Check for updates

Journal of KIIT. Vol. 19, No. 10, pp. 105-113, Oct. 31, 2021. pISSN 1598-8619, eISSN 2093-7571 105
http://dx.doi.org/10.14801/jkiit.2021.19.10.105

Jamming Selection Method against Unknown Radar Signals based on Deep Learning using Co-occurrence Matrix

Jeil Jo*, Jae Min Ahn**

Abstract

In recent studies, certain deep learning methods have been adopted to select the jamming technique, in electronic warfare. Although they provide good solutions for selecting the jamming technique against known signals, they are inadequate against unknown signals and impractical to implement on embedded systems. To resolve these limitations, this study proposes a novel jamming selection method against unknown radar threats based on deep learning using a co-occurrence matrix. The proposed method uses a feature extraction algorithm to generate a co-occurrence matrix in pulse description word that transforms into a transition matrix for extracting the characteristics of the unknown signal. A deep learning technique that utilizes the deep belief network algorithm is used. Performance tests are executed ten times with the ten-fold method, learning nine folds as training signals and testing the other fold as the unknown signal. With the proposed method, experimental results demonstrate 98% classification performance against unknown radar signals for which the conventional method is unsuitable.

요 약

최근 전자전에서 딥 러닝을 적용하여 재밍 기법을 선정하는 방법에 대해 연구가 진행되었다. 대부분의 연구는 알고 있는 신호에 대해서 효과적이지만 미상 신호에 대해서는 부적합하며 임베디드시스템에 적용하기에도 부적합 경우가 많다. 이러한 제한 사항을 극복하기 위해 코어커런스 매트릭스를 이용한 딥 러닝 기반의 미상 신호에 대한 재밍기법 선정 방법을 제안한다. 제안한 방법은 미상의 신호의 특성을 PDW로부터 코어커런스 매트릭스를 발생하는 특징 추출 알고리즘을 사용한다. 심층 신뢰 신경망을 사용하는 딥 러닝 기법을 적용하였다. 성능 시험은 9개 폴드는 학습과 검증에 사용하고 나머지 1개의 폴드를 미상의 신호로 테스트하는 것을 순차적으로 10번 수행하여 평균하였다. 기존 방법으로는 미상 신호에 대해 재밍 기법을 생성하지 못하지만 제안한 방법은 미상 신호에 대해 98% 이상의 확률로 적절한 재밍기법을 생성하는 성능을 보였다.

Keywords
co-occurrence matrix, deep learning, jamming selection, unknown threat

* Agency for Defense Development Senior researcher
- ORCID: https://orcid.org/0000-0002-3437-2916

** Chungnam National University Department of Radio and Information Communications Engineering professor
- ORCID: https://orcid.org/0000-0002-6261-0010

· Received: Jul. 13, 2021, Revised: Aug. 06, 2021, Accepted: Aug. 09, 2021

· Corresponding Author: Jae Min Ahn
Department of Radio and Information Communications Engineering, Chungnam National University, Korea
Tel.: +82-42-821-6650, Email: jmahn@cnu.ac.kr

Ⅰ. Introduction

Electronic attack that restricts and neutralizes the enemy's usage of radio waves has become essential for ensuring the success of a friendly-force mission. Radar jamming is a form of electronic attack that internally sends out radio frequency signals interfere with the operation of radar. Radar jamming techniques included in the self-protection equipment employed in fighter aircraft and ships can significantly contribute to the increase in operational effectiveness by deploying counter measures against threats such as radar tracking or missiles[1][2].

The conventional method of selecting a jamming technique against a radar signal involves modeling and simulation (M&S) or experiments through hardware-in-the-loop simulation. A library containing radar-signal information and the selected jamming technique is used in electronic warfare equipment. Before electronic attack, signal analysis and identification are required, and several methods based on machine learning are used for analyzing the threat signals.

In [3], a 64-dimensional vector for a signal was constructed based on the second difference of the pulse time of arrivals(TOAs), and a three-layer multi layer perceptron(MLP) was trained to classify radar signals into four pulse repetition interval(PRI) modulation types. Moreover, a study classified radar signals according to the PRI modulation types by defining a set of five features based on the histogram of the pulse intervals and the second difference of TOAs, and by training an MLP with a hidden layer[4]. An automatic method for recognizing seven PRI modulation types using a CNN is discussed in[5].

Another study [6] used an encoding method to deal with inconsistent features; a unidimensional convolutional neural network(U-CNN) was used to classify encoded high-dimension sequences with big data. In [7], a weighted XGBOOST model was used to classify the radar. However, all these studies do not involve jamming-technique selection. Although these methods provide good solutions to analyze the signal for selecting the jamming technique against known threats, they are inadequate against unknown threat signals. Therefore, a method for selecting the jamming technique against an unknown signal is essential.

To resolve these limitations, a novel method for selecting the jamming technique against an unknown threat, based on deep learning using a co-occurrence matrix is proposed in this study. The proposed method uses a feature extraction algorithm to generate a co-occurrence matrix, which represents the distributions of the intensities and information about relative positions of neighboring pixels of image[8][9], in pulse description word(PDW)[10] that transforms into a transition matrix for extracting the characteristics of the unknown signal.

The performance is evaluated using the 10-fold method. The entire data set is divided into 10-folds: nine are used for learning and the other is classified as the unknown threat. With the proposed method, experimental results show 98% classification performance against unknown radar signals.

Ⅱ. Proposed Method

2.1 Conventional method for selecting a Jamming Technique against an unknown threat signal

Fig. 1 shows the general jamming procedure for a known threat signal. The conventional jammer uses a library, which includes information on the threats and the relevant jamming techniques, to select a suitable jamming technique. Against an unknown that is not in the library, such as new radar waveform or changes in the radar mode, this method uses noise jamming because the correct radar jamming technique is unavailable; the jammer functions in a look-through mode that allows the receiver to periodically sample the signal environment for checking signal existence.

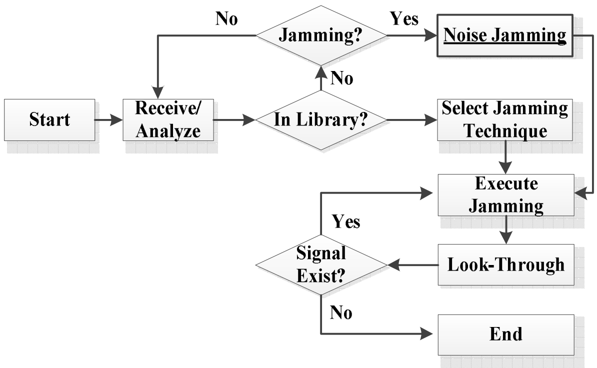


Fig. 1. General procedure for conventional jammer

Noise jamming does not secure the effectiveness of jamming against unknow threat. For better jamming effectiveness, a method for selecting the jamming technique against an unknown threat is necessary instead of noise jamming.

2.2 Proposed procedure and feature extraction algorithm usning a co-occurrence matrix

In this section, we propose a new feature extraction algorithm based on the co-occurrence matrix for radar-jamming technique classification against unknown signals. By converting the radar signal into a geometric feature, the proposed algorithm can model a more efficient jamming technique regardless of the signal type. Fig. 2 depicts the feature extraction algorithm based on the co-occurrence matrix.

The proposed feature extraction algorithm for jamming technique classification includes a co-occurrence matrix generation module that transforms the input signal into a geometric expression. The transition and data-distribution generation modules convert the co-occurrence matrix into specific distribution values. The moment module creates features based on the distribution values[11]. Finally, the normalization module normalizes the features that are input to a deep belief network(DBN)[12]. The details of each block are discussed in the subsequent sections.

The co-occurrence matrix is generally defined as a gray level co-occurrence matrix(GLCM) that converts the number of concurrent pixels into a distribution for image analysis or time-series data analysis[13], as shown in Equations (1)

$$C_{\Delta x,\Delta y}(i,j)= \sum_{x=1}^{n}\sum_{y=1}^{m}\begin{cases}1 & \text{if } I(x,y)=i \text{ and } I(x+\Delta x, y+\Delta y)=j\\ 0, & otherwise\end{cases} \tag{1}$$

where i and j are the pixel values, and x and y are the spatial positions in $n\times m$ image I; offsets $(\Delta x, \Delta y)$ define the spatial relation for which this matrix is calculated; $I(i,j)$ indicates the pixel value at pixel (x,y).

In this study, co-occurrence matrices for the frequency and pulse repetition interval (PRI) are generated in accordance with Equations (1).

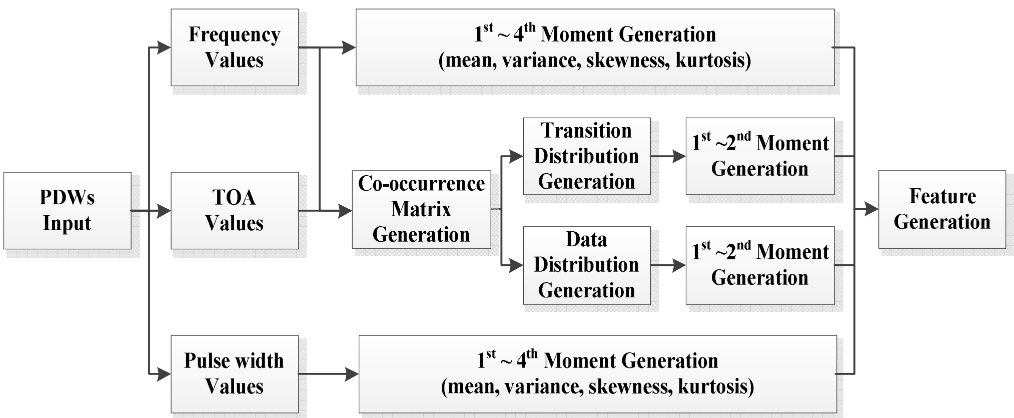


Fig. 2. Feature-extraction algorithm flow chart

N and M are the frequency bandwidth, and c is a frequency value generated in an adjacent frequency bandwidth. The co-occurrence matrix is generated by quantification.

Fig. 3, 4, and 5 depict examples of the transformation of major PRI types such as jitter, stagger, and dwell and switch (D&S) PRI signals into co-occurrence matrices.

Fig. 6, 7, and 8 depict examples of the transformation of frequency types such as agile, hopping, and patterned (sine) signals into co-occurrence matrices. The fixed PRI and frequency type are not transformed into co-occurrence matrices.

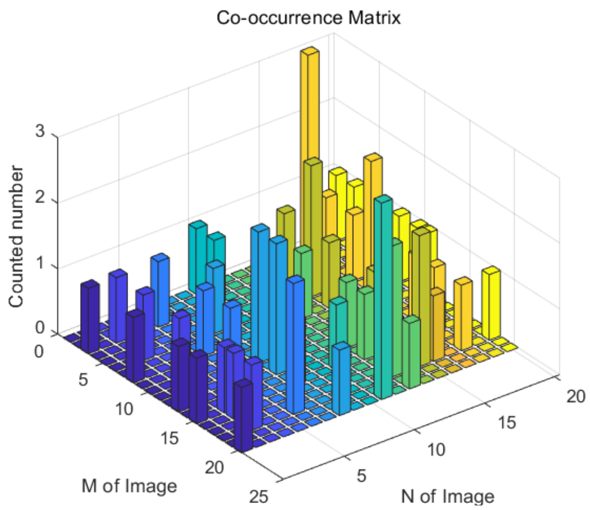


Fig. 3. Jitter PRI co-occurrence matrix

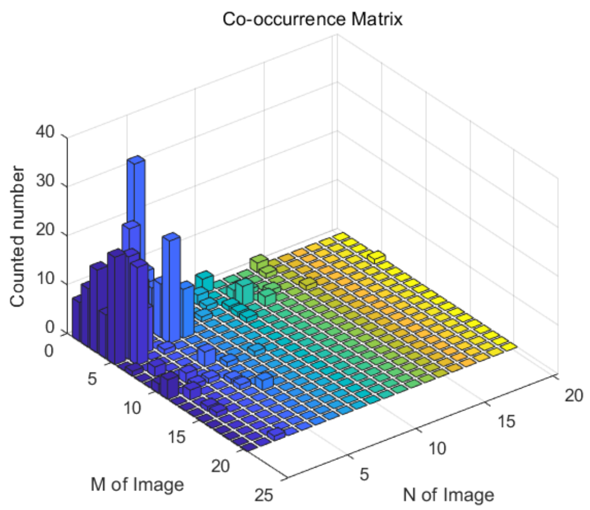


Fig. 4. Staggered PRI co-occurrence matrix

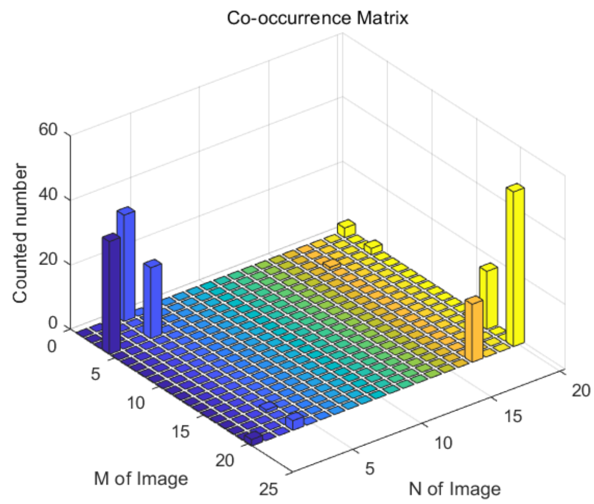


Fig. 5. Dwell and Switch PRI co-occurrence matrix

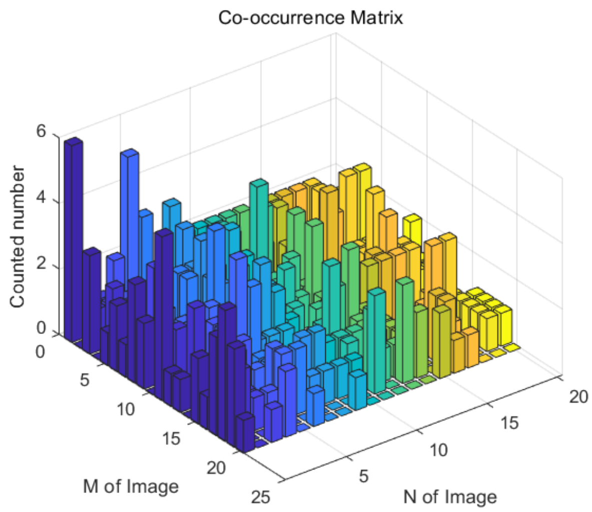


Fig. 6. Agile frequency co-occurrence matrix

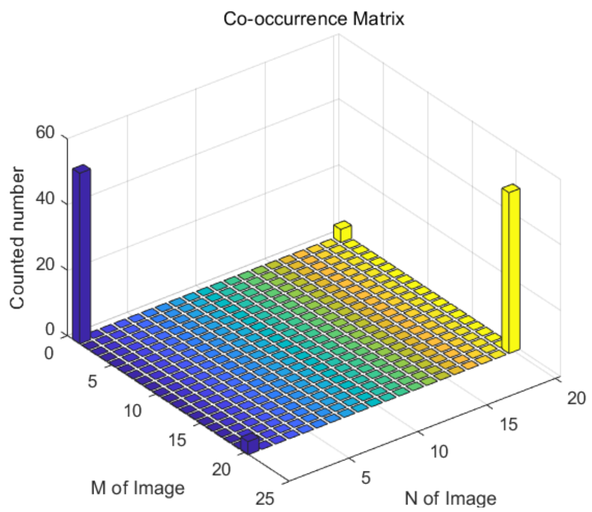


Fig. 7. Hopping frequency co-occurrence matrix

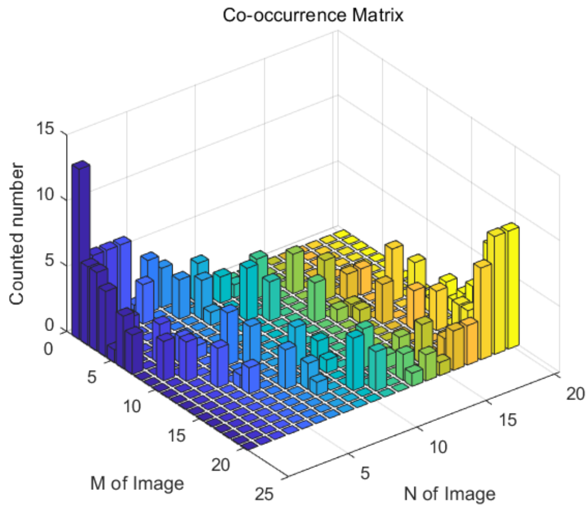


Fig. 8. Patterned (sine) frequency co-occurrence matrix

2.3 Feature extraction based on the co-occurrence matrix

The transformed data using the co-occurrence matrix can be mapped to the feature space through various statistical techniques. In general, a feature is extracted using the marginal probability mass function(PMF), which is extracted using the fourth-order moment from the calculated marginal PMF.

Equations (2) - (6) describe the marginal PMF and fourth-order moment. $P_{xy}(i,j)$ is the normalized value of an $n \times n$ co-occurrence matrix; μ_y is the mean, σ_y^2 is the variance, m_3 is the skewness, and m_4 is the kurtosis.

$$P_y(j) = \sum_{i=1}^{n} P_{xy}(i,j) \tag{2}$$

$$\mu_y = \sum_{j=1}^{n} j \Delta t P_y \tag{3}$$

$$\sigma_y^2 = \sum_{j=1}^{n} (j\Delta t)^2 P_y(j) - \mu_y^2 \tag{4}$$

$$m_3 = \sum_{j=1}^{n} \left(\frac{j\Delta t - \mu_y}{\sigma_y} \right)^3 \tag{5}$$

$$m_4 = \sum_{j=1}^{n} \left(\frac{j\Delta t - \mu_y}{\sigma_y} \right)^4 \tag{6}$$

In this study, two marginal PMFs are computed: the transition and data distributions. Transition distribution is a graph that analyzes the change in value by calculating the marginal PMF in the diagonal direction, whereas data distribution is a graph that analyzes the change in value after calculating the marginal PMF in the horizontal direction. Fig. 9 displays the algorithm for the co-occurrence matrix and the marginal PMF extracted from it. The second-order moment is extracted from each of the last-two generated marginal PMFs. In this study, the features are extracted using the mean and variance.

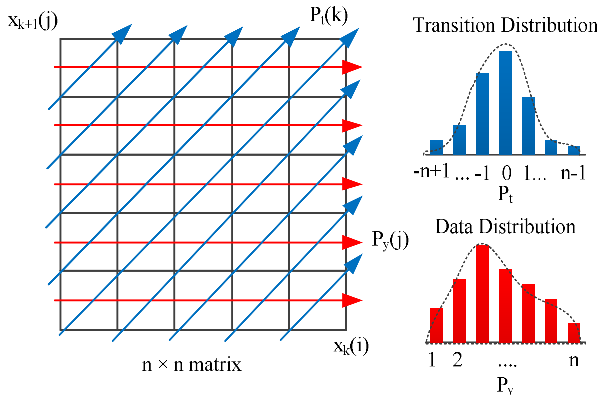


Fig. 9. Co-occurrence matrix and marginal PMF (transition distribution and data distribution)

2.4 Jamming technique selection using a DBN

The design of the proposed jamming selection against unknown radar using a DBN, which is a type of deep-learning algorithm, is presented here. Although deep learning algorithms are popular, they are too slow to be applied to the embedded software of defense systems because the learning time is considerable, and recognition cannot be made in real-time. Therefore, the jamming technique classifier is designed such that the DBN has sufficient improvements in the learning speed and recognition speed compared to a convolutional neural network

(CNN) or long short-term-memory(LSTM) in selecting the deep learning model[14].

According to [15], the learning speed of a DBN is at least 1.79 times more than that of an LSTM. For pretraining the DBN model, the model initialization formula proposed by Kaiming He[16] that enables faster learning is used instead of the restricted Boltzmann machine(RBM). This is an algorithm that improves the initialization method proposed by Xavier [17] using a Gaussian distribution with certain standard deviations and zero mean. The initialization formula applied for pretraining the DBN model for jamming technique classification is shown in Equations (7) and (8).

$$Var[y_L] = Var[y_1]\left(\prod_{l=2}^{L}\frac{1}{2}n_L Var[w_l]\right) \tag{7}$$

$$\frac{1}{2}n_l Var[w_l] = 1,\ \forall\, l \tag{8}$$

where L is the total number of layers, l is the designation of the layer, and Var is the variance.

The rectified linear unit (ReLu), which is a transfer function used for resolving the vanishing effect problem, is applied as a dropout algorithm to solve the overfitting problem in learning. The ReLu is given by Equations (9).

$$f(x) = \max(0, x) \tag{9}$$

Dropout is an algorithm that causes certain neurons to reset to zero randomly, when transferring data to the forward pass for dealing with the overfitting problem[18]. The dropout algorithm is depicted by the following equations for the forward path. For any layer l, $r^{(l)}$ is a vector of independent Bernoulli random variables each of which has probability p of being 1. This vector is sampled and multiplied element-wise with the outputs of that layer, $y^{(l)}$, to create the thinned outputs $\tilde{y}^{(l)}$[18]. $r_j^{(l)}$ is a value that determines whether dropout occurs, multiplied by the existing $y^{(l)}$ to render the neuron value zero.

$$r_j^{(l)} \sim bernoulli(p) \tag{10}$$

$$\tilde{y}^{(l)} = r^{(l)} * y^{(l)} \tag{11}$$

$$z_i^{(l+1)} = w_i^{(l+1)}\tilde{y}^{(l)} + b_i^{(l+1)} \tag{12}$$

The structure of the DBN model for unknown radar jamming, developed by applying the above algorithm, is shown in Fig. 10. The input layer is composed of 20 nodes to receive 20 features extracted by the feature extraction algorithm. The features have 12 values acquired from 1st to 4th moment of frequency, PRI and PW, and 8 values acquired from mean and variance of transition and data distribution of co-occurrence matrix.

There are three hidden layers, and each layer includes 90, 120, and 90 nodes, respectively. The output layer, which has five outputs, connects SoftMax and converts the output value to reliability. This system classifies five radar jamming techniques, divided into four types of jamming: noise jamming, range deception, speed deception, and angle deception.

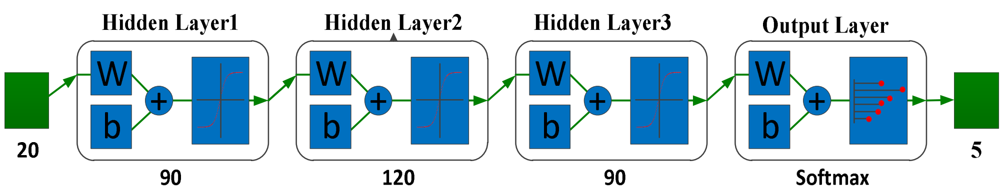


Fig. 10. Unknown-signal jamming DBN structure

III. Result

The performance of the proposed algorithm against unknown threats was evaluated. The applied data set comprised PDWs labeled with the jamming technique. Five jamming techniques were selected among the noise, deception, and combined jamming techniques[19].

The PDW lists were generated from more than 2,000 radar models that contain various signals such as frequency and PRI modulations[20]. The types of PRI modulation are stable, stagger, dwell and switch, jitter and patterned. The types of frequency modulation are fixed, hopping, agile and patterned.

Each list included a minimum of 1,000 and maximum of 9,000 PDWs. The threats used in this experiment were divided into 10-folds of the entire test data set: nine were used for learning, and the other was classified as an unknown attack. The data set configuration for each test case is shown in Fig. 11.

In each fold, the five jamming techniques were labeled with approximately 50%, 16%, 20%, 9%, and 5% of the data of jamming techniques 1, 2, 3, 4, and 5, respectively. The experiment yielded the recognition rate as the performance measure. Approximately 150,000–190,000 unknown threat data sets were tested per experiment. Table 1 depicts the amount of data used for learning and testing the unknown threat signals in each folder.

The experimental results are displayed in Table 2. The learning rates denote the trained results with 70% of the remaining data. The validation results denote the validation results with 30% of the remaining data. The results for unknown threats denote the test results with each fold as the unknown threat. The proposed algorithm recognized the radar jamming technique with 98% possibility against unknown threats. This indicates that a jammer equipped with the proposed algorithm can effectively respond to unknown radar threat signals with the proper jamming technique, unlike conventional jammers which do not perform jamming against unknown radar threat signals.

Table 1. Data for learning and testing (unknown threats)

10 Folds	Data for learning	Unknown threats
Fold 1	762,500	152,000
Fold 2	768,000	141,000
Fold 3	737,500	202,000
Fold 4	761,500	154,000
Fold 5	755,000	167,000
Fold 6	751,500	174,000
Fold 7	743,500	190,000
Fold 8	748,000	181,000
Fold 9	739,000	199,000
Fold 10	747,000	183,000

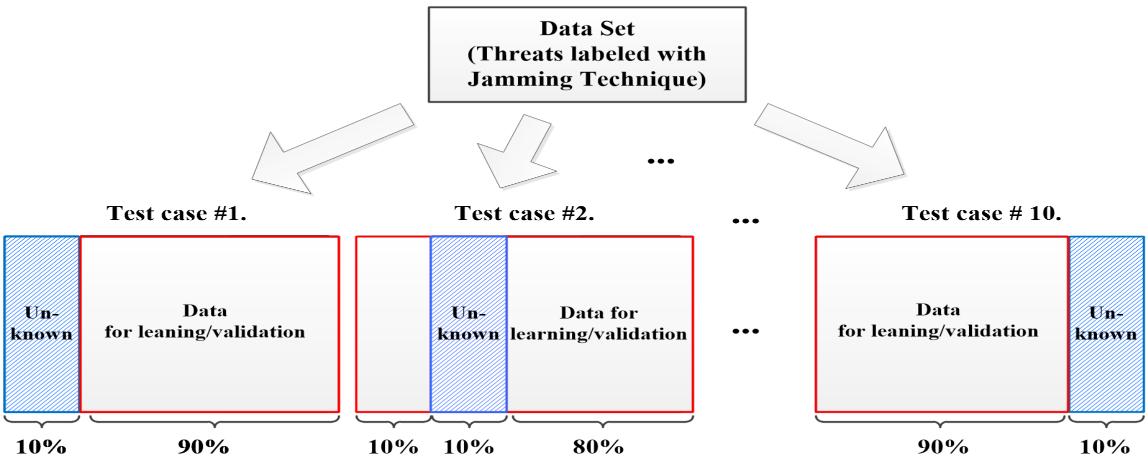


Fig. 11. Data set configuration for each test case

Table 2. Learning, testing, and unknown threat results

10 Folds	Learning rate	Validation results	Test results for unknown
Unknown Fold 1	99.86	99.86	98.67
Unknown Fold 2	99.63	99.63	96.51
Unknown Fold 3	99.82	99.82	98.46
Unknown Fold 4	99.73	99.73	97.27
Unknown Fold 5	99.91	99.91	97.65
Unknown Fold 6	99.79	99.79	98.84
Unknown Fold 7	99.85	99.85	97.55
Unknown Fold 8	99.82	99.82	99.30
Unknown Fold 9	99.91	99.91	98.40
Unknown Fold 10	99.80	99.80	98.82
Average	99.81	99.81	98.15

Ⅳ. Conclusions

A novel method to select the jamming technique against unknown threat signals that do not exist in libraries was proposed in this study. A co-occurrence matrix for extracting the features of unknown signals and radar jamming technique classification for unknown signals, with five types of jamming schemes, was proposed in association with a deep-learning algorithm.

The performance of the proposed algorithm with DBN based deep-learning using a co-occurrence matrix was verified. With data generated from general radar signal types, 10% were tested as unknown threats and the remaining 90% were learned. Approximately 7.6 million data sets were used for training and approximately 150,000–190,000 data sets per experiment were tested as unknown threats. Unlike the conventional method, which cannot respond suitably to unknown threats, the proposed algorithm demonstrated a classification recognition rate of 98% for unknown threats. For future work, it is necessary to apply and compare other algorithms for the method of selecting jamming techniques against unknown signals.

References

[1] M. I. Skolnik, "Introduction to RADAR Systems, 3rd edition", Tata McGraw-Hill publishing company limited. Singapore, pp. 547, Dec. 2002.

[2] L. Neng-Jing and Z. Yi-Ting, "A survey of radar ECM and ECCM", IEEE Trans. Aerosp. Electron. Syst., Vol. 31, No. 3, pp. 1-6, Jul. 1995. https://doi.org/10.1109/7.395232.

[3] G. Noone, "A neural approach to automatic pulse repetition using convolutional neural network", ICONIP'99. ANZIIS'99 & ANNES'99 & ACNN'99. in Proc. of 6th International Conference on Neural Information Processing, (Cat. No.99EX378), Perth, WA, Australia, Vol. 3, pp. 213-218, Nov. 1999.

[4] J. Kauppi and K. Marikainen, "An efficient set of features for pulse repetition interval modulation recognition", in Proc. IET Intl. Conf. on Radar Systems, Edinburgh, UK, Oct. 2007. http://dx.doi.org/ 10.1049/cp:20070548.

[5] X. Li, Z. Huang, F. Wang, X. Wang, and T. Liu, "Toward convolutional neural networks on pulse repetition interval modulation recognition", IEEE Commun. Lett., Vol. 22, No. 11, pp. 2286-2289, Nov. 2018. https://doi.org/10.1109/LCOMM.2018.2864725.

[6] J.Sun, G. Xu, W. Ren, and Z. Yan, "Radar emitter classification based on unidimensional convolutional neural network", IET Radar Sonar Navig., Vol. 12, No. 8, pp. 862-867, Aug. 2018. http://dx.doi:10.1049/iet-rsn.2017.0547.

[7] W.Chen, K. Fu, J. Zua, et al., "Radar emitter classification for large data set based on weighted-xgboost", IET Radar Sonar Navig., Vol. 11, No. 8, pp. 1203-1207, Jun. 2017. http://dx.doi:10.1049/ iet-rsn.2016.0632.

[8] R.M.Haralick, K. Shanmugam, and I. Dinstein, "Textural Features for Image Classification", IEEE Transactions on Systems, Man, and Cybernetics, Vol. 3, No. 6, pp. 610-621, Nov. 1973. https://doi.org/10.1109/TSMC.1973.4309314.

[9] A. Eleyani and H. Demirel, "Co-occurrencematrix and its statistical features as a new approach for

face recognition", Turkish Journal of Electrical Engineering and Computer Sciences, Vol. 19, No. 1, Jan. 2011. http://dx.doi:10.3906/elk-0906-27.

[10] V. Iglesias, J. Grajal, O. Yeste-Ojeda, M. Garrido, M. A. Sánchez, and M. López-Vallejo, "Real-time radar pulse parameter extractor", 2014 IEEE Radar Conference, pp. 0371-0375, Aug. 2014. http://dx.doi:10.1109/RADAR.2014.6875617.

[11] C. M. Jeong, Y. G. Jung, and S. J. Lee, "Neural network-based radar signal classification system using probability moment and ApEn", Soft Comput., Vol. 22, No. 13, pp. 4205-4219, 2018. http://dx.doi:10.1007/s00500-017-2711-7.

[12] G. E. Hinton, S. Osindero, and Y.-W. Teh, "A fast learning algorithm for deep belief nets", Neural Comput., Vol. 18, No. 7, pp. 1527-1554, Jul. 2006. http://dx.doi:10.1162/neco.2006.18.7.1527, PMID:16764513.

[13] Z. Cömert and A. F. Kocamaz, "Study based on gray level co-occurrence matrix and neural network community for determination of hypoxic fetuse", in International Artificial Intelligence and Data Processing Symposium, Malatya, Turkey, pp. 569-573, Sep. 2016.

[14] K. Cao et al.,"CNN-LSTM coupled model for prediction of waterworks operation data", Int. J. Inf. Process. Syst., Vol. 14, No. 6, pp. 1508-1520, Dec. 2018. http://dx.doi:10.3745/JIPS.02.0104.

[15] G. H. Lee, J. Jo, and C. H. Park, "Jamming prediction for radar signals using machine learning methods", Secur. Commun. Netw., Vol. 2020, No. 3, pp. 1-9, Jan. 2020. http://dx.doi:10.1155/2020/2151570.

[16] K. He, X. Zhang, S. Ren, and J. Sun, "Delving deep into rectifiers: surpassing human-level performance on Image Net classification", Intl. Conf. on Comput.Vis. (ICCV), Feb. 2015. http://dx.doi.org/10.1109/ICCV.2015.123.

[17] X. Glorot and Y. Bengio, "Understanding the difficulty of training deep feed forward neural networks", Proc. Thirteenth Intl. Conf. on Artificial Intelligence and Statics, PMLR, Que'bec, Canada, pp. 249-256, Sep. 2010.

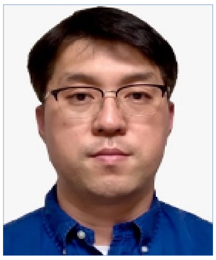
[18] N. Srivastava, G. Hinton, A. Krizhevsky, I. Sutskever, and R. Salakhutdinov, "Dropout: a simple way to prevent neural networks from overfitting", J. Mach. Learn. Res., Vol. 15, No. 1, pp. 1929-1958, Jun. 2014.

[19] C. Schleher, Introduction to Electronic Warfare, Artech House, 1986.

[20] J. L. Eaves and E. K. Reedy, Principles of Modern Radar, Van Nostrand Reinhold, 1987.

Authors

Jeil Jo



2000 : BS degree in Department of Electronic and Electrical Engineering, Kyungpook National University

2005 : MS degree in Department of Electronic Engineering, Kyungpook National University

2005 ~ present : Agency for Defense Development Senior researcher

Research interests : electronic warfare, jamming technique, adaptive and intelligent jammer system

Jae Min Ahn

1987 : BS degree in Department of Electronic Engineering, Seoul National University

1994: PhD degrees in Department of Electronic Engineering, KAIST

1999 ~ present : Professor at Chungnam National University

Research interests : communication signal processing and systems, navigation systems, geolocation, and information theory