

# Application of Modified Chaotic Sine Map in Secure Communication

Bibhakar Saha

Dept. of ECE, GITAM Institute  
of Technology  
Visakhapatnam, India

Sai Tej Malasani

Dept. of ECE, GITAM Institute  
of Technology  
Visakhapatnam, India

J. B. Seventline

Dept. of ECE, GITAM Institute  
of Technology  
Visakhapatnam, India

## ABSTRACT

In the recent years, a lot of research has been done in the field of covert chaotic communication involving many known chaotic maps and the results have been very promising. In this paper the generation of binary sequence using modified chaotic sine map is discussed. The auto correlation and the cross correlation properties of the generated sequence is observed. Also, the BER of chaotic shift keying system is analyzed to check the feasibility of the generated sequence in communication purpose. The possibilities of using the generated binary sequences in radar pulse compression techniques is also explored and Peak Side lobe Ratio (PSLR) obtained is compared with other existing binary sequences.

## General Terms

Modified sinusoidal iterator, secure communication technique, Pulse compression

## Keywords

CSK, Chaotic sin map, PSLR, BER

## 1. INTRODUCTION

In a conventional radio communication mechanism the transmitted signal is transmitted in a narrow frequency band. The high power spectral density has its own disadvantages which includes selective fading, interference from other radio channels etc. Chaos communication is used to overcome such problems. Chaos communication systems have the characteristics such as non-periodicity, wide-band, and non-predictability [1]. In chaos communication systems, binary sequences generated using chaotic maps called chaotic sequences are used. These maps are simple polynomial maps or simple nonlinear dynamic equations which exhibits simple chaotic behavior. Also, chaos communication system is decided by initial conditions of equation, and it has sensitive characteristic depending on the initial condition, because chaos signal is changed to different signal when initial condition is changed [2][3]. Because of these characteristics, the security of chaos communication system is superior to digital communication system. Chaotic sequences increases the bandwidth of the transmitted signal greater than the required bandwidth for the signals transmission. The characteristics of an ideal code or a sequence that is required to spread the signal involves properties that includes zero or near zero cross correlation, impulse like auto correlation, codes need to be wideband to be able to spread the signal and should be easy to generate. The added advantages of using chaotic spreading sequences are that an infinite number of spreading sequences exist and that the spread signal is less vulnerable to interception [4].

In this paper, a modified sine map for Chaotic shift keying (CSK) spread spectrum communication is proposed and is compared with the existing sine map and logistic chaotic

maps. Chaos users evaluate the BER performance according to chaos modulation system [5] [6]. The proposed new chaos map has a better BER performance according to analysis of probability density function.

In pulse compression technique of pulse radars, the transmitted signal or carrier is frequency or phase modulated and the received signal is processed in the receiver by the matched filter which is used to increase the range resolution as well as the signal to noise ratio [7]. A sequence or code defines the manner in which the carrier is modulated in the phase coded pulse compression technique. The autocorrelation property which is the compressed output of the matched filter and the Peak Side lobe Ratio (PSLR) is an essential criteria in determining the performance of a range resolution pulse radar. The PSLR is obtained from the auto-correlation function. Binary barker sequences are generally used for radar pulse compression, but, they exist only up to a length of 13 with a PSLR of -22.3 dB [8]. Since longer length sequences with low PSLR values are required in some applications, binary chaotic pulse compression codes generated using chaotic logistic map was reported recently [9]. The advantage of this code over the other existing binary codes are they can be generated easily for any length.

In this paper, the application of another chaotic map called modified sinusoidal iterator used to generate binary pulse compression codes is discussed. The performance analysis of the generated code is compared with other existing codes.

## 2. CHAOS SEQUENCE

### 2.1 Sinusoidal Iterator

A simple sinusoidal iterator is studied in this section [10]. The simplified sinusoidal iterator is represented by equation (1)

$$x_{n+1} = A * \sin[\pi * x_n] \quad (1)$$

It generates chaotic sequence in (0, 1).

### 2.2 Modified Sinusoidal Map

The modified sinusoidal map is a scaled and shifted version of equation (1)

$$y_{n+1} = 2 * (x_{n+1} - 0.5) \quad (2)$$

where,  $y_{n+1}$  is the output chaotic sequence and  $A=1$ .

Figure (1), gives a two-dimensional phase diagram of the modified sinusoidal map for initial value of 0.1, and it clearly shows the quadratic curve of the difference equation which also exists for other famous maps such as logistic map, henon map etc.. Scaling and shifting the chaos map will not change the chaotic properties of the generator but will provide an increase in the signal power ( $P_s$ ) and a decrease in the variance ( $\sigma^2$ ) which is used to determine the BER [11].

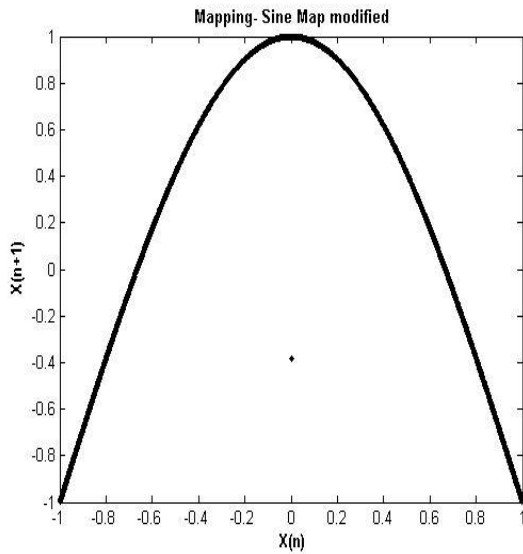


Figure 1. Two- dimensional phase diagram

The generated sequence largely depends on the initial conditions, as we can clearly observe from figure 2, the chaotic behavior of the map with initial conditions  $x_0 = 0.1$  and  $x_0 = 0.0999$  vary a lot resulting into generation of sequences with zero or near zero cross-correlation property.

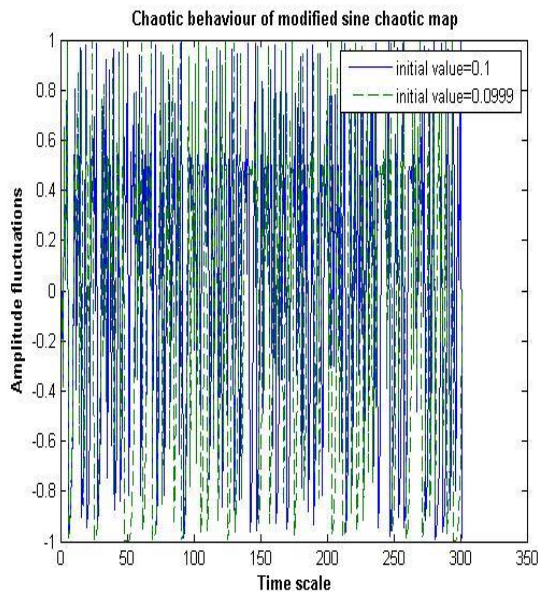


Figure 2. Chaotic behavior of modified sine map of sequence length 300 with initial conditions  $x_0 = 0.1$  and  $x_0 = 0.0999$ .

### 2.3 Generated Binary Sequence

The generated random sequence using equation (2) is quantized into two defined levels based on the threshold level 'a' (here  $a = 0$ ) to obtain the binary sequence. Since the sequences are generated using chaotic functions, they exhibit randomness properties.

The auto-correlation property of the generated binary sequence of length 100 using modified chaotic signal using equation (3) [12] is shown in figure 3. The impulse like nature

of the auto correlation function explains why the power spectrum of the chaotic signal exhibits a wideband feature. These wideband and noise like features of a chaotic signal are particularly good for spread-spectrum communications.

$$r(k) = \sum_{i=0}^{N-1-k} y_i y_{i+k} \quad (3)$$

where  $k = 0, 1, 2, \dots, N - 1$ .

The cross-correlation property of the generated binary sequence of length 100 using equation (4) [12] is observed in figure 4. The cross-correlation values are near zero and hence these sequences can be used in multipath environments and used in spread spectrum communication [13] [14].

$$r(k) = \sum_{i=0}^{N-1-k} z_i y_{i+k} \quad (4)$$

where  $k = 0, 1, 2, \dots, N - 1$ .

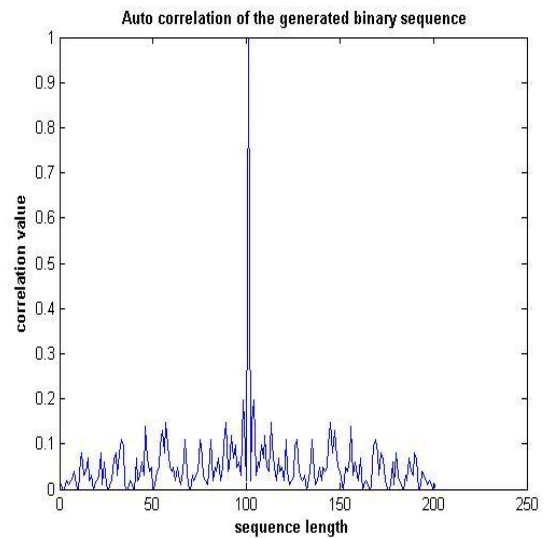


Figure 3. Auto-correlation pattern of sequence of length 100

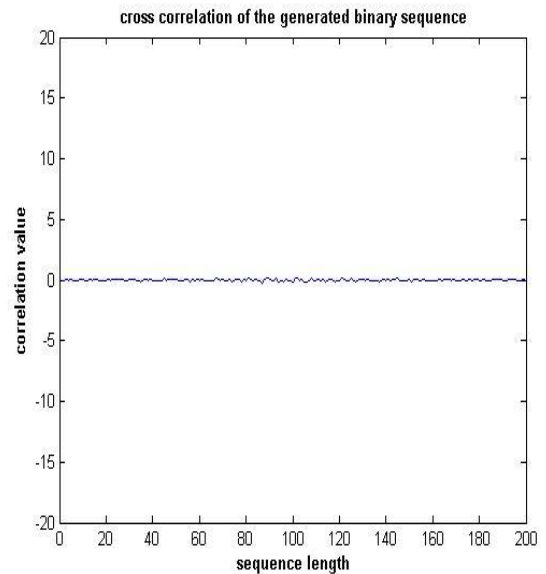


Figure 4. Cross-correlation pattern of sequence of length 100

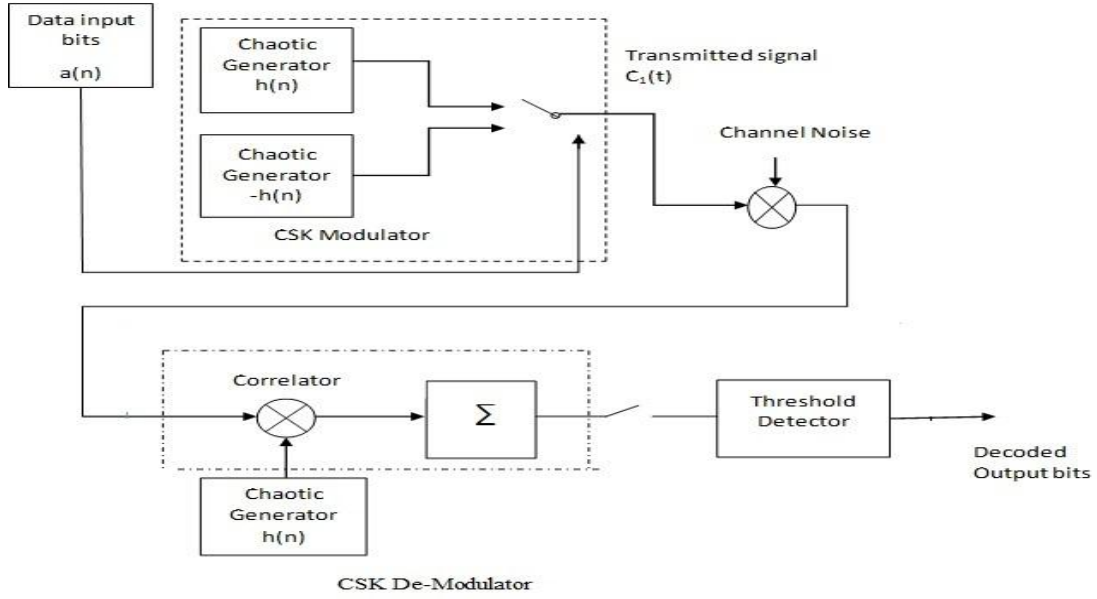


Figure 5. Modulator and demodulator block diagram for chaos shift keying

### 3. CHAOS SHIFT KEYING

In contrast to a conventional digital modulation scheme, where the transmitted symbols are mapped to a finite set of periodic waveform segments for transmission over a channel, every transmitted symbol in a chaotic modulation scheme is mapped to a non-periodic set of sequences popularly known as chaotic sequences [15]. The cross correlation between the non-periodic sequences behave like random white noise.

In chaos shift keying the binary information bits are transmitted using a pair of chaotic signals ( $h_1$  and  $h_2$ ) of different bit energies [16]. These binary chaotic signals are generated using the chaotic sequence generator ( $h(n)$ , as shown in figure 5) using different initial conditions.

The performance of the CSK system in an AWGN environment has been derived by Francis C. M. Lau et al. in [17]. The correlator output for the  $n^{\text{th}}$  bit is given by

$$y_n = \sum_{k=2\beta(n-1)+1}^{2\beta n} r_k h_k \quad (5)$$

Where,  $r_k = h_k + \eta_k$  is the received signal in an AGWN environment and  $\eta_k$  is an additive Gaussian white noise. The number of chaotic symbols transmitted for one data bit is dependent on the spreading factor ( $2\beta$ ) [11]

$$y_n = \alpha_n \sum_{k=2\beta(n-1)+1}^{2\beta n} h_k^2 + \sum_{k=2\beta(l-1)+1}^{2\beta n} \eta_k h_k \quad (6)$$

The BER as derived in [6] [11] is given as:

$$BER_{CSK} = \frac{1}{2} \operatorname{erfc} \left( \frac{1}{\sqrt{\frac{4\beta \sigma^2 + N_0}{E_b^2} + \frac{N_0}{E_b}}} \right) \quad (7)$$

Where  $E_b = 2\beta P_s$ . From equation (7), the BER can be improved by reducing the variance of  $h_k^2$ , increasing the spreading factor ( $2\beta$ ), or increasing the signal power  $P_s$  [11].

To obtain the BER performance for each sinusoidal map, the signal power ( $P_s$ ) and the variance ( $\sigma^2$ ) are either calculated from their probability density function (pdf) or numerically using MATLAB. The probability density function for this system is not provided in the literature and hence we use MATLAB for numerical analysis. The theoretical BER can be calculated using equation (5). The BER performances for this modified sinusoidal map when compared to the existing maps such as simple and modified logistic map are shown in Figure 6(a-e).

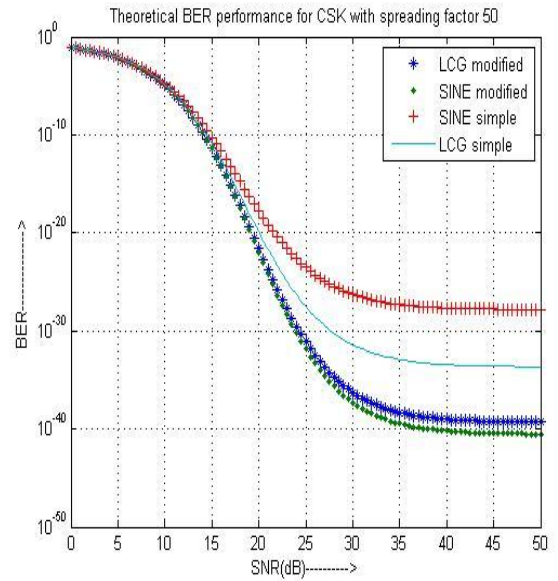


Figure 6(a). Theoretical BER performance of CSK in AWGN Channel with SF=50.

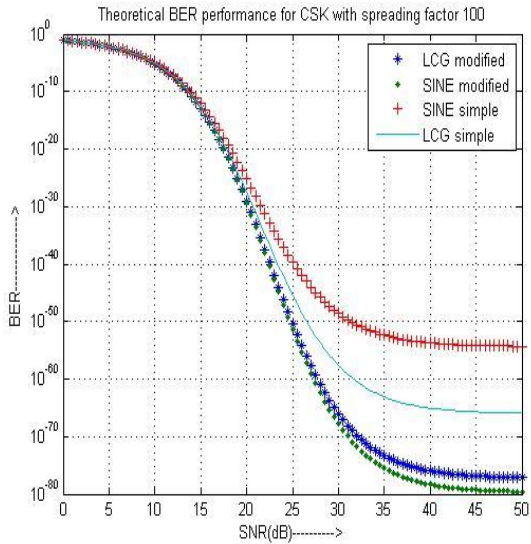


Figure 6(b). Theoretical BER performance of CSK in AWGN Channel with SF=100.

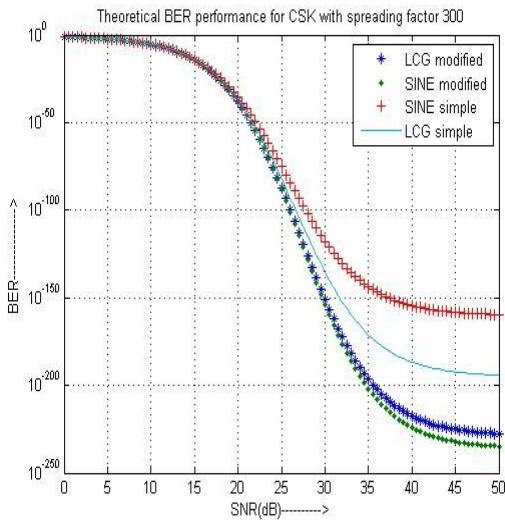


Figure 6(c). Theoretical BER performance of CSK in AWGN Channel with SF=300.

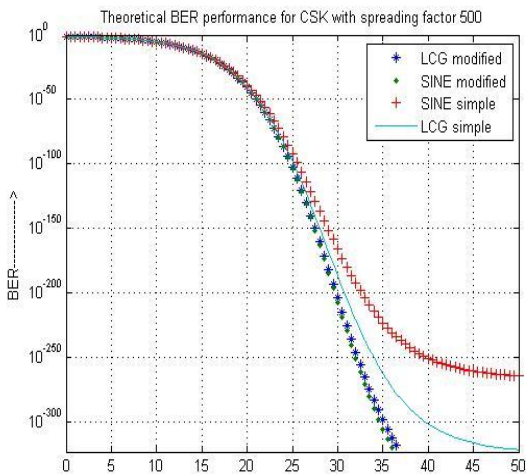


Figure 6(d). Theoretical BER performance of CSK in AWGN Channel with SF=500.

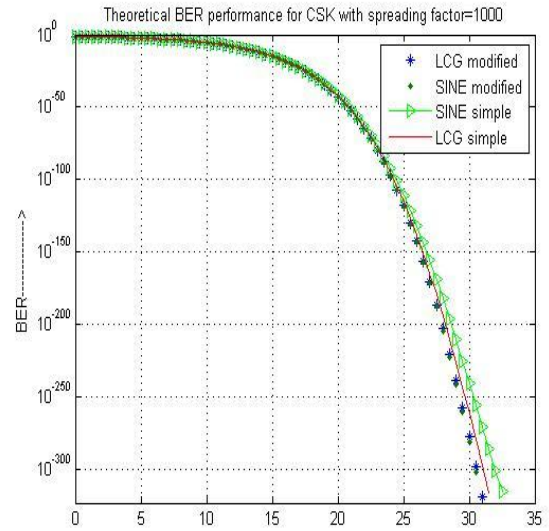


Figure 6(e). Theoretical BER performance of CSK in AWGN Channel with SF=1000.

We observe that the modified sine map will provide better BER performance for higher SNR values when compared to other three maps. At lower SNR values it proves to be an alternative to the logistic map. The extra BER is obtained at the cost of the extra bifurcation parameter which is used to enhance security in logistic maps and is not present in the sinusoidal iterator. However, when the spreading factor reaches the higher value ranges (larger than 500), the BER performance curves of the four maps approach each other.

#### 4. APPLICATION IN RADAR SYSTEMS

In this section the performance analysis of the generated chaotic binary sequence for pulse coded radar pulse compression is discussed. The autocorrelation pattern of the coded sequence has been already explored in the above sections and has been found to be good.

##### 4.1. Peak Side Lobe Ratio

The Peak Side Lobe Ratio is defined from the autocorrelation pattern  $r(k)$  as the ratio of the peak side lobe amplitude to the main lobe peak amplitude and is expressed in decibels. It is given by

$$PSLR = 20 \log_{10} \frac{\text{Max}(r(k))}{r(0)} \quad (8)$$

where  $k \neq 0$

$r(k)$  is defined as the auto-correlation value of the sequence generated using equation 3.

The PSLR values that have been obtained using the modified chaotic map and other existing maps for various lengths ranging from 10 to 5000 is tabulated in Table.1. This is further explained using the figure (7), where the samples (i.e. PSLR) values have been taken from 10 to 1000 at an interval of 10. Comparing the three different mapping methods, the performance of codes generated by all the three maps are good but the modified sine map provides better PSLR in patches when compared to the traditional sine map and logistic map. We can also observe that the PSLR decreases with the length of the sequence.

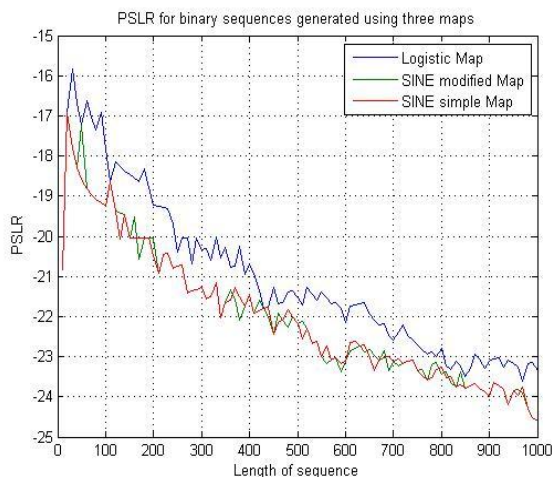
**Table 1. Comparison of PSLR of binary sequences**

Length of sequence	Peak side lobe ratio (in dB)		
	Logistic Map	Sine Map	Modified Sine Map
10	-20.8279	-20.8279	-20.8279
20	-16.9020	-16.9020	-16.9020
30	-15.8478	-17.7860	-17.7860
50	-17.2494	-18.5884	-17.2494
100	-17.8076	-19.2586	-19.2586
150	-18.4741	-20.0577	-20.0577
200	-19.2155	-20.4888	-20.0433
300	-20.3234	-21.2719	-21.2719
400	-20.6989	-21.4333	-21.4333
500	-21.5318	-22.1755	-22.1755
1000	-23.3585	-24.5916	-24.5916
2000	-25.4373	-25.9385	-25.9385
3000	-26.8745	-27.1999	-27.0683
4000	-27.9610	-28.3495	-28.2367
5000	-28.7797	-28.7321	-28.7321

## 5. CONCLUSION

The performance of binary sequences generated using modified sine map was studied for secure communication applications. It is therefore concluded that these sequences can be used for secure communication in chaotic shift keying technique as the necessary conditions such as good auto correlation, good cross correlation and a better BER is satisfied. Sequences of lengths greater than 100 with good PSLR proves that these sequences can be used to increase the signal to noise ratio and easy detection of targets in pulse radar system.

This work can be further extended by investigating the possibilities of using the proposed modified map for various other applications which includes UWB communication, Image processing and other communication techniques.



**Figure 7. Comparison plot of PSLR of binary sequences**

## 6. REFERENCES

[1] Sushchik, Mikhail, Lev S. Tsimring, and Alexander R. Volkovskii. "Performance analysis of correlation-based communication schemes utilizing chaos." *Circuits and Systems I: Fundamental Theory and Applications*, IEEE Transactions on 47.12 (2000): 1684-1691.

[2] Hong, Sung Il, and Eun Young Jang. "FPGA implementation of digital transceiver using chaotic

signal." *Korea Institute of Information Technology Review* 8.8 (2010): 9-15.

[3] Q. Ding and J. N. Wang, "Design of frequency-modulated correlation delay shift keying chaotic communication system," *Communications, IET*, vol. 5, no. 7, pp. 901-905, May 2011.

[4] F.C.M. Lau and Chi. K. Tse, "Performance of chaos-based communication systems under the influence of coexisting conventional SS systems, *IEEE Trans. Circuits Syst. I: Fundamental Theory and Applications*", Vol. 50, No. 11, pp. 1475-1481, Nov. 2003.

[5] S. Arai and Y. Nishio, "Noncoherent correlation-based communication systems choosing different chaotic maps," *Proc. IEEE Int. Symp. On Circuits and Systems*, New Orleans, USA, pp. 1433-1436, June 2007.

[6] Junyeong Bok and Heung-Gyoon Ryu, "Digital chaotic communication system based on CDSK modulation," *The Journal of the Korean Institute of Communications and Information Sciences*, vol. 38A, no. 6, pp. 479-485, June 2013.

[7] J. R. Klauder, A. C. Price, S. Darlington and W. J. Albersheim, "The Theory and Design of Chirp Radars," *Bell System Technical Journal* 39, 745 (1960)

[8] Rao, B. V., Deshpande, A. A. Why the barker sequence bit length does not exceed thirteen. *Journal of IETE*, Nov-Dec 1998, vol. 34, no. 6, pp. 461-462.

[9] Xin Wu, Weixian Liu, Lei Zhao, Jeffrey S. Fu, *Chaotic Phase Code for Radar Pulse Compression*, in proceedings of IEEE National Radar Conference, Atlanta, USA, 2001, pp.279-283.

[10] Heinz-Otto Peitgen, Hartmut Jürgens, Dietmar Saupe. *Fractals for the classroom: Part 1: Introduction to fractals and chaos*. Springer-Verlag New York Inc. (1992).

[11] Lau, Yuu-Seng, and Zahir M. Hussain. "A new approach in chaos shift keying for secure communication." *Information Technology and Applications*, 2005. ICITA 2005. Third International Conference on. Vol. 2. IEEE, 2005.

[12] Seventline, J. B., D. Elizabeth Rani, and K. Raja Rajeswari. "Ternary Chaotic Pulse Compression Sequences." *Radioengineering* 19.3 (2010): 415.

[13] Xia, Yongxiang, C. K. Tse, and Francis CM Lau. "Performance of differential chaos-shift-keying digital communication systems over a multipath fading channel with delay spread." *Circuits and Systems II: Express Briefs, IEEE Transactions on* 51.12 (2004): 680-684.

[14] Francis CM. Lau, and Chi Kong Tse. *Chaos-based digital communication systems*. New York: Springer, 2003.

[15] Kolumbán, Géza, Michael Peter Kennedy, and Leon O. Chua. "The role of synchronization in digital communications using chaos. II. Chaotic modulation and chaotic synchronization." *Circuits and Systems I: Fundamental Theory and Applications*, IEEE Transactions on 45.11 (1998): 1129-1140.

[16] Kolumbán, Géza, et al. "Chaotic communications with correlator receivers: theory and performance limits." (2002).

[17] Lau, Francis CM, et al. "Coexistence of chaos-based and conventional digital communication systems of equal bit rate." *Circuits and Systems I: Regular Papers, IEEE Transactions on* 51.2 (2004): 391-408.