RF-Based Drone Detection with Deep Neural Network: Review and Case Study

Norah A. Almubairik[1,3] and El-Sayed M. El-Alfy[2,3](✉)

[1] Networks and Communications Department, Imam Abdulrahman Bin Faisal University, Dammam, Saudi Arabia
[2] SDAIA-KFUPM Joint Research Center for Artificial Intelligence, IRC for Intelligent Secure Systems (IRC-ISS), KFUPM, Dhahran, Saudi Arabia
[3] College of Computing and Mathematics, King Fahd University of Petroleum and Minerals (KFUPM), Dhahran, Saudi Arabia
alfy@kfupm.edu.sa

Abstract. Drones have been widely used in many application scenarios, such as logistics and on-demand instant delivery, surveillance, traffic monitoring, firefighting, photography, and recreation. On the other hand, there is a growing level of misemployment and malicious utilization of drones being reported on a local and global scale. Thus, it is essential to employ security measures to reduce these risks. Drone detection is a crucial initial step in several tasks such as identifying, locating, tracking, and intercepting malicious drones. This paper reviews related work for drone detection and classification based on deep neural networks. Moreover, it presents a case study to compare the impact of utilizing magnitude and phase spectra as input to the classifier. The results indicate that prediction performance is better when the magnitude spectrum is used. However, the phase spectrum can be more resilient to errors due to signal attenuation and changes in the surrounding conditions.

Keywords: Border security · Drone detection · Radio-frequency signals · FFT spectrum · Deep learning

1 Introduction

Unmanned Aerial Vehicles (UAV) or pilotless or uncrewed aircraft, commonly known as drones, were once considered a restricted technology that only official authorities, such as the military and government, could use. Currently, UAVs are also being used at a growing scale in commercial and personal services, e.g. to distribute goods and services in different industries. There are various potential use cases for drones, including, but not limited to, logistics, monitoring traffic, monitoring and fertilizing crop fields, building safety inspection, surveillance and border control, photography, and recreational services [12]. Despite the variety of beneficial applications of drones, their misuse threatens national and international security and public safety. There is a growing amount of reported incidents on local and global scales. For instance, Saudi Arabia has cut oil and gas production due to drone attacks on two major oil facilities run by the state-owned

B. Luo et al. (Eds.): ICONIP 2023, CCIS 1969, pp. 16–27, 2024.
https://doi.org/10.1007/978-981-99-8184-7_2

company, Aramco, in 2019 [BBC News[1]]. In the UK, a serious incident occurred in London between the 19th and 21st of December 2018, when Gatwick Airport was forced to shut down due to a drone strike. Around 1000 flights were either diverted or canceled, affecting an estimated number of 140,000 passengers [The telegraph[2]].

Drone detection is crucial for border security and public safety. It is an important step for identifying, locating, tracking, altering, and intercepting unauthorized drones. Different approaches have been proposed for drone detection based on various types of sensors used: (1) Radar-based, (2) Optical or video-based, (3) Radio Frequency (RF) based, and (4) Acoustic-based sensors. Radar-based detection systems have a fast-tracking mechanism and 360-degree coverage; however, they fail to detect small UAV objects [18,19]. In the same manner, video-based detection systems are unable to detect drones in long-range scenarios and foggy conditions [6]. Moreover, acoustic-based techniques are affected by noisy environments and have a short range of detection. Detecting drones using radio frequency, on the other hand, is not affected by the size of the UAV, its distance, foggy conditions, or noisy environments. In addition, it is considered a relatively reliable and low-cost solution. RF fingerprinting techniques depend on the particular characteristics of the radio frequency waveform emitted from the drone and/or its controllers. Experiments have shown that the majority of commercial UAVs have distinct RF signatures as a result of the electronics design, modulation techniques, and body vibration. Consequently, RF fingerprints obtained from the UAV or its remote controller signals can be used to identify and classify UAVs and their activities [8].

Over the past few years, deep learning (DL), a sub-field of machine learning, has gained popularity and has been a driving force behind several recent innovations. In comparison to other paradigms, deep learning techniques are widely recognized as being one of the most efficient and effective end-to-end modeling techniques that embody feature analysis and extraction from raw data, relaxing human experts from the tedious process of feature engineering. Over time, deep learning has been able to solve increasingly complex applications in natural language processing and computer vision with high accuracy [5].

The aim of this paper is to first present a review of work related to deep learning for RF-based drone detection and classification. Additionally, it provides a case study by extending the work done in [2] to compare the performance of a deep neural network model with the magnitude and phase spectra of RF signals. The RF signals are transformed using the Fast Fourier Transform (FFT) then the magnitude and phase spectra are computed and normalized. After that, two sets of experiments are conducted using neural networks of multiple layers, and the results are analyzed using various types of features of segmented signals in order to: (i) detect drone presence, and (ii) detect the drone and recognize its type.

The remainder of this paper is arranged as follows. Section 2 reviews work related to drone detection systems using Radio Frequency and deep learning

[1] https://cutt.ly/0hAlsjZ.

[2] https://cutt.ly/2bxdUaO.

techniques. Section 3 describes a case study including the experimental setup and the methodology followed as well as a description of various conducted experiments and analysis of the results. Finally, Sect. 4 concludes the paper and highlights recommendations some potential issues for future work.

2 Background

A drone is a form of aircraft that does not have a human pilot on board. Its main parts include drone body, remote control device, and energy device. It can be remotely or autonomously controlled. It has become a widely-used technology due to the significant reduction in costs and sizes. It has several potential applications, such as express shipping and package delivery, aerial photography for journalism and film, weather forecasting, crop spraying, entertainment, etc. However, the misuse of drone technology can have major impacts on public safety and national security. They can threaten flight safety, engage in criminal acts, and invade personal privacy as they are supplemented with high-quality cameras [10,17]. This includes, but is not limited to, offensive reconnaissance and monitoring of individuals.

Drones can be classified into the following main categories:

- Fixed-Wing Systems: A term used specifically in the aviation industry to describe aircraft that use fixed rigid wings to produce lift in conjunction with forwarding airspeed. Yaacoub et al. describe fixed-wing systems as follows: “They are based on the Vertical Take-Off and Landing (VTOL) principle” [23]. Traditional airplanes, surface-attached kites, and various kinds of gliders, such as hang gliders or para-gliders, are examples of this type of aircraft [7,21]
- Multi-Rotor Systems: Airplanes that produce lift using rotary wings. A traditional helicopter is a common example of a rotorcraft, which can have one or many rotors. Multiple small rotors, which are required for their stability, are often fitted with drones using rotary systems [7,21]. DJI Phantom and Parrot Bebop are considered commercial multi-rotor drones.
- Hybrid-Wing Drones: These types of drones have been developed with fixed or rotary wings to reach the intended location faster and hover over the air using their rotor wings [23]. They can cover a maximum of 150km in a single plane and are easy to control.
- Ornithopter Drones: This category includes unmanned aircraft that fly by imitating insect or bird wing motions (i.e. flapping their wings). The majority of these ornithopters are scaled in relation to the birds or insects they represent [7,21]. The flapping wing mechanism converts the motor’s rotary motion into the ornithopter’s reciprocating motion, allowing it to provide the necessary lift and thrust to travel steadily [11]. Delfly explorer and the micro-mechanical flying insect are two examples of ornithopter drones.

The existence of various types of drones with a variety of characteristics makes their detection and the design of anti-drone systems a daunting task.

Al-Sa'd et al. [2] developed a drone detection mechanism. They captured a large number of drone's RF signals and created a dataset called DroneRF. Then, the RF signals have been transformed using FFT magnitude for different frequency segments and fed into three separate Deep Neural Networks (DNNs) to detect drones and recognize their types and operational states. The overall accuracy of the designed system decreased when the number of classes was increased. The classification accuracy reached 99.7%, 84.5%, and 46.8% for binary, four-class, and ten-class classification problems, respectively.

Al-Emad and Al-Senaid [1] have also utilized the same dataset DroneRF and proposed a drone detection system using a Convolutional Neural Network (CNN) instead of DNN. The results confirmed that drone detection mode identification using CNN outperformed the drone detection solutions performed using DNN. Similarly, Allahham et al. [4] applied CNN for the DroneRF dataset to develop a drone detection, identification, and classification approach. Their analysis shows that Drone and Background activity spectra are significantly distinguishable. However, the RF spectra of different types of drones as well as different operation modes are either identical or overlapped. For that reason, they channelized the spectrum into multiple channels and considered each one as a separate input into the classifier. The results showed perfect drone detection but the accuracy is reduced to 94.6% and 87.4% for identifying drone types and states, respectively.

Nguyen et al. [15] developed a MATTHAN algorithm that detects drone's body movements, namely body shifting and body vibration. The algorithm analyzes the radio frequencies emitted from the communication between the drone and its remote controller. The algorithm gathers evidence from multiple sources (e.g. moving object detection, body shifting patterns, body vibration). Then, the algorithm combines these sources of evidence to form a binary classifier. The MATTHAN algorithm is evaluated across seven different drones and three different environments. The results showed that the more time the drone stays in the coverage area, the more accurate the results are. Furthermore, the detection accuracy increased when relying on several sources of evidence. In addition, the findings revealed that when the distances between the drone and the anti-drone system increased, the detection percentage decreased. To illustrate, when the drone was 10 m away from the detection system, the accuracy reached 96.5% but when the distance increased, the detection accuracy reduced to 89.4%

Nguyen et al. [14] examined a drone detection system that is developed to autonomously detect and characterize drones via RF signals. They combined two techniques: Passive (i.e. Radio Frequency) and Active (i.e. Radar), to identify the presence of potential invading drones. The proposed system depends mainly on three characteristics: the drone's rotating propellers, the drone's communication, and the drone's body vibration. As for the rotating propellers, the detection system uses a WiFi receiver (e.g. Alfa WiFi Network Adapter) and analyzes the significance of the signal reflected from its propellers. Regarding the drone's communication, it is noticed that the communication link between the wireless mobile devices and their connected access points is reaching 10 times per second whereas drones and their controllers reach 30 cycles per second. This is because of the importance of automatically changing the drone status. The third feature is the drone's body vibration in which the receiver monitors any modifications in the reflected signal intensity generated by the vibration of the drone body. The distance between the drone and the receiver can be measured using either phase variations or Received Signal Strength (RSS).

Xiao and Zhange [22] worked on drone detection and classification based on RF signal buried in ambient noise (e.g., WiFi signal). Their classification technique focused on the RF signature extracted from the down-link communication between the drone and its controller rather than the up-link communication. The RF signature consists of cyclostationarity features (i.e. a signal having statistical characteristics that differ cyclically over time), kurtosis (i.e. monitoring tailedness of a Gaussian scattered signal and the impact of central-limit such as conditions), and spectrum factors. The created RF signature is fed into two machine-learning classifiers: Support Vector Machine (SVM) and K-Nearest Neighbor (KNN). Different Signal-to-Noise Ratios (SNRs) and feature selection methods were considered while testing the drone signals. The testing results showed that the KNN classifier outperformed SVM.

AirID dataset was developed by Mohanti at Genesys Lab at the Northeastern University. It includes raw Interleaved Quadrature (IQ) samples taken from over-the-air transmissions of four USRP B200mini radios, each of which was mounted as a transmitter on a DJI M100 UAV and transmitted with a different IQ imbalance. Every recording in this dataset is made up of two files: a metadata file and a dataset file. The metadata file holds information about the dataset while the dataset file is a binary file containing digital samples. The metadata and data are in compliance with the Signal Metadata Format (SigMF) [13].

DroneRC is another RF-based dataset generated and utilized in some other works for drone detection and classification. For instance, Ezuma et al. [9] utilized the DroneRC dataset to develop a micro-UAV detection and classification system using RF fingerprints of signals emitted from the UAV remote controllers (RCs) and captured through an antenna and a high-frequency oscilloscope. The utilized dataset contained 100 RF signals collected from each of 14 different types of micro-UAV controllers. The duration of each signal was 0.25 ms and was represented by a vector of 5 million samples. The dataset was fed into wavelet analysis to reduce possible bias. Then, several machine learning classifiers have been applied, including SVM, KNN, and neural network (NN). Using KNN classification, all of the micro-UAVs were correctly identified, with an overall precision of 96.3%.

Ozturk et al. [16] used the DroneRC dataset to look at the issue of classifying UAVs based on RF fingerprints at low SNRs. They used CNNs trained on RF time-series images and spectrograms of 15 separate off-the-shelf drone controller RF signals. They reached a classification accuracy ranging from 92% to 100% for an SNR range of -10 dB to 30 dB, which outperformed current methods substantially. Similarly, Ezuma et al. [8] investigated drone detection and classification of UAVs in the presence of Bluetooth and WiFi interference signals. At 25 dB SNR, the KNN classifier achieved a classification accuracy of

98.13%. The efficiency of classification was also studied for a group of 17 UAV controllers at various SNR stages. In [20], the authors focused on drone detection in the presence of interference. They utilized RSS feature-based detectors to detect the presence of a drone signal buried in the RF interference and thermal noise. Using RSS feature requires a high SNR to ensure that the RF signal is insusceptible to interference with other background signals. The findings showed that the detection probability changes in a non-monotonic pattern.

3 Case Study

This study implements a drone detection and classification system for border security intelligence using Radio Frequency Signals and Deep Learning. The aim is to compare the impact of using the magnitude and phase spectrum of the FFT on the performance. This section describes how the research was conducted in details.

3.1 System Overview and Experimental Setup

Figure 1 illustrates the overall drone detection and recognition methodology. The system is composed of five modules: the drone under analysis, drone remote controller, RF sensing module, RF analyzer, and drone detection and classification module. The first three modules were conducted by Al-Sa'd et al. [2,3] and the DroneRF dataset was created. The last two modules are the focus of our research.

Different drones can emit different RF signals, which can then be used by intelligent systems to detect and identify them. During data collection, three types of drones were used, namely, DJI Phantom 3, Parrot Bebop, and Parrot AR Drone. The drone remote controller can also be a cellphone that sends and receives RF commands to and from the drones under investigation in order to change the drone's flight mode. Controlling the drones with a mobile phone necessitates mobile applications customized to each drone, e.g. "FreeFlight Pro," "AR.FreeFlight," and "DJI Go". Other applications can be used as well; however, for this dataset collection, the drone's official application was utilized.

The drone's communications with the flight control module were intercepted by an RF receiver connected to a laptop via a cable, which runs a program that retrieves, processes, and stores the RF data in a database, named "DroneRF". The aim of this module is to capture all unlicensed RF bands used by drones without making any assumptions about their flight mode. The dataset contains recordings of RF activities of the three types of drones (AR, Bepop and Phantom) as well as background signals (no drones). There are four operating modes: on and connected, hovering, flying but no video recording, and flying while recording video. The total number of segments in the dataset is 227 segments distributed as follows: 84 segments for Bepop (4 modes), 81 segments for AR (4 modes), 21 segments for Phantom (one mode) and 41 segments for Background. Each segment duration is 250 ms and captured using two simultaneous receivers with a sampling rate 40M sample/s per channel: one for the lower half

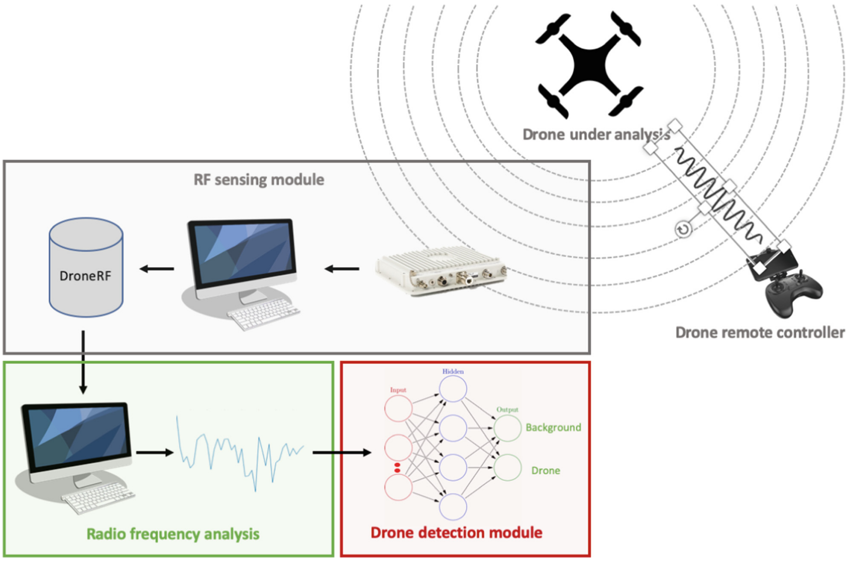


Fig. 1. Illustration of the main modules of the RF-based drone detection and classification system

of the frequency band (10M samples) and the other for the upper half of the frequency band (10M samples). For binary classification, there are two classes: No drone (82 segments) and Drone (372 segments). For 4-class classification, the drone class is divided into three other types: Phantom (42 segments), AR (162 segments), and Bepop (168 segments).

Signal analysis is used to discover hidden information in the recorded RF signals that can be used to improve detection. In this study, we adopted the Fast Fourier transform (FFT) to analyze the frequency-domain spectrum of the recorded RF signals. It is an invertible function, i.e. and an approximate form of the signal can be reconstructed using the inverse FFT (IFFT). FFT provides a fast method for computing the Discrete Fourier Transform (DFT), which is widely used in several other signal-processing applications such as remote sensing, communication, speech, and financial time series. It decomposes a signal into a series of sinusoidal (harmonic) components or vibrations to show how the signal energy is distributed over a particular range of frequencies (signal bandwidth).

Mathematically, a signal uniformly-sampled in time or a sequence of N values $\{x_n \; : x_0, x_1, x_2, \ldots, x_{N-1}\}$ is transformed into another sequence of N complex numbers in frequency domain $\{X_k \; : X_0, X_1, X_2, \ldots, X_{N-1}\}$ as follows:

$$X_k = \frac{1}{N} \sum_{n=0}^{N-1} x_n e^{\frac{-j2\pi kn}{N}} \tag{1}$$

where $j = \sqrt{-1}$. Alternatively, using Euler formula $e^{j\theta} = cos\theta + jsin\theta$, the FFT transform can be rewritten as,

$$X_k = \frac{1}{N} \sum_{n=0}^{N-1} x_n \cdot \left[\cos \frac{2\pi}{N} kn - j \cdot \sin \frac{2\pi}{N} kn \right] \tag{2}$$

FFT of a real-time signal is the sum of complex numbers z; each can be represented by a real part $real(z)$ and an imaginary part $img(z)$ or a magnitude part $|z|$ and a phase part $\angle z$. These quantities are mathematically related as follows:

$$|z| = \sqrt{real(z)^2 + img(z)^2} \tag{3}$$

$$\angle z = \tan^{-1} \frac{img(z)}{real(z)} \tag{4}$$

Figure 2 presents a sample of RF signals (segment #1 of the background and drone activities) as well as their magnitude and phase spectra. The FFT of each observed segment is calculated two times since the DroneRF dataset captures the entire 2.4 GHz bandwidth using two receivers (i.e. the first receiver captures the lower half frequency and the second receiver captures the upper half frequency). After extracting both the magnitude and phase spectra, they are used as the inputs to a deep neural network in three sets of experiments. For comparison purpose, each network is composed of three dense layers with Adam optimizer and ReLU activation for inner layers and sigmoid activation for output layer. The results are reported for stratified 10-fold cross validation, batch size = 10, and number of epochs = 200.

3.2 Results and Discussions

For binary classification experiments, the performance results of three DNN models are presented in the confusion matrices shown in Fig. 3 as well as accuracy, recall, precision, and F1 score. In the first two models, the magnitude spectrum and phase spectrum are used separately as input to the DNN model whereas in the third model, they are combined and used as input. The results show that the magnitude alone has the highest performance.

The binary classification problem is further divided into sub-problems: *Background vs AR*, *Background vs Bebop*, and *Background vs Phantom*. This decomposition may help to understand why the signal phase feature performed lower than the signal magnitude feature. The experimental results also show that the performance is consistent among all drones when the magnitude spectrum feature is utilized alone. On the other hand, when phase feature is considered, the detection system effectively classifies Phantom activities from background activities with an accuracy of 99.34%. The predictive performances for Bebop and AR drones are reduced to 79.94% and 66.12% (approx. to 2 decimal places), respectively.

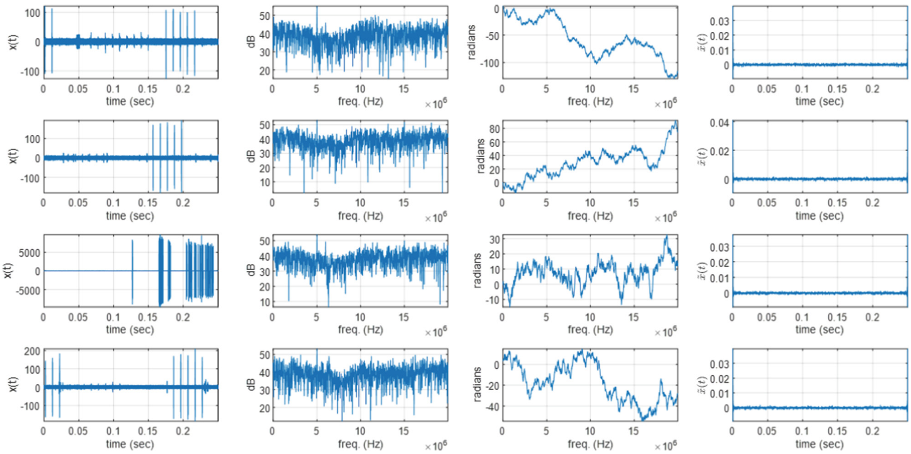
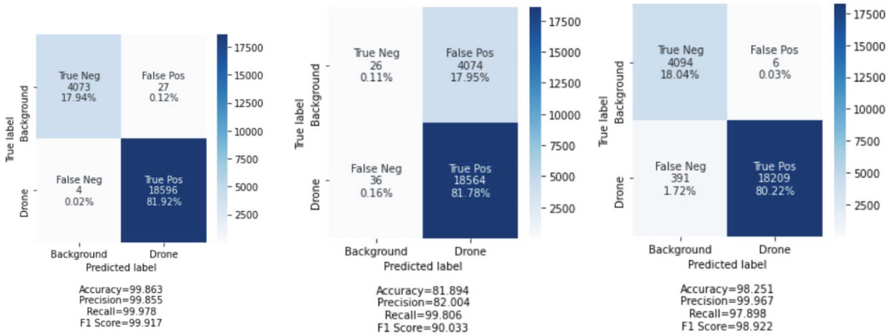


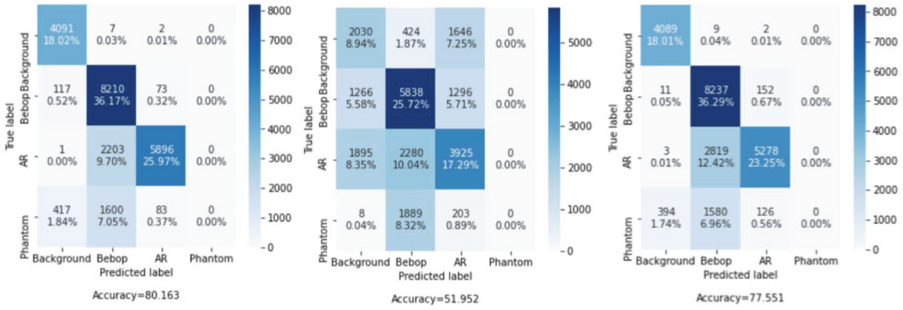
Fig. 2. Sample RF signals (segment#10) and its magnitude and phase spectra (1st and 2nd rows for Background signal low and high band channels, 3rd and 4th rows are for Bepop low and high band channels, 1st column is the time-domain of the original signals, 2nd column is the magnitude spectrum in dB, 3rd column is the unwrapped phase spectrum, 4th column is the reconstructed signal in time-domain from the magnitude only (i.e. zero phase))



(a) Magnitude (b) Phase (c) Magnitude and phase

Fig. 3. Overall performance comparison of binary classification for drone detection (Drone presence vs Background)

The same techniques were also applied to the four-class classification problem and similar results were obtained which confirms that the magnitude spectrum based features is more accurate than the phase spectrum based features, as shown in Fig. 4. As a final conclusion, the magnitude spectrum is sufficient to detect and classify drones. However, the magnitude spectrum is susceptible to noise and other environmental conditions that can degrade the signal quality and hence the models' performance. Yet, more future work is recommended to study the impact of various conditions on the system performance.



(a) Magnitude (b) Phase (c) Magnitude and phase

Fig. 4. Performance evaluation of four-class classification problem (Background - Bebop - AR - Phantom)

4 Conclusion

UAVs are becoming more common, posing a threat to public safety and personal privacy. In order to reduce these threats, it is critical to efficiently identify invading UAVs. In this research, we used FFT to analyze Radio Frequency emitted by civilian drones, implemented Deep Learning-based models for drone detection and classification, compared signal magnitudes and phases of drone and background activities, and evaluated the effectiveness of the detection system using several evaluation metrics. The experimental results show that using the magnitude of the segmented signal has a different predictive performance than using the phase feature. By using the signal phase based features to solve binary classification problems, the classification accuracy is 81.894%, which is about 16% lower than when using the signal magnitude based features. For future research, it is suggested to add new types of drones such as fixed wings and hybrid wings to the dataset. This work can be also extended by investigating phase and magnitude features operation mode classification with deteriorated RF signals.

Acknowledgments. The authors would like to thank King Fahd University of Petroleum and Minerals for providing support during this work. The second author would also like to acknowledge the fellowship support at SDAIA-KFUPM Joint Research Center for Artificial Intelligence under grant no. JRC-AI-RFP-04.

References

1. Al-Emadi, S., Al-Senaid, F.: Drone detection approach based on radio-frequency using convolutional neural network. In: IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT), pp. 29–34 (2020)
2. Al-Sa'd, M.F., Al-Ali, A., Mohamed, A., Khattab, T., Erbad, A.: RF-based drone detection and identification using deep learning approaches: an initiative towards a large open source drone database. Futur. Gener. Comput. Syst. **100**, 86–97 (2019)
3. Allahham, M.S., Al-Sa'd, M.F., Al-Ali, A., Mohamed, A., Khattab, T., Erbad, A.: DroneRF dataset: a dataset of drones for RF-based detection, classification and identification. Data Brief **26**, 104313 (2019)
4. Allahham, M.S., Khattab, T., Mohamed, A.: Deep learning for RF-based drone detection and identification: a multi-channel 1-D convolutional neural networks approach. In: IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT), pp. 112–117 (2020)
5. Bengio, Y., Goodfellow, I., Courville, A.: Deep Learning, vol. 1. MIT Press, Massachusetts (2017)
6. Bisio, I., Garibotto, C., Lavagetto, F., Sciarrone, A., Zappatore, S.: Unauthorized amateur UAV detection based on WiFi statistical fingerprint analysis. IEEE Commun. Mag. **56**(4), 106–111 (2018)
7. Custers, B. (ed.): The Future of Drone Use. ITLS, vol. 27. T.M.C. Asser Press, The Hague (2016). https://doi.org/10.1007/978-94-6265-132-6
8. Ezuma, M., Erden, F., Anjinappa, C.K., Ozdemir, O., Guvenc, I.: Detection and classification of UAVs using RF fingerprints in the presence of Wi-Fi and Bluetooth interference. IEEE Open J. Commun. Soc. **1**, 60–76 (2019)
9. Ezuma, M., Erden, F., Anjinappa, C.K., Ozdemir, O., Guvenc, I.: Micro-UAV detection and classification from RF fingerprints using machine learning techniques. In: IEEE Aerospace Conference, pp. 1–13 (2019)
10. Liu, Z., Li, Z., Liu, B., Fu, X., Raptis, I., Ren, K.: Rise of mini-drones: applications and issues. In: Workshop on Privacy-Aware Mobile Computing, pp. 7–12 (2015)
11. Mahendran, S., Asokan, R., Kumar, A., Ria, V., Jayadeep, S.: Development of the flapping wing for ornithopters: a numerical modelling. Int. J. Ambient Energy **43**(1), 795–802 (2022). https://doi.org/10.1080/01430750.2019.1662841
12. Merkert, R., Bushell, J.: Managing the drone revolution: a systematic literature review into the current use of airborne drones and future strategic directions for their effective control. J. Air Transp. Manag. **89**, 101929 (2020)
13. Mohanti, S., Soltani, N., Sankhe, K., Jaisinghani, D., Di Felice, M., Chowdhury, K.: AirID: injecting a custom RF fingerprint for enhanced UAV identification using deep learning. In: IEEE GLOBECOM 2020-IEEE Global Communications Conference, pp. 370–378 (2020)
14. Nguyen, P., Ravindranatha, M., Nguyen, A., Han, R., Vu, T.: Investigating cost-effective RF-based detection of drones. In: 2nd Workshop on Micro Aerial Vehicle Networks, Systems, and Applications for Civilian Use, pp. 17–22 (2016)
15. Nguyen, P., Truong, H., Ravindranathan, M., Nguyen, A., Han, R., Vu, T.: Matthan: drone presence detection by identifying physical signatures in the drone's RF communication. In: 15th Annual International Conference on Mobile Systems, Applications, and Services, pp. 211–224 (2017)
16. Ozturk, E., Erden, F., Guvenc, I.: RF-based low-SNR classification of UAVs using convolutional neural networks. arXiv preprint arXiv:2009.05519 (2020)

17. Samland, F., Fruth, J., Hildebrandt, M., Hoppe, T., Dittmann, J.: AR.Drone: security threat analysis and exemplary attack to track persons. In: Intelligent Robots and Computer Vision XXIX: Algorithms and Techniques, vol. 8301, p. 83010G. International Society for Optics and Photonics (2012)
18. Schmidt, M.S., Shear, M.D.: A drone, too small for radar to detect, rattles the white house. New York Times **26** (2015)
19. Shi, X., Yang, C., Xie, W., Liang, C., Shi, Z., Chen, J.: Anti-drone system with multiple surveillance technologies: architecture, implementation, and challenges. IEEE Commun. Mag. **56**(4), 68–74 (2018)
20. Sinha, P., Yapici, Y., Güvenç, İ., Turgut, E., Gursoy, M.C.: RSS-based detection of drones in the presence of RF interferers. In: 2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC), pp. 1–6. IEEE (2020)
21. Vergouw, B., Nagel, H., Bondt, G., Custers, B.: Drone technology: types, payloads, applications, frequency spectrum issues and future developments. In: Custers, B. (ed.) The Future of Drone Use. ITLS, vol. 27, pp. 21–45. T.M.C. Asser Press, The Hague (2016). https://doi.org/10.1007/978-94-6265-132-6_2
22. Xiao, Y., Zhang, X.: Micro-UAV detection and identification based on radio frequency signature. In: IEEE 6th International Conference on Systems and Informatics (ICSAI), pp. 1056–1062 (2019)
23. Yaacoub, J.P., Salman, O.: Security analysis of drones systems: attacks, limitations, and recommendations. Internet Things, 100218 (2020)