www.czasopisma.pan.pl PAN POLSKA AKADEMIA NAUK www.journals.pan.pl

jet INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2017, VOL. 63, NO. 2, PP. 145-150
Manuscript received September 9, 2016; revised April, 2017. DOI: 10.1515/eletel-2017-0019

Countering a Self-protection Frequency-shifting Jamming against LFM Pulse Compression Radars

Samer Baher Safa Hanbali and Radwan Kastantin

***Abstract*— the well-known range-Doppler coupling property of the LFM (Linear Frequency Modulation) pulse compression radar makes it more vulnerable to repeater jammer that shifts radar signal in the frequency domain before retransmitting it back to the radar. The repeater jammer, in this case, benefits from the pulse compression processing gain of the radar receiver, and generates many false targets that appear before and after the true target. Therefore, the radar cannot distinguish between the true target and the false ones.**

In this paper, we present a new technique to counter frequency shifting repeater jammers. The proposed technique is based on introducing a small change in the sweep bandwidth of LFM waveform. The effectiveness of the proposed technique is justified by mathematical analysis and demonstrated by simulation.

***Keywords*— Anti-jamming, LFM, Range-Doppler coupling, Frequency-shifting jammer, Repeater jammer.**

I. Introduction

SEVERAL waveforms were used in pulse compression radar. However, the LFM (Linear Frequency Modulation) waveform is the most commonly used one, in both search and track radars, due to its high Doppler tolerance. However, the range-Doppler coupling property of LFM waveform makes radar more vulnerable to repeater jammer that shifts radar signal in frequency and instantly retransmitting it back to the victim radar. Since the jammer signal, in this case, looks like the radar return, it benefits from the pulse compression processing gain of the radar receiver and produces at its output false targets that appear before and after the true target. In this way, the radar cannot discriminate the true target [1-2].

The common ECCM (Electronic counter-countermeasures) techniques are effective against some types of jammers. However, these techniques have some drawbacks that make them unsuitable to counter frequency-shifting jammer. The coherence check technique compares between the pulse rising time and the detected target (after matched filter) range position in order to discriminate the true target. Of course, this is applicable only at a certain SNR (signal to noise ratio) of the incoming jamming pulse [3]. The pulse-width discriminator technique measures the width of each received pulse, again this is applicable only at a certain SNR [3], if the received pulse is not of approximately the same width as the transmitted pulse, and it is rejected. However, this technique cannot help in rejecting frequency-shifting jammers because the jamming pulses have the same width of the radar-transmitted pulse. Pulse-to-pulse PRI (Pulse repetition interval) jitter technique identifies the false targets returns if the deception jammer uses a delay that is greater than a PRI period to generate false targets return [4], but this technique is inefficient in the case of instantaneously retransmitting the radar pulse after shifting it in frequency. The frequency agility technique changes the radio frequency of radar to make it impossible to know what the radio frequency of the next pulse will be, but if the jammer has a DIFM (Digital Instantaneous Frequency Measurement Receiver) that measures approximately the first 50 ns of a pulse, it can quickly set to that radio frequency. Because modern radars typically have pulses of several microseconds long [4]. Orthogonal waveforms technique transmits successive orthogonal waveforms that have low cross-correlation [5-6], when jammer pulse lags behind the true target pulse, it will not benefit from the pulse compression gain, but this situation is not applicable in the case of instantaneous frequency-shifting jammer.

To overcome the limitations of the mentioned ECCM techniques that are only effective under a high SNR or when jamming pulses lag behind the true target echo, we propose countering the frequency-shifting jammer by small changing the sweep bandwidth of the LFM waveform so that the time-bandwidth product (pulse compression gain) of LFM waveform is unaffected. In this case, the radar transmits M pulses of the normal sweep bandwidth and M pulses of smaller sweep bandwidth alternately. True that the false target echo will gain from the integration process in both cases at the detector, but it will appear now in two adjacent range bins, whereas the true target will remain in the same range bin, and thus it can be discriminated.

The paper is organized as follows. The LFM pulse compression radar is introduced in Section 2. In Section 3, mathematical representation of the frequency-shifting jamming at the output of the matched filter is presented. In Section 4, a new technique to counter frequency-shifting repeater jammer is proposed. Finally, simulation results are demonstrated in section 5.

S. Baher Safa Hanbali is with the Higher Institute of Applied Sciences and Technology, Damascus, Syria (e-mail: Samer.Hanbali@hiast.edu.sy).

R. Kastantin is with the Higher Institute of Applied Sciences and Technology, Damascus, Syria (e-mail: Radwan.Kastantin@hiast.edu.sy).

II. LFM Pulse Compression Radar

The complex envelope $x(t)$ of a LFM waveform, that has a sweep bandwidth B and a pulse width T, is given by [7]:

$$x(t) = \frac{1}{\sqrt{T}} rect\left(\frac{t}{T}\right) e^{j\pi k t^2} \tag{1}$$

where $rect$ is the rectangular function, and $k = B/T$ is LFM modulation slope.

The ambiguity function diagram of the LFM waveform exhibits range-Doppler coupling property. Thus, the output of the matched filter remains approximately constant for Doppler shift up to $B/10$ [4]. However, this property makes radar vulnerable to repeater jammer that shifts radar signal in the frequency domain [1-2].

The output of the matched filter due to LFM waveform when $BT \gg 1$ can be written as [1]

$$|y(t)| = \sqrt{BT} \,.\, sinc(\pi B t) \tag{2}$$

The pulse compression gain of the matched filter equals to:

$$G = 10 log_{10}(BT) \tag{3}$$

III. Jamming LFM Pulse Compression Radar

Active jamming is the process of transmitting undesired signals towards victim radar with the objective of degrading its ability to detect the targets or to make it obtains wrong information of them. Mainly the jammers can be classified as a cover jammer and deceptive jammer [8]. In the former, the jammer transmits interference signals (usually noise) in order to prevent victim radars from detecting friendly targets. While in the second, the jammer transmits interference signals similar to the radar returns that processed by the victim radar receiver as a valid return signal, in order to prevent the radar from obtaining the correct range, velocity and/or angle information of the targets [8].

According to the jamming topology, we can distinguish between self-protection and stand-off jammers. In self-protection topology, the jammer is carried by the same vehicle or airplane to be protected from detection or tracking by a hostile radar. While, in stand-off jammers, the target is protected by a jammer carried by other friendly platform (vehicle or airplane) or located at some distance far from the victim radar [8].

Cover jamming masks the targets by continuous transmission of high power noise signal concentrated around the operational radar frequency. However, most of practical radar periodically changes its RF frequency. Thus, the jammer has to measure the radar RF frequency in order to be effective. The effectiveness of such jammers is usually measured by Jamming-to-Signal Ratio (JSR). The victim radar can usually mitigate the effectiveness of this type of jammer by reducing the radar antenna sidelobe, either by reshaping the antenna pattern or by using sidelobe canceller (SLC) circuit [3]. When countering LFM radar by transmitting noise signal, the jammer does not benefit from the gain of the matched filter. Therefore, the jammer has to increase its power in order to disable the radar capability, which is not always realizable especially for airborne jammer. On the other hand, increasing the jammer power make it more vulnerable to be destroyed by anti-radiation missile.

Different deceptive jammer techniques were proposed, in the literature, in order to jam LFM-PC (LFM pulse compression) radar more effectively by using low power signal. These techniques benefit from the range-Doppler coupling properties of LFM waveform. The aim of these techniques is to distort the output of radar matched filter and to generate false targets at its output. Actually, this can be achieved by transmitting modified version of the radar signal, so the jammer partially benefits from the processing gain of the matched filter [1-2]. These techniques can be used simultaneously to jam search and track radars. Generating false targets at the detector output, in search radar, prevents it from the identification of the true target and overload its processing unit. While, in track radar, these false targets can degrade its range tracker performance [3].

Digital Radio Frequency Memory (DRFM) repeater jammer is example of deceptive jammer that has been widely used in Electronic Counter Measures (ECM) systems. In DRFM, the jammer stores radar pulses digitally in a memory after down-conversion. Then the stored samples may be amplitude-, frequency- or phase-modulated. The resulting samples are converted back to analog signal and up-converted and retransmitted back in synchronization with next received radar pulse toward the victim radar [9]. Since the jammer retransmits pulses lag behind the radar pulses so it can be recognized by radar system easily [9]. The limitations of DRFM jammer can be overcome by instantaneously retransmitting the radar pulse after shifting it in frequency [1]. Thus, many false targets are generated at the output of matched filter. The aim of this work is to counter this type of repeater jammer that has one or more of the following modulations:

- One Frequency-shifting.
- Multiple Frequency shifting

A. One Frequency-Shifting Jamming

Repeater jammer can generate a false target at the output of LFM radar detector simply by frequency shifting the radar signal. The amount of the frequency shift determines the relative distance between the true target and the false one. In this case, the jamming signal equals [1]:

$$x_J(t) = x(t) \cdot e^{j2\pi f_J t} \tag{4}$$

where f_J is the frequency shift of the jammer, and $x(t)$ is the radar signal that is given in eq. 1. When $f_j < B$ the output of the matched filter, due to jamming signal, can be approximate by [1]:

$$|y(t)| \approx \sqrt{BT}\left|1 - \frac{f_J}{B}\right| . sinc\left[\pi\left(B - f_J\right)\left(t + \frac{f_J}{k}\right)\right] \tag{5}$$

The false target leads the true target when ($f_J > 0$) as shown in Fig. 1, and lags behind it when ($f_J < 0$). The relative distance between the true target and the false one equals [1]:

$$d = cf_j/2k \tag{6}$$

where c is the speed of light.

The amplitude of the false target is slightly lower than the amplitude of the true one by the value $|1 - f_J/B|$. Therefore, the jammer has to increase its power in order to compensate for this loss.

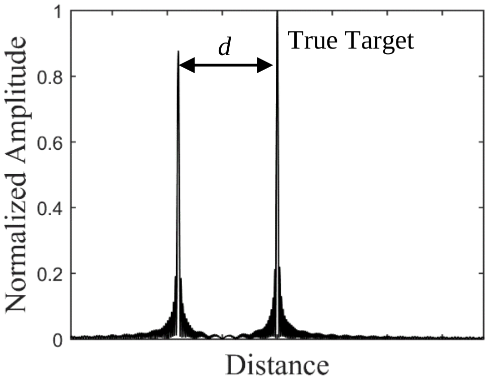

Fig.1 The matched filter output in case of one frequency-shifting jamming.

B. Multiple Frequency-shifting Jamming

Many false targets can be generated simultaneously at the output of matched filter if the repeater jammer modulates the radar signal by a periodic square train that has amplitude ± 1 .

The periodic square train which has amplitude ± 1 and frequency f_m, can be represented by:

$$m(t) = \sum_{n\ odd}^{\infty} \frac{2}{j\pi n} e^{j2\pi n f_m t} \tag{7}$$

where $n = \pm 1, \pm 3, \ldots$ In this case, the jamming signal can be written as:

$$x_j(t) = m(t) \cdot x(t) \tag{8}$$

where $x(t)$ the radar signal that is given in eq.1. From the multiplication property of Fourier transform, the frequency spectrum of jamming signal is given by:

$$X_j(f) = X(f) * \sum_{n\ odd}^{\infty} \frac{2}{j\pi n} \delta(f - nf_m) \tag{9}$$

Which can finally be written as:

$$X_j(f) \ = \sum_{n\ odd}^{\infty} \frac{2}{j\pi n} X(f - nf_m) \tag{10}$$

The last equation shows that the modulation of radar signal by a periodic square train is equivalent to frequency shift of radar signal by the odd-harmonics of periodic square train. The spectrum of the output of the matched filter, in this case, can be written as:

$$Y(f) = X_j(f) \cdot H(f)$$

$$= \left[\sum_{n\ odd}^{\infty} \frac{2}{j\pi n} X(f - nf_m) \right] . H(f) \tag{11}$$

Using the ambiguity function, it can be shown that the output of the matched filter due to jammer signal is given as:

$$y(t) \ = \sum_{n=-\infty}^{\infty} a_n u_n(t) \tag{12}$$

where $a_n = 2/j\pi n$, and $u_n(t)$ is given by:

$$u_n(t) = sinc[\pi(nf_m + kt)(T - |t|)] \cdot \left(1 - \frac{|t|}{T}\right) e^{j\pi n f_m t} \tag{13}$$

Based on (12) and (13), it is clear that the output of the matched filter consists of many false target $\{u_n(t)\}$, each with a frequency shift nf_m and a scale factor of a_n as seen by the matched filter.

The number of false targets, N_f, that lead or lag the true target determined by maximum value of n satisfies:

$$f_m \times (2n - 1) \leq 2B \tag{14}$$

which implies,

$$N_f \ = \left\lfloor \frac{(B/f_m) + 1}{2} \right\rfloor \tag{15}$$

where $\lfloor x \rfloor$denotes the nearest integer less or equal x.

Fig.2 shows the false targets at the output of matched filter when radar signal is modulated by a periodic square train. This figure shows that the farther the false target from the true target, the lower its power. In effect, equation (12) shows that the amplitude of the harmonics of periodic square train decrease with n. Thus, jammer has to increase its power.

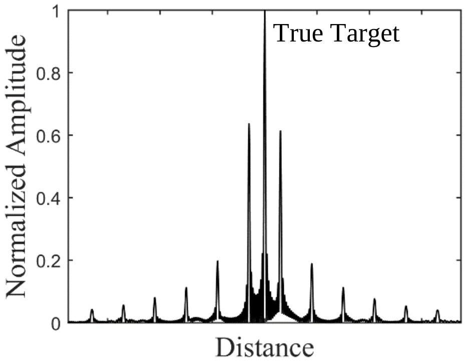

Fig.2 The output of the matched filter when LFM radar signal modulated by a periodic square train

We can generalize equation (8) by using an appropriate modulating signal $m(t)$. For example, if we multiply radar signal by sawtooth signal, instead of periodic square train, we can duplicate the number of false targets and make them closer to each other, as shown in Fig .3, because the sawtooth signal contains odd and even harmonics.

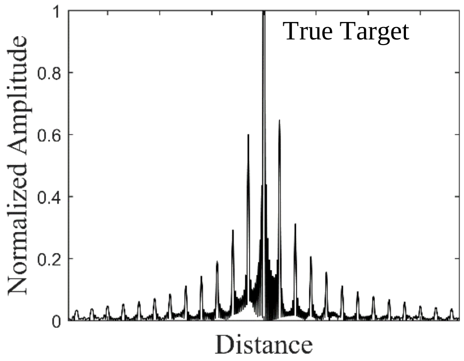

Fig.3 The output of the matched filter when LFM radar signal modulated by a periodic sawtooth signal

IV. Countering frequency Shifting Repeater Jammers

In the previous section, we presented frequency shifting repeater jammers that benefit from the Doppler-range coupling property of LFM signal to generate false targets at the output of the matched filter.

The distribution of these false targets is a function of the jammer parameters and the sweep bandwidth of the LFM waveform. Since this type of repeater jammer does not analyse the radar signal, the radar can counter this jamming and detect the true target by changing the sweep bandwidth (B) of the transmitted LFM waveform. The matched filter is always matched to the transmitted pulse, i.e., the matched filter is altered as the sweep bandwidth of the signal is changed. By changing B, the SNR of the received signal does not change whereas the range resolution does [10].

When the radar changes the sweep bandwidth of the LFM waveform, the relative distances (d) between the true target and the false ones will change. Consequently, false targets appear in different range bins, but the true target remains nearly in the same range bin, because the jammer frequency shift is much bigger than Doppler shift of the true target.

We suppose, for simplicity, that the jammer shifts the LFM waveform by a single frequency f_J. This introduces one false target, at the output of the matched filter, spaced from the true target by $cf_j/2k$.

According to eq. 6, if the radar increases the LFM sweep bandwidth, the false target will be closer to the true one, and it may overlap on it and may be confused with it. Furthermore, this will impose more complexity on the radar receiver. To get rid of these problems, the radar can decrease the sweep bandwidth instead of increasing it. However, this will decrease the radar range resolution because it is related to sweep bandwidth [10]:

$$\Delta R = \frac{c}{2B} \tag{16}$$

The appropriate value of the new sweep bandwidth β that makes the false target to be in a different range bin (one radar range resolution) can be calculated as follows. Let's d_1 and d_2 denote the relative distance between the true target and the false one at sweep bandwidth B and β respectively then we need that:

$$d_2 = d_1 + \Delta R \tag{17}$$

from eq. 6, we have:

$$d_2 = \frac{B}{\beta}\, d_1 \tag{18}$$

by substitution eq. 6 and 18 in eq. 17 we obtain:

$$\beta = \frac{B f_J T}{(\, f_J T + 1)} \tag{19}$$

When the false target is far from the true target, which is the case the jammer usually aims, a small decrease in radar bandwidth is required. However, when the false target is relatively close to the true target, a higher decrease in radar bandwidth is required as illustrated in Fig. 4.

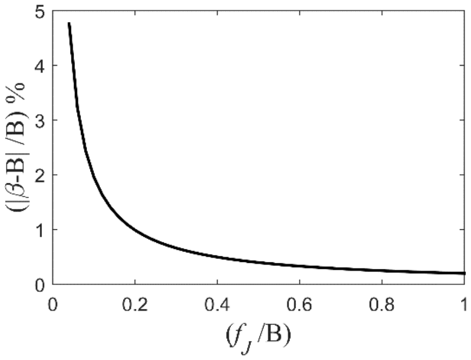

Fig.4 The required decrease in the sweep bandwidth vs. jammer frequency shift relative to sweep bandwidth

As shown in Fig. 5 and Fig. 6, the radar range resolution and the matched filter gain will not degrade too much. Therefore, the proposed countering technique will not degrade radar performance significantly. In Fig. 5, ΔR_B and ΔR_β denote the radar range resolution at sweep bandwidth B and β respectively. And in Fig. 6, G_B and G_β denote the matched filter gain at sweep bandwidth B and β respectively.

Of course the jammer frequency shift is unknown for the radar, so the anti-jamming calculation for the new sweep bandwidth can be considered for the worst case when f_j is very small. According to Fig. 4, Fig. 5 and Fig .6 this means the required decrease in B is about 5% and the degradation of ΔR and G is 5% and 0.8% respectively, and this could be practically acceptable.

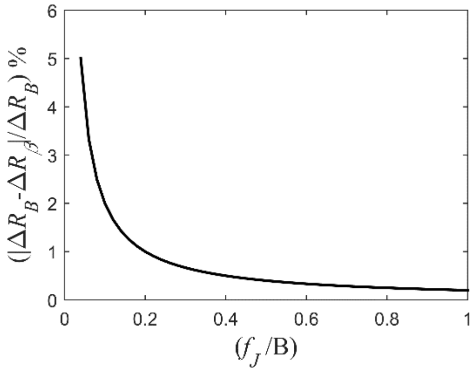

Fig.5 The degradation of radar range resolution vs. jammer frequency shift relative to sweep bandwidth.

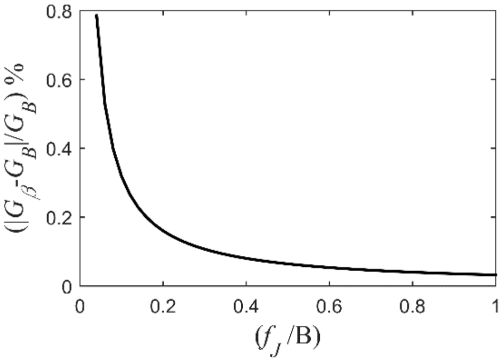

Fig.6 The degradation of matched filter gain vs. jammer frequency shift relative to sweep bandwidth.

Now, we show the effect of changing B by about 5% on the apparent range of the true target. The range offset of the true target due to the Doppler shift equals:

$$R_{of} = \frac{c\, f_d}{2k} \tag{20}$$

The change of R_{of} due to the change of B by 5% equals:

$$\Delta R_{of} = \frac{c\, f_d T}{2B} - \frac{c\, f_d T}{2(0.95B)} \tag{21}$$

$$\Delta R_{of} = 0.05\frac{c\, f_d T}{2B} \tag{22}$$

$$\Delta R_{of} = 0.05 f_d T \cdot \Delta R \tag{23}$$

Practically we have $0.05 f_d T < 1$, then $\Delta R_{of} < \Delta R$ so the apparent range of true target displaced by a fraction of ΔR and can be considered in the same range bin.

Figure 7 shows the block-diagram of the proposed anti-jamming technique which is very similar to the standard radar structure except there is a multiplexer to switch between the two transmitted signals $x_1(t), x_2(t)$. Where $x_1(t)$ is the radar signal, $x_2(t)$ is the anti-jamming radar signal that has a sweep bandwidth equals β, $r(t)$ is the received signal, and $x_T(t)$ is the transmitted signal.

$$x_1(t) = \frac{1}{\sqrt{T}} rect\left(\frac{t}{T}\right) e^{j\pi \frac{B}{T} t^2} \tag{24}$$

$$x_2(t) = \frac{1}{\sqrt{T}} rect\left(\frac{t}{T}\right) e^{j\pi \frac{\beta}{T} t^2} \tag{25}$$

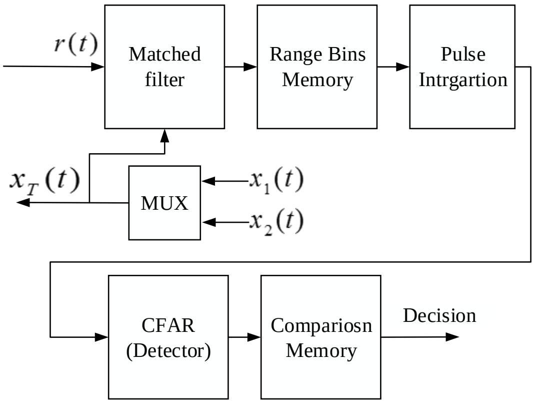

Fig.7 block-diagram of the proposed anti-jamming technique

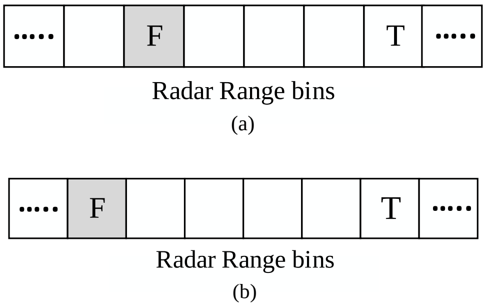

Fig.8 comparison memory (a) transmission of $x_1(t)$ *(b)transmission of* $x_2(t)$

Alternately, the radar transmits M pulses of $x_1(t)$ and M pulses of $x_2(t)$. The detected targets in both cases are stored in different memory locations as shown in Fig.8, where T and F denote true target and false ones, respectively. By comparing the detection results, the true target remains in the same range bin, but the false target appears in the adjacent range bin.

V. Simulation and Results

In the following, we present Matlab simulation results of our proposed approach presented in section 4. We assume $T = 100\,\mu s$, $B = 5\,MHz$, $\Delta R = 30\,m$ and $f_j = 200\,KHz$. The Fig. 9 (solid curve) shows the output of the radar receiver when $B = 5\,MHz$. It can be seen that the false target leads the true target by $d_1 = 600m$ which is consistent with the eq. 6. The same figure (dotted curve) shows the same results when $\beta = 4.76\,MHz$ as eq. 19. It is clear that the true target remains in the same range bin but the false target appears in another range bin. The new relative distance between the true target and false one becomes $d_2 = 630m$ (see eq. 18). Consequently, the true target can be discriminated easily.

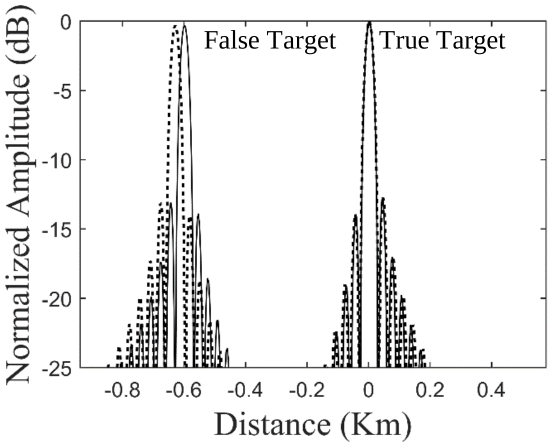

Fig.9 The output of the radar receiver when $B = 5MHz$ (solid curve) and $\beta = 4.76MHz$ (dotted curve)

VI. Conclusion

In this paper, we proposed a new technique to counter frequency shifting repeater jammers against LFM radar. The proposed technique is based on introducing a slight change in the sweep bandwidth of the radar signal. By doing that, the true target at the radar detector output will remain in the same range bin, whereas the false target will appear in other different range bins. Consequently, the true target can be discriminated easily. The simulation results show that the proposed method suffers a slight degradation compared with case where there is no modification nor jamming, as the mathematical analysis has shown. The proposed technique is better than other ECCM techniques that require a high SNR or assume that jamming pulses lag behind the true target echo that is not true in the case of instantly retransmitting the radar pulse after frequency-shifting.

REFERENCES

[1] Yong Yang, Wen-ming Zhang, Jian-hua Yang,”Study on Frequency-shifting Jamming to Linear Frequency Modulation Pulse Compression Radars”, IEEE Wireless Communications & Signal Processing. International Conference 2009, DOI: 10.1109/WCSP.2009.5371387

[2] D. Curtis Schleher, “Electronic Warfare in the Information Age”, ©1999 Artech House, ISBN: 978-0-89006-526-6, pp. 201–229.

[3] Merrill Skolnik,”Radar Handbook 3rd Ed”, McGraw-Hill, 2008. ISBN: 978-0071485470, pp. 24.1–24.64.

[4] David L Adamy, ”EW 104, EW against a New Generation of Threats”, © 2015 *ARTECH HOUSE*. ISBN 13: 978-1-60807-869-1, chapter 4.

[5] Hai Deng,”Polyphase Code Design for Orthogonal Netted Radar Systems”, IEEE TRANSACTIONS ON SIGNAL PROCESSING, VOL. 52, NO. 11, NOVEMBER 2004, DOI:10.1109/TSP.2004.836530

[6] Chen, Wenwu, Zhengyu Cai, Rushan Chen, and Zhao Zhao. "Optimizing polyphase sequences for orthogonal netted radar systems." Journal of Systems Engineering and Electronics 23, no. 4 (2012): 529-535. DOI:10.1109/JSEE.2012.00067

[7] Nadav Levanon, Eli Mozeson, “RADAR Signals”, Wiley Publication, 2004. ISBN: 978-0-471-66307-2, pp. 57–60.

[8] Hugh Griffiths, Christopher Baker, David Adamy, “Introduction to Airborne Radar 3rd Edition”, © IET 2014. ISBN: 978-161353022, pp. 509–519.

[9] De Martino, Andrea. Introduction to Modern EW Systems. © 2012 by Artech House. ISBN: 978-1-60807-207-1

[10] BASSEM R MAHAFZA, “Radar Systems Analysis and Design Using MATLAB 3rd edition”, © 2013 Taylor & Francis Group, LLC, ISBN: 978-1439884959, pp. 238–239.