engineering proceedings

MDPI

Proceeding Paper

Satellite Navigation Signal Interference Detection and Machine Learning-Based Classification Techniques towards Product Implementation †

Jelle Rijnsdorp [1,*,‡], Annemarie van Zwol [2,‡] and Merle Snijders [2]

[1] S[&]T, 2616 LR Delft, The Netherlands
[2] Netherlands Aerospace Centre (NLR), 1059 CM Amsterdam, The Netherlands; annemarie.van.zwol@nlr.nl (A.v.Z.); merle.snijders@nlr.nl (M.S.)
* Correspondence: jelle.rijnsdorp@stcorp.nl
† Presented at the European Navigation Conference 2023, Noordwijk, The Netherlands, 31 May–2 June 2023.
‡ These authors contributed equally to this work.

Abstract: Many critical applications highly depend on Global Navigation Satellite Systems (GNSS) for precise and continuously available positioning and timing information. To warn a GNSS user that the signals are compromised, real-time interference detection is required. Additionally, real-time classification of the interference signal allows the user to select the most effective mitigation methods for the encountered disturbance. A compact proof of concept has been built using commercial off-the-shelf (COTS) components to analyse the jamming detection and classification techniques. It continuously monitors GNSS frequency bands and generates warnings to the user when interference is detected and classified. Various signal spectrum analyses, consisting of kurtosis and power spectral density (PSD) calculations, as well as a machine learning model, are used to detect and classify anomalies in the incoming signals. The system has been tested by making use of a COTS GNSS signal simulator. The simulator is used to generate the upper L-band GNSS signals and different types of interferences. Successful detection and classification is demonstrated, even for interference power levels that do not degrade the performance of a commercial reference receiver.

Keywords: GNSS; jamming detection; machine learning; jamming classification; product implementation

Citation: Rijnsdorp, J.; van Zwol, A.; Snijders, M. Satellite Navigation Signal Interference Detection and Machine Learning-Based Classification Techniques towards Product Implementation. *Eng. Proc.* **2023**, *54*, 60. https://doi.org/10.3390/ENC2023-15449

Academic Editors: Tom Willems and Okko Bleeker

Published: 29 October 2023

1. Introduction

Many critical applications exhibit a high dependency on Global Navigation Satellite Systems (GNSS) for precise and continuously available positioning and timing information. Interference of the low-power GNSS signals has become an increasing threat for society [1,2]. In terms of intentional Radio Frequency Interference (RFI), jamming aims to disrupt GNSS signals by overpowering them, leading to the receiver losing the position, velocity and timing (PVT) solution. To warn a GNSS user that the GNSS signals are compromised, real-time interference detection is required. Additionally, real-time classification of the interference signal allows the user to select the most effective mitigation methods for the encountered disturbance. Classification can also be used to estimate disturbance signal properties and help point the user towards likely sources of the interference signal.

Previous publications [3–5] have shown the potential of using artificial intelligence for pre-correlation interference classification. The aim in this paper is to use various signal spectrum analysis methods as well as a machine learning model to develop a compact GNSS interference detection and classification module. The module is constructed using widely available commercial off-the-shelf (COTS) components. The goal is to continuously monitor GNSS frequency bands, generate warnings to the user when interference is detected and inform the user on how the interference signal is classified.

This paper is structured to first provide an overview of the implemented interference detection and classification techniques. Then, hardware and software designs of the module are briefly discussed. The strategy and results of an initial over-the-cable test campaign are presented, and finally, a short outlook on future product development is provided.

2. Detection

This section elaborates on the techniques that are used for jamming detection. As the monitoring system is designed to be independent of a GNSS receiver, the selected detection techniques are based on the signal spectrum that is obtained directly from the antenna.

2.1. Statistical Analysis

The first method is a statistical analysis based on the spectrum of the incoming GNSS signal. The method consists of a calculation of the Kurtosis value K of the spectrum, and is defined as:

$$K = \frac{\mu^4}{\sigma^4}, \tag{1}$$

where μ is the fourth central moment and σ is the standard deviation of the spectrum. For natural thermal emissions, the distribution is Gaussian and has a nominal Kurtosis of 3.0. Since GNSS signals are buried under the noise level, a sample data set containing GNSS signals should resemble white noise. If the signal is corrupted by RFI of sufficient power, the distribution will deviate from normality, leading to a deviation from the nominal Kurtosis value. The Kurtosis calculation can be used to detect jammer types that add non-noise-like energy to the signal.

2.2. Power Spectral Density Ratio (PSD)

For partial band and narrowband interference signals, analysis of the frequency domain provides valuable information in terms of detection. By calculating the power spectral density (PSD) ratio, the presence of additive energy in the signal spectrum can be detected. The frequency spectrum X can be computed using the discrete Fourier transform:

$$X_k = \sum_{n}^{N-1} x[n] e^{-j\frac{2\pi n}{N}}, \tag{2}$$

where x is the GNSS signal, k is the frequency bin, N is the number of samples in the frequency bin and n is an iterator. From the frequency domain, the PSD can be calculated. The algorithm that is implemented in the monitoring system uses the PSD from both the received signal, as well as the PSD of a pre-defined reference signal, which is recorded in a non-RFI scenario and provides a baseline of the received power by the system. The maximum PSD ratio r_{max} is then defined as

$$r_{max} = \max\left(\frac{\|X_{test}\|^2}{\left\|X_{ref}\right\|^2}\right), \tag{3}$$

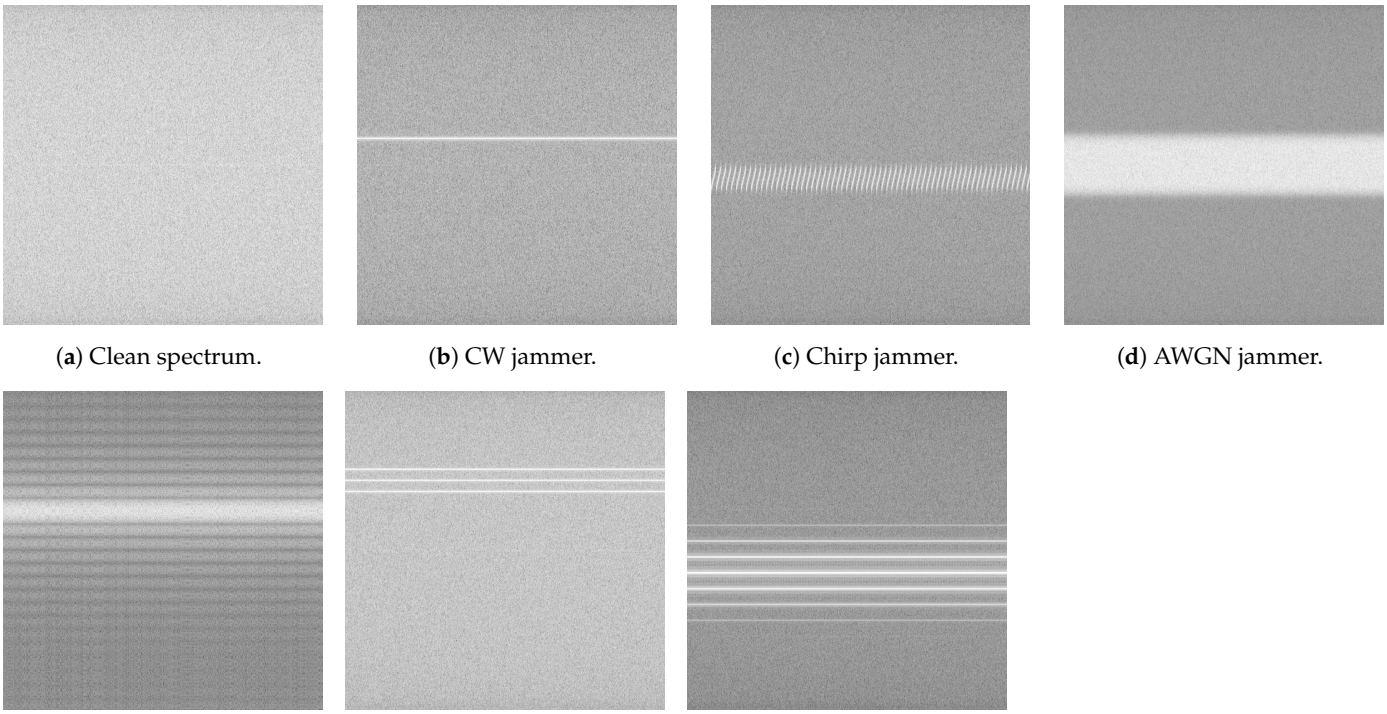
and if increased above a certain threshold, it indicates an RFI signal in the spectrum. This detection technique is used for finding added energy to the signal spectrum and is not bound to specific jamming types.

3. Classification

As an extension to the aforementioned jamming detection methods, a classification model can be used to provide classification of the type of jamming signal, which is useful information when considering mitigation techniques. Additionally, it can be used as a detection technique.

3.1. Model Setup

The classification model is constructed using a Convolutional Neural Network (CNN) in combination with transfer learning and is trained on recognizing spectral features in images created by taking a spectrogram of the incoming GNSS signal. As the different jammer types induce different spectral features, this method can be very effective for the classification of jamming. The set of included jammer types consist of Continuous Wave (CW), chirp or Swept Continuous Wave (SCW), Additive White Gaussian Noise (AWGN), Pseudo-Random Noise (PRN), Amplitude Modulation (AM) and Frequency Modulation (FM). Figure 1 shows the spectral features on which the classification model is trained.



(**a**) Clean spectrum. (**b**) CW jammer. (**c**) Chirp jammer. (**d**) AWGN jammer.

(**e**) PRN jammer. (**f**) AM jammer. (**g**) FM jammer.

Figure 1. Spectrograms of the clean signal without RFI and with different types of jamming signals. The horizontal axis shows the time domain and the vertical axis shows the frequency domain.

The jamming types of which the spectra are shown in Figure 1 are described in Table 1. In these models, y_J denotes the jamming signal, a_J is the (initial) amplitude, f_c is the centre frequency, t is the time and ϕ_J is the phase.

3.2. Model Training

As a baseline for the CNN, the family of EfficientNet [6] models that were specifically developed for increased accuracy and efficiency with respect to MobileNet [7] and ResNet [8] models are used. The actual model that is selected for implementation is the EfficientNet-B5 model, which has 83.6% top 1 accuracy and 96.7% top 5 accuracy, while containing more than five times fewer parameters than comparable models [6]. Training is conducted on a set of input images that contain spectrograms of the GNSS signal with and without different types of jamming signals. The Adam algorithm for gradient descent optimisation is used, which is commonly used to ensure fast training that is robust to potential noise in the input features [9]. To assess the performance of the classification model, a confusion matrix can be used which visualises the expected probability of correct classification and the expected probability for misclassification for all combinations of true and predicted classes. The confusion matrix corresponding to the model described in this section is shown in Figure 2.

Table 1. Jammer models (derived from [3,4]) that are included in the classification model.

Type	Model	Description
CW	$y_J = a_J \cdot \exp(2j\pi f_c t + \phi_J)$	Generates a single-tone jamming signal, which shows a distinct peak at a constant frequency in the signal spectrum. This translates to a horizontal line in the spectrogram (Figure 1b).
Chirp	$y_J = a_J \cdot \exp\left(2j\pi\left(f_c t \pm \frac{1}{2T}(f_{max} - f_{min})t^2\right) + \phi_J\right)$	Generates a frequency-sweeping signal that shows a moving peak over a certain range in the signal spectrum. In the spectrogram, it is characterised by a sawtooth pattern (Figure 1c) with a bandwidth enclosed by minimum and maximum frequencies f_{min} and f_{max} and width of a single tooth defined by the sweep time T.
AWGN	$y_J = a_J \cdot \int_0^t n(\tau)d\tau \cdot \exp(2j\pi f_c t + \phi_J)$	Generates a signal consisting of white Gaussian noise filtered to a specific bandwidth, which translates in a horizontal band in the spectrogram (Figure 1d). The noise n is modelled by a finite impulse response filter applied on a Gaussian distribution with zero mean and variance $\sigma^2 \sim \mathcal{N}(0, \sigma^2)$.
PRN	$y_J = a_J \cdot \int_0^t p(\tau)d\tau \cdot \exp(2j\pi f_c t + \phi_J)$	Generates one PRN-code and shows multiple peaks in the spectrogram (Figure 1e). The PRN-code p is modelled by a finite random sequence of values -1 and 1 and is repeated every millisecond.
AM	$y_J = a_J \cdot [1 + m\cos(2\pi f_m t + \phi_m)] \cdot \exp(2j\pi f_c t + \phi_J)$	Generates a carrier wave signal of which the amplitude is modulated by a message signal with frequency f_m and phase ϕ_m. This translates into a peak at the carrier frequency and two sidebands at a frequency difference of $\pm f_m$ (Figure 1f). Finally, m defines the modulation index, which is a measure for the ratio between the power of the carrier and the message signal.
FM	$y_J = a_J \cdot \exp(2j\pi f_c t + m\sin(2j\pi f_m t + \phi_m) + \phi_J)$	Generates a carrier wave signal of which the frequency is modulated by a message signal with frequency f_m and phase ϕ_m. This translates into a peak at the carrier frequency and multiple sidebands, each with a frequency shift of $n \cdot f_m$, where n is an integer (Figure 1g). Again, m denotes the modulation index, which defines the relative height of the peaks according to a set of Bessel functions.

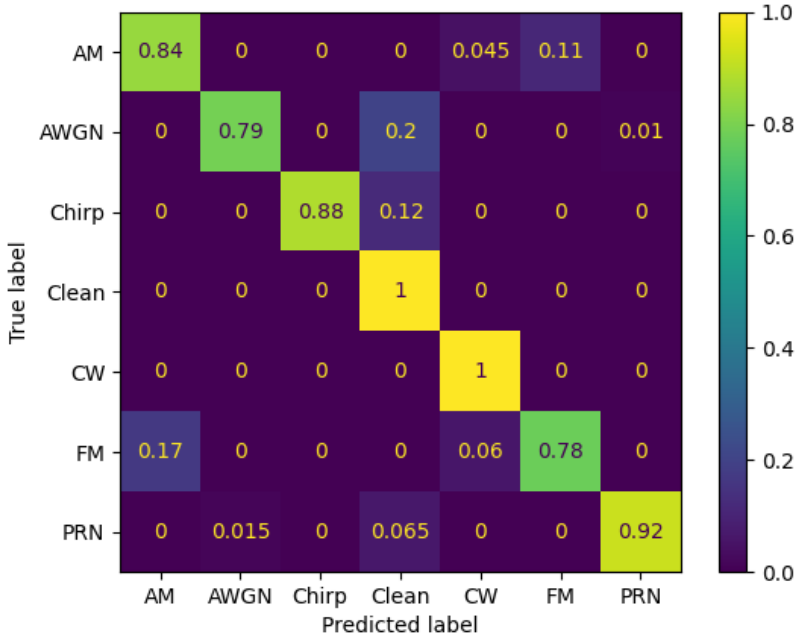


Figure 2. Confusion matrix of the classification model.

This matrix shows excellent results for the clean class and CW and good results for the other classes. The non-zero off-diagonal entries show that the spectral features of some class pairs may be similar, which is especially the case for low-power jamming scenarios. For low-power narrowband waveforms, such as AM and FM, the spectrum may not contain all sub-peaks, leading to misclassification of AM jammers as CW and FM jammers as either CW or AM, depending on the number of visible sub-peaks. The misclassification of an AWGN or PRN jammer as a non-RFI case can be explained by the fact that the energy of these waveforms is spread over a relatively large band of frequencies and the signals themselves resemble noise, which make them barely detectable for low-power scenarios.

4. Product Implementation

Moving from the theoretical methods and techniques that were described in Sections 2 and 3 towards product implementation requires a practical solution for a number of problems. The GNSS monitoring device is required to operate in real time and is to be used in a hand-held configuration. This poses limitations on the computational power, dimensions, weight and power consumption of the hardware to be used. Eventually, the hardware selection influences the software design, which should be able to fulfil the capability of (real-time) jamming detection and classification with limited available computational resources. The designed hardware and software setup are described in this section.

4.1. Hardware Setup

The aim is to keep the hardware design of the monitoring system as simple as possible by limiting the amount of hardware components. It is designed to be managed by a microprocessor that runs the software and controls the other components. To retrieve the signal, the microprocessor will be connected to a Software-Defined Radio (SDR) that is tuned to the GPS L1 frequency with an instantaneous bandwidth of 25 MHz. This SDR contains an input port for a GNSS antenna, which poses the flexibility for the user to use their own GNSS antenna. The data stream from the SDR to the microprocessor contains I/Q data, which are further handled by the software package that is described in Section 4.2.

Results from the jamming detection and classification processes will be communicated to the user via an LCD monitor that can be connected externally. When the device is used in a more mobile setting and the LCD monitor is not used, simple results and other relevant information are communicated via a status LED. To accommodate for mobile usage, a battery pack is included, which is able to power the unit for several hours; additionally, the device can be connected to an external power supply for direct power and to recharge the battery pack.

The flow diagram of the hardware design can be seen in Figure 3. All components except for the external antenna and LCD monitor will be integrated in a protective casing. As mentioned earlier in this section, the monitoring device should be usable in a hand-held configuration, which limits the size of the hardware components. Additionally, using components specifically designed for this particular system is avoided, and therefore it is chosen to use only COTS hardware.

4.2. Software Setup

The microprocessor that was mentioned in the previous paragraph contains the monitoring software, which is enabled when the device is powered on. This software package controls the SDR by starting all relevant processes that lead to the SDR providing I/Q data that describe the GNSS signal. The computational power of the microprocessor is insufficient for processing the complete 25 M samples/s I/Q data stream, and thus the data are reduced before the jamming detection and classification methods are enabled. For detection, data blocks of 100 ms are found to be sufficient, whereas for classification, blocks of only 10 ms are used.

After slicing the data into these blocks, process pools are generated, which will contain the individual processes that execute the detection and classification algorithms. This will ensure concurrency and optimization of the limited computational resources of the microprocessor. When a process is finished, it will pull new I/Q data in and again perform the detection or classification method. The results from all the algorithms are then synchronised and, with a fixed interval, a decision algorithm is executed. This algorithm compares the individual detection and classification results with specified thresholds, which will provide a single alert containing a jamming flag and corresponding jamming class, if applicable. These are then displayed by the status LED and, if connected, the LCD monitor. Additionally, more extensive results from the individual algorithms, as well as general system status, is logged to the SD card of the microprocessor.

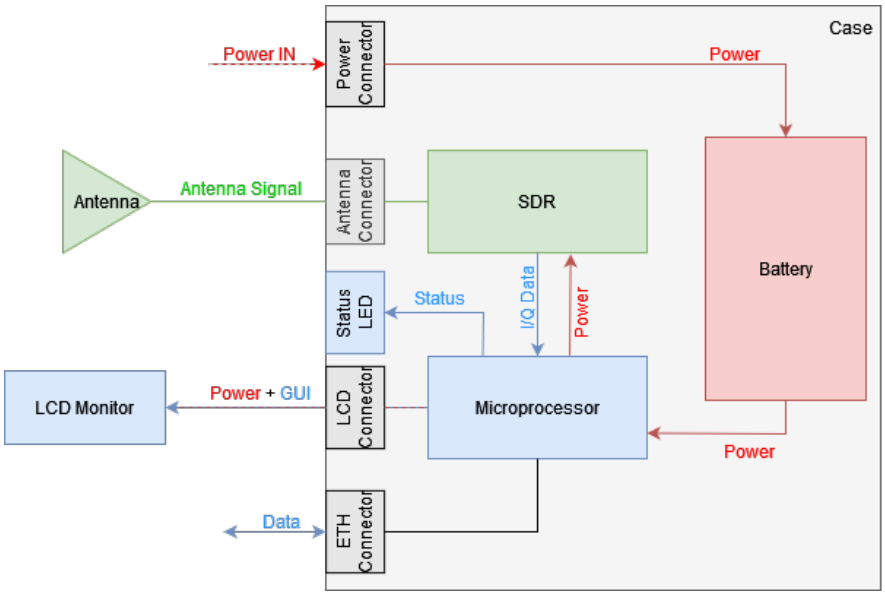


Figure 3. Schematics of the hardware setup of the GNSS monitoring device.

5. Product Tests

An initial test campaign is performed to test the performance of the proposed detection and classification module. The goal of this test campaign is threefold: validate the implemented detection strategy, validate the implemented classification strategy and obtain an initial benchmark of the jammer-to-signal ratios (J/S) for which the module can reliably detect and classify interference signals.

5.1. Experimental Setup

To ensure a clean, controlled, and repeatable test scenario and to exclude any accidental over-the-air interferences the tests are performed over-the-cable in a controlled lab environment. The device under test (DUT) is provided with a series of different input signals in which the true GNSS component is the same for every run and the characteristics of the interference are varied.

A COTS GNSS signal simulator (Orolia GSG-8) is used to simulate the clean GNSS signals, a realistic Gaussian noise floor and the interference signals. Since the DUT only operates in the L1 frequency band, only GPS L1 C/A, Galileo E1 B/C and SBAS L1 signals are included in the input signal. An overview of the settings used to generate the clean input GNSS signals for all test scenarios can be found in Table A1 in Appendix A.

The clean GNSS signals and the interference signals are simulated on two different channels and combined by an RF combiner. To be able to provide the test signal not only to the DUT, but also to a COTS reference receiver (Septentrio AsteRx3 HDC), an active four-way RF signal splitter is used to split the combined input stream to two identical output streams. In Figure 4, the schematics of the test setup are displayed.

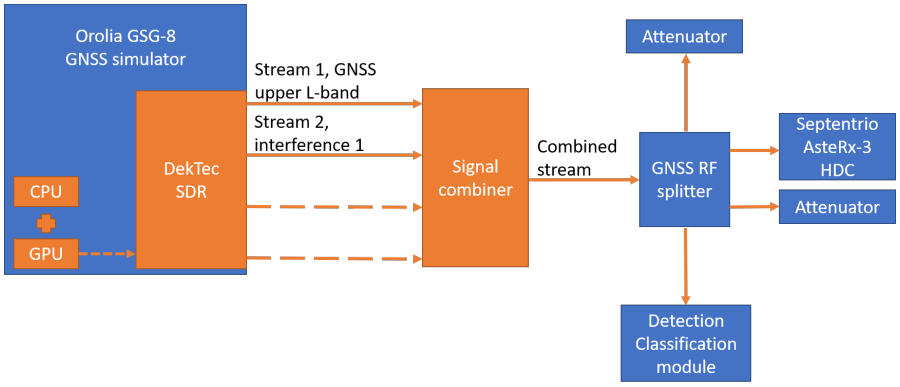


Figure 4. Schematic overview of the test setup. The GNSS simulator is used to generate the test signals. The generated signals are streamed to the DUT and reference receiver.

5.2. Experimental Results

The DUT and a reference receiver are subjected to two test scenarios in which the jamming power is increased over time. First, a wide range of J/S is used, where the ratio is increased in steps of 3 dB. For every step in this scenario, the J/S is kept constant for 60 s to allow the reference receiver to acclimatise. The second scenario, which entails a smaller range of J/S with a step size of 0.5 dB and a step duration of only 10 s, is used to improve the accuracy of the detection and classification results. The waveform characteristics of the interference signals used in this test campaign are summarised in Table A2 in Appendix A. Detection and classification are triggered when the thresholds are exceeded for three out of five subsequent measurements to reduce the number of false alarms. The reference receiver is used to monitor the effect of the interference signal on the resolving capability of a targeted GNSS receiver. The J/S for which the reference receiver experiences first loss of its PVT solution is used to put the performance of the DUT in perspective.

Both detection and correct classification take place even before the first loss of a tracked satellite is registered. The classification model proves to be the most sensitive detection method, as it is able to recognise the spectral features of an interference signal before the thresholds on the detection parameters are exceeded (highlighted values in Table 2). It will cause the system to trigger a jamming warning, albeit that no reliable classification can be made yet. The PSD method proves to be effective for narrowband waveforms, whereas the kurtosis can be used for all waveforms except for the AWGN. All detection methods are triggered at significantly lower J/S than the ratio where the reference receiver experiences loss of its PVT solution. The relatively 'late' correct classification of the FM jammer can be explained by the fact that for lower J/S, only the first sub-peaks on either side of the carrier frequency are visible, and thus this jammer is classified as an AM jammer. With the current parameters, it is expected that the module can issue a warning before a GNSS user is seriously affected by the presence of interference.

Table 2. Test results (J/S) for the different detection and classification parameters of the DUT. First loss of tracked satellite and loss of PVT are obtained from the reference receiver. The values for which the system first triggers a jamming warning are highlighted. All values are given in dB.

Interference Waveform	**CW**	**Chirp**	**AWGN**	**PRN**	**AM**	**FM**
First loss tracked satellite	−6	3	15	6	15	15
Loss of PVT	21	24	33	27	21	21
Kurtosis ($2.99 < K < 3.01$)	7	6.5	no detection	6.5	8	7.5
PSD (1 dB increase)	**−7**	6	11	6	−1	0
Detection with classification model	**−7**	**−1**	**1.5**	**1.5**	**−4**	**−4**
Correct classification	−6	−0.5	3.5	1.5	−4	11

6. Conclusions

The initial test results are promising, as the system is able to both detect and classify interferences before first loss of a tracked satellite by the reference receiver. It can be concluded that in terms of detection, the classification model proves to be successful as it can notice changes in the signal spectrum in low-power jamming scenarios. The PSD ratio and kurtosis are computationally inexpensive methods that can contribute to the confidence of the interference detection when the jamming power has increased a bit further. Concerning classification, the model seems to be capable of correctly classifying the jammer type before the COTS reference receiver first loses track of a satellite, although it is seen that there is significant difference in performance for different jamming waveforms.

In this paper, the implementation of real-time jamming detection strategies in an operational product are discussed. As stated, these methods will provide the user with knowledge concerning possible jamming attacks, but not with information regarding spoofing. To extend the capabilities of the product, real-time spoofing detection is considered to be implemented. In a spoofing attack, a set of counterfeit GNSS signals is created and transmitted, with the aim to misdirect a receiver into computing a false position and timing solution. Effort is already being put in the development of a spoofing detection functionality: Structural Power Content Analysis (SPCA) can be used on the pre-despreaded signal to find additional PRNs in the signal [10], thereby indicating a spoofing attack. For future development of the GNSS monitoring system, the use of SPCA as an additional detection parameter is investigated.

For the development of the operational device, it is advised to perform additional tests, which should not only account for the different waveforms, but also for variations in waveform characteristics like bandwidth, central frequency and sweeping time. The results of the additional tests can not only verify the robustness of the module against waveform variations but will also allow for fine-tuning of the implemented detection and classification thresholds. Validation should be carried out by exposing the system to real jamming and spoofing scenarios, where more fine-tuning can be performed to rule out, for example, unintentional interference sources, such as multipath.

Author Contributions: Hardware and software design and implementation, J.R.; Test design, A.v.Z and M.S.; Test execution, J.R., A.v.Z. and M.S.; Writing, review and editing, J.R., A.v.Z. and M.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Research data provided in article. For more information, please contact one of the authors.

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

Abbreviations

The following abbreviations are used in this manuscript:

AM	Amplitude Modulation
AWGN	Additive White Gaussian Noise
BPSK	Binary Phase Shift Keying
CNN	Convolutional Neural Network
COTS	Commercial Off-The Shelf
CW	Continuous Wave
DUT	Device Under Test
FM	Frequency Modulation
GNSS	Global Navigation Satellite System

J/S	Jammer-to-Signal Ratio
MDPI	Multidisciplinary Digital Publishing Institute
PRN	Pseudo-Random Noise
PSD	Power Spectral Density
PVT	Position, Velocity and Time
RFI	Radio Frequency Interference
SCW	Swept Continuous Wave
SDR	Software-Defined Radio
SPCA	Structural Power Content Analysis

Appendix A. Simulator Settings and Test Signal Waveform Characteristics

Table A1. Simulator settings used to simulate the GNSS signals.

Setting	Value
Centre frequency	1575.42 MHz
Sample rate	50 Msamples/s
Simulation start time	1 April 2023, 12:00:00 (date, time)
Ionospheric model	Klobuchar
Tropospheric model	Stanag
Signal power GPS L1 C/A	−3.00 dB (with respect to −131.5 dBm at 5° elevation)
Signal power Galileo E1	−2.00 dB (with respect to −131.5 dBm at 5° elevation)
Signal power SBAS L1	0.50 dB (with respect to −131.5 dBm at 5° elevation)
Receiver position	Lat: 52.6757761°, Lon: 5.9247521°, Alt: 2.00 m
Transmitter position	Lat: 52.6803418°, Lon: 5.9119103°, Alt: 2.00 m

Table A2. Characteristics of the waveforms for which the DUT is tested.

Interference Waveform	Central Frequency	Characteristics
CW	1575.00 MHz	
Chirp	1575.42 MHz	Bandwidth: 1 MHz, sweeping time: 100 µs
AWGN	1575.42 MHz	Bandwidth: 2 MHz
PRN	1575.42 MHz	Modulation scheme: Binary Phase Shift Keying (BPSK), code rate: 1.023 MHz, code length: 1 ms
AM	1575.42 MHz	modulation index: 1, modulation frequency: 1 MHz
FM	1575.42 MHz	modulation index: 1, modulation frequency: 1 MHz

References

1. UK Government Office for Science. *Satellite-Derived Time and Position: A Study of Critical Dependencies*; Blackett review; UK Government Office for Science: London, UK, 2018.
2. EGNSS Centre of Excellence. *IKUS-II: Inventarisatie Kwetsbaarheden Uitval Satellietnavigatie*, Ministerie Infrastructuur en Waterstaat; EGNSS Centre of Excellence: Noordwijk, NL, 2022.
3. Morales Ferre, R.; de la Fuente, A.; Lohan, E.S. Jammer classification in GNSS bands via machine learning algorithms. *Sensors* **2019**, *19*, 4841. [CrossRef] [PubMed]
4. Wu, Z.; Zhao, Y.; Yin, Z.; Luo, H. Jamming signals classification using convolutional neural network. In Proceedings of the 2017 IEEE International Symposium on Signal Processing and Information Technology (ISSPIT), Bilbao, Spain, 18–20 December 2017; pp. 062–067.
5. Swinney, C.J.; Woods, J.C. GNSS jamming classification via CNN, transfer learning & the novel concatenation of signal representations. In Proceedings of the 2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), Dublin, Ireland, 14–18 June 2021; pp. 1–9.

6. Tan, M.; Le, Q.V. EfficientNet: Rethinking Model Scaling for Convolutional Neural Networks. In Proceedings of the 36th International Conference on Machine Learning, Long Beach, CA, USA, 9–15 June 2019.
7. Howard, A.G.; Zhu, M.; Chen, B.; Kalenichenko, D.; Wang, W.; Wey, ; T.; Andreetto, M.; Adam, H. MobileNets: Efficient Convolutional Neural Networks for Mobile Vision Applications. *arXiv* **2017**, arXiv:1704.04861v1
8. He, K.; Zhang, X.; Ren, S.; Sun, J. Deep Residual Learning for Image Recognition. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, Las Vegas, NV, USA, 27–30 June 2016; pp. 770–778.
9. Kingma, D.P.; Ba, J. Adam: A Method for Stochastic Optimization. In Proceedings of the 3rd International Conference for Learning Representations, San Diego, CA, USA, 7–9 May 2015.
10. Jafarnia Jahromi, A. GNSS Signal Authenticity Verification in the Presence of Structural Interference. Ph.D. Thesis, University of Calgary, Calgary, AB, USA, 2013.