Australian Journal of Basic and Applied Sciences, 4(7): 1691-1698, 2010
ISSN 1991-8178

Implementation of Digital Chaotic Signal Generator Based on Reconfigurable LFSRs for Multiple Access Communications

Lwaa Faisal Abdul Ameer

Department of Information and Communications, Alkhwarizmi Engineering College, Baghdad University,

Abstract: This paper presents the implementation of digital chaotic signal generator "twisted map" based on reconfigurable LFSRs. The robust digital implementation eliminates the variation tolerance and electronic noise problems common in analog chaotic circuit. In this paper an improved piece-wise linear one-dimensional iterative map such as "twisted map" with reconfigurable LFSRs is used to generate the chaotic signal for all users. The initial conditions of the sequence generators can be randomly selected to produce reconfigurable chaotic sequence with good correlation properties. The main advantages of this paper are to increase security of the transmission and to ease the generation of a great number of distinct sequences. In practice, the following simulation results on MATLAB software platform and DSP builder show that the effectiveness of the model described which has very low cross-correlation (approximately 0.002 for this architecture). For the proposal system, the bandwidth is extended from approximately 50 Hz to 50 MHz. The period length and the cross-correlation properties of the resulted sequence are compared to m-sequence, gold-sequence and other chaotic sequences generators such as tent map.

Key words: Reconfigurable, chaotic, twisted map, multiple access.

INTRODUCTION

Chaos based communications have drown increasing attention over the past two- decade. Chaotic signals are derived from non-linear dynamic systems. They are aperiodic, broadband, deterministic and appears random on the time domain. These properties are fundamental requirements for carrier signals in communications system (Andrew, C., 2007). Chaos generators have been proposed as sources of noise like signals in many applications (Azzinnari, L., 2001). In the presence implementation, a chaos source needed in code division multiple access (CDMA) communications system. One of the properties of low-dimensional chaotic dynamics which make this proposal attractive is their ability to generate complex and aperiodic spreading signal from simply specified systems (Vigoda, B., 2003). Conventional PN sequences are typified by the class of a maximal length (m-sequences) generated by LFSRs. However, the number of such sequences generated by LFSRs may be insufficient for wideband DS-CDMA systems with a very large number of users. In addition, LFSR techniques provide limited flexibility in incorporating security into multiple user systems (Chiang, P., 2001). Standard PN sequences have limited properties in both low cross-correlation between sequences and large sequences (Andrew D., Jose P. , 1999). Chaotic sequences must seem absolutely random. Therefore, we need a digital chaotic generator with good cryptographic properties, such as, balance on {0,1}; long-cycle length; high linear complexity; δ-like auto-correlation; cross-correlation near to zero (Awad, A., 2008). Unfortunately, this facility cannot be directly utilized in multiple access or high noise environment (Graham, C., 1996). The dominating schemes of chaos and unavoidable parameter derivation in electronic device render exact regeneration of the chaotic signals in analog systems, difficult and only digital schemes are compatible with random communications system (Ling, C., X. Wu, 2001). There is a sensitive dependence on initial conditions, any variations are subject to exponential divergence. This can be used to the advantage of a secure communications system where a slight mismatch in initial conditions between transmitter and receiver will produce very different modulation and demodulation codes. There are an infinite number of sequences for any given chaotic system, each obtainable by changing the initial conditions (Rao, S., S. Howard, 1996). The aim of the percent paper is to generate long, changeable sequences with very low cross-correlation. The

Corresponding Author: Lwaa Faisal Abdul Ameer, Department of Information and Communications, Alkhwarizmi Engineering College, Baghdad University,
E-mail: lwaa_khamass@yahoo.com

reconfigurable LFSRs circuit is added to the chaotic circuit "twisted map circuit" to improve the performance of cross-correlation (near to zero) and auto-correlation (Delta-like). In this paper, the chaotic signal generator with reconfigurable LFSRs is implemented with different polynomials (70, 62, 56, 48)-bit, each have different initial conditions.

2. Background Theory:

2-1 Dynamical Systems:

A dynamical system may be through of as any set of equations giving the time evaluation of the state of a system from a knowledge of its previous history. A common setting is a system of k first-order autonomous ordinary differential equations,

$$\dot{x} = F(x) \tag{1}$$

where x = ($x^{(1)}$, $x^{(2)}$, ---, $x^{(k)}$) denotes k state components, considered as a vector in k-dimensional phase space, F(x) = ($F^{(1)}$(x), $F^{(2)}$(x), ---, $F^{(3)}$(x)) is a k-dimensional vector function of x, and denotes the time derivative dx/dt. It is also important to consider dynamical systems where time is a discrete variable, let n be an integer-valued (discrete) time variable, then the k-dimensional map,

$$x_{n+1} = G(x_n) \tag{2}$$

where is again a k-vector and *G(X)* is a k-dimensional function of (Ott, E., 1995).

Symbolized dynamics is a part of the general theory of dynamical systems. The dynamical systems generated by the twisted map in the spaces of sequences (Afraimovich, V. and Sze-Bi Hsu, 2002),

$$w = \{W_k\} \tag{3}$$

A chaotic signal is derived from non-linear dynamics system (Andrew, C., 2007). Figure (1) plots a chaotic signal generated by a one-dimensional chaotic map against normalized time (Wai M., 2007). It can be observed that the signal never repeat itself, looks random-like and is bounded in the interval [-1 ,+ 1].

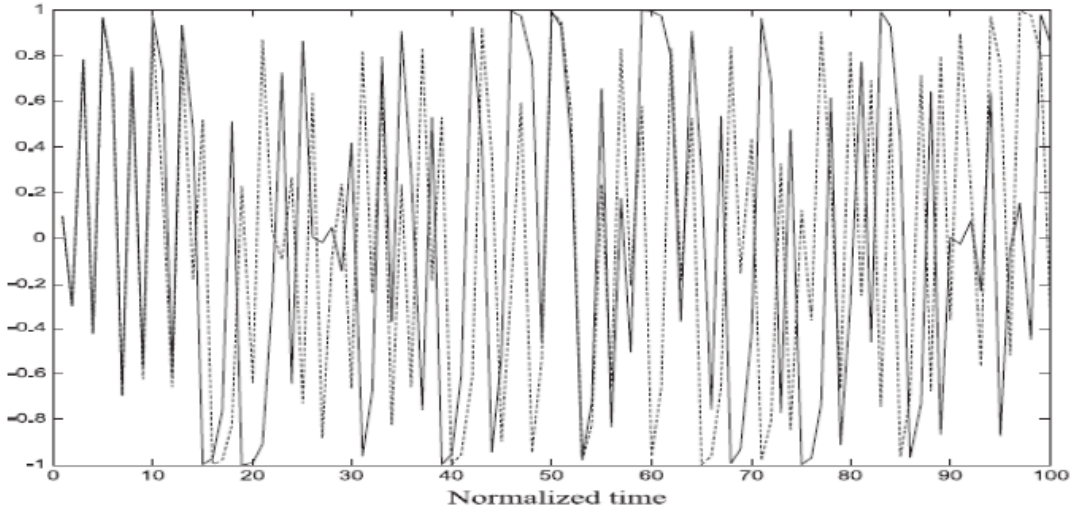

Fig. 1: Waveforms of chaotic signals with slightly different initial values plotted against normalized time. The chaotic signal is generated by using the cubic map $x(n) = 4x^3(n\text{-}1) - 3x(n\text{-}1)$.

2-2 Mathematical Representation:

A proper piece-wise linear one-dimensional map together with delay element can be used as a discrete time chaos source (Azzinnari, L., 2001). To generate random numbers with constant probability density function, the use of twisted map is done.

Markov property that partition points map to partition points. Markov map generate signals with two useful properties; they are, when suitably quantized, indistinguishable from signals generated by Markov chains; they are close, in a sense to signals generated by more general eventually expanding maps (Isabelle, S.H., 1995). These two properties lead to applications of Markov maps for generating random numbers and approximately other signals. The chaotic generator used in this paper is twisted map, described by the following equations

$$x(n) = F[x(n-1)]$$

$$x(n) = \begin{cases} \frac{x(n-1)}{2p} + 2p, if\ 0 \le X(n-1) < p \\ \frac{x(n-1)}{2p} - 2p, if\ p \le X(n-1) < 0.5 \\ F[1 - x(n-1)], if\ 0.5 \le x(n-1) < 1 \end{cases} \quad (4)$$

Where the positive control parameter p ϵ (0, 0.5) and x(i) ϵ(0, 1). if p= 0.25, then the dynamics of the twisted map is obtained as shown below:

$$x(n) = \begin{cases} 2\boldsymbol{x(n-1)} + 0.5, if\ 0 \le x(n-1) < 0.25 \\ 2\boldsymbol{x(n-1)} - 0.5, if\ 0.25 \le x(n-1) < 0.5 \\ (1 - 2\boldsymbol{x(n-1)}) + 0.5, if\ 0.5 \le x(n-1) < 0.75 \\ (1 - 2\boldsymbol{x(n-1)}) + \boldsymbol{1.5}, if\ 0.75 \le x(n-1) < 1 \end{cases} \quad (5)$$

These equations have a phase space which spans in the unit interval. Binary partition (0 or 1) for generating symbolic dynamics is shown in figure (2).

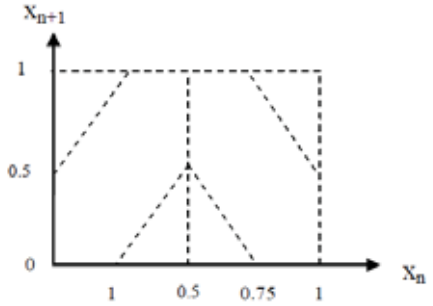

Fig. 2: Generating partition of twisted map

The initial condition is unique to each user and the resulting sequence is balanced between ± 1. Chaotic systems are characterized by sensitivity on initial conditions, impulse like auto-correlation and very low cross-correlation (Andrew, C., 2007).

An iterated function is a discrete-time function generated by recursive evaluation of some function mapping (Andrew D., Jose P., 1999), as shown in Figure (3).

3. System Design and Implementation:

3-1 4- Stage Twisted Map Implementation:

Table (1) illustrate the sequence generated by the chaotic twisted map. Assume that the initial state of the register is "0001". During operation, the system reaches the following states:

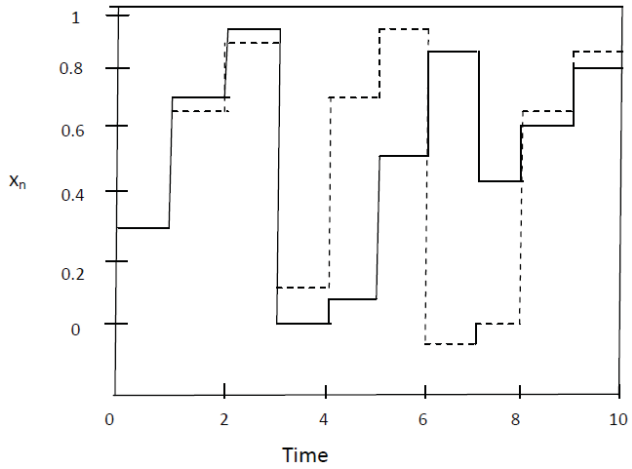

Fig. 3: Sensitive dependence upon initial conditions

Table 1: 4-stage chaotic twisted map sequence generation

No.	xn	Xn+1	No.	xn	Xn+1
0	0.5	0.8125	8	0.125	0.3125
1	0.8125	0.875	9	0.3125	0.0
2	0.875	0.0	10	0.0	0.625
3	0.0	0.375	11	0.625	0.5
4	0.375	0.9375	12	0.5	0.375
5	0.9375	0.5625	13	0.375	0.25
6	0.5625	0.3125	14	0.25	0.4375
7	0.3125	0.125	15	0.4375	0.5

The implementation of the twisted map is shown in figure (4).

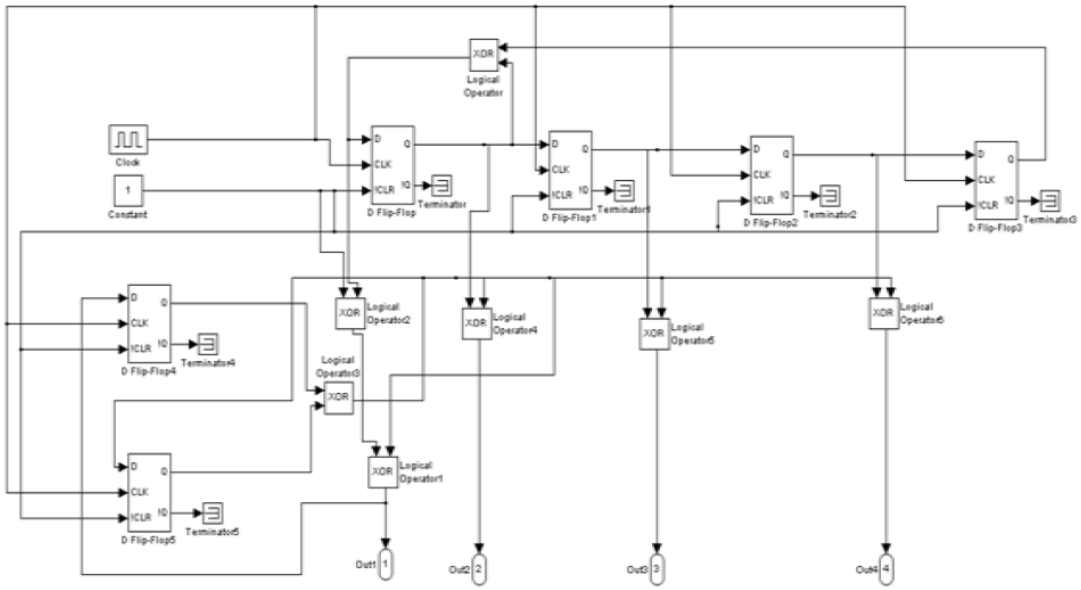

Fig. 4: Digital realization of the twisted map

3-2 Reconfigurable LFSRs Design:

The design of the proposed reconfigurable LFSRs is shown in figure (5). The reconfigurable LFSR consists of four LFSR each with different polynomials and with different initial conditions. The LFSR components consists of 70-DF/Fs, 62-DF/Fs, 56-DF/Fs and 48-DF/Fs. Each group is driven by different initial condition.

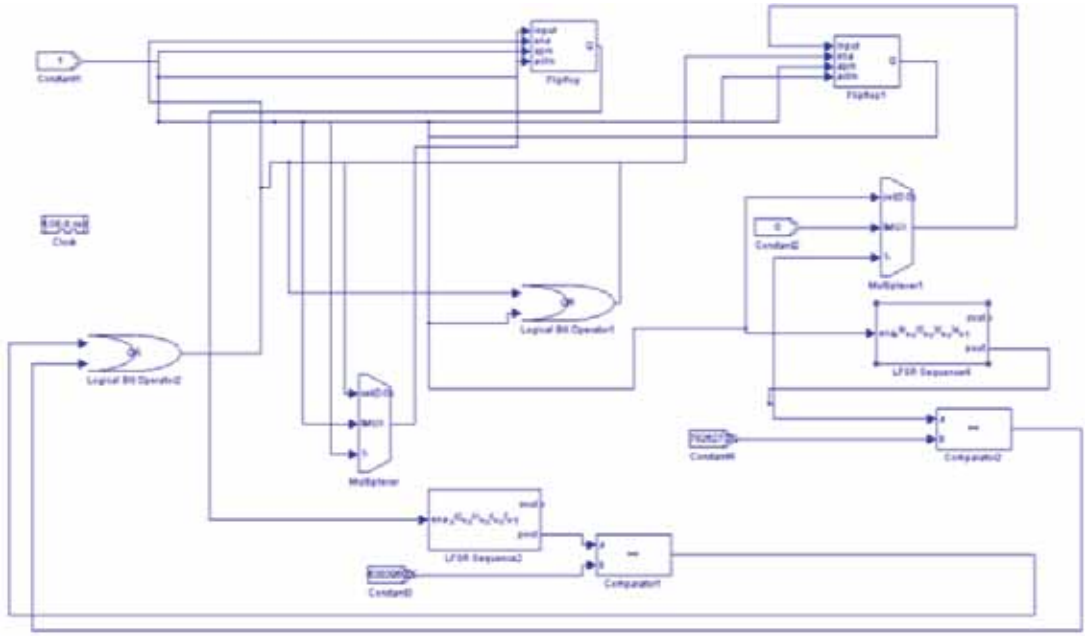

Fig. 5: Digital realization of reconfigurable LFSR 5

3-3 Proposed Reconfigurable LFSRs/Chaotic Signal Generator Design:

A combination of reconfigurable LFSRs and chaotic signal generator is proposed to generate very long sequences with cross-correlation closed to zero. Figure (6) represent the block diagram of the chaotic signal generator "twisted map" (figure 4)/reconfigurable LFSRs (figure 5).

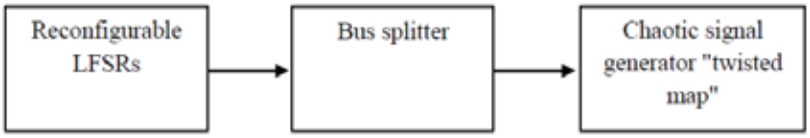

Fig. 6: The reconfigurable LFSRs/chaotic signal generator combination design.

4. Simulation Results:

The output sequences have been characterized with respect to their auto-correlation and cross-correlation properties. Table (2) summarized results from software simulations of the implemented system along with conventional m-, gold, chaotic "tent map" sequences. The first selection shows maximum period length and cross-correlation value for standard value for standard m-sequence with length of 2^{15}-1bits. In the second selection is the value for Gold sequence of the same length. In the third row is the value for chaotic "tent map (2^{15}-1) sequence. The bottom raw shows results for the reconfigurable LFSRs with chaotic "twisted map" sequence generated by the new architecture. The cross-correlation properties for the current work are excellent as well. The correlation performance will improve further as sequence length is switching between various polynomials and as sequence length is increased. This is particularly important in multiple access communications system. Figures (7-a) and (7-b) depicts the cross-correlation plot and auto-correlation plot, for typical sequences generated by this architecture respectively. Figures (7-a) and (7-b) indicates that the cross-correlation is very closed to zero and the auto-correlation is -like. Figured (7-c) and (7-d) indicate the power spectrum extends both to the region of very low frequencies as well as to high frequencies, for the proposed system, the bandwidth is extended from approximately 50 Hz to 50 MHz . The plots are based on truncated correlation computations using window of length (1024).

Table 2: Period length and cross-correlation Comparison of various Generators with clock frequency of 100 MHz.

	Period length(sec)	Cross-correlation
m-sequence 2^{15}-1=32767-bit with clock (50MHz)	0.00065535	0.06638
Gold-sequence 2^{15}-1=32767-bit with clock(50MHz)	0.00065535	0.00784
Chaotic-sequence"tent map" 2^{15}-1=32767-clock(50MHz)	0.01495	0.00394
Reconfigurable LFSRs with chaotic map" [(2^{70}-1), (2^{62}-1), (2^{56}-1) and (2^{48}-1) with clock 100 MHz. (current work)	The sequence varies 11805916207174.11, 461168601 84.27, 720575940.37 and 2814749.76	0.002

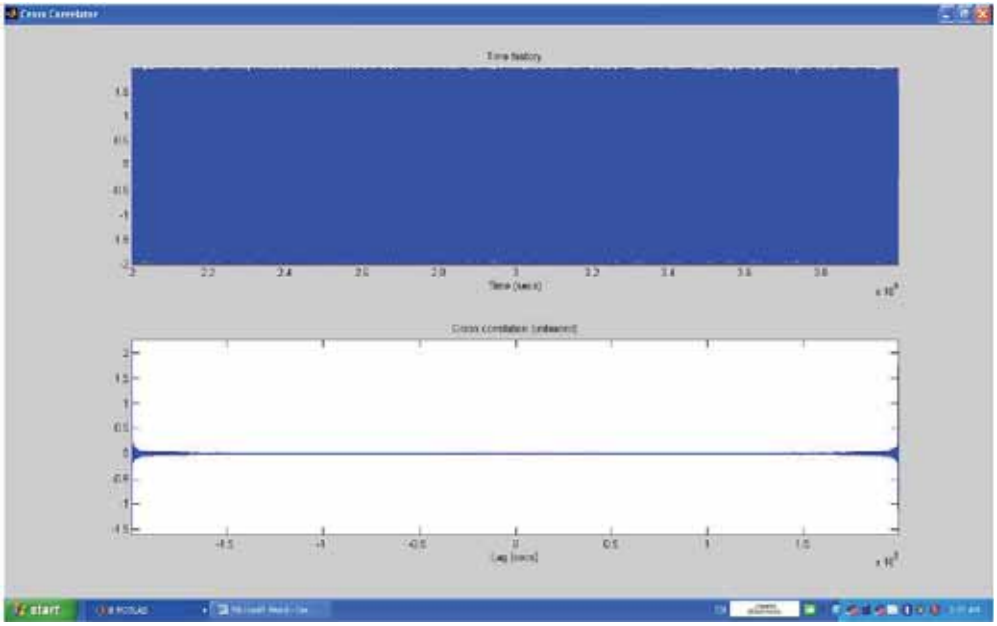

Fig. (7-a): The cross-correlation

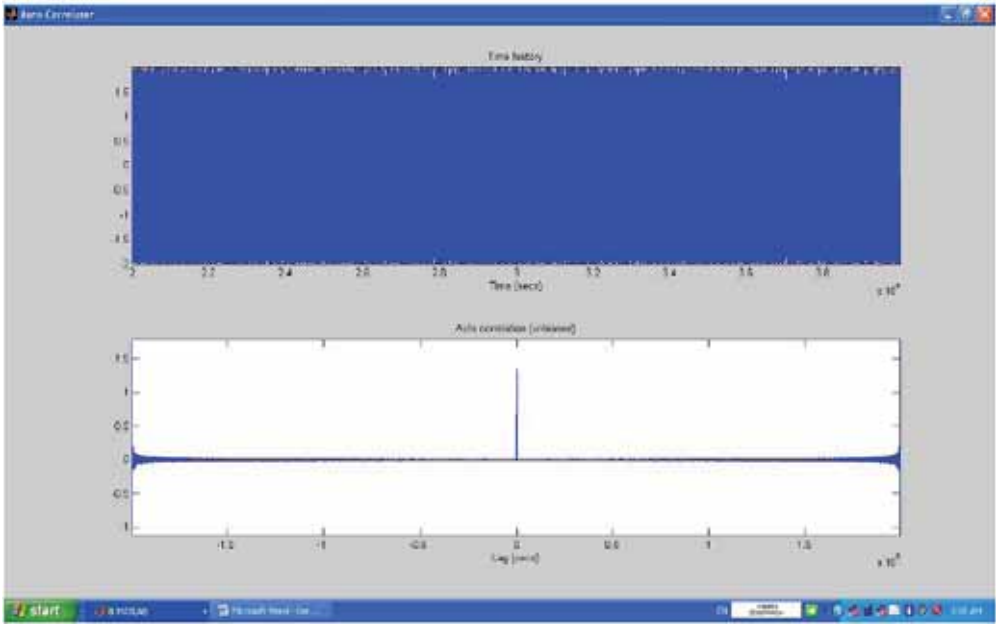

Fig. (7-b): The auto-correlation

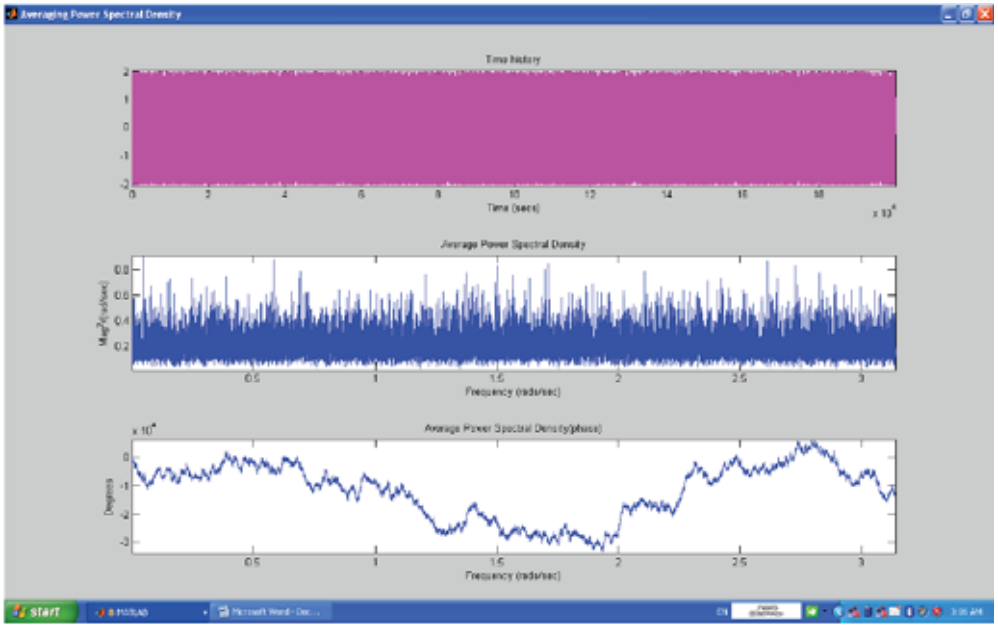

Fig. (7-c): The average power spectral density

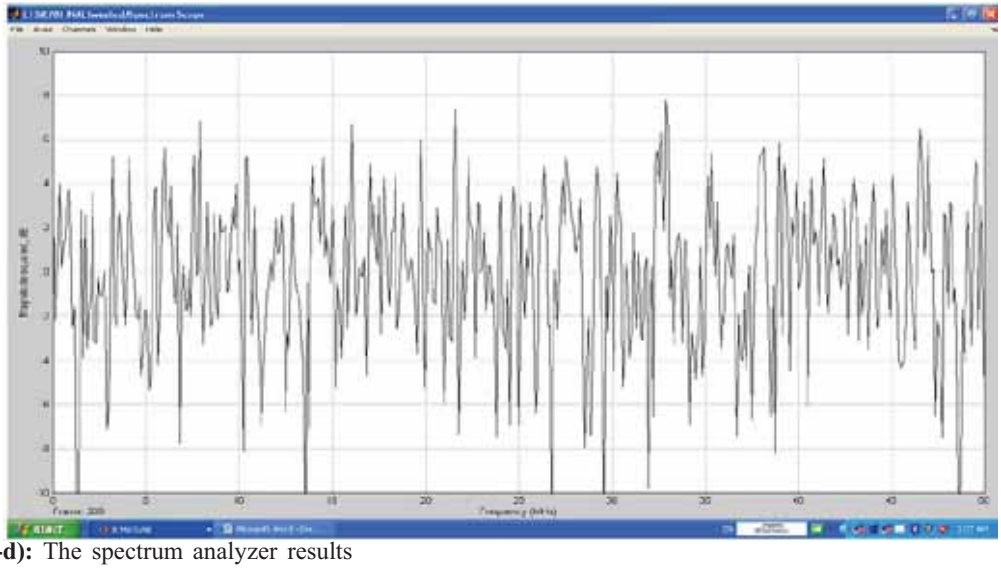

Fig. (7-d): The spectrum analyzer results

Fig. 7: Cross-correlation, auto-correlation, average power spectral density and spectrum analyzer

5. Conclusions:

In the proposed system, the reconfigurable LFSRs circuit is added to the chaotic circuit specially twisted map circuit to improve the performance of cross-correlation (near to zero) and auto-correlation (Delta-like). The main goal of this work is to generate a digital chaotic signal through reconfigurable LFSRs. The important advantages of the reconfigurable chaotic sequences results is in their very high sensitivity on very small changes of initial conditions and to highlight the long sequences to provide high security. Circuit simulation proved that the reconfigurable chaotic signal generator generate the long sequences and are changed at each LFSR.. In CDMA systems, cross-correlation closed to zero, long sequences, wide bandwidth properties are required. Figure (7) show that the system is provided the required properties in CDMA systems where the cross-correlation is approximately 0.002, -like auto-correlation and the bandwidth is extended from approximately 50 Hz to 50 MHz.

REFERENCES

Andrew, C., 2007. “An Investigation into Chaos-Based Communication systems” University of Auckland.

Azzinnari, L., A. Mozsary, K. Krol, V. Porra, 2001. “A Simple Digital FPGA Pseudo-Chaos Generator”, ECCTDEuropean Conference on Circuit Theory and Design, August 28-31, Espoo, Finland, pp: 25-28.

Andrew D., P. Jose, 1999. “Chaotic Generation OF PN Sequences: AVLSI Implementation”, IEEE, pp: 454-457.

Awad, A., S. El Assad, W. Qianxue, C. Vladeanu and B. Bakhache, 2008. " Comparative Study of 1-D Chaotic Generators for Digital Data Encryption", IAENG International Journal of Computer Science.

Afraimovich, V. and Sze-Bi Hsu, 2002. "Lectures on Chaotic Dynamical systems" American Mathematical Society.

Chiang, P., W. Dally, E. Lee, 2001. "Monolithic chaotic communications system", Stanford University.

Graham, C., Freeland and S. Tariq, 1996. "Fractal PN signals for broadband communications interpolation functions and PN wavelets", IEEE.

Isabelle, S.H., 1995. *“A Signal Processing Framework for the Analysis and Application of Chaos”,* Ph.D. thesis, M.I.T., Cambridge, MA, Also RLE Tech. Rep. No. 593.

Ling, C., X. Wu, 2001. “Design and Realization of an FPGA-Based Generator for Chaotic Frequency Hopping Sequences”, IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS-FUNDAMENTAL THEORY AND APPLICATIONS, 48(5): 521-532.

Ott, E., T. Sauer and J.A. Yorke, 1995. "Analysis of Chaotic Data and the Exploitation of Chaotic Systems",© Joun Wiley & Sonic, Inc.

Rao, S., S. Howard, 1996. "Correlation performance of chaotic signals in spread spectrum systems", IEEE Digital Signal Processing Workshop.

Vigoda, B., 2003. "Analog Logic: Contiuous-Time Analog Circuits for Statistical Signal Processing", Thesis, Doctor of Philosophy, pp: 41.

Wai M., Tam, Francis C.M. Lau and Chi K. Tse, 2007. “ Digital Communications with chaos” © Elsevier Ltd.