МИНОБРНАУКИ РОССИИ

Федеральный исследовательский центр «Информатика и управление» РАН
Национальный комитет при президиуме РАН по распознаванию образов и анализу изображений
Институт информационных технологий Национальной академии наук Азербайджана
Институт проблем передачи информации им. А.А. Харкевича РАН
Издательство «Наука и технологии»
Национальный исследовательский Томский государственный университет
Федеральный исследовательский центр «Карельский научный центр РАН»
Федеральное государственное бюджетное образовательное учреждение высшего образования «Юго-Западный государственный университет»

ОПТИКО-ЭЛЕКТРОННЫЕ ПРИБОРЫ И УСТРОЙСТВА В СИСТЕМАХ РАСПОЗНАВАНИЯ ОБРАЗОВ И ОБРАБОТКИ ИЗОБРАЖЕНИЙ

Распознавание – 2021

Сборник материалов XVI Международной научно-технической конференции

14–17 сентября 2021 года

Редакционная коллегия:
С. Г. Емельянов, В. С. Титов (отв. ред.),
Т. А. Ширабакина, Э. И. Ватутин,
В. С. Панищев

Курск 2021

УДК 621.383.68.3: 681.785
ББК В 338.4
О 66

Рецензент
Доктор технических наук, профессор *А. С. Сизов*

О 66 **Оптико-электронные приборы и устройства в системах распознавания образов и обработки изображений. Распознавание – 2021**: сб. материалов XVI Междунар. науч.-техн. конф. / ред. кол.: С. Г. Емельянов, В. С. Титов (отв. ред.) [и др.]; Юго-Зап. гос. ун-т. – Курск, 2021. – 284 с.

ISBN 978-5-7681-1520-3

Сборник содержит материалы XVI Международной научно-технической конференции «Оптико-электронные приборы и устройства в системах распознавания образов и обработки изображений» (Курск, 14–17 сентября 2021 г.), целью которой является ознакомление с имеющимися достижениями по созданию оптико-электронных приборов, систем и внедрение информационных технологий в научные исследования, учебный процесс и промышленность, а также координация по эффективному их применению в системах распознавания образов и обработки изображений.

Сборник предназначен для научных сотрудников, преподавателей, аспирантов и студентов вузов.

Издание осуществлено с авторских оригиналов. Редакция не несет ответственности за ошибки авторов.

Материалы для публикации одобрены программным комитетом Международной научно-технической конференции.

УДК 621.383.68.3: 681.785
ББК В 338.4

ISBN 978-5-7681-1520-3

СОДЕРЖАНИЕ

As can be seen from Table, SimpleNN showed the highest results for the detection of drones. CNN showed low results on all metrics. The algorithm was almost unable to recognize Thunderstorm class samples, and the model's scores on Accuracy, Recall, and F1-score metrics were 0.31, 0.30, and 0.47, respectively.

A visual representation of the results in Table 1 is shown in Figure 3 (first line SimpleNN, second line CNN).

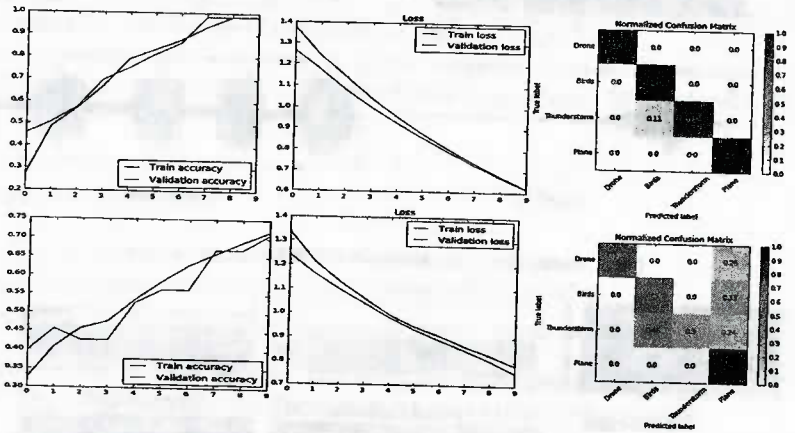


Fig. 3. Visual representation of the experimental results (SimpleNN-first row; CNN-second row)

As can be seen from the confusion matrix in figure 3, the algorithm was able to collect points diagonally across all classes. This algorithm showed an accuracy of 0.89, recognizing 4 points incorrectly from the class Thunderstorms. CNN was able to recognize only samples from the Plane class, and made mistakes in the other 3 classes.

1. Malicious UAVs Detection. URL: https://www.kaggle.com/sonain/malicious-uavs-detection.

UDK 004.056.5

F. J. Abdullayeva[1], O. V. Valikhanli[1]
e-mail:a_farqana@mail.ru, orkhanvalikhanli@gmail.com
[1] *Institute of Information Technology of ANAS, Baku, Azerbaijan*

A METHOD OF DETECTING GPS SPOOFING ATTACKS ON UNMANNED AERIAL VEHICLES

In this paper, the detection method of GPS spoofing attacks on UAV (Unmanned Aerial Vehicles), based on CNN (Convolutional Neural Network) is proposed.

There are several types of attacks against UAVs, including Man-In-The-Middle attack, Denial of Service, Malware Injection and GPS Spoofing. In this work, GPS Spoofing attack is considered. During GPS Spoofing attack against UAVs, attacker transmits counterfeit signals to the GPS receiver on the UAV by using special hardware. Thus, an attacker can hijack UAV or crash it on purpose [1, 2, 3].

The proposed method is based on the analysis of log files. Log files contain information about flight data. By analyzing these data it is possible to predict a GPS spoofing attack. Data contains a total of 88 features, which 37 of them are used in the analysis. The dataset is used in this work is «UAV attack dataset». The method uses CNN as main algorithm. The structure of proposed CNN is shown in figure 1:

```
Model: "sequential"
_________________________________________________________________
Layer (type)                 Output Shape              Param #
=================================================================
conv1d (Conv1D)              (None, 36, 32)            96
_________________________________________________________________
dense (Dense)                (None, 36, 8)             264
_________________________________________________________________
max_pooling1d (MaxPooling1D) (None, 18, 8)             0
_________________________________________________________________
flatten (Flatten)            (None, 144)               0
_________________________________________________________________
dense_1 (Dense)              (None, 2)                 290
=================================================================
```

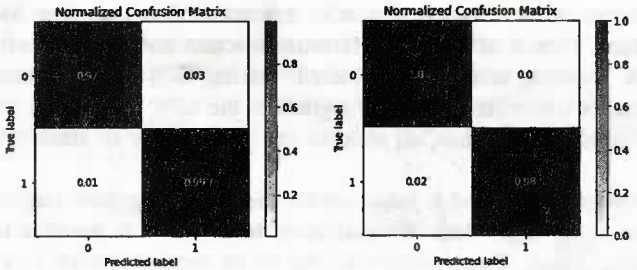
Fig. 1. Structure of proposed CNN model

The detection accuracy, precision, recall and F1-score of the proposed GPS Spoofing detection method for UAVs are shown in Table.

As shown in Table 1, CNN for this particular problem has produced good results. The normalized confusion matrix of GPS Spoofing detection method for UAVs is shown in figure 2.

Accuracy, precision, recall and F1-score of the proposed GPS Spoofing detection method for UAVs

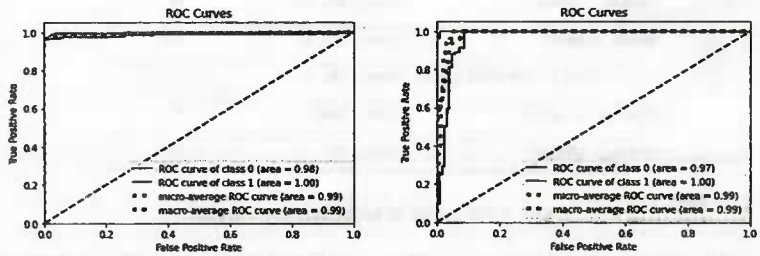
Datasets	Classes	Accuracy	Precision	Recall	F1-score
1	Normal	0.99	0.99	0.97	0.98
	GPS Spoofing		0.97	0.99	0.98
2	Normal	0.99	0.97	1	0.99
	GPS Spoofing		1	0.98	0.99



a) b)

Fig. 2. Normalized confusion matrixes of the CNN model (a) – for dataset 1, b) – for dataset 2)

For performance measurement of the model, ROC curves constructed on the true positive and true negative parameters. Visual representation of ROC curves is shown in figure 3.



a) b)

Fig. 3. ROC curves of CNN model (a) – for dataset 1, b) – for dataset 2)

REFERENCES

1. Mohsen Riahi Manesh, Naima Kaabouch Cyber Attacks on Unmanned Aerial System Networks: Detection, Countermeasure, and Future Research Directions // Computers & Security. 2019. P. 386–401.

2. Borhani-Darian Parisa, Li Haoqing, Wu Peng, Closas Pau Deep Neural Network Approach to Detect GNSS Spoofing Attacks. Proceedings of the 33rd International Technical Meeting of the Satellite Division of The Institute of Navigation. 2020. P. 3241–3252.

3. Psiaki M. L., Humphreys T. E. GNSS Spoofing and Detection // Proceedings of the IEEE. 2016. N 104 (6). P. 1258–1270.