International Journal of Enhanced Research in Science Technology & Engineering, ISSN: 2319-7463
Vol. 4 Issue 6, June-2015, pp: (111-117), Impact Factor: 1.252, Available online at: www.erpublications.com

Improvement of radar's distance resolution and decryption of PN code

Sufian H. Ali
Electrical Engineering Department, College of Engineering, Tikrit University, Iraq

Abstract: Distinguishing between adjacent targets is a major problem in radar system. Two targets located in the detection area of radar appear as one point on the radar screen if the distance between the two adjacent targets is less than the distance resolution of radar and the angle between these adjacent targets is less than the angle resolution of the radar.

This paper discusses how to increase the distance resolution using the spread-spectrum signal with pseudo noise (PN) code. This code has good specifications in terms of achieving high compression of the pulse and good protection from interference. Another feature of PN code is its security property because the code cannot be easily decrypt and the only way to decrypt is discussed in this work.

MATLAB is used as a simulation tool to evaluate the pulse compression of the received signal. It is also used to study the possibility of decryption the Pseudo-Noise (PN) code by illegal person.

Keywords: Radar, Resolution, Pulse Compression, PN code, Gold code.

Introduction

Resolution means the ability of detection the neighboring targets. We explain the resolution by example, if the distance resolution 1.5km,the angle resolution 2o and the difference distance and angle between the neighboring objects 1km and 1.5o, respectively, cannot distinguish two targets separately and it appears on the screen as one spot(bright point) [1][2]. Signal to Noise Ratio increased in the receiver using signal compression by correlation and realized an increase in the distance resolution [2]. PN code with good specifications in terms of achieving high compression of the pulse and good protection from interference [3] [4].

Wide transmitted pulse has high energy and narrow frequency band. Increasing the width of frequency spectrum may be doing by modulation inter wide transmitted pulse. Increasing width of frequency spectrum gets the compression of the pulse in the receiver. Thus the resolution become higher on the one hand and on the other hand increases the energy of the transmitted pulse [2].The two poplar kind method used in the pulse inter modulation are linear frequency modulation and phase shift keying (PSK) modulation with PN sequence as a modulating signal[4][5] .

Radar Principle

The function of the radar is the measure of distance and direction (angle) for targets that located within the detection area of radar. The fundamental components of the radar are antenna, TR switch, transmitter, receiver, synchronizer and indicator [4]. Synchronizer is used to synchronize all components of the radar system. The transmitter generate the video pulses and modulate those pulses by frequency carrier to get the radio pulses with high frequency. Pulses are then amplified in the transmitter and delivered to the antenna. The receiver is frequency select and amplifies weak radio pulses coming from the antenna through TR switch. These pulses are detected in the receiver and delivers to circuits measuring range and direction. Antenna used to transmission (radiation) pulses of high-power radio frequency in space and receives the weak radio pulses after reflection from the targets(echo signal)[1][2]. The basic block diagram of radar system is shown in figure1[1].

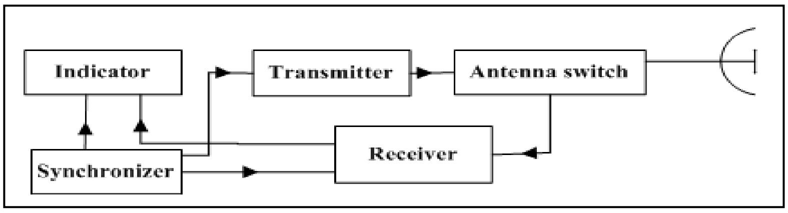

Figure 1: Radar block diagram

International Journal of Enhanced Research in Science Technology & Engineering, ISSN: 2319-7463
Vol. 4 Issue 6, June-2015, pp: (111-117), Impact Factor: 1.252, Available online at: www.erpublications.com

Radar equation is that in which it could find distance of target and written as follows:

$$R_{max} = \sqrt[4]{\frac{P_t \times G^2 \times \lambda^2 \times \sigma}{(4\pi)^3 \times S_{min}}} \times \frac{1}{L_s} \qquad (1)$$

Where R_{max} represents the maximum detection range, P_t is the transmitted signal power, G is the antenna gain, λ is the wavelength , radar cross section is σ, the sensitivity (minimum detectable signal) of the receiver is represented by S_{min}, and L_s is the loss resulting from the impact of all atmosphere effect, polarization mismatch and other factors (Practically $1 < L_s \leq 2$)[1] [2] [4].

Distance Resolution

Distance resolution depends on the transmitted pulse width and calculated by the following formula:

$$\delta = (t_p \times C) / 2 \qquad (2)$$

Where t_p is the pulse width, and C is the Speed of light.

Figure 2 illustrates the distance resolution for three adjacent targets: δ greater than R1 and less than R2 so it cannot distinguish targets T1 and T2 and flashed on the screen as one target. Target T3 appears on the screen as the target independently because R2 is greater than δ. Ambiguity function for signal f(t) is defined as the modulus squared of its two dimensional correlation function , i.e.,

$$|\psi(\tau, f_d)|^2 = \left|\int_{-\infty}^{\infty} f(t) f^*(t-\tau) e^{j2\pi\mu t} dt\right|^2 (3)$$

τ- time shift and μ- frequency shift. Ambiguity function used to determine the distance resolution and how the effect of frequency Doppler decrease this resolution.

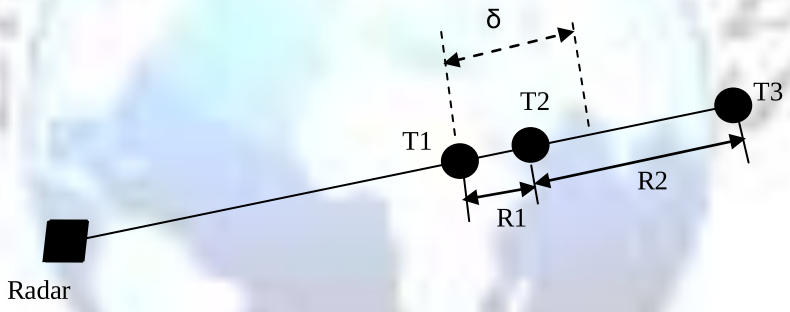

Figure 2: Distance resolution

Pulse Compression

Wide pulse has narrow frequency bandwidth. Increasing the width of frequency spectrum may be accomplished by a liner inter-modulation of wide transmitted pulse. Increasing width of frequency spectrum means the compression of the pulse at the receiver. Thus the resolution become higher and in the same time the energy of transmitted pulse is increased [3].

First method for pulse compression is the inter-linear frequency modulation for transmitted pulse. The second method of pulse compression is the phase shift keying inter modulation of transmitted pulse with PN code. This method is modern and better than the pulse inter-linear frequency modulation method.

Proposed Method

Phase Shift Keying (PSK) Signal with PN code

PSK signal is a long pulse containing a train of short pulses. The phase of these short pulses variable and usually takes two values: zero or 180 degrees [1][3][5][6].Every short pulse (called the elements of the long pulse) with length equal to ζe. Phase of elements change according to selected code. Long pulse is transmitted with high energy. In the receiver the long pulse is compressed using matching filter or correlation circuit. Pulse width after the compression is equal to the width of the single element ζe and the distance resolution increasing as in the following relationship [1] [2] [4]:

$$\delta = \frac{C \times \zeta_e}{2} \qquad (4)$$

Compression coefficient is equal to the number of elements in the long pulse (Ne = Q_{com}). One of the codes used in radar is Barker code which is characterized with low side-lobes for the correlation function (autocorrelation function) but the length is limited no more than 13 elements in the pulse [2].PN code, is widely used in radar and communication with a spread spectrum. This binary code modulates the high frequency carrier and the type of modulation is PSK. PN code with statistical properties similar to the properties of statistical noise, but they differ from the noise as repeating itself periodically. Spread-spectrum signals with wide spectrum, as well as be in the form of special sequence code. After the signal detection at the receiving, the correlation process is occurred for the purpose of pulse compression. Correlation functions for the pseudo-noise sequence similar to the correlation function of white noise. Ambiguity function of these signals has a one major top in the frequency and time domains (μ, ζ) [7]. The height and width(in time domain) of this top are equal to Ne (Ne- number elements of the code) and ζe respectively. Energy after the compression signal (after correlation) is equal to the energy of all elements of the sequence (Ne). The level of side-peaks of correlation function is not more than $\frac{1}{\sqrt{N_e}}$. The length of PN sequence is calculated by the following relationship:

Ne = 2n-1, n = 1, 2, 3, ... (5)

Where, n is the number of elements for PN generator (number of taps).

The number of one's almost equal to the number of zero's. For example: 0 0 0 111 101 011 001.

Decrypt of PN sequence

PN Code can be decrypt by knowing a part of the binary digits in the code sequence. This part should be equal twice the number of taps. For example, take the generator with four taps (flip-flop).

The outputs of this taps generators are as follows:

Q1= q1(1) q1(2) q1(3) q1(4) q1(5) q1(6) q1(7) q1(8) q1(9) q1(10) q1(11) q1(12) q1(13) q1(14)q1(15).

Q2= q2(1) q2(2) q2(3) q2(4) q2(5) q2(6) q2(7) q2(8) q2(9) q2(10) q2(11) q2(12) q2(13) q2(14) q2(15).

Q3= q3(1) q3(2) q3(3) q3(4) q3(5) q3(6) q3(7) q3(8) q3(9) q3(10) q3(11) q3(12) q3(13) q3(14) q3(15).

Q4 = q4(1) q4(2) q4(3) q4(4) q4(5) q4(6) q4(7) q4(8) q4(9) q4(10) q4(11) q4(12) q4(13) q4(14) q4(15).

Suppose that the initial states are as follows: Q1 =1 and Q2 =0 and Q3 =, and Q4 =1. The outputs will be:

Q1 = 1 0 1 1 1 1 0 0 0 1 0 0 1 1 0,

Q2 = 0 1 0 1 1 1 1 0 0 0 1 0 0 1 1,

Q3 = 1 0 1 0 1 1 1 1 0 0 0 1 0 0 1,

Q4 = 1 1 0 1 0 1 1 1 1 0 0 0 1 0 0.

Taking the output from one of these flip-flops (i.e. Q3), we can generate the following two matrices:

$$G_1 = \begin{bmatrix} q_3(5) & q_3(4) & q_3(3) & q_3(2) \\ q_3(6) & q_3(5) & q_3(4) & q_3(3) \\ q_3(7) & q_3(6) & q_3(5) & q_3(4) \\ q_3(8) & q_3(7) & q_3(6) & q_3(5) \end{bmatrix}$$

$$G_2 = \begin{bmatrix} q_3(4) & q_3(3) & q_3(2) & q_3(1) \\ q_3(5) & q_3(4) & q_3(3) & q_3(2) \\ q_3(6) & q_3(5) & q_3(4) & q_3(3) \\ q_3(7) & q_3(6) & q_3(5) & q_3(4) \end{bmatrix}$$

Substitution of the Q3's outputs in the above matrices (: -1 represents zero), we get:

$$G_1 = \begin{bmatrix} 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

$$G_2 = \begin{bmatrix} -1 & 1 & -1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{bmatrix}$$

Then we can obtain the matrix A by matrix division, such that:

$$A = \frac{G_2}{G_1} = \begin{bmatrix} -1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

As we mentioned earlier for every clock pulse the state of flip-flops changes. We represent the status of flip-flops for any clock pulse by a matrix with one dimension, and then by multiplying this matrix with the matrix A we get the matrix of one dimension with elements of the new status of flip-flops for the coming clock pulse. Also by multiplying the last matrix with the matrix A we get other new matrix of one dimension. This latter represents the new status of flip-flops. For example, if we take the status for the tenth clock pulse, the matrix with one dimension:

S10 = [q1 (10), q2 (10), q3 (10), q4 (10)] = [1, -1, -1, -1] .

Multiplying it with matrix A, we get:

S11 = A * S10 = [-1, 1, -1, -1], and so on.

From this process we can obtain all elements (bits) of PN code generator. Also we can get the pseudo-noise sequence from any flip-flop output of generator. At the receiver side we can decrypt all the elements of successive pseudo-noise sequence if the eight elements of a row (twice the number of flip-flops) are known before we start analysis using the method above. This method becomes more useful especially when the number of flip-flops is large. For example, if the number 'n' is 10 then by knowing 20 bits before starting the of decrypt process of the sequence, we can find(decrypt) all the elements (1023bits) of the sequence.

Sequence Analysis using MATLAB

MATLAB program consists of two parts, as follow:

A. First part of MATLAB program used to design a PN generator consists of seven flip-flops to generate two PN sequences with length of 127 bits for each sequence .We get two sequences first from seventh flip-flop and second from sixth flip-flop of generator. A third sequence is obtained by summation of the first and the second sequences. This third sequence is called gold code. Also this part of program included a correlation function of the sequences of the three above as in the Figure 3.

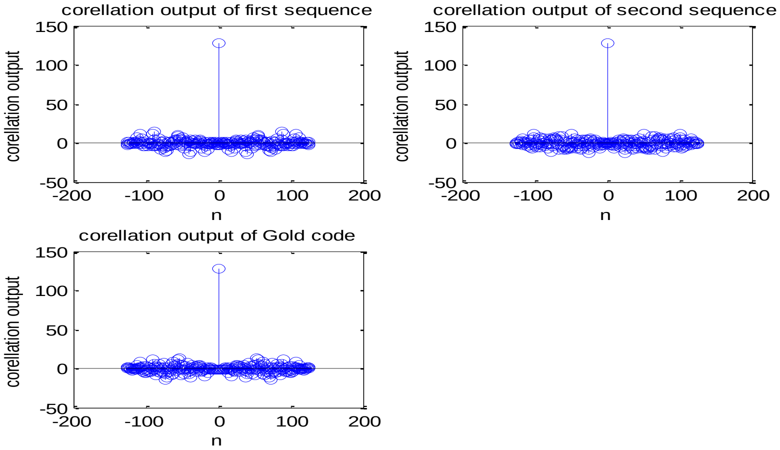

Figure 3: Correlation of PN code

International Journal of Enhanced Research in Science Technology & Engineering, ISSN: 2319-7463
Vol. 4 Issue 6, June-2015, pp: (111-117), Impact Factor: 1.252, Available online at: www.erpublications.com

From Figure 3 is clear that the correlation function has one center peak is equal to 127 for every sequence and side lobes(peaks) no higher than 10% with respect to center peaks. Make the threshold level higher than the largest top of side lobes to detect only the center peak. This mean the pulse is compressed by 127 times and the distance resolution increased by 127. Doppler effect cause a shift of the received carrier frequency and the correlation function is distorted. The Doppler effect in this work not discussed. The ambiguity diagram in Figure 4 for pulse modulated by PN code with length 31 bits (elements) shows the main peak and side peaks. Main peak located in the center when time delay and frequency shift equal zero.

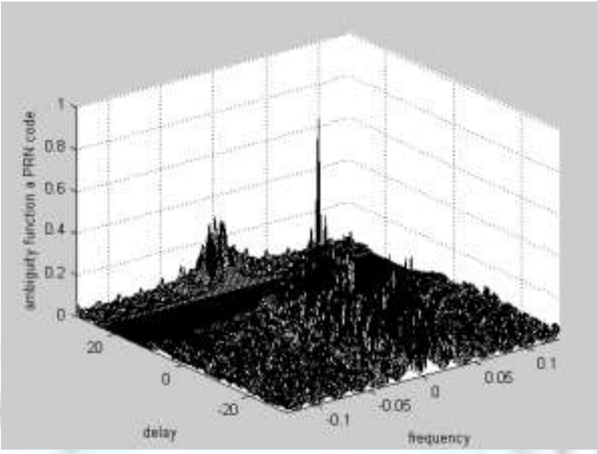

Figure 4: Ambiguty function of PN code with PSK

Figure 5 shows the ambiguity diagram in plan when frequency shift equal zero.

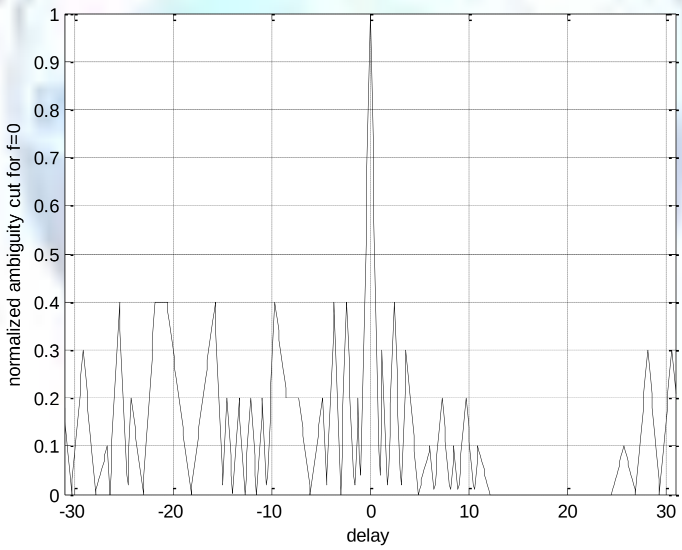

Figure 5. Zero Doppler cut for ambiguity function

B. Second part of the program particularly the decryption and analysis of PN sequence length of 127 bit. In that program the simulations to decrypt the sequence(127 bit) after knowing the 14 digits successive digits from the sequence with 127 bit.

The steps of decryption as follows:

Step 1: First PN sequence generation length 2^7-1 = 127 bits as follows: PN1 = -1 1 -1 1 -1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 1 -1 1 1 1 1 1 -1 -1 1 1 1 1 -1 1 -1 1 1 1 -1 -1 -1 -1 1 1 -1 1 1 1 -1 1 -1 -1 1 1 -1 -1 -1 1 -1 1 -1 1 1 -1 -1 -1 -1 -1 1 -1 1 1 11 -1 -1 -1 1 1 1 -1 1 1 -1 1 1 -1 -1 1 -1 -1 1 -1 1 -1 -1 1 -1 -1 -1 -1 1 -1 -1 1 1 1 -1 -1 1 -1 1 1 -1 1 -1 -1 -1 1 -1 -1 -1 1 1 -1 -1 1 1 -1 1

Step 2: Generate matrices G1 and G2 and A as follows:

$$G1=\begin{bmatrix} -1 & -1 & -1 & -1 & 1 & -1 & 1 \\ -1 & -1 & -1 & -1 & -1 & 1 & -1 \\ -1 & -1 & -1 & -1 & -1 & -1 & 1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ 1 & -1 & -1 & -1 & -1 & -1 & -1 \\ 1 & 1 & -1 & -1 & -1 & -1 & -1 \\ 1 & 1 & 1 & -1 & -1 & -1 & -1 \end{bmatrix}$$

$$G2=\begin{bmatrix} -1 & -1 & -1 & 1 & -1 & 1 & -1 \\ -1 & -1 & -1 & -1 & 1 & -1 & 1 \\ -1 & -1 & -1 & -1 & -1 & 1 & -1 \\ -1 & -1 & -1 & -1 & -1 & -1 & 1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ 1 & -1 & -1 & -1 & -1 & -1 & -1 \\ 1 & 1 & -1 & -1 & -1 & -1 & -1 \end{bmatrix}$$

$$A=\begin{bmatrix} -1 & 0 & 0 & 1 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

Step 3: Using the above procedure (Sn=Sn-1*A) we find (decrypt) the same last PN sequence if successive 14(2n) bits of this sequence is known as ,

PN2 = -1 1 -1 1 -1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 1 -1 1 1 1 1 1 -1 -1 1 1 1 1 -1 1 -1 1 1 1 -1 -1 -1 -1 1 1 -1 1 1 1 -1 1 -1 -1 1 1 -1 -1 -1 1 -1 1 -1 1 1 -1 1 1 -1 -1 -1 -1 -1 1 -1 1 1 1 1 -1 -1 -1 1 1 1 -1 1 1 -1 1 1 -1 -1 1 -1 -1 1 -1 1 -1 -1 1 -1 -1 -1 -1 1 -1 -1 1 1 1 -1 -1 1 -1 1 1 -1 1 -1 -1 -1 1 -1 -1 -1 1 1 -1 -1 1 1 -11.

Successive new PN2(at the receiver side after decrypt) is the same PN1 sequence, indicating that the PN code of length 127 bit can be decrypt after knowing 14 Successive bits generated(transmitted) sequence.

From the above we see the following:

- The PN sequence can be decrypt at the receiver side only after knowing the part of this sequence ,which the length of this part equal to twice the number of flip-flops of the PN generator.
- The use of PN signal gives high protection from noise and interference because the spread spectrum of signal is very wide(high process gain).
- After modulating the high frequency carrier by PN signal, the spectrum of modulated signal is spreading over a wide range of frequencies so it cannot be sensitive this signal when the code is not knowing of that signal.
- The use of PN signal gives high resolution between the adjacent objects in the case of measuring the distance of objects by radar.
- The use of PN signals in radar helps to distinguish objects that are detected by radar because of the pulse is shorted by compression, which provides high accuracy in the measurement of parts of the object, which helps determine the components of the this object.

Conclusion

In this paper , a compression of pulse using pseudo noise(PN) binary code is proposed to increase the distance resolution between objects by using a good correlation property of PN code. Also a PN code easy to use and provides high signal to noise ratio to get good detection of objects .Also in this paper is analyzed the method of decryption the PN.

References

[1]. Skolnik, M., "Introduction to Radar systems", McGraw-Hill, New York, 1982.
[2]. Skolnik.M., "Radar Handbook", 2nd editor, McGraw-Hill, New York, 1990.
[3]. J. S. Chitode, "Digital Communication", Second Revised Edition, Technical publications pune, 2003.
[4]. Van den Enden, AWM Discrete time signal processing.NAMVerhoeckx, prentice-Hall, 1989.
[5]. Bassem R. Mahafza, "Radar systems analysis and design using Matlab",2000.
[6]. Carpentier, M. H." Principles of modern radar systems", Artech House, Norwood, 15 Feb. 2009.
[7]. Herbert Taub and Donald L. Schilling, "Principles of communication systems", Tata McGraw-Hill Publishing company Limited, New Delhi, 2003.
[8]. Jing liu, Huichang Zhao and Yanping Zhu,"The ambiguity function of PN-chirp pulse signal".IEEE,2011.