Improving Robustness and Defense with Signal Augmentation for Modulation Identification

Chuanjin Zou, Chenqiu Yu*, Jibin Guo, Ronghai Guo, Junzhong Pang, Weijun Zeng

1Departments of Communication engineering, Army Engineering University of PLA, Nanjing 210000, China
2Military Representative Office of the Army in Nanchang, Nanchang 330000, China
Email: zcj740141613@163.com

Abstract: Based on the Convolutional Neural Network, we consider finding an automatic recognition method of signal modulation. Electronic warfare (EW) is one of the most important forms of war, and the outcome of the war depends largely on it. Fast, accurate, secure and continuous communication is increasingly important, and the identification of signal modulation is one of the key links to ensure communication. The traditional recognition method is artificial recognition, which is inefficient and error-prone. In this paper, aiming at several common modulation signals, the automatic recognition system of modulation signals based on Convolutional Neural Network is designed by analyzing mathematical models and important parameters, then upgrade and improve the feasibility and effectiveness of the project.

1. Introduction

1.1. Research Significance and Research Status
As the number of radio application services increases, so does the demand for spectrum to find the signal[1]. However, the traditional modulation recognition method relies on the experience of professionals. It is not only slow to identify the signal, but also wastes manpower and resources. In addition, when the SNR is relatively low or the channel is not ideal, the signal features are often not easy to extract, and multiple features need to be integrated. The traditional recognition algorithm is often complex and has a poor real-time performance. Compared with artificial recognition, automatic recognition has a great advantage, which can overcome the situation of low recognition rate and artificial error, and greatly improve the efficiency of modulation type recognition, so as to liberate manpower. Automatic modulation classification was used in the military to identify signals of the enemy in warfare[2]. Efficient electronic countermeasures also require automatic modulation classification[3]. However, automatic recognition also has its own defects. In today's increasingly complex electromagnetic environment, noise interference leads to the reduction of SNR and decreases modulation recognition accuracy. Therefore, it is urgent to study a new modulation signal recognition system to improve the real time and accuracy of signal modulation type recognition.

In recent years, Deep Learning has played an important role in the research of video, speech and image processing[4]. In Deep Learning, Convolutional Neural Network is a typical model, because of its simple structure and mature theory, it is used in image recognition and other fields widely[5].
1.2. Main Work of the Paper
This paper realizes modulation signal recognition based on CNN. Eight modulation types: BPSK, QPSK, 8-PSK, GFSK, CPFSK, 4-PAM, 16-QAM and 64-QAM are contained in the data set. For these data set, we designed a Convolutional Neural Network for training and recognition. In addition, we accomplished the following 3 tasks:

(1) On the basis of the constructed neural network, the training set was modified, random noise was added, and the robustness of the training results was improved by adding the background fitting the actual complex electromagnetic environment.

(2) To improve the success of training results, the random data feeding method was improved into the specified data feeding method.

(3) The classifier is used in the military background, assuming that the enemy has a similar classifier, the method to decrease the probability of the enemy decoding our signal is studied by modifying the test set.

2. Related Theories and Techniques

2.1. Modulation Automatic Classification System
Feature extraction and classification algorithm make up the modulation automatic classification system. The former extracts feature from the receiving signal, while the latter preprocesses each received signal, and outputs the modulation of the signal with the features formed in the previous stage as input. As shown in FIG 1:

![Modulation automatic classification system](image)

FIG 1. Modulation automatic classification system [6].

2.2. Convolutional Neural Network
Convolutional Neural Network is a kind of Deep Neural Network with a convolutional structure. The characteristics of convolutional structure are reducing the amount of memory occupied and the number of parameters. Weight sharing, pooling and other operations can alleviate the problem of overfitting.

The hierarchical structure of Convolutional Neural Network mainly includes input layer, convolution computation layer, activation function, pooling layer and full connection layer. The flow chart of the Convolutional Neural Network model is shown in FIG 2. The Convolutional Neural Network learns from the training data, optimizes the performance of the classifier, and thus predicts the output results for the input.

The Convolutional Neural Network is characterized by simplified network structure, strong adaptability and high efficiency in processing high-dimensional data. In addition, the Convolutional Neural Network has strong operability because it omits the feature extraction steps.
2.3. The Data Set

The data set used in this paper is radio machine learning (RML) data set[8]. The RML data set contains 11 modulation classes, which has 8 digital modulation classes and 3 analog modulation classes, with SNR values ranging from -20db to 18dB and step sizes is 2.

Since this paper only involves digital modulation scheme, the analog modulation part will be deleted. The final data set consists of 8 digital modulation classes, with SNR values ranging from -20db to 18dB. The data set are in the form of a Python dictionary. After selecting only the numeric modulation type, we get 160 (modulation, SNR) pairs, each of which is assigned an array (1000,2,128), which means that there are 1,000 samples in each dictionary key, and each sample is an array (2,128). In total, there are 160,000 samples. Therefore, the given data set is an array (160000,2,128). The Convolutional Neural Network is trained on the original time series data rather than on the characteristics of the design. From each pair of samples (modulation, SNR), half of the samples were randomly selected to be included in the training set and the other half was left as the test set, so that the Convolutional Neural Network could be trained on 80,000 samples and tested on 80,000 samples. The first step is to standardize the data so that all the features are in the same range. Each sample is a (2,128) array. Therefore, the input is treated as an image with a height of 2 and a width of 128.

3. Data Feeding Method

The original neural network batch_size is constant 1024. Random function is used to randomly select 1024 groups of training data from the data set and feed them into the network for training. In this way, the feeding data can be guaranteed to cover range of 20 db and 8 modulation methods, which will make the feeding training data more random. Then, this data feeding method is improved: dividing the training set and defining parameter named x. Parameter x is used as the limit, the training set with an SNR greater than x db is divided into the part with a higher SNR, and the training set with a smaller SNR is divided into the part with a lower SNR. Defining batch size = 1024, and then defining a constant “n”, which is relatively small. From the training set of the part with high SNR, we took batch_size - n data, and then took “n” data from the part with low SNR and added them up to get 1024 sets of training data, which were fed into the neural network for learning.

This approach did not change the total amount of the feed data, but artificially adjusted the type of the feed data to reduce the random range of the feed data, so as to increase the recognition accuracy of the neural network model.

When n=50 and x=-14db, the two network recognition accuracy rates before and after the improvement are compared:
FIG 3. When n=50 and x=-14db, the two network recognition accuracy rates are compared.

Table 1. Accuracy of CNN when x=-12 and x=-14.

| SNR   | Original | Improved |
|-------|----------|----------|
|       | -14      | -12      |
| 2 db  | 77.95%   | 80.12%   |
| 4 db  | 80.73%   | 82.30%   |
| 6 db  | 80.22%   | 82.16%   |
| 8 db  | 81.09%   | 83.01%   |
| 10 db | 81.62%   | 83.36%   |
| 12 db | 81.45%   | 83.21%   |
| 14 db | 81.46%   | 82.89%   |
| 16 db | 81.81%   | 83.24%   |
| 18 db | 81.83%   | 84.43%   |

As shown in Table 1, the recognition accuracy of the improved part is promoted to 83% in the part greater than 0 db.

We next investigate the effect of the feeding data method furtherly, define n=50, x=-10 and -18 db. Keep consistent with the original network training number of 80,000 times, then make n=50, x=-10 training 40,000 times and make n=50, x=-18 training 40,000 times too. The results are as follows:

FIG 4. Accuracy when n=50 and x=-10&-18db.
As shown in FIG 4, the improved neural network significantly improves the accuracy in the above 0 db and the -8 to -4 db part. when n=30, we work in the same way.

### Table 2. Accuracy of CNN when n=30 and n=50.

| SNR       | Original n=30 | Improved n=30 | Improved n=50 |
|-----------|---------------|---------------|---------------|
| 4 db      | 80.73%        | 82.43%        | 82.96%        |
| 6 db      | 80.22%        | 82.42%        | 82.47%        |
| 8 db      | 81.09%        | 83.07%        | 83.31%        |
| 10 db     | 81.62%        | 84.23%        | 82.99%        |
| 12 db     | 81.45%        | 83.89%        | 83.49%        |
| 14 db     | 81.46%        | 83.22%        | 83.17%        |
| 16 db     | 81.81%        | 82.71%        | 83.84%        |
| 18 db     | 81.83%        | 82.88%        | 83.35%        |

### 4. Defense

In battlefield environment, the two sides tried to get the other's intelligence. Our purposes not only minimize the accuracy of the intruder by adding artificial noise interference but also ensure that the expected receiver can still restore the messages.

#### 4.1. Add Interference to the Training Set

In the actual electromagnetic environment, there is a lot of noise interference to the signal. Therefore, for the training set whose data are all sampled from ideal signals, the training is carried out after adding noise to improve the robustness of the training results. The three variables of the training set interval, the data dimension and the variance of the added noise are studied.

Firstly, the interval of the training set with added noise is studied. Keep the 2*8 dimension of added noise and the noise variance of 0.001 unchanged, and set the parameter threshold. Add interference to the part which is greater than the threshold. It is found that there is some improvement in the condition of negative SNR -12 to -6db.

### Table 3. Accuracy of CNN 2*8 dimension.

| SNR  | -12db | -10db | -8db | -6db |
|------|-------|-------|------|------|
| Original | 16.98% | 19.42% | 26.87% | 34.66% |
| Improved | **18.22%** | **22.97%** | **28.05%** | **37.35%** |

Next, the dimension range of added noise is studied: The threshold is 10 and the noise variance were kept unchanged at 0.01. We found that the accuracy of the neural network was significantly improved from 0 db to 18 db when the noise was added to the 2*18 to 2*26 dimensions data.

### Table 4. Accuracy of CNN different dimension.

| SNR | Dimension | Original | Improved |
|-----|-----------|----------|----------|
| 2   | 2*18      | 77.95%   | **80.70%** |
|     | 2*20      | 79.73%   | 80.30%   |
Then the noise variance is studied. When threshold is 10, the 2*26-dimensional data was un-
changed and the variance was 0.0007, the recognition accuracy was significantly improved in the
range of -12 to -6 and 0 to 18 db, especially in the condition of negative SNR.

![FIG 5. Accuracy of CNN when variance is 0.0007.](image)

When the variance is 0.0007, it improves the recognition accuracy in different dimensions, which is
showed in Table 5.

Table 5. Accuracy in different dimensions when variance is 0.0007.

| SNR | Original | Improved |
|-----|----------|----------|
|     | 2*26     | 2*32     | 2*36     |
| -10 | 19.42%   | 23.01%   | 20.65%   | 21.10%   |
| -8  | 26.87%   | 28.89%   | 28.29%   | 29.41%   |
| -6  | 34.66%   | 37.37%   | 38.19%   | 37.54%   |
| -4  | 49.03%   | 49.03%   | 51.21%   | 52.10%   |
| -2  | 63.23%   | 63.23%   | 65.28%   | 65.78%   |
| 0   | 72.92%   | 72.92%   | 74.65%   | 75.13%   |

4.2. Add Interference to the Test Set

In this section, we consider the ideal case of no additional environment noise interference signal and
reduces the recognition accuracy of the enemy classifier.

The solution proposed in this paper is to add artificial noise n to signal S and find the following so-

\[ S_{after} \approx S + n \]  

(1)
Make $n$ in a range as small as possible to reduce the recognition accuracy when enemy receiving the signal $S_{after}$.

In order to mask our signal modulation scheme while maintaining a reasonable bit error rate, our objective is to seek to minimize human perturbation $n$ to maximize the misleading effect of the enemy classification identifier. Appropriate artificial perturbation $n$ can successfully achieve the effect of interfering with the enemy classifier. However, in practical applications, we can only control the input $x$ of the channel, and the output is not only influenced by the input but also by the channel noise. Therefore, this study is based on an ideal scenario. In addition, this part is based on the state of the known enemy classifier, such a method is called white box attack.

In the program, the constant $n$ was added to the I and Q channels. We found that the recognition accuracy of the model in the part of high SNR was reduced to 50% when $n$ is about 0.000003, which could effectively interfere with the work of the enemy in recognizing our signals.

![FIG 6. Accuracy of CNN adding constant.](image)

5. Conclusions
This paper realizes the establishment of Convolutional Neural Network. Through training, the visualization of the results is realized. Finally, we established a model with a high accuracy rate and stored the trained model to preliminarily realize the application of Convolutional Neural Network in signal classification and recognition. However, there are still many deficiencies that need further discussion. Firstly, the algorithm discussed is simple and only the Convolutional Neural Network is simply analyzed. Secondly, our paper lacks horizontal comparison. Thirdly, there is no corresponding research on other branches of machine learning.

References
[1] O. A. Dobre, A. Abdi, Y. Bar-Ness, and W. Su. (2007) Survey of automatic modulation classification techniques: classical approaches and new trends. J. IET Commun., vol. 1, no. 2, pp. 137–156.
[2] Z. Zhu, (2014) Automatic classification of digital communication signal modulations. Ph.D. dissertation. Eng, Brunel Univ. London, Uxbridge, United Kingdom.
[3] A. Hazza, M. Shoaib, S. A. Alshebeili, and A. Fahad. (2013) An overview of feature-based methods for digital modulation classification. In: International Conference on Communications, Signal Processing, and their Applications. Sharjah. pp. 1–6.
[4] I. Goodfellow, Y. Bengio, and A. Courville, (2016) Deep Learning. MIT Press, Cambridge.
[5] A. Karpathy, (2017) CS231n convolutional neural networks for visual recognition. https://cs231n.github.io/convolutional-networks
[6] A. K. Nandi and E. E. Azzouz, (1998) Algorithms for automatic modulation recognition of communication signals. IEEE Trans. Commun., vol. 46, no. 4, pp. 431–436.
[7] A. Geron. (2017) Hands-On Machine Learning with Scikit-Learn and TensorFlow. O’Reilly, Sebastopol.
[8] T. J. O’Shea and N. West. (2016) Radio machine learning dataset generation with GNU radio. In: GNU Radio Conf. Boulder. pp. 1–6