Soft Comput (2018) 22:4205–4219
https://doi.org/10.1007/s00500-017-2711-7

FOCUS

Neural network-based radar signal classification system using probability moment and ApEn

Chang Min Jeong[1] · Young Giu Jung[2] · Sang Jo Lee[3]

Published online: 10 July 2017

Abstract Most of the existing electronic warfare systems use a threat library to identify radar signals. In this paper, new feature parameters for classifying various types of radar signals are introduced. The conventional method uses frequency, pulse repetition interval and pulse width sampled from the pulse description word column as characteristics of a signal. Such sampling technique cannot effectively model each radar signal when dealing with a complex signal array. This paper proposes probability moment and ApEn as an effective feature for the development of high-performance radar signal classifier. As shown in results, the proposed method can effectively classify ambiguous radar signals in the existing system because the signal values are similar but the order is different. In order to verify the performance of the proposed system, 100 types of radar signals in various bands were simulated, and the performance yielded 99% positive classification rate of the 100 radar signals.

Communicated by J. Park.

✉ Chang Min Jeong
min@add.re.kr

Young Giu Jung
youngq.jung@ym-naeultech.com

Sang Jo Lee
sjlee@knu.ac.kr

[1] Agency for Defense Development, Yuseong, Daejeon, Republic of Korea

[2] YM-Naeultech, Inharo, Namgu, Incheon, Republic of Korea

[3] Department of Computer Engineering, Kyungpook National University, Daegu, Republic of Korea

Keywords Threat library · Probability moment · Approximate entropy · Feature extraction

1 Introduction

Most of the existing electronic warfare systems use a threat library to identify radar signals. The threat library is written in feature table format with feature information such as radio frequency (RF), pulse width (PW), pulse repetition interval (PRI) and scan (SCAN). This feature information is extracted from previously collected radar signals. Electronic warfare systems use this rule-based threat library to identify received radar signals during tactical operation. However, this method requires a trained expert on the feature table creation and ongoing updates, and it has been proved to be deficient in accurately identifying radar signals in the increasingly complicated electronic warfare environment (Lee-Urban et al. 2015). In addition, when noise is mixed with the collected radar signals, recognition accuracy could be low (Granger et al. 2001; Arik and Akan 2015).

This paper proposes a novel feature extraction method based on probability moment and entropy for radar signal classification. The proposed method not only effectively reduces the dimension of the input signal but also has the advantage of effectively expressing the radar signal sequence with varying lengths, and shows higher performance in radar classification than any other feature. In order to verify the performance of the proposed system, 100 types of radar signals in various bands were simulated.

This paper is organized as follows. In Sect. 2, the related work is analyzed. In Sect. 3, threat signal feature extraction algorithm using the probability moment and ApEn is shown. In Sect. 4, we explain our data set and the results of our experiment. Finally, in Sect. 5, the conclusion of the study is drawn.

2 Related work

In order to effectively solve these deficiencies of existing rule-based systems, a research effort is underway to construct a radar signal classification system using statistical models, such as neural networks (Wu et al. 2012; Zhu and Jin 2012). These statistical models have been applied in various fields as well as radar signal classification systems (Keegan et al. 2016; Sato et al. 2015; Cho and Moon 2015). Studies based on statistical classification techniques for identifying radar signals have been in progress since the early 1990s. There are two main categories of the studies using statistical classification techniques. One is the study of feature vector extraction for the statistical classification by analyzing various signal characteristics of radar, and the other category is the statistical classification algorithms, such as backpropagation (BP), adaptive resonance theory MAP (ARTMAP) and self-organizing map (SOM) (Lin and Chen 2014; Petrov et al. 2013). Feature extraction studies are based on RF, PW, PRI and direction of arrival (DOA) of the radar signals (Yuan et al. 2006). The values from 0 to 1 are generally used in the feature normalization method for neural network experiments. In previous studies, the number of emitters to identify was three or seven, and the number of data used was limited (Yuan et al. 2006; Anjaneyulu et al. 2008; Lin and Chen 2014).

Anjaneyulu et al. (2008) proposed a method of classifying three emitter types using fuzzy ARTMAP network. In this study, RF, PW, PRI and DOA are used as feature vectors. After min/max of each features is set, if the feature point of the input signal is within feature point of an emitter type, the learning is performed using the ART neural network so that the input feature point is recognized as the corresponding emitter type. This system classifies three emitter types.

Lin and Chen (2014) proposed an interval type 2 fuzzy neural network to consider the uncertainty of the pulse information collected in a noisy environment. The system used RF, PW and PRI as feature points, classified all five radar types and displayed good performance in noisy data.

Shieh and Lin (2002) proposed a BP method called vector neural network which was based on the characteristics of RF, PW and PRI. In this study, radar signal classification was split into two stages: deinterleaving and vector neural network (VNN) recognition. Deinterleaving is a method to distinguish the type of radar primarily by setting an interval range for each radar. This is intended to solve the problem that the interval range is limited by radar types. In the learning method using VNN, entropy algorithm is used to calculate the learning error to solve the problem of reaching the local area in BP.

Petrov et al. (2013) have researched on dividing 29,094 signals into 125 radar types and generating characteristic parameters. In this paper, 12 feature points were extracted to be used as input parameters of a neural network. They showed an average of 80% accuracy in classifying 11 radar types (7 military radars and 4 civilian radars) using the neural network.

3 Threat signal feature extraction algorithm using probability moment and ApEn

This paper proposes a novel feature extraction method based on probability moment and entropy for radar signal classification. The proposed method not only effectively reduces the dimension of the input signal but also has the advantage of effectively expressing the radar signal sequence with varying lengths, and shows higher performance in radar classification than any other feature. In the next section, feature extraction algorithm using probability moment and entropy is described.

3.1 Feature extraction using probability moment

Probability moment (Spanos 1999) is a statistic that generalizes the effect of weighting at arbitrary points by probability distribution and can be used as a new parameter by representing the one-dimensional pattern as statistic. Generally, there are various kinds of probability moments such as moment about origin, central moment, factorial moment and joint moment.

In this paper, a feature extraction algorithm is proposed for radar signal identification using a fourth moment and a different fourth moment. The first to fourth moments are mean, variance, skewness and kurtosis, respectively. This algorithm extracts the first to fourth probability moments and the different fourth moments for radar signals with frequency, PRI and PW. Using a different fourth moment, radar signals can be effectively classified with the same value but different order in PRI. The following is a method for extracting a feature vector from an input signal using each probability moment.

(1) **Mean**
Mean is an indicator of the average of the variables and is defined as follows.

$$\text{Mean} = \frac{\sum x}{n}.$$

(2) **Variance**
Variance is an index that calculates the degree of dispersion of a variable.

$$\text{Variance} = \frac{1}{N-1}\sum_{i=1}^{N}(x_i - \bar{x})^2 .$$

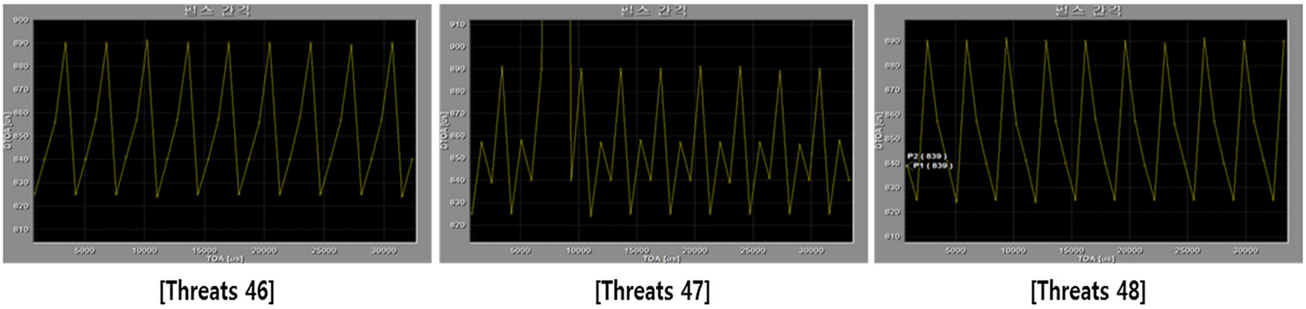


Fig. 1 Threats whose RF and PW are the same, but the orders of staggered PRI are different

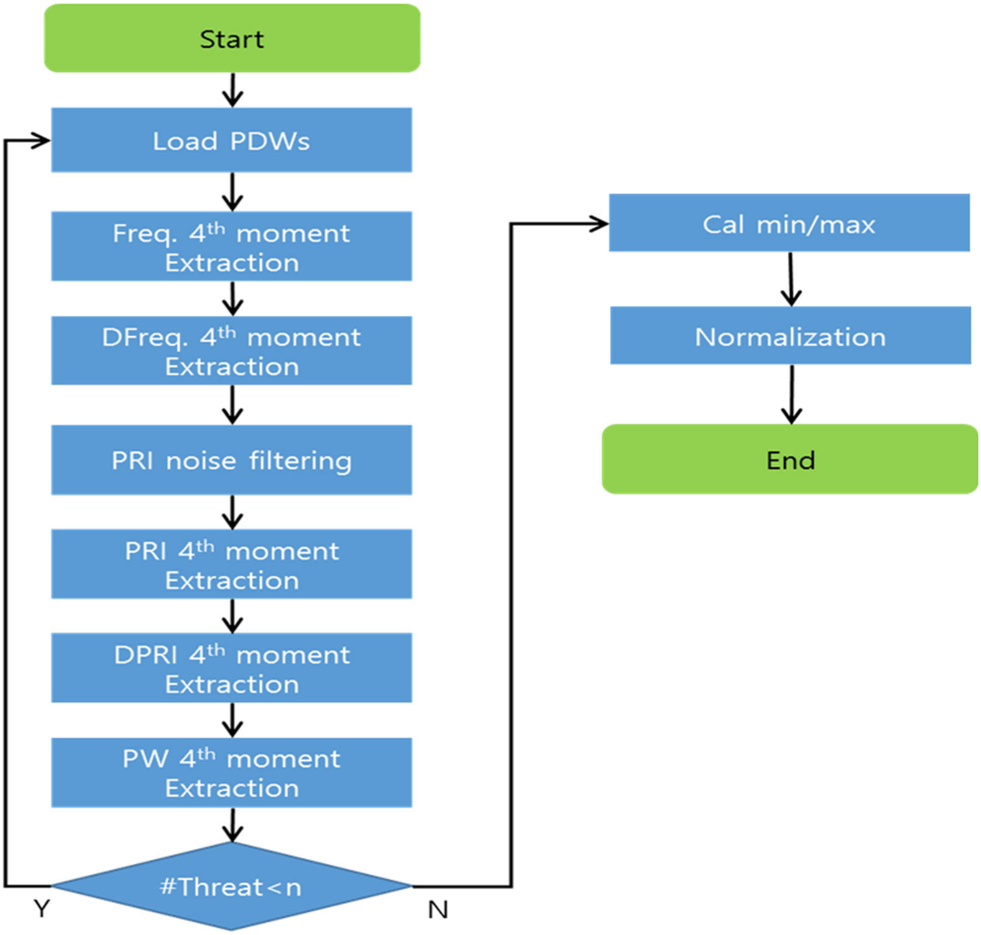

Start
Load PDWs
Freq. 4th moment Extraction
DFreq. 4th moment Extraction
PRI noise filtering
PRI 4th moment Extraction
DPRI 4th moment Extraction
PW 4th moment Extraction
#Threat<n
Y
N
Cal min/max
Normalization
End

Fig. 2 Feature extraction flowchart

(3) **Skewness**
Skewness is a value that measures whether the distribution of data is symmetric or not and is defined as follows.

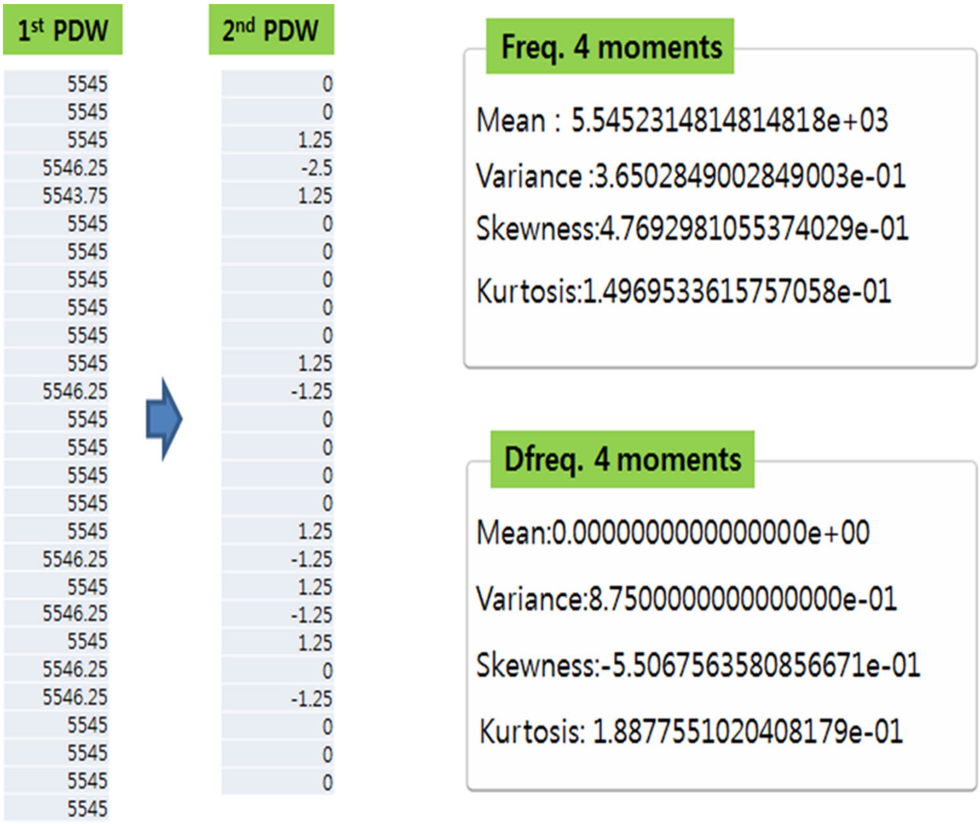
$$\text{Skewness} = \frac{\sum (x_i - \bar{x})^3 / n}{\left[\sum (x_i - \bar{x})^2 / (n-1)\right]^{3/2}}.$$

If the data are symmetric from the center, the value of the skewness is zero, the value is negative when skewed to the right, and skewed to the left has a positive value.

(4) **Kurtosis**
The kurtosis is a measure of how sharp the distribution of data is, and is defined as follows.

$$\text{Kurtosis} = \frac{\sum (x_i - \bar{x})^4 / n}{\left[\sum (x_i - \bar{x})^2 / (n-1)\right]^2} - 3.$$

If the distribution of the data is more acute than the normal distribution, the value of the kurtosis is represented as



1st PDW	2nd PDW
5545	0
5545	0
5545	1.25
5546.25	-2.5
5543.75	1.25
5545	0
5545	0
5545	0
5545	0
5545	0
5545	1.25
5546.25	-1.25
5545	0
5545	0
5545	0
5545	0
5545	1.25
5546.25	-1.25
5545	1.25
5546.25	-1.25
5545	1.25
5546.25	0
5546.25	-1.25
5545	0
5545	0
5545	0
5545	

Freq. 4 moments

Mean : 5.5452314814814818e+03

Variance :3.6502849002849003e-01

Skewness:4.7692981055374029e-01

Kurtosis:1.4969533615757058e-01

Dfreq. 4 moments

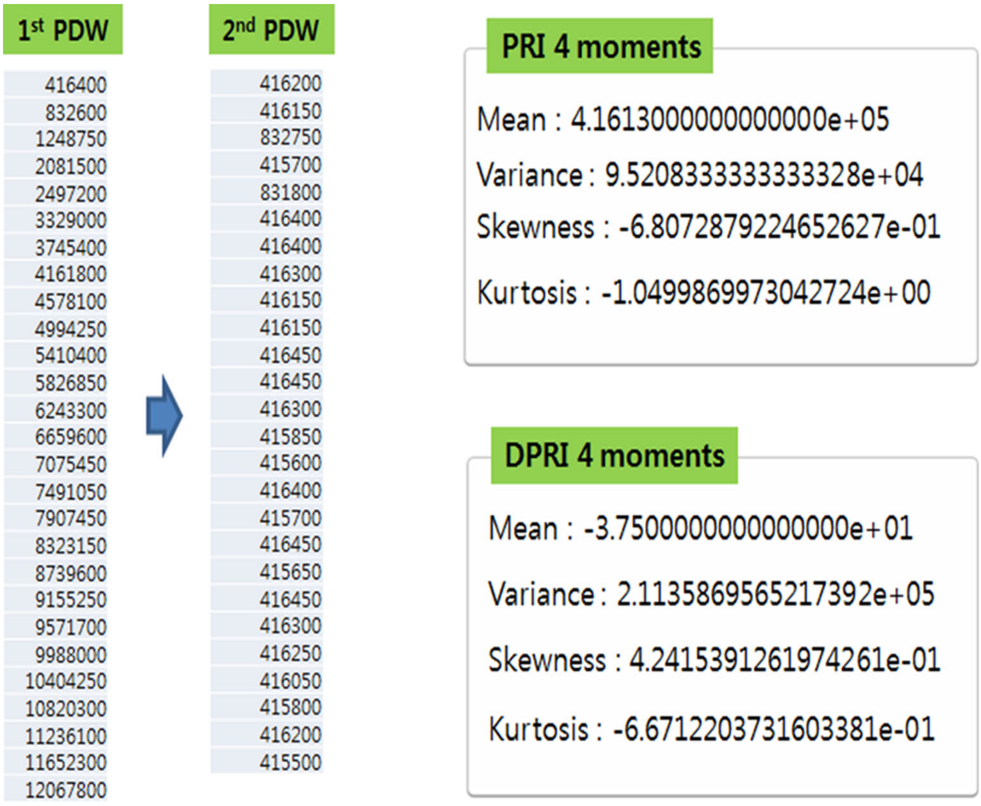
Mean:0.0000000000000000e+00

Variance:8.7500000000000000e-01

Skewness:-5.5067563580856671e-01

Kurtosis: 1.8877551020408179e-01

Fig. 3 Example of the frequency feature extraction using moment



1st PDW	2nd PDW
416400	416200
832600	416150
1248750	832750
2081500	415700
2497200	831800
3329000	416400
3745400	416400
4161800	416300
4578100	416150
4994250	416150
5410400	416450
5826850	416450
6243300	416300
6659600	415850
7075450	415600
7491050	416400
7907450	415700
8323150	416450
8739600	415650
9155250	416450
9571700	416300
9988000	416250
10404250	416050
10820300	415800
11236100	416200
11652300	415500
12067800	

PRI 4 moments

Mean : 4.1613000000000000e+05

Variance : 9.5208333333333328e+04

Skewness : -6.8072879224652627e-01

Kurtosis : -1.0499869973042724e+00

DPRI 4 moments

Mean : -3.7500000000000000e+01

Variance : 2.1135869565217392e+05

Skewness : 4.2415391261974261e-01

Kurtosis : -6.6712203731603381e-01

Fig. 4 Example of the PRI feature extraction using the probability moment

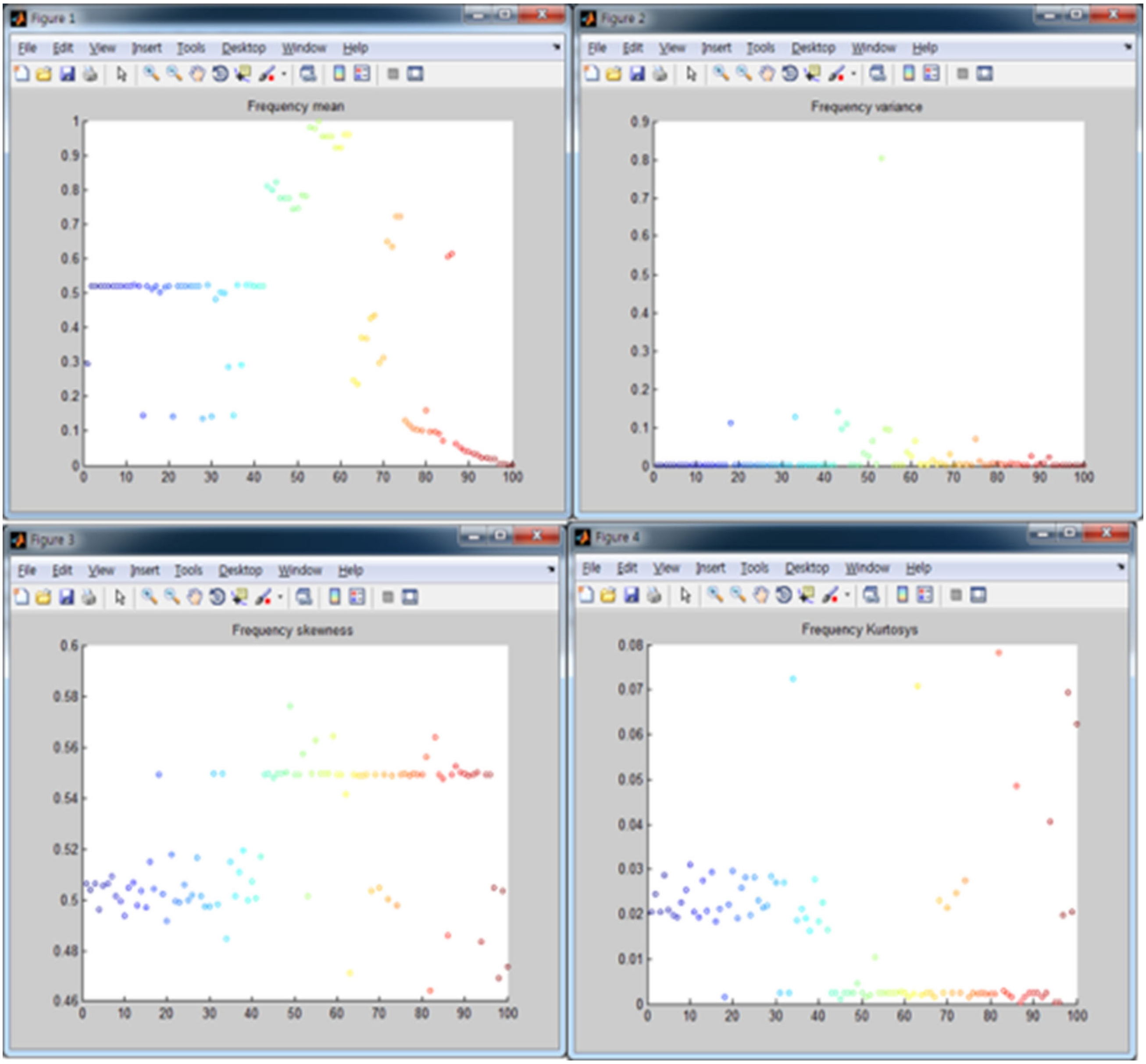


Fig. 5 Distribution of a fourth moment parameters to frequency

a positive value; otherwise, it is represented as a negative value.

We can confirm that the parameter generation method based on the probability moment is more stable than the sampling method as a result of application to 100 threats. However, there are many threats whose data are the same but whose sequence changes only in the threat signal. When using only the proposed probability moment, there is a deficiency that the threats cannot be effectively classified. The following are cases of four step staggered PRI in which frequency and PW are the same, but the orders of staggered PRI are different. As a result, 46th threat and 48th threat were recognized as 47th threat (Fig. 1).

Threats 46: 4 step staggered PRI 825, 840, 857, 890
Threats 47: 4 step staggered PRI 825, 857, 890, 840
Threats 48: 4 step staggered PRI 840, 825, 890, 857

In order to solve this problem, we introduce a new different probability moment. It is a method of generating the signal sequence using the difference of input signal sequence and extracting the first to fourth moments of the generated signal sequence. As a result of applying difference of mean, difference of variance, difference of skewness and difference of kurtosis to RF and PRI, most of the errors that occurred when simply applying the probability moment were resolved effectively. Figure 2 describes the algorithm applied to the

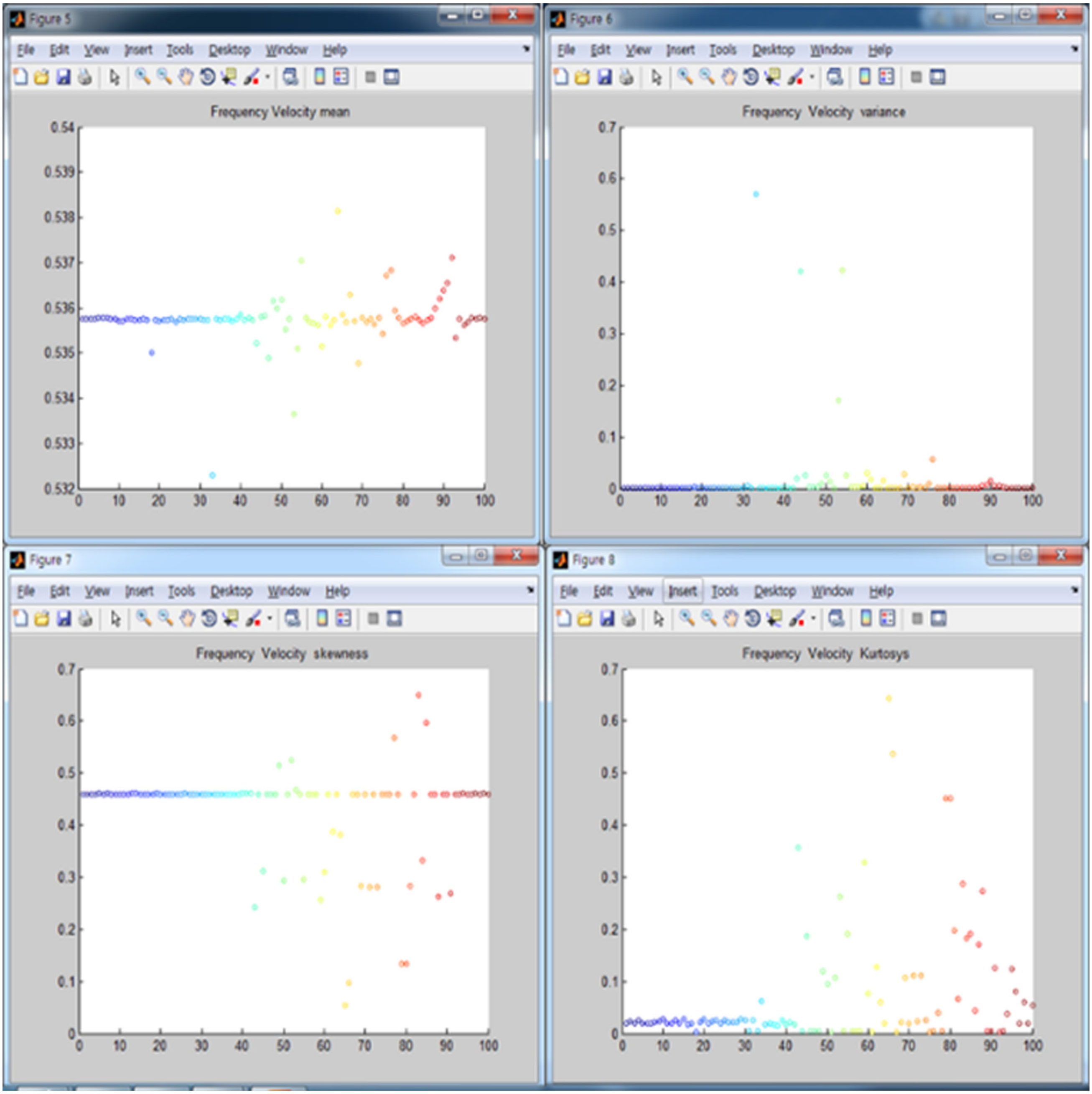


Fig. 6 Different fourth-order probabilistic moment distribution over frequency

neural network recognition using the aforementioned probability moment and different probability moment.

After loading the pulse description word (PDW) (Wiley 1982) of the threat, the mean, variance, skewness and kurtosis for the frequency are extracted, and the difference frequency for the frequency is calculated. D-mean, D-variance, D-skewness and D-kurtosis are then extracted. Mean, variance, skewness, kurtosis, D-mean, D-variance, D-skewness and D-kurtosis are extracted by using the same process for PRI. Finally, mean, variance, skewness and kurtosis are extracted for PW. Figures 3 and 4 show specific examples of probability moment characteristics extracted by applying the algorithm of Fig. 2 to the frequency and PRI. The primary PDW is the input signal sequence, and the secondary PDW is the PDW signal sequence using the difference of the input signal.

In the next step, an analysis is performed on the probability moment and the different probability moment on 100 types of radar signals through the graph. Figures 5, 6 show the distribution of the probability moment and the different moment for frequency, PRI and PW for 100 threats. Figure 5

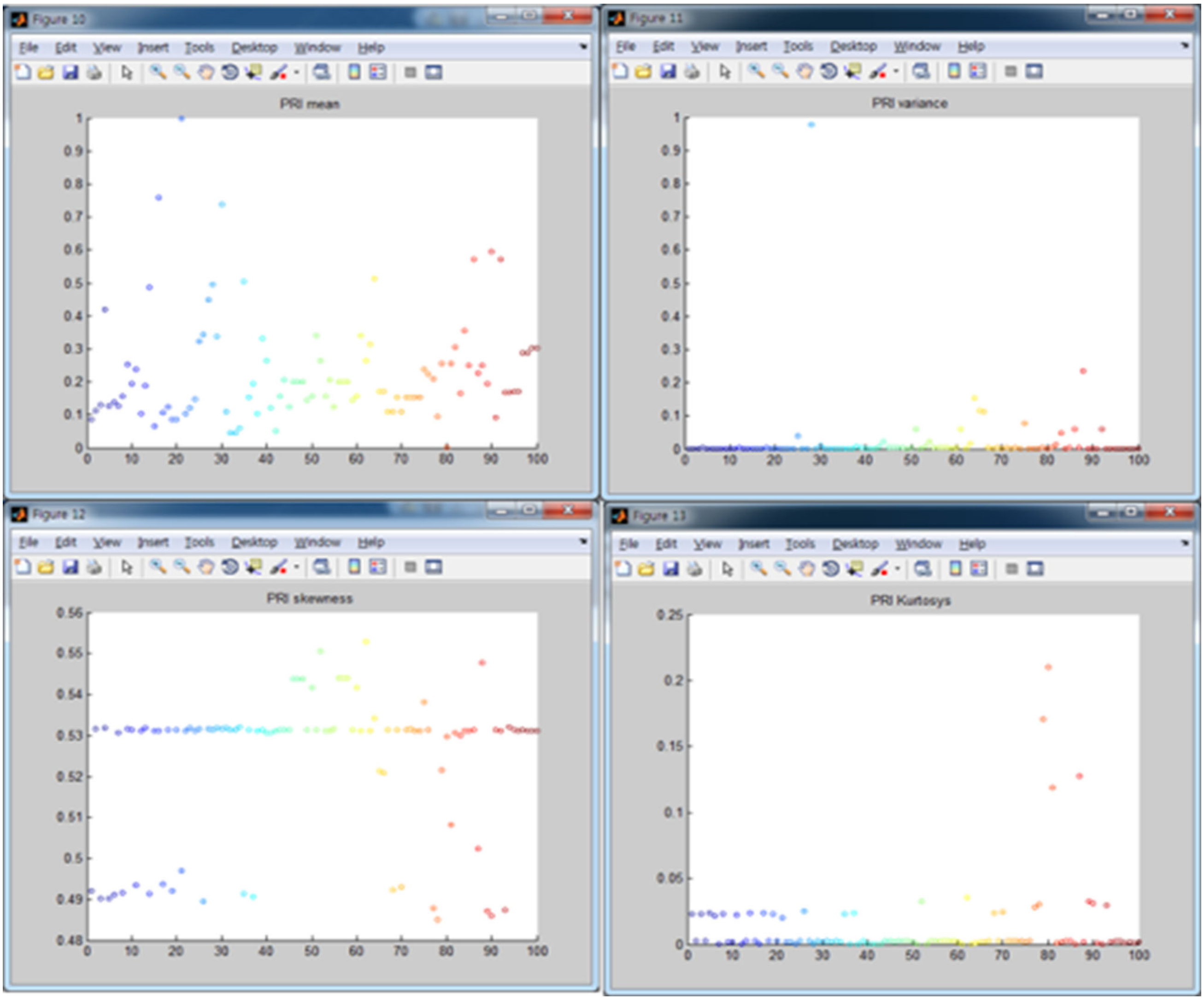


Fig. 7 Distribution of the parameters on the fourth moment of PRI

shows the distribution of the parameters of the first to fourth moments relative to the frequency signal. The horizontal axis is the type of threat, and the vertical axis is the average of 1000 data per threat.

In the figure 5, good parameters are evenly distributed over the entire screen with variety of colors. In the mean of the frequencies, it is not a good feature to classify threats from 1 to 45, but it is considered to be a good parameter for classifying threats after the 45th threat. In the case of frequency variance, it is seemingly almost indistinguishable from the total threat, and the skewness of the frequency is analyzed as a good feature for classifying threats from 1 to 45. In the case of frequency of kurtosis, it is considered to be effective to classify threats 1 to 40.

Figure 6 shows the distribution of the parameters of different fourth-order moment for frequency. The frequency D-mean is relatively small compared to the frequency mean, and the discrimination power is not adequate for the threats after 45th. The frequency D-variance has almost no discriminating power as the characteristic of the frequency variance. In the D-kurtosis, the distribution which does not appear in the existing moment is well represented.

Figure 7 shows the analysis result of the PRI parameter feature. In the case of PRI mean, there is a distinctive distribution of total threats. In the case of the variance of the PRI, it seems to be almost indistinguishable from total threats, and the skewness of the PRI shows partial discrimination against threats from 1 to 45. In case of kurtosis of PRI, there is little discriminating power.

In the PRI D-mean case, there is almost no discrimination against whole threats, unlike the PRI mean. In the case of the PRI D-variance, there is little discriminating power over the whole threats as the PRI variance. The D-skewness of the PRI shows partial discrimination against threats after 45th.

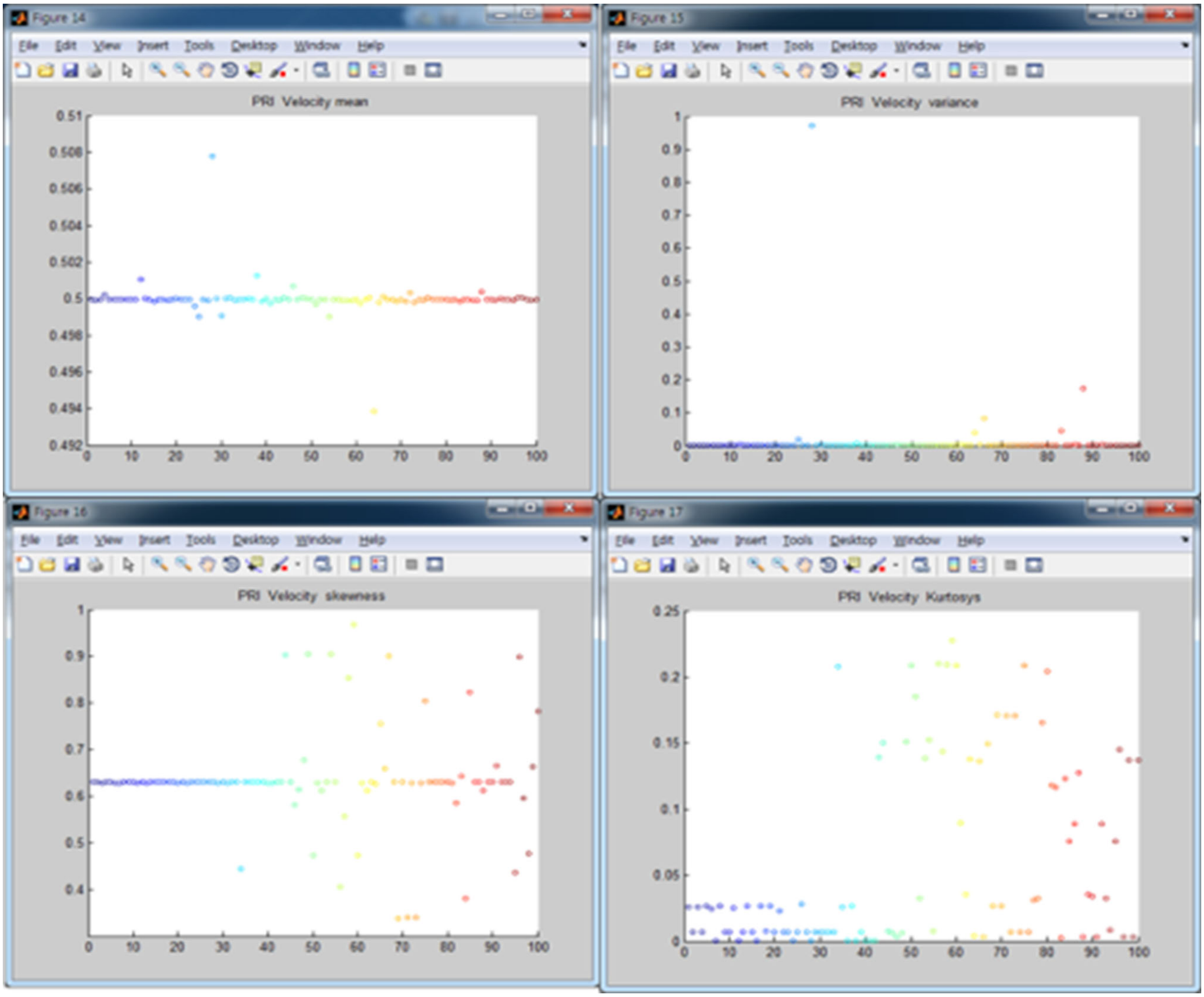


Fig. 8 Distribution of the parameters on the fourth different moments of PRI

The D-kurtosis of PRI is different from the kurtosis of PRI in that it has high discrimination against threats after 45th (Fig. 8).

The mean of PW generally has a differentiating power against whole threats, but the discriminating power itself is low. This is because the distance between threats is so close that the adjacent threats may be misunderstood. PW variance also shows the discrimination power against the whole threat, but it is considered to have high false identification rate due to the small feature range between each threat. The distance between threats before the 45th threat is small but big after the 45th threat, so the skewness of PW is deemed to be a good characteristic to judge each threat by showing difference. Finally, PW kurtosis has the same phenomenon as skewness, and it is seemingly guaranteed to yield high performance when used as an input to the neural network classifier (Fig. 9).

3.2 Feature extraction using ApEn

In this section, a parameter extraction method based on approximate entropy (ApEn) (Pincus et al. 1991) is shown to more effectively analyze signal sequences that cannot be processed by the previously presented probability moments. ApEn is an algorithm used to quantify the unpredictability of variability and the amount of regular patterns. This is because the data with regularity can be analyzed with most of the probability moments, but it cannot be analyzed with the existing probability moments in the case of the data having the similar value or the irregularity. A similar occurrence is observed in the case of radar signals. Fixed signals and jitter signals are the prime examples of the similarity and irregularity. In the case of those signals, there are frequent cases of false classification by using only the moment analysis. The following example shows the difficulty of the existing

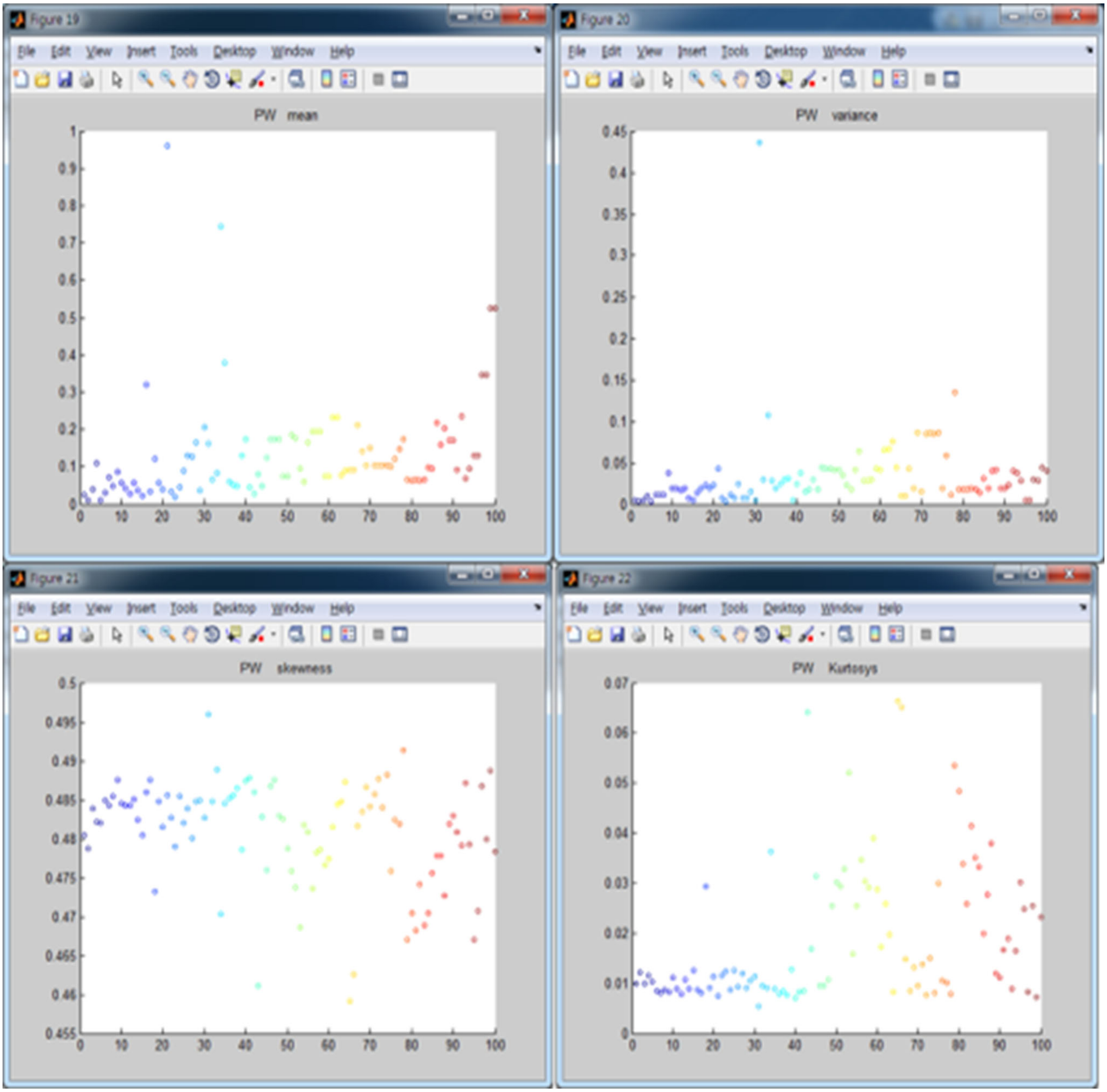


Fig. 9 Distribution of the parameters on the fourth moment of PW

moment methods in distinguishing random signals from the same range of signals with regularity:

series1 : (10, 20, 10, 20, 10, 20, 10, 20, 10, 20, 10, 20...),
series2 : (10, 10, 20, 10, 20, 20, 20, 10, 10, 20, 10, 20, 20...).

With these signal sequences, it is difficult to distinguish between two signal sequences using the moment based on mean or variance. The reason for this is that, in series2, the mean and variance of this signal are almost the same as those of series1. When analyzing such similar signals as these, it is possible to effectively distinguish between the two signals by measuring the randomness of the signals, which can be processed by an algorithm called ApEn. The following is the procedure of the ApEn algorithm.

Figures 10, 11, 12 show ApEn distribution analysis of 100 types of threats on frequency, PRI and PW. The discrimination power of all kinds of threat signals is very high in the figures. It is obvious that there are threats with small scale differences, but it can be concluded that high-performance recognizers can be developed by combining ApEn with existing probability moment feature vectors.

```
Step1:  Enter data in the same time interval in chronological order
        Sn= {u(1), u(2),…. u(N)}
Step2:  Set m and r value
        m: The number of data constituting the set
        r: filtering level
Step3:  Make sequence of vector x(1),x(2),…x(N-m+1)
        x(i) = [u(i), u(i+1), …, u(i+m-1)]
Step4:  Calculate the following equation using the vector created
          in Step 3
        $C_i^m(r) = \frac{(numberof\,x(j)such\ that\,d[x(i),x(j)]<r}{(N-m+1)}$,
          $d[x, x^*] = max \mid u(a) - u^*(a) \mid$
Step5:  Calculate $\Phi^m$(r) = $(N - m + 1)^{-1} \sum_{i=1}^{N-m+1} \log(C_i^m(r))$
Step6:  Calculate ApEn = $\Phi^m$(r) -$\Phi^{m+1}$(r)
```

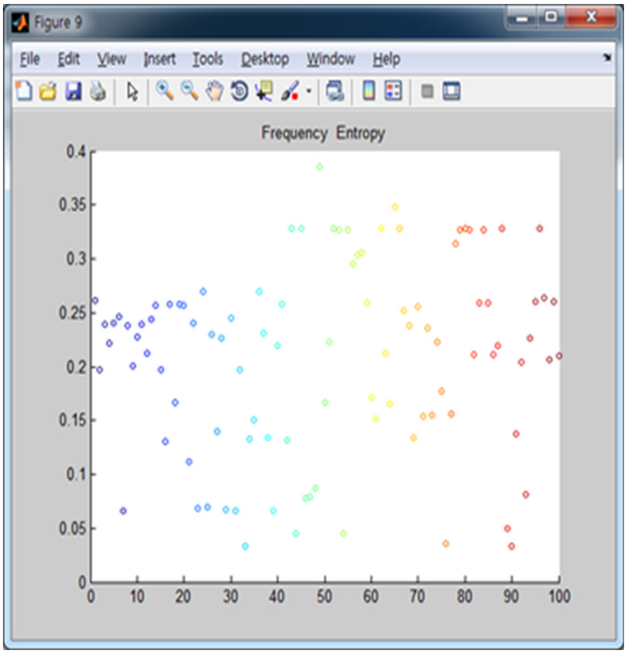


Fig. 10 ApEn distribution of frequency for 100 types of radars

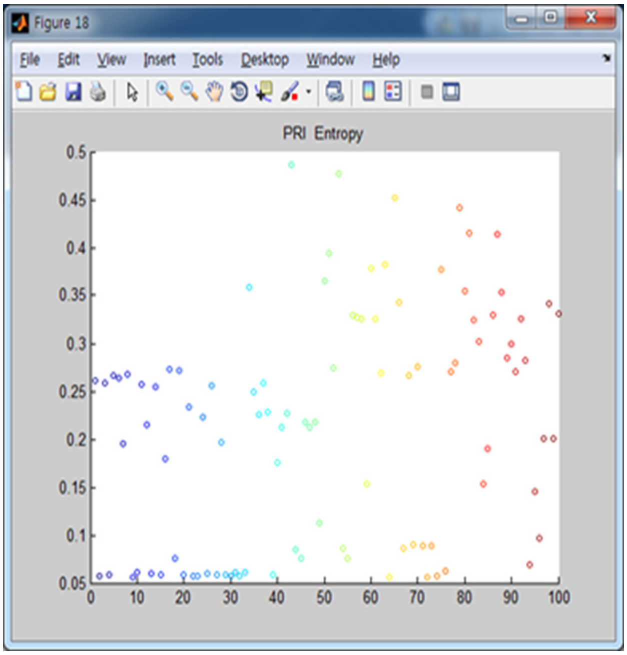


Fig. 11 ApEn distribution of PRI for 100 types of radars

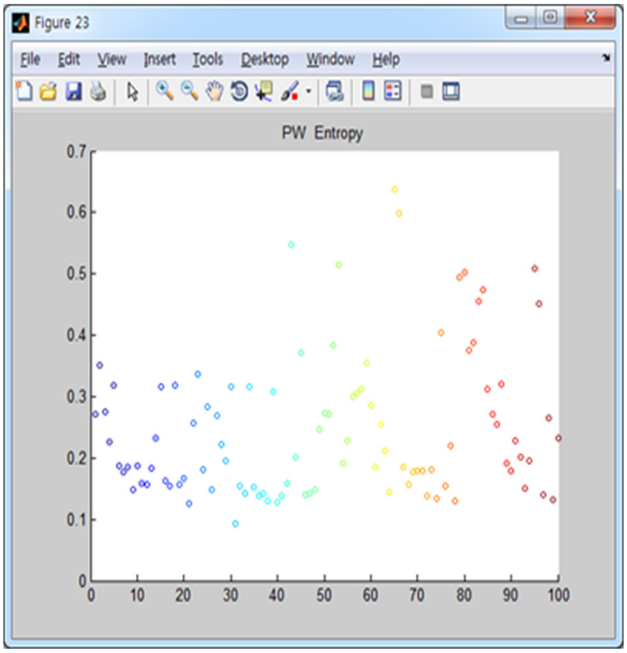


Fig. 12 ApEn distribution of PW for 100 types of radars

4 Experiment

In this paper, 100 types of radar signals (emitters) are tested to verify the performance of the proposed radar classifier using neural network model, which has an independent neural network structure of the existing neural network topology.

4.1 Data set

Figure 13 shows the experimental data configuration for this experiment. The total data set consists of 100 sets, and each radar signal consists of ten types of beams. Each beam is composed of a pulse description word (PDW) set. A PDW describes information such as frequency, pulse width (PW), pulse amplitude (PA), time of arrival (TOA) and modulation type.

In this paper, a threat environment is generated with a threat signal simulator with self-generating PDWs. The simulator serves to generate the corresponding PDWs when the user defines a radar signal. The number of PDWs for representing one beam varies from 20 to 400. Figure 14 shows the types of beams composed of a set of PDWs.

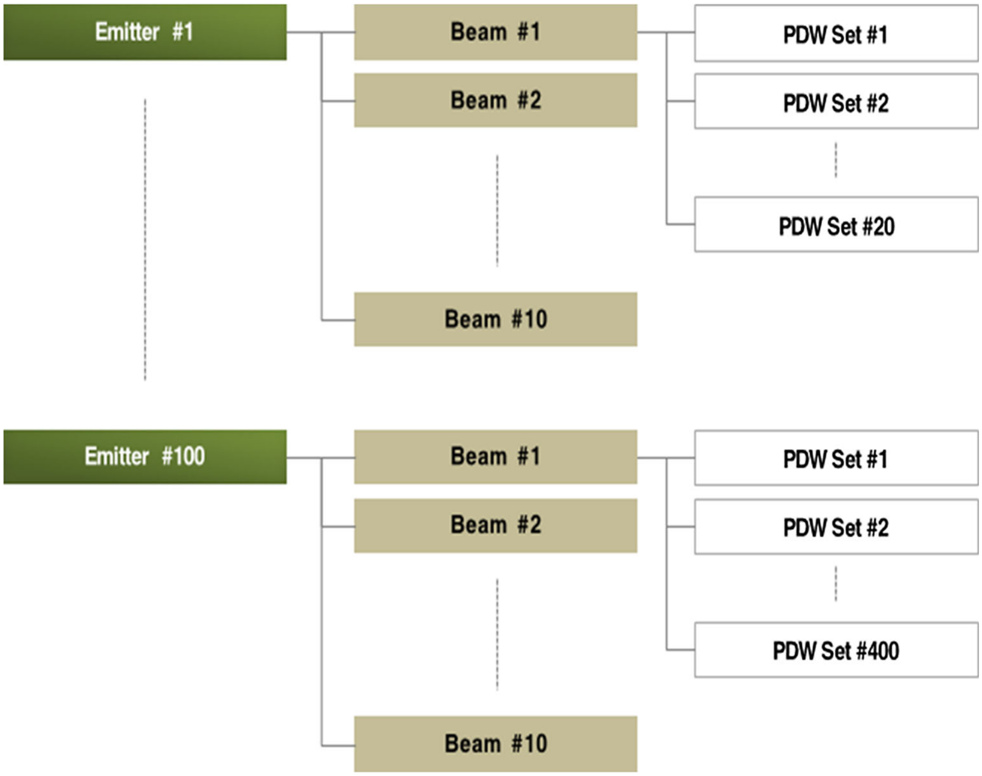


Fig. 13 Experiment data configuration

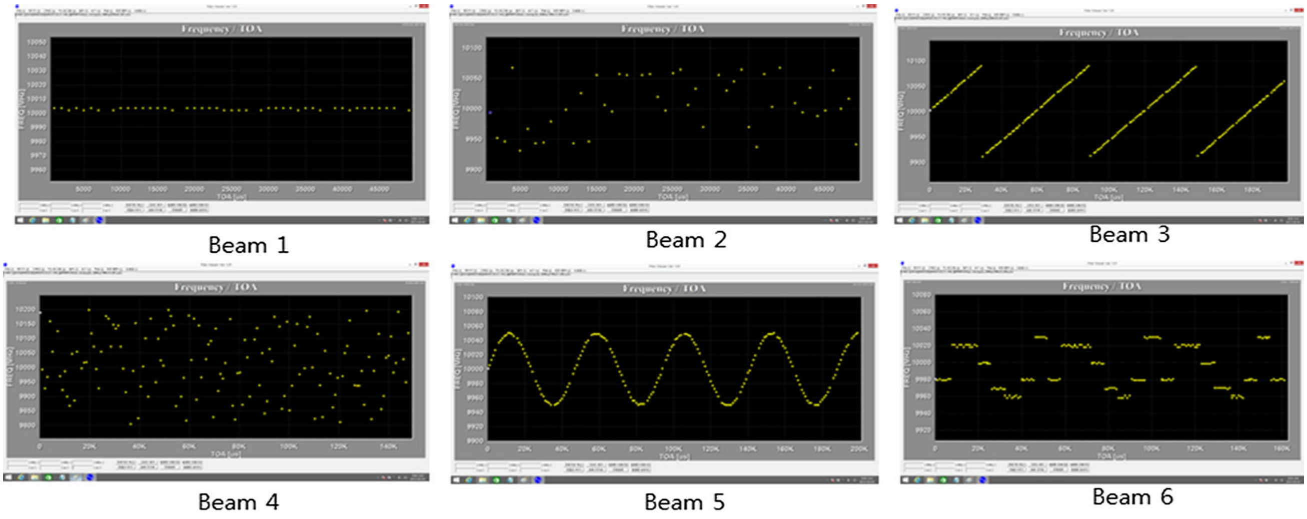


Fig. 14 Beam sample

The frequency range of this experiment is from 500 to 18,000 MHz, PRI from 5 to 4000 ms and PW from 500 to 6000 µs. In each datum, frequencies are formed as fixed, agile, hopping and pattern. PRI is configured to include various types of signals such as stable, stagger, jitter, dwell and switch, and pattern. Table 1 shows the type and number of threat signals used in this experiment.

Figure 15 shows the frequency band distribution of 100 types of emitters. The 40 of the 100 were obtained by processing the actual marine radar signals. The rest of the data were generated within the distribution band between 0.5 and 18 GHz.

Figure 16 shows the PRI distribution for 100 types of signals.

Table 1 Type and number of threat signals

Type	Range	Subtype (number)
Frequency	500–18,000 MHz	Fixed (51), random agile (15), hopping (20) and pattern agile (14)
PRI	50–4000 µs	Stable (24), stagger (21), jitter (23), dwell and switch (18) and pattern (14)
PW	500–6000 ns	–

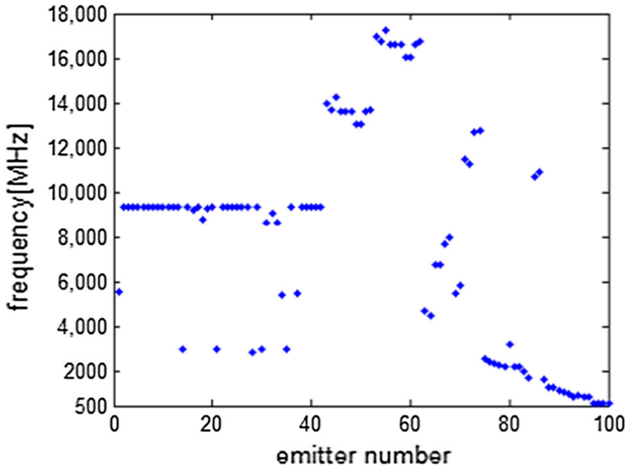


Fig. 15 Frequency band distribution of 100 types of radars

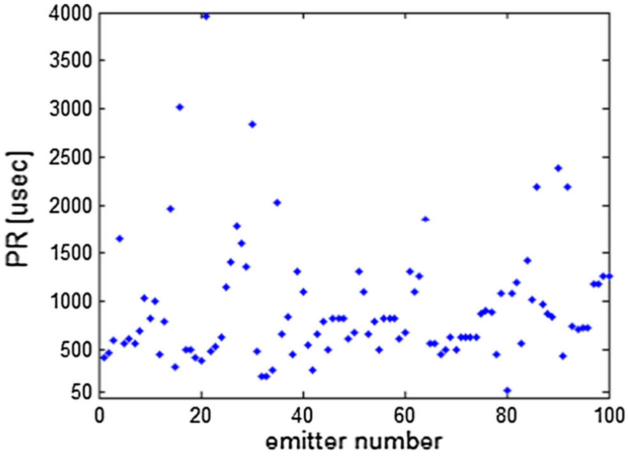


Fig. 16 PRI distribution for 100 types of radars

4.2 Neural network

Figure 17 shows the neural network model used for this experiment. The neural network model uses an independent neural network model designed to identify electronic warfare threats. The neural network model used in the experiment has an independent neural network structure of the existing neural network topology. That is because frequency, PRI and PW do not depend on each other.

4.3 Result

Our experimental data are as follows. Frequency, PRI and PW are used as features of mean and variance, respectively. Skewness, kurtosis and input signal are calculated, and a fourth probability moment is calculated and used as an additional feature. The approximate entropy (ApEn) is applied in experiment. The experimental results are presented by using these features. The final experiment shows that ApEn yields the highest performance.

Table 2 shows the recognition rate when only the mean and variance are used in the frequency, PRI and PW signal sequences in the radar signal properties. The neural network inputs are as follows. The experimental results show that the learning is not performed normally:

- Frequency: mean, variance
- PRI: mean, variance
- PW: mean, variance.

Table 3 shows the results of recognition rate when the first to fourth moments are extracted from the frequency, PRI and PW, respectively. The neural network inputs are as follows:

- Frequency: mean, variance, skewness, kurtosis
- PRI: mean, variance, skewness, kurtosis
- PW: mean, variance, skewness, kurtosis.

The results of this experiment show that the learning is not performed normally, either.

In Table 3, the error data are mostly generated in classes 46 to 48 and 56 to 58, and the main reason of the error is that almost similar signal sequences are changed in order. In classes 46 to 48 and 56 to 58, their frequencies, PWs and the values of staggered or D&S (Dwell and Switch) PRIs are the same, but the order of steps of staggered or D&S PRIs is different.

In order to solve the above problems, different probability moments and ApEn are applied. Table 4 shows the performance measurement result when the two feature vectors are added. In this feature, five parameters are added for frequency and PRI, respectively, and one parameter is added for PW. The neural network input characteristics are as follows:

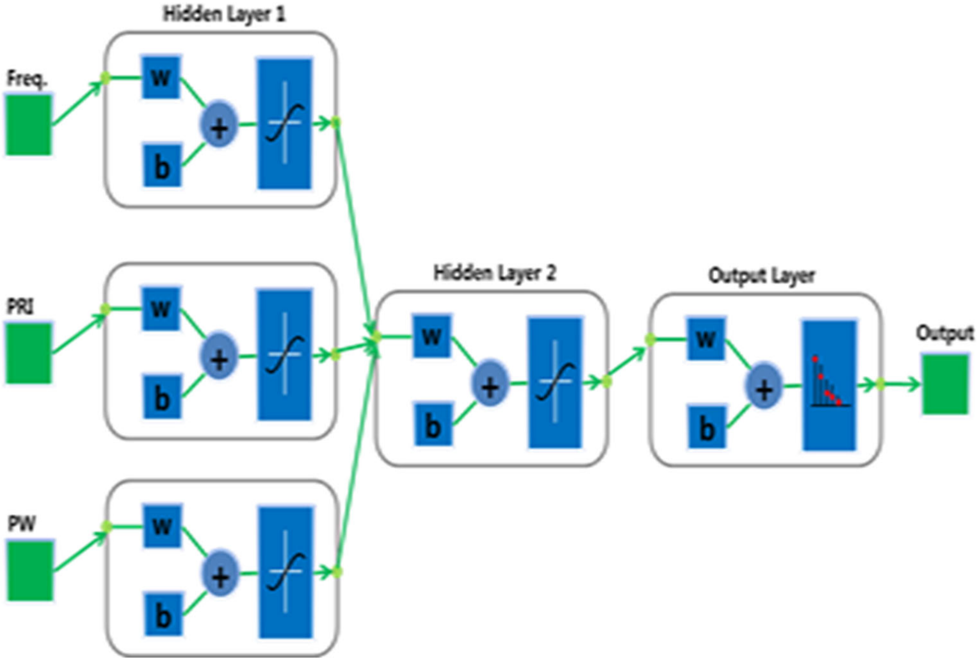


Fig. 17 Independently connected neural network

Table 2 Recognition rate of class of threat signal recognizer based on mean, variance of frequency, PRI and PW

Class number	1	2	3	4	5	6	7	8	9	10
Recognition rate	100	100	100	100	100	100	100	100	100	100
Class number	11	12	13	14	15	16	17	18	19	20
Recognition rate	100	96.2	100	100	100	100	97.2	100	100	99.6
Class number	21	22	23	24	25	26	27	28	29	30
Recognition rate	100	98.2	99.2	100	100	100	100	100	99.8	100
Class number	31	32	33	34	35	36	37	38	39	40
Recognition rate	100	100	100	100	100	100	100	96	100	100
Class number	41	42	43	44	45	46	47	48	49	50
Recognition rate	98.4	100	100	100	100	25.8	0.6	72.2	100	100
Class number	51	52	53	54	55	56	57	58	59	60
Recognition rate	100	100	100	100	100	67.4	30	4.4	100	100
Class number	61	62	63	64	65	66	67	68	69	70
Recognition rate	100	100	100	100	82.4	98.4	100	100	100	100
Class number	71	72	73	74	75	76	77	78	79	80
Recognition rate	100	100	100	100	100	100	100	100	46.6	100
Class number	81	82	83	84	85	86	87	88	89	90
Recognition rate	64	100	100	100	100	100	100	100	100	100
Class number	91	92	93	94	95	96	97	98	99	100
Recognition rate	100	100	100	99.4	84.4	84.2	38	76	68.6	55.2

– Frequency: mean, variance, skewness, kurtosis, D-mean, D-variance, D-skewness, D-kurtosis, ApEn
– PRI: mean, variance, skewness, kurtosis, D-mean, D-variance, D-skewness, D-kurtosis, ApEn
– PW: mean, variance, skewness, kurtosis, ApEn.

Table 4 shows that the recognition rate has increased. When applying the different probability moment, signals with similar value but different orders can be effectively classified among the various classes. ApEn can effectively discriminate the randomly changing signal in the same range.

Table 3 Recognition rate of class of threat signal recognizer based on a fourth probability moment of frequency, PRI and PW

Class number	1	2	3	4	5	6	7	8	9	10
Recognition rate	100	100	99.8	100	99.2	100	98.4	100	100	100
Class number	11	12	13	14	15	16	17	18	19	20
Recognition rate	99.6	97.4	99.8	100	100	100	96	100	97	99.8
Class number	21	22	23	24	25	26	27	28	29	30
Recognition rate	100	98.6	99.2	100	100	99.4	100	100	100	100
Class number	31	32	33	34	35	36	37	38	39	40
Recognition rate	99.8	100	100	100	100	100	100	98.2	100	100
Class number	41	42	43	44	45	46	47	48	49	50
Recognition rate	98.4	100	100	100	100	50.8	34.2	19.6	100	100
Class number	51	52	53	54	55	56	57	58	59	60
Recognition rate	100	100	100	100	100	64.8	29.6	1.2	100	100
Class number	61	62	63	64	65	66	67	68	69	70
Recognition rate	100	100	100	100	84.2	97.6	100	100	100	100
Class number	71	72	73	74	75	76	77	78	79	80
Recognition rate	100	100	100	100	100	100	100	100	84.4	100
Class number	81	82	83	84	85	86	87	88	89	90
Recognition rate	86	99.4	100	100	100	100	100	100	100	100
Class number	91	92	93	94	95	96	97	98	99	100
Recognition rate	100	100	100	99.6	62.2	86.4	61.8	80.2	59.4	84

Table 4 Recognition rate of class of threat signal recognizer based on a fourth probability moment and ApEn of frequency, PRI and PW

Class number	1	2	3	4	5	6	7	8	9	10
Recognition rate	100	99.6	99.2	100	99.8	100	99.6	99.8	100	100
Class number	11	12	13	14	15	16	17	18	19	20
Recognition rate	99.4	98	99.8	100	100	100	97.6	100	98.6	98.8
Class number	21	22	23	24	25	26	27	28	29	30
Recognition rate	100	99.8	99.8	99.8	100	99.4	100	100	100	100
Class number	31	32	33	34	35	36	37	38	39	40
Recognition rate	100	99.4	100	100	100	99.6	100	98	100	100
Class number	41	42	43	44	45	46	47	48	49	50
Recognition rate	99	100	100	100	100	99.6	99.8	100	100	100
Class number	51	52	53	54	55	56	57	58	59	60
Recognition rate	100	100	100	100	99.6	100	100	100	100	100
Class number	61	62	63	64	65	66	67	68	69	70
Recognition rate	100	100	100	100	100	100	100	100	100	100
Class number	71	72	73	74	75	76	77	78	79	80
Recognition rate	100	100	100	100	100	100	100	100	100	100
Class number	81	82	83	84	85	86	87	88	89	90
Recognition rate	100	99.8	100	100	100	100	100	100	100	100
Class number	91	92	93	94	95	96	97	98	99	100
Recognition rate	100	100	99.2	99	100	100	100	99.8	100	100

In the case of fixed and jitter signals, it can be seen that it is classified ambiguously using the probability moment but effectively classified when ApEn is applied.

Table 5 summarizes the threat signal recognizer performance measurement results based on the types and number of feature. The results show that the probability moment and

Table 5 Threat signal recognizer performance measurement results based on the types and number of feature

Number of features	Types of features	Recognition rate	Learning rate
6	Frequency: mean, variance	92.78	92.66
	PRI: mean, variance		
	PW: mean, variance		
12	Frequency: mean, variance, skewness, kurtosis	93.66	93.65
	PRI: mean, variance, skewness, kurtosis		
	PW: mean, variance, skewness, kurtosis		
23	Frequency: mean, variance, skewness, kurtosis, D-mean, D-variance, D-skewness, D-kurtosis, ApEn	99.8	99.87
	PRI: mean, variance, skewness, kurtosis, D-mean, D-variance, D-skewness, D-kurtosis, ApEn		
	PW: mean, variance, skewness, kurtosis, ApEn		

ApEn are good parameters for identifying the electronic warfare threat.

5 Conclusion

In this paper, new feature parameters for classifying various types of radar signals are introduced. Frequency, PRI and PW signals are sampled in the PDW column, which are used for the existing radar signal classification. Such sampling technique cannot effectively model each radar signal when dealing with complex radar signals.

This paper proposes probability moment and ApEn as an effective feature for the development of high-performance radar signal classifier. The proposed method can effectively classify ambiguous radar signals in the existing system because the signal values are similar but the order is different. In order to verify the performance of the proposed system, 100 types of radar signals in various bands were simulated, and the performance yielded 99% positive classification rate of the 100 types of radar signals.

Compliance with ethical standards

Conflict of interest The authors declare that they have no conflict of interest.

Ethical approval This article does not contain any studies with human participants or animals performed by any of the authors.

References

Anjaneyulu L, Murthy NS, Sarma N (2008) Radar emitter classification using self-organising neural network models. In: International conference on MICROWAVE

Arik M, Akan OB (2015) Enabling cognition on electronic counter measure systems against next-generation radars. In: MILCOM

Cho YS, Moon SC (2015) Recommender system using periodicity analysis via mining sequential patterns with time-series and FART analysis. J Converg 6(2):9

Granger E, Rubin MA, Grossberg S, Lavoie P (2001) A what-and-where fusion neural network for recognition and tracking of multiple radar emitters. Neural Netw 3:325–344

Keegan N, Ji S-Y, Chaudhary A, Concolato C, Yu B (2016) A survey of cloud-based network intrusion detection analysis. Hum-centric Comput Inf Sci 6:19

Lee-Urban S , Trewhitt E, Bieder I, Odom J, Boone T, Whitaker E (2015) CORA: A flexible hybrid approach to building cognitive systems. In: Third annual conference on advances in cognitive systems

Lin CM, Chen YM (2014) A self-organizing interval type-2 fuzzy neural network for radar emitter identification. Int J Fuzzy Syst 16(1):20

Petrov N, Jordanov IN, Roe J (2013) Radar emitter signals recognition and classification with feedforward networks. Procedia Comput Sci 22(1877–0509):1192–1200

Pincus SM, Gladstone IM, Ehrenkranz RA (1991) A regularity statistic for medical data analysis. J Clin Monit Comput 7(4):335–345

Sato A, Huang R, Yen NY (2015) Design of fusion technique-based mining engine for smart business. Hum-centric Comput Inf Sci 5:23

Shieh CS, Lin CT (2002) A vector neural network for emitter identification. IEEE Trans Antennas Propag 50(8):1120–1127

Spanos A (1999) Probability theory and statistical inference. Cambridge University Press, New York, pp 109–130

Wiley RG (1982) ELINT, the interception and analysis of radar signals. Dedham, Artech House

Wu Z, Yang Z, Yin Z, Zuo L, Gao H (2012) A novel RBF neural network for radar emitter recognition based on rough sets. J Chin Inst Eng 35:901

Yuan X, Huang G, Zhang Q (2006) Implementation of radar emitter intelligent recognition system based on neural network. In: CIE'06 international conference on radar

Zhu Bin, Jin Wei-dong (2012) Radar emitter signal recognition based on EMD and neural network. J Comput 7(6):1413–1420