceedings of the 2011 IEEE Pacific Rim Conference on Communications, Computers and Signal Processing, Victoria, BC, Canada, 23–26 August 2011; pp. 809–814.
36. Pelechrinis, K.; Iliofotou, M.; Krishnamurthy, S.V. Denial of Service Attacks in Wireless Networks: The Case of Jammers. *IEEE Commun. Surv. Tutor.* **2011**, *13*, 245–257. [CrossRef]
37. Poiselr, R.A. Introduction to Communication Electronic Warfare Systems. In Proceedings of the 2014 IEEE Global Communications Conference, Austin, TX, USA, 8–12 December 2014.
38. Qian, L.; Li, X.; Wei, S. Anomaly Spectrum Usage Detection in Multihop Cognitive Radio Networks: A Cross-Layer Approach. *JCM* **2013**, *8*, 259–266. [CrossRef]
39. Amuru, S.; Buehrer, R.M. Optimal jamming strategies in digital communications-Impact of modulation. In Proceedings of the 2014 IEEE Global Communications Conference, Austin, TX, USA, 8–12 December 2014; pp. 1619–1624.
40. Amuru, S.; Buehrer, R.M. Optimal Jamming Against Digital Modulation. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 2212–2224. [CrossRef]
41. Moser, E.; Moran, M.K.; Hillen, E.; Li, D.; Wu, Z. Automatic modulation classification via instantaneous features. In Proceedings of the 2015 National Aerospace and Electronics Conference (NAECON), Dayton, OH, USA, 15–19 June 2015; pp. 218–223.
42. Gardner, W.A. Signal interception: A unifying theoretical framework for feature detection. *IEEE Trans. Commun.* **1988**, *36*, 897–906. [CrossRef]

43. Møller, M.F. A scaled conjugate gradient algorithm for fast supervised learning. *Neural Netw.* **1993**, *6*, 525–533. [CrossRef]
44. Lee, S.H.; Kim, K.Y.; Shin, Y. Effective Feature Selection Method for Deep Learning-Based Automatic Modulation Classification Scheme Using Higher-Order Statistics. *Appl. Sci.* **2020**, *10*, 588. [CrossRef]
45. Mughal, M.O.; Kim, S. Signal Classification and Jamming Detection in Wide-Band Radios Using Naïve Bayes Classifier. *IEEE Commun. Lett.* **2018**, *22*, 1398–1401. [CrossRef]
46. Hameed, F.; Dobre, O.A.; Popescu, D.C. On the likelihood-based approach to modulation classification. *IEEE Trans. Wirel. Commun.* **2009**, *8*, 5884–5892. [CrossRef]
47. Shi, W.; Liu, D.; Cheng, X.; Li, Y.; Zhao, Y. Particle Swarm Optimization-Based Deep Neural Network for Digital Modulation Recognition. *IEEE Access* **2019**, *7*, 104591–104600. [CrossRef]
48. Hu, S.; Pei, Y.; Liang, P.P.; Liang, Y.C. Deep neural network for robust modulation classification under uncertain noise conditions. *IEEE Trans. Veh. Technol.* **2019**, *69*, 564–577. [CrossRef]
49. Zhang, X.; Ge, T.; Chen, Z. Automatic Modulation Recognition of Communication Signals Based on Instantaneous Statistical Characteristics and SVM Classifier. In Proceedings of the 2018 IEEE Asia-Pacific Conference on Antennas and Propagation (APCAP), Auckland, New Zealand, 5–8 August 2018; pp. 344–346. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.