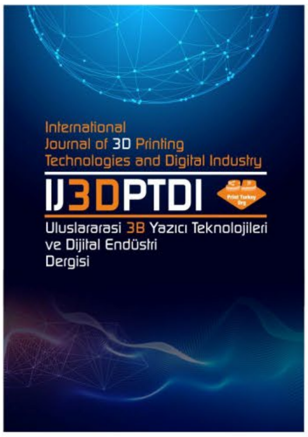

ULUSLARARASI 3B YAZICI TEKNOLOJİLERİ
VE DİJİTAL ENDÜSTRİ DERGİSİ

INTERNATIONAL JOURNAL OF 3D PRINTING TECHNOLOGIES AND DIGITAL INDUSTRY

ISSN:2602-3350 (Online)

URL: https://dergipark.org.tr/ij3dptdi

MALICIOUS UAVs CLASSIFICATION USING VARIOUS CNN ARCHITECTURES FEATURES AND MACHINE LEARNING ALGORITHMS

Yazarlar (Authors): Ahmet Feyzioğlu*, Yavuz Selim Taşpınar

Bu makaleye şu şekilde atıfta bulunabilirsiniz (To cite to this article): *Feyzioğlu A.,Taşpınar Y.S., "Malicious UAVs Classification Using Various CNN Architectures Features and Machine Learning Algorithms" Int. J. of 3D Printing Tech. Dig. Ind., 7(2): 277-285, (2023).*

DOI: 10.46519/ij3dptdi.1268605

Araştırma Makale/ Research Article

Erişim Linki: (To link to this article): https://dergipark.org.tr/en/pub/ij3dptdi/archive

MALICIOUS UAVs CLASSIFICATION USING VARIOUS CNN ARCHITECTURES FEATURES AND MACHINE LEARNING ALGORITHMS

Ahmet Feyzioğlu[a]*, Yavuz Selim Taşpınar[b]

[a]Marmara University, Technology Faculty, Mechanical Engineering Department, TÜRKİYE
[b]Selcuk University, Doganhisar Vocational School, Transport and Traffic Services,TÜRKİYE

* *Corresponding Author: ahmet.feyzioglu@marmara.edu.tr*

(**Received:** 21.03.23; **Revised:** 03.04.23; **Accepted:** 11.04.23)

ABSTRACT

Aircraft are used in many fields such as engineering, logistics, transportation and disaster management. With the development of drones, aerial vehicles have become more widely used for entertainment purposes. However, in addition to its useful applications, its malicious use is also becoming widespread. It has become a necessity to eliminate this problem, especially since it poses a significant danger to other aircraft. In order to identify the aircraft and solve this problem quickly, in this study, five different aircraft were classified based on images. In the study, a five-class dataset containing aeroplane, bird, drone, helicopter and malicious UAV (Unnamed Aerial Vehicle) images was used. Three different CNN (Convolutional Neural Network) models were employed to extract the images of features. Image features extracted with SqueezeNet, VGG16, VGG19 models were classified with Artificial Neural Network (ANN), Support Vector Machine (SVM) and Logistic Regression (LR) machine learning methods. As a result of the experiments, the most accuracyful result, 92%, was obtained from the classification of the features extracted with the SqueezeNet model with ANN. The models proposed in the study will be integrated into various systems and used in the field of aviation to detect malicious UAVs and take necessary precautions.

Keywords: Drone, UAV, Aeroplane, CNN, Machine Learning.

1. INTRODUCTION

Different types of drones are used for many different purposes and have become frequently used in the surveillance, security and defense industries. However, drones can be used for malicious purposes as well as in other areas. Its use is also increasing in order to harm people, nature and other aircraft [1]. For these reasons, a decision should be made about whether drones are detected in advance and whether they are harmful [2]. In order to detect drones, image processing methods [3], sensors [4] and acoustic sounds are used [5]. However, the use of these systems can be quite costly. In addition, its use on another drone may create a disadvantage in terms of weight and cost [6]. Each drone detection method has advantages and disadvantages [7]. Drone detection through images is one of the cheapest and fastest methods [8].

In recent years, drone detection and classification applications have gained more importance with the increasing use of drones. Drone detection can be done with object detection methods [9]. In these studies, there is only one type of class and detection models are trained by tagging the drone object on the images [10]. With the Object recognition methods, it is possible to detect and identify different objects on the same image [11]. In Object classification methods, the images can be classified as a whole and the objects in the image can be classified. In the classification method, there is no need to label the object on the image. For this reason, this method is often preferred in artificial intelligence applications [12].

Mendis et al. They proposed a radar system for unmanned aerial systems using Doppler signatures and spectral correlation functions.

They used deep belief networks to classify the data. With their proposed method, they classified the unmanned aerial vehicles with an accuracy of over 90% [13]. Kim et al. suggested using the Doppler signature as the basis for CNN classification. They achieved a maximum classification accuracy of 100% in the classifications they made with the dataset they used [12]. Rozantsev et al. They propose an approach to classify aircraft that are still moving with a moving camera. They used both image and motion features to solve this challenging problem. They suggested that they achieved higher classification accuracy with spatio-temporal image cubes than with the latest techniques. They created the dataset they used and it is not open to the public [14]. Yoshihashi et al. They made classifications with their proposed recurrent correlational network using datasets containing bird and unmanned aerial vehicle images. In their experiments, they suggested that the method they proposed outperformed other object classification models [15]. On the other hand, Aker et al. They proposed a convolutional neural network based object detection model. They proposed a comprehensive dataset generation algorithm using images removed from the background so that the model can be trained using little data. They obtained high precision and recall values with the model they proposed [9]. According to Saqib et al. They have made drone classification using CNN architectures such as VGG16. In their experimental results, they said that the VGG16 architecture with R-CNN showed higher performance than other architectures [16]. Lee et al. In their studies, they performed drone detection through images. The model they recommend is designed to work on camera drones. They performed drone detection with 89% accuracy using the OpenCV library [17].

When the studies in the literature are examined, different feature extraction CNN models and classification processes with these features are not done in detail. Considering the studies in the literature, the classification of malicious drones was carried out in this study. The processes performed in this study and the contributions of the study are as follows:

• A 5-class image dataset is used to objectively evaluate the classification performance of Malicious drones.
• The dataset contains images of birds, aeroplanes, drones, helicopters and malicious drones.
• Extraction of the features of the images was performed with 3 different CNN models. These models are SqueezeNet, VGG16 and VGG19.
• Three different machine learning models were used to classify the images obtained from CNN models. These models are ANN, SVM and LR.
• With the proposed models, 9 different classification results were obtained.
• Confusion matrix and different performance metrics were utilized to analyze the performance of the models.

The rest of the study is organized as follows: In the 2nd section, general information about the dataset, methods and performance metrics used in the study is given. In the 3rd section, the experimental results are given. In section 4th section, the results and recommendations obtained from the study are given.

2. MATERIAL AND METHODS

In this section, general information about the dataset used, CNN models used for feature extraction, machine learning models, confusion matrix and performance metrics are given. The flow chart showing the planning of the study is shown in Figure 1.

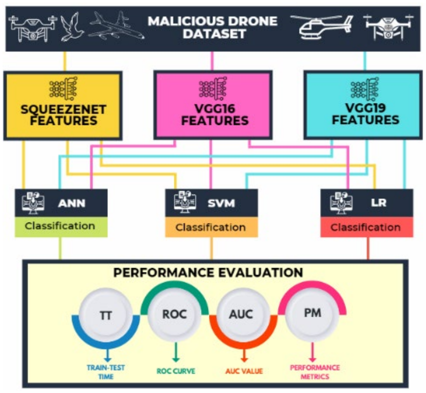

Figure 1. Flow chart of the study.

2.1. Malicious Drone Dataset

In the dataset used in the study, there are a total of 776 images in 5 classes. Includes footage of Malicious UAVs, drones, helicopers, aeroplanes and birds. The dataset was obtained from kaggle.com [18]. Each image contains a single object according to its class. This makes the dataset usable in classification problems. The sample images of the dataset and the number of data by classes are shown in Figure 2.

Figure 2. Malicious drone dataset example images for all class.

2.2. Convolutional Neural Networks (CNN)

CNN can offer an end-to-end solution with many layers of computation. It is a structure that includes convolution, pooling, activation and fully connected layers. Thanks to the convolution layers, feature maps of the images are obtained [19]. Parameter redundancy is eliminated by reducing the size of feature maps with pooling layers. With the activation layers, the data is drawn to the specified intervals. In the fully connected layer, the classification of the obtained feature maps is carried out [20]. A kind of artificial neural network, this layer. Images can be given to CNN models in raw form. In this way, there is no need for an extra feature extraction process [21]. CNN models were used for feature extraction from images in this study. Image properties can be retrieved just before the fully connected layer, which is the last layer in CNN models. Imported features can be classified by different machine learning models. Brief descriptions of the CNN architectures used in the study are given.

SqueezeNet: Iandola et al. Despite its small size, this architecture can achieve high classification accuracy. Model depth is 18. It contains 1.24M parameters in total. The size of the pre-trained SqueezeNet model is 5.2MB. Model size and number of parameters is the biggest advantage of this model [22-23].

VGG16: Developed by Simonyan and Zisserman, this model has a depth of 16. It contains 138M parameters in total. The size of the pre-trained VGG16 model is 515MB [24].

VGG19: As a difference from the VGG16 architecture, a 19-layer architecture was obtained by adding 3 more layers. The depth of this model is 19. The size of the pre-trained VGG19 model is 535MB. It contains 144M parameters in total [25].

The feature extraction capabilities of the three CNN models used in the study were utilized. The SqueezeNet model extracts 1000 features from each image [26]. The VGG16 and VGG19 models extract 4096 features from each image. Obtained images are given as input to machine learning models.

2.3. Machine Learning Methods

Machine learning algorithms are structures that can make predictions by learning patterns through training data. Labeled data given as input to supervised machine learning algorithms can be learned by the algorithm and can predict new data. More accurate and faster results can be obtained by selecting machine learning algorithms according to the problem to be solved. Supervised machine learning algorithms do not have features such as extracting features from images. For this reason, it is necessary to extract the features of the images beforehand and give them as input to these algorithms. The number of input parameters of machine learning algorithms is equal to the number of features obtained from images. The number of outputs is equal to the number of classes in the dataset. The explanations of the machine learning algorithms used in the study are as follows:

ANN: a type of machine learning that mimics biological neurons. It works similarly to the human brain to solve problems. Classification processes are performed by establishing a connection between inputs and outputs in artificial neural networks. It contains 3 layers to perform these operations. These layers are the input layer, hidden layer and output layer. Each layer contains neurons. The connections between neurons in the input, hidden and output layers are called weights and learning is carried out through these weights. It is often preferred because of its computation time and high accuracy advantages. It is a non-linear type of machine learning [27].

SVM: SVM, which is a supervised learning algorithm, includes statistical learning operations. SVM has high generalization ability compared to other machine learning methods. Nonlinear learning is a type of machine learning. It performs the classification process by specifying a plane. It is also used in the classification of multi-class datasets. For these purposes, classification processes are carried out by determining more than one hyperplane [28].

LR: It is a machine learning method often used in classification problems. In this method, it is realized by establishing a connection between output variables (dependent variable) and input values (independent variable). It is a statistical machine learning method. This method is preferred because of its speed and high accuracy advantages [20]. The hyperparameters of the machine learning algorithms used in the study are given in Table 1.

Table 1. Training parameters of machine learning methods.

ANN	SVM	LR
Hidden layer neurons: 100 Activation: ReLu Solver: Adam Regularization: 0.0001 Iteration: 200	Kernel: RBF Numerical tolerance: 0.001 Iteration: 100	Regularization type: Ridge (L2) Strength C = 1

2.4. Confusion Matrix and Performance Metrics

Confusion matrix is a table created for performance evaluation of a classification model. The columns of the matrix show the predicted value, while the rows show the actual values. True Positive (TP), True Negative (TN), False Positive (FP) and False Negative (FN) values are found on the matrix. These values are determined according to the results of the classification model. Confusion matrices with two or more classes can be used [29-33]. A two-class confusion matrix and a five-class confusion matrix used in the study are shown in Figure 3.

		Predicted Class	
		Positive	Negative
Actual Class	Positive	TP	FN
	Negative	FP	TN

(a)

		Predicted Class				
		C1	C2	C3	C4	C5
Actual Class	C1	TN	FP	TN	TN	TN
	C2	FN	TP	...	...	FN
	C3	TN	...	TN	TN	TN
	C4	TN	...	TN	TN	TN
	C5	TN	FP	TN	TN	TN

(b)

Figure 3. (a) Two class confusion matrix (b) Five class confusion matrix.

Performance metrics of models can be calculated using confusion matrix data. The formulas of the performance metrics used to evaluate the performance of the models in this study are shown in Table 2.

Table 2. Performance metrics formulas.

Metrics	Equation
Accuracy (ACC)	$\frac{TP + TN}{TP + TN + FP + FN} x100$
Precision (PSC)	$\frac{TP}{TP + FP}$
Recall (RCL)	$\frac{TP}{TP + FN}$
F-1 Score (FSC)	$2x\frac{Precision\ x\ Recall}{Precision + Recall}$

3. EXPERIMENTAL RESULTS

In this section, the classification operations made using Malicious Drone Dataset data are included. SqueezeNet, VGG16 and VGG19 models were used to extract the features of the images in the dataset. The parameters used in the models are as follows: Validation Frequency

5, Max Epochs 8, Mini Batch Size 11, Initial Learn Rate 0.0001, Solver sgdm, L2 Regularization 0.0001, Execution Environment GPU. Obtained features are given as input to ANN, SVM and LR machine learning models. As a result of the trainings and tests conducted, confusion matrices and performance metrics were obtained for each model. Performance evaluations of the models were made according to the metrics obtained. The computer used in the study has Intel® Core i7™ 12700K 3.61 GHz, NVIDIA GeForce RTX 3080Ti, and 64GB RAM. The cross validation method was used for training and testing the models. In the cross validation method, the dataset is divided into 10 parts and each part is used as test data. The performance metrics of the classification models are obtained by taking the average of the obtained 10 classification results. As a result of using three feature extraction and three machine learning methods, 9 different classification models were obtained. Obtained results are given under headings.

3.1. SqueezeNet Features Classification Results

With the SqueezeNet CNN model, 1000 features were obtained for each image. Obtained features are given as input to ANN, SVM and LR machine learning models. Confusion matrices obtained as a result of training and testing of these models are shown in Figure 4.

The performance metrics of the classification models were created utilizing the information from the confusion matrix shown in Figure 4. The performance metrics of the 1000 feature classifications obtained from the SqueezeNet model are shown in Table 3.

In Table 3, the model with the highest accuracy in the classifications made with SqueezeNet features is the ANN model with 92%. The lowest classification accuracy belongs to the SVM model. When other performance metrics are examined, the accuracy metric in these metrics shows a similar order.

Predicted

Actual	Aeroplane	Bird	Drone	Helicopter	Malicious UAV	Σ
Aeroplane	94	1	1	1	8	105
Bird	2	100	0	0	3	105
Drone	3	2	182	2	11	200
Helicopter	4	0	2	157	4	167
Malicious UAV	6	3	7	2	181	199
Σ	109	106	192	162	207	776

(a)

Predicted

Actual	Aeroplane	Bird	Drone	Helicopter	Malicious UAV	Σ
Aeroplane	82	2	2	1	18	105
Bird	2	92	3	0	8	105
Drone	1	2	184	1	12	200
Helicopter	3	0	1	156	7	167
Malicious UAV	2	2	9	0	186	199
Σ	90	98	199	158	231	776

(b)

Predicted

Actual	Aeroplane	Bird	Drone	Helicopter	Malicious UAV	Σ
Aeroplane	90	1	1	3	10	105
Bird	2	101	0	0	2	105
Drone	4	1	180	4	11	200
Helicopter	2	0	3	158	4	167
Malicious UAV	7	2	12	2	176	199
Σ	105	105	196	167	203	776

(c)

Figure 4. Confusion matrix of (a) ANN, (b) SVM and (c) LR models with SqueezeNet features.

Table 3. Performance metrics of ANN, SVM and LR models with SqueezeNet features.

	ACC	FSC	PSC	RCL	AUC
ANN	92.0%	0.92	0.921	0.920	0.990
SVM	90.2%	0.903	0.908	0.902	0.987
LR	90.9%	0.909	0.909	0.909	0.989

3.2. VGG16 Features Classification Results

4096 features were obtained for each image from the VGG16 model. Obtained features are given as input to ANN, SVM and LR classification models. Confusion matrices obtained as a result of trainings and tests are shown in Figure 5.

The performance metrics of models were calculated using the data of the confusion matrices in Figure 5. These metrics are shown in Table 4.

Predicted

Actual	Aeroplane	Bird	Drone	Helicopter	Malicious UAV	∑
Aeroplane	86	3	0	2	14	105
Bird	2	96	2	0	5	105
Drone	2	3	177	2	16	200
Helicopter	3	1	8	152	3	167
Malicious UAV	10	4	9	4	172	199
∑	103	107	196	160	210	776

(a)

Predicted

Actual	Aeroplane	Bird	Drone	Helicopter	Malicious UAV	∑
Aeroplane	76	0	5	4	20	105
Bird	1	86	8	1	9	105
Drone	2	3	178	2	15	200
Helicopter	4	0	11	146	6	167
Malicious UAV	9	1	18	3	168	199
∑	92	90	220	156	218	776

(b)

Predicted

Actual	Aeroplane	Bird	Drone	Helicopter	Malicious UAV	∑
Aeroplane	90	1	0	1	13	105
Bird	1	92	4	1	7	105
Drone	3	4	178	3	12	200
Helicopter	4	0	5	155	3	167
Malicious UAV	9	1	10	5	174	199
∑	107	98	197	165	209	776

(c)

Figure 5. Confusion matrix of ANN, SVM and LR models with VGG16 features.

Table 4. Performance metrics of ANN, SVM and LR models with VGG16 features.

	ACC	FSC	PSC	RCL	AUC
ANN	88	0.881	0.882	0.88	0.977
SVM	84.3	0.843	0.849	0.843	0.974
LR	88.8	0.888	0.889	0.888	0.981

In Table 4, the model with the highest classification accuracy is the LR model. The classification model with the lowest accuracy is the SVM model. A parallel ranking to the ACC metric was observed in other performance metrics as well.

3.3. VGG19 Features Classification Results

4096 features were obtained for each image from the VGG19 model. These features are given as an introduction to the ANN, SVM, and LR models. Confusion matrices obtained as a result of the train and test operations are shown in Figure 6.

The performance metrics of the models were calculated using the data of the confusion matrices in Figure 6. The performance metrics of each classification model are shown in Table 5.

Predicted

Actual	Aeroplane	Bird	Drone	Helicopter	Malicious UAV	∑
Aeroplane	87	2	0	4	12	105
Bird	4	95	2	0	4	105
Drone	1	10	172	2	15	200
Helicopter	3	1	5	155	3	167
Malicious UAV	14	4	13	1	167	199
∑	109	112	192	162	201	776

(a)

Predicted

Actual	Aeroplane	Bird	Drone	Helicopter	Malicious UAV	∑
Aeroplane	68	2	8	4	23	105
Bird	3	79	14	1	8	105
Drone	1	2	177	2	18	200
Helicopter	4	1	10	144	8	167
Malicious UAV	7	2	19	0	171	199
∑	83	86	228	151	228	776

(b)

Predicted

Actual	Aeroplane	Bird	Drone	Helicopter	Malicious UAV	∑
Aeroplane	88	0	3	3	11	105
Bird	3	92	2	2	6	105
Drone	1	5	171	5	18	200
Helicopter	3	1	4	156	3	167
Malicious UAV	13	0	11	3	172	199
∑	108	98	191	169	210	776

(c)

Figure 6. Confusion matrix of ANN, SVM and LR models with VGG19 features.

Table 5. Performance metrics of ANN, SVM and LR models with VGG19 features.

	ACC	FSC	PSC	RCL	AUC
ANN	87.1	0.872	0.873	0.871	0.977
SVM	82.3	0.823	0.833	0.823	0.974
LR	87.5	0.875	0.877	0.875	0.981

In Table 5, the model with the highest classification accuracy is the LR model. The SVM model has the least classification accuracy of all the models.

3.4. Comparison of All Classification Results

The features obtained from SqueezeNet, VGG16 and VGG19 models were classified with ANN, SVM and LR models and performance metrics were calculated. Classification accuracyes of classification models according to all feature extraction models are given in Table 6. Comparison graph of classification achievements is shown in Figure 7.

Table 6. Comparison of classification accuracy for all models.

	ANN	SVM	LR
SqueezeNet	92	90.2	90.9
VGG16	88	84.3	88.8
VGG19	87.1	82.3	87.7

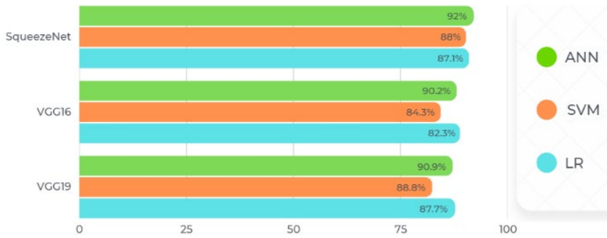

Figure 7. Classification accuracy graph.

According to Table 6 and Figure 7, the highest classification accuracy was obtained from classification of SqueezeNet features with ANN. The lowest classification accuracy was obtained from the classification of VGG19 features with SVM. The train and test times of the classification models according to all feature extraction models are given in Table 7.

Table 7. Comparison of train-test time of all models (second).

	ANN		SVM		LR	
	Train	**Test**	**Train**	**Test**	**Train**	**Test**
SqueezeNet	16.01	1.83	26.95	2.74	27.12	0.93
VGG16	102.2	25.8	159.5	29.7	99.99	4.24
VGG19	61.5	7.76	121.3	11.4	131.8	4.23

According to Table 7, the lowest train time was obtained as a result of training with SVM using SquzeeNet features. The lowest test time was obtained as a result of the test with LR using the SqueezeNet model features. The highest train time was obtained as a result of training with SVM using VGG16 features. The highest test time was obtained from the same model. Figure 8 displays the ROC curves that were produced as a consequence of the models' classification. According to Figure 8, ANN showed the highest accuracy in classifications made with SqueezeNet features. LR showed the highest accuracy in classifications made with VGG16 and VGG19 features.

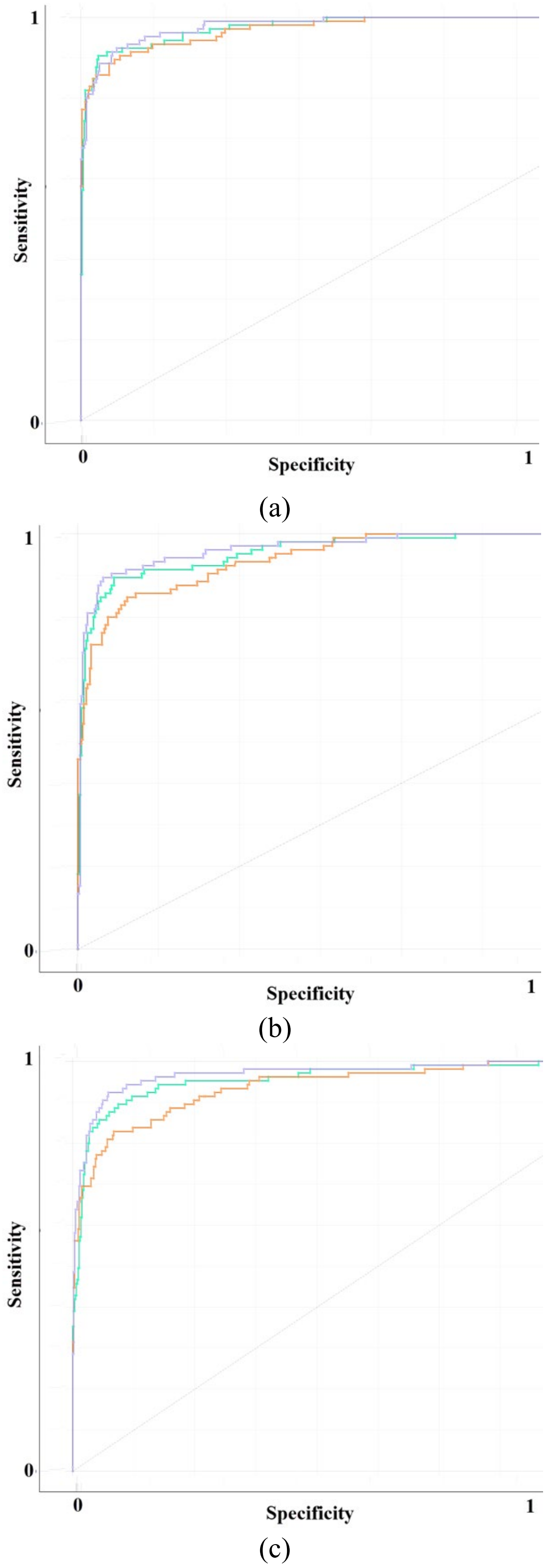

Figure 8. ROC curves of all classification models for (a) SqueezeNet features, (b) VGG16 features, (c) VGG19 features (Purple: ANN, Green: LR, Orange: SVM)

4. CONCLUSIONS

Malicious drone detection is extremely important for security. Since drones are very fast and maneuverable vehicles, they must be detected quickly and necessary precautions must be taken. Based on these problems, in this study, classification experiments of malicious drones were carried out using a dataset containing images in five different classes. SqueezeNet, VGG16, VGG19 models were used to extract the image features. Obtained features were classified by ANN, SVM and LR. As a result of the experiments, the highest classification accuracy of 92% was obtained as a result of the classification of the features obtained from the SqueezeNet model with ANN. The lowest classification accuracy The lowest classification accuracy of 82.3% was attained when the VGG19 features were classified using SVM. As a result of the experiments, it has been determined that malicious drones will be classified quickly and with high accuracy with CNN feature extraction models and machine learning models. Malicious drone detection with image processing is a low-cost method. Therefore, it can be easily integrated into defense systems. Higher classification accuracyes can be achieved with different CNN models and different machine learning methods. More comprehensive and accurate classifications can be made by increasing the number of data and classes in the dataset.

REFERENCES

1. Shi, X., C. Yang, W. Xie, C. Liang, Z. Shi, and J. Chen, “Anti-drone system with multiple surveillance technologies: Architecture, implementation, and challenges”, IEEE Communications Magazine, Vol 56, Issue 4, Pages 68-74, 2018.

2. Solodov, A., A. Williams, S. Al Hanaei, and B. Goddard, “Analyzing the threat of unmanned aerial vehicles (UAV) to nuclear facilities”, Security Journal, Vol. 31, Issue 1, Pages 305-324, 2018.

3. Ye, D.H., J. Li, Q. Chen, J. Wachs, and C. Bouman, “Deep learning for moving object detection and tracking from a single camera in unmanned aerial vehicles (UAVs)”, Electronic Imaging, Vol. 2018, Issue 10, Pages 466-1-466-6, 2018.

4. Basak, S., S. Rajendran, S. Pollin, and B. Scheers, “Combined RF-based drone detection and classification”, IEEE Transactions on Cognitive Communications and Networking, Vol. 8, Issue 1, Pages 111-120, 2021.

5. Mezei, J., V. Fiaska, and A. Molnár, “Drone sound detection”, in 2015 16th IEEE International Symposium on Computational Intelligence and Informatics (CINTI), IEEE, 2015.

6. Drozdowicz, J., M. Wielgo, P. Samczynski, K. Kulpa, J. Krzonkalla, M. Mordzonek, M. Bryl, and Z. Jakielaszek, “35 GHz FMCW drone detection system”, in 2016 17th International Radar Symposium (IRS), IEEE, 2016.

7. Taha, B. and A. Shoufan, “Machine learning-based drone detection and classification: State-of-the-art in research”, IEEE access, Pages 138669-138682, 2019.

8. Lee, D.-H., “CNN-based single object detection and tracking in videos and its application to drone detection”, Multimedia Tools and Applications, Vol. 80, Issue 26, Pages 34237-34248, 2021.

9. Aker, C. and S. Kalkan, “Using deep networks for drone detection”, in 2017 14th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS), IEEE, 2017.

10. Singha, S. and B. Aydin, “Automated Drone Detection Using YOLOv4”, Drones, Vol. 5, Issue 3, Pages 95, 2021.

11. Jia, X., Y. Cao, D. O’Connor, J. Zhu, D.C. Tsang, B. Zou, and D. Hou, “Mapping soil pollution by using drone image recognition and machine learning at an arsenic-contaminated agricultural field”, Environmental Pollution, Issue 270, Pages 116281, 2021.

12. Kim, B.K., H.-S. Kang, and S.-O. Park, “Drone classification using convolutional neural networks with merged Doppler images”, IEEE Geoscience and Remote Sensing Letters, Vol. 14, Issue 1, Pages 38-42, 2016.

13. Mendis, G.J., T. Randeny, J. Wei, and A. Madanayake, “Deep learning based doppler radar for micro UAS detection and classification”, in MILCOM 2016-2016 IEEE Military Communications Conference, IEEE, 2016.

14. Rozantsev, A., V. Lepetit, and P. Fua, “Detecting flying objects using a single moving camera”, IEEE transactions on pattern analysis and machine intelligence, Vol. 39, Issue 5, Pages 879-892 , 2016.

15. Yoshihashi, R., T.T. Trinh, R. Kawakami, S. You, M. Iida, and T. Naemura, “Differentiating objects by motion: Joint detection and tracking of

small flying objects", arXiv preprint arXiv:1709.04666, 2017.

16. Saqib, M., S.D. Khan, N. Sharma, and M. Blumenstein, "A study on detecting drones using deep convolutional neural networks", in 2017 14th IEEE international conference on advanced video and signal based surveillance (AVSS), IEEE, 2017

17. Lee, D., W.G. La, and H. Kim, "Drone detection and identification system using artificial intelligence", in 2018 International Conference on Information and Communication Technology Convergence (ICTC), IEEE, 2018.

18. "Malicious Drone Dataset", https://www.kaggle.com/datasets/sonainjamil/malicious-drones, October 20, 2022

19. Taspinar, Y.S., M. Dogan, I. Cinar, R. Kursun, I.A. Ozkan, and M. Koklu, "Computer vision classification of dry beans (Phaseolus vulgaris L.) based on deep transfer learning techniques", European Food Research and Technology, Vol. 248, Issue 11, Pages 2707-2725, 2022.

20. Taspinar, Y.S. and M. Selek, "Object recognition with hybrid deep learning methods and testing on embedded systems", International Journal of Intelligent Systems and Applications in Engineering, Vol. 8, Issue 2, Pages 71-77, 2020.

21. Unal, Y., Y.S. Taspinar, I. Cinar, R. Kursun, and M. Koklu, "Application of Pre-Trained Deep Convolutional Neural Networks for Coffee Beans Species Detection", Food Analytical Methods, 2022.

22. Kursun, R., I. Cinar, Y.S. Taspinar, and M. Koklu, "Flower Recognition System with Optimized Features for Deep Features", in 2022 11th Mediterranean Conference on Embedded Computing (MECO). 2022.

23. Iandola, F.N., S. Han, M.W. Moskewicz, K. Ashraf, W.J. Dally, and K. Keutzer, "SqueezeNet: AlexNet-level accuracy with 50x fewer parameters and<0.5 MB model size", arXiv preprint arXiv:1602.07360, 2016.

24. Simonyan, K. and A. Zisserman, "Very deep convolutional networks for large-scale image recognition", arXiv preprint arXiv:1409.1556, 2014.

25. Singh, D., Y.S. Taspinar, R. Kursun, I. Cinar, M. Koklu, I.A. Ozkan, and H.-N. Lee, "Classification and Analysis of Pistachio Species with Pre-Trained Deep Learning Models", Electronics, Vol. 11, Issue 7, Pages 981, 2022.

26. Kishore, B., A. Yasar, Y.S. Taspinar, R. Kursun, I. Cinar, V.G. Shankar, M. Koklu, and I. Ofori, "Computer-Aided Multiclass Classification of Corn from Corn Images Integrating Deep Feature Extraction, Computational Intelligence and Neuroscience", Vol. 2022, Pages 2062944, 2022.

27. Koklu, M., R. Kursun, Y.S. Taspinar, and I. Cinar, "Classification of date fruits into genetic varieties using image analysis", Mathematical Problems in Engineering, 2021.

28. Yilmaz, A.B., Y.S. Taspinar, and M. Koklu, "Classification of Malicious Android Applications Using Naive Bayes and Support Vector Machine Algorithms", International Journal of Intelligent Systems and Applications in Engineering, Vol. 10, Issue 2, Pages 269-274, 2022.

29. Koklu, M., I. Cinar, and Y.S. Taspinar, "Classification of rice varieties with deep learning methods", Computers and electronics in agriculture, Vol. 187, Pages 106285, 2021.

30. Ersöz, T. And F. Ersöz, "Data Mining And Machine Learning Approaches In Data Science: Predictive Modeling Of Traffic Accident Causes", International Journal of 3D Printing Technologies and Digital Industry, Vol. 6, Issue 3, Pages 530-539.

31. Çinarer, G., K. Kiliç, And T. Parlar, "A Deep Transfer Learning Framework For The Staging Of Diabetic Retinopathy", Journal of Scientific Reports-A, Issue 051, Pages 106-119.

32. Koklu, M. and Y.S. Taspinar, "Determining the extinguishing status of fuel flames with sound wave by machine learning methods", İEEE Access, Issue 9, Pages 86207-86216, 2021.

33. Taspinar, Y. S., Cinar, I., & Koklu, M., "Prediction of computer type using benchmark scores of hardware units", Selcuk University Journal of Engineering Sciences, Vol. 20, Issue 1, Pages 11-17.