Kufa Journal of Engineering
Vol. 8, No. 1, January 2017, P.P.16-25
Received 21 February 2016, accepted 20 June 2016

A NEW CHAOTIC MAP FOR GENERATING CHAOTIC BINARY SEQUENCE

Saad Muhi Falih[1]

[1] **Lecturer, Department of Computer Technical Engineering, Islamic University**

College, Al Najaf al Ashraf, Iraq, saadmuheyfalh@gmail.com

ABSTRACT

In this paper, a new quadratic map (NQM) is proposed. Using this NQM, a chaotic signal can be generated directly by assuming an initial condition to NQM which can be converted into binary sequence to get a chaotic binary sequence. The chaotic binary sequences that were evolved in this system are typically broadband and noise-like sequence. However, because of these properties the chaotic binary sequence generating potentially provides an important class of signals which can be utilized in various communication systems. The results showed that the presented method generates a chaotic binary sequence with several advantages, such as the stability, broadband, difficult to predict, noise-like, and high randomness statistical properties.

KEYWORDS: Chaos communication; Chaotic binary sequence; Chaotic map; Nonlinear system; Chaotic cipher

مخطط فوضوي جديد لتوليد المتواليات الثنائية الفوضوية

سعد محي فالح

مدرس/ قسم هندسة تقنيات الحاسوب/ الكلية الاسلامية الجامعة/ النجف الأشرف, العراق

الخلاصة

في هذا البحث تم أقتراح مخطط تربيعي جديد ((NEW QUADRATIC MAP (NQM). وقد استخدم هذا المخطط التربيعي الجديد في توليد إشارة الفوضى (CHAOTIC SIGNAL) بصورة مباشرة عن طريق افتراض قيم أولية للمخطط المقترح وحولت الإشارة الفوضوية المتولدة الى الترميز ثنائي للحصول على متوالية ثنائية الفوضوية (CHAOTIC BINARY SEQUENCE). ان المتوالية الثنائية الفوضوية التي تم الحصول عليها باستخدام المخطط التربيعي المقترح إمتازت بنطاقها الترددي العريض وشَبهها بالمتوالية الضوضائية. وبسبب هذه الخصائص للمتوالية الثنائية الفوضوية المقترحة فإنها تُعد فئةً هامة من الإشارات التي يمكن استخدامها في أنظمة الاتصالات المختلفة. أظهرت النتائج أن الطريقة المقترحة تولد متواليات ثنائية فوضوية لها العديد من المميزات كالاستقرارية وسعة النطاق الترددي وصعوبة الاكتشاف وشبهها بالضوضاء البيضاء اضافة الى خصائصها العشوائية الجيدة.

1. INTRODUCTION

In the recent years, sequences derived from chaotic phenomena are being considered for use in secure communications and for spread spectrum systems (Sajic et al., 2013). Chaotic sequences are generated from nonlinear dynamical systems. These are unpredictable, deterministic systems, and often described by the system of parameterized differential equations (Lorentz system[1], Chua's oscillator[2], etc.). Their essential feature is that they exhibit noisy-like behavior because of their strong sensitivity to the initial conditions. Also, a simple method to obtain chaotic sequences is to use mapping functions (Sajic et al., 2013).

In Wideband Code-Division Multiple Access (WCDMA) system as example, each user is separated by using PN sequence code. A Pseudorandom Numerical (PN) sequence is a binary sequence that exhibits randomness properties, but has a finite length and it is therefore deterministic. Chaotic codes having a wideband nature have been proposed as carriers for spread spectrum systems. Chaotic signals are non-periodic in nature and hence the message spread with chaotic sequence cannot be intercepted easily and accordingly, it provides enhanced security. In addition, chaotic signals have very good auto and cross-correlation properties. These are important features for spread spectrum multiple access environments because they can produce low co-channel interference, and hence they provide a better performance (Das and Mandal, 2013).

Random binary sequences are widely used in the field of secure communications (Sajic et al., 2013). There are three different types of random generators used: pseudo-random, chaotic, and true random binary sequence generators (Sajic et al., 2013).

An important class of random sequences is so called "class of chaotic sequences" (Sajic et al., 2013). Although there is no universally accepted mathematical definition of chaos, a commonly used one for chaotic sequence says that it is a random-like deterministic sequence which is generated sequentially by using a mapping function $X_{n+1} = f(X_n)$ and an initial value X0, but whose distribution looks like white noise (Sajic et al., 2013). This sequence has merit that is knowing by only two givens, namely: a mapping function and an initial value; the same sequence can be regenerated. These sequences are also widely used in spread spectrum communications and cryptography (Sajic et al., 2013).

Chaotic signals are random like, however they are produced by deterministic systems and can be reproduced. Chaotic sequences are easy to generate and store; only few parameters and functions are needed for generating very long sequences. Chaotic systems are sensitive to the initial conditions, hence even with a small difference in the initial conditions they will lead to the generation of the very different signals from the same dynamical system (Mandi et al., 2010). In addition, an enormous number of different sequences can be generated simply by changing its initial conditions. Also the natures of chaotic signals are deterministic, reproducible, uncorrelated, and random like, which can be very helpful in enhancing the security of transmission in communication (Mandi et al., 2010).

In this work, a binary random number generator based on the new quadratic map (NQM) is proposed. An analog chaotic signal can be generated directly from proposed quadratic map by assuming an initial condition. However, this analog chaotic signal can be converted into a binary sequence to get a chaotic binary sequence. The experimental results showed that the presented method generates a chaotic binary sequence with several advantages, such as the stability, broadband, difficult to predict, noise-like, and high randomness statistical properties.

[1] Lorentz system is a simple system of three ordinary differential equations developed by Edward Lorenz in 1963 (see Hirsch et al.., 2004).
[2] Chua's oscillator (also known as a Chua circuit) is a simple electronic circuit that exhibits a classic chaos theory behavior (see Chua et al., 1993).

The rest of this paper is organized as follows: section 2 introduced the general principles of the chaotic map. The stable region in chaotic map is discussed in section 3. Section 4 presents the proposed chaotic sequence generator. The simulation study is presented in section 5. Finally, Conclusions will be presented in section 6.

2. CHAOTIC MAP

A chaotic dynamical system is one that is deterministic but appears not to be so, as a consequence to its extreme sensitivity to the initial conditions. Any chaotic system can be described by the general discrete-time state-space formula (Azou et al., 2002):

$$x_n = f(x_{n-1}) \quad , \quad n = 0, 1, 2, \tag{1}$$

Where x_n is called the state at time index n, and f (…) represents a nonlinear function in x_{n-1}, which maps the state x_{n-1} to the next state x_n .

Given the same initial conditions, two chaotic systems with the same state parameters will result in exactly the same sequence of the output samples. On the other hand, any minor difference between the initial states will lead to an eventual divergence of the output streams from the two systems. Asymptotically, the output streams will be completely decorrelated.

The dynamical systems with chaos appear to be a good choice for encryption algorithms. Indeed, because block-encryption algorithms can be rewritten as discrete-time dynamical systems, $x_n = f(x_{n-1})$ where the initial condition x_0 is a plain-text to be encrypted, and the final state x_n is a cipher text, then it is the property of the map being chaotic that implies "spreading out of the influence of a single plaintext digit over many cipher text digits". To ensure a complicated structure of the dynamical system proposed for an encryption algorithm, we assume that in addition to being chaotic the system should be mixed (more precisely K mixing). Moreover, to ensure that the parameters of the system can be used as encryption keys, we postulate that the system has robust chaos; the system is chaotic for a large set of parameters.

A chaotic map does not have to be very complicated. However, in a context of Code Division Multiple Access (CDMA) application, the map has to possess a δ-like auto-correlation function, for a proper signal detection, and low cross-correlation function for proper signal separation. Moreover, a zero-mean symmetric sequence is desirable (Azou et al., 2002).

The quadratic map is proposed here as the chaotic sequence generator:

$$x_n = 1 - r(x_{n-1})^2 \tag{2}$$

This system exhibits a great variety of dynamics, depending upon the value of the bifurcation parameter.

3. STABILE REGION IN CHAOTIC MAP

To find the stable region in chaotic map, let we assume x is an element of the chaotic map, then:

$$x = 1 - rx^2 \tag{3}$$

$$r.x^2 + x - 1 = 0 \tag{4}$$

Then

$$x = \frac{-1 \pm \sqrt{1+4r}}{2r} \tag{5}$$

Now, we can test stability of this fixed point as:

Let $x_n = x + \delta_n$, where δ is a small distance.

Then x_{n+1} becomes:

$$x_{n+1} = 1 - r(x_n)^2 \quad (6)$$

$$x_{n+1} = 1 - r(x + \delta_n)^2 \quad (7)$$

$$x_{n+1} = 1 - rx^2 - 2r\delta_n x - r{\delta_n}^2 \quad (8)$$

Because $x_{n+1} = x + \delta_{n+1}$ and $x = 1 - rx^2$

$$x + \delta_{n+1} = x - 2r\delta_n x - r{\delta_n}^2 \quad (9)$$

Because δ_n is a small length therefore ${\delta_n}^2$ is even smaller and can be disregard, so:

$$\delta_{n+1} = -2r\delta_n x \quad (10)$$

This is the equation that determines the stability of x. If $|\delta_{n+1}| < |\delta_n|$, then there is an attraction towards x, and x is stable. If $|\delta_{n+1}| > |\delta_n|$, then there is a repulsion away from x, and x is unstable.

Since r in our equation $x = 1 - rx^2$ can be any constant value, then the value of r is crucial in determining the stability of x. Solving for r using our fixed points is necessary.

$$x = \frac{-1 \pm \sqrt{1+4r}}{2r} \quad (11)$$

Substitute (11) in (10) we get:

$$\delta_{n+1} = -2r\delta_n \left(\frac{-1 \pm \sqrt{1+4r}}{2r}\right) \quad (12)$$

Now, get the absolute value for the both sides of (12)

$$|\delta_{n+1}| = |\delta_n|\left|+1 \pm \sqrt{1+4r}\right| \quad (13)$$

However, in stabile region $|\delta_{n+1}|$ must be less than $|\delta_n|$ then:

$$\left|+1 \pm \sqrt{1+4r}\right| \leq 1 \tag{14}$$

From (14), one can prove the chaotic map has a stable margin in the range:

$$-1/4 \leq r \leq 0.75 \tag{15}$$

On the other hand, one can get the complete picture of the chaotic map behaviors by studying the bifurcation diagram, which is a graphical depiction of the relationship between the values of one parameter and the behavior of the system in which the parameter is being measured (Pratt, 2008). Fig. 1 is showing the bifurcation diagram of the proposed chaotic map; it is clear from the figure that the bifurcation parameter (r) must be greater than 1.43 to get the chaotic behavior. However, there is some stable islands in this chaotic margin located at r= 1.477, 1.631, and 1.75. These stable islands must be avoided to get a good chaotic signal from this map.

The final test one can do on chaotic map to distinguish the stable regions from the chaotic regions is done by calculating the value of the Lyapunov exponent which is a powerful tool for understanding the chaotic behavior.

The Lyapunov exponent for a one dimension map is defined as (Diks, 1999):

$$\lambda = \lim_{n\to\infty} \left(\frac{1}{n}\sum_{i=0}^{n-1} \ln\left|\acute{f}(x_i)\right|\right) \tag{16}$$

Where $\acute{f}(x_i)$ is the first derivative of $f(x_i) = x_{n+1}$, which equals to $(1 - r(x_n)^2)$ in the proposed chaotic map.

$$\lambda = \lim_{n\to\infty} \left(\frac{1}{n}\sum_{i=0}^{n-1} \ln(\,|-2rx_i|)\right) \tag{17}$$

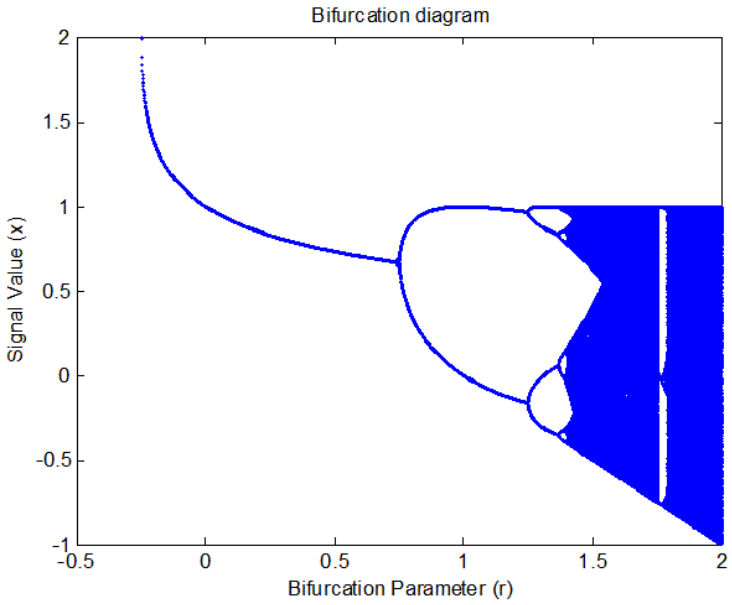

Fig. 1. Bifurcation diagram of the proposed chaotic map.

The magnitude of the Lyapunov exponent is an indicator of the behavior of the system; if the value of Lyapunov exponent is negative then this refers to the stable behavior of the system, on the other hand, the positive value refers to the chaotic behavior (Diks, 1999). However, Fig. 2 shows the value of Lyapunov exponent with respect to bifurcation parameter (r). In this figure the location of the stable islands and the chaotic region are very clear in the diagram depending on the value of Lyapunov exponent as described previously.

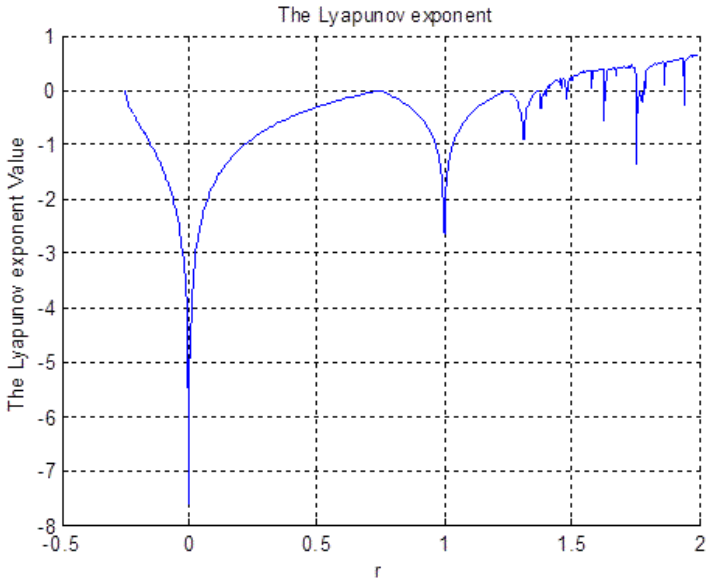

Fig. 2. Lyapunov exponent value as a function of bifurcation parameter of the proposed chaotic map.

4. CHAOTIC BINARY SEQUENCE GENERATOR

The block diagram for the proposed chaotic sequence generator is shown in Fig. 3. The chaotic sequence generator shown in the block diagram generates a random

chaotic signal from the chaotic quadratic map for a different initial value x_0 and the bifurcation parameter r. The random chaotic signal is mapped to binary to generate the final chaotic binary sequence.

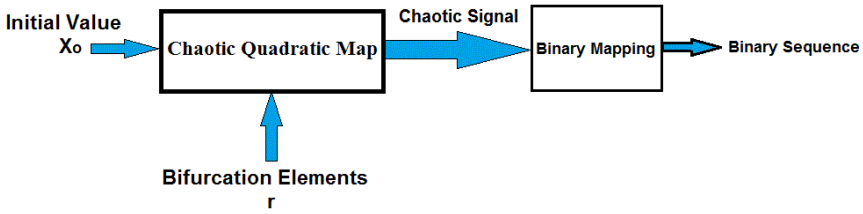

Fig. 3. Block diagram for chaotic sequence generator.

5. SIMULATION STUDY

The proposed chaotic sequence generator shown in Fig. 3 is built in Matlab environment. However, the initial conditions of the chaotic map used in this simulation program has taken as $x_0 = 0.2$ and r=2.

Fig. 4 is showing the chaotic stream generation using proposed chaotic map. On the other hand, the chaotic binary sequence generation by the proposed generator is showing in Fig. 5.

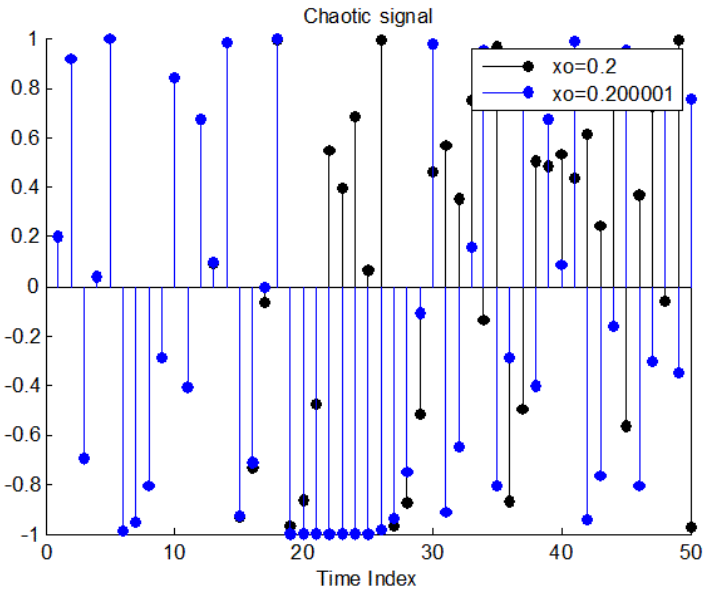

Fig. 4. the chaotic stream generation using proposed chaotic map.

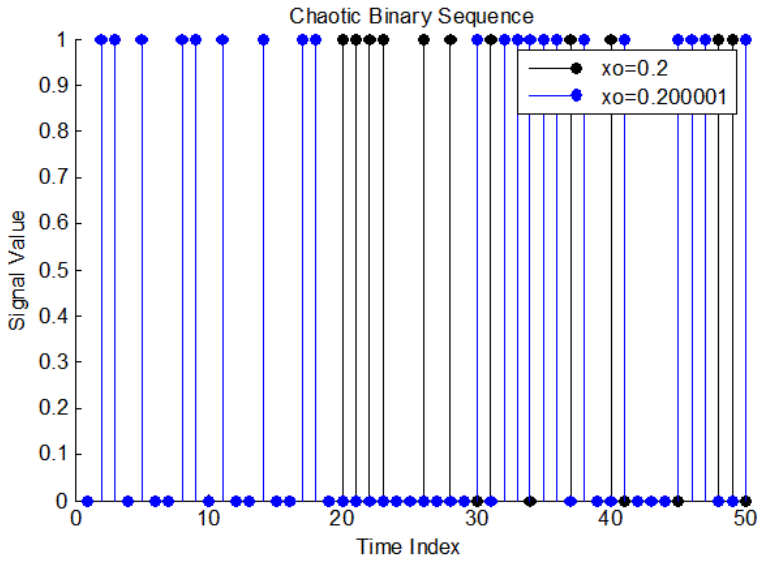

Fig. 5. The chaotic binary sequence genration by proposed genrator.

The auto-correlation function is one of the statistical parameters used to assess the random nature of sequences; it has delta-function form for a perfect pseudo random noise sequence. The auto-correlation property of the generated binary sequence of length 1000 using modified chaotic signal using Eq. 18 (Seventline et al., 2010) is shown in Fig. 6.

$$r(k) = \sum_{i=0}^{N-1-k} x_i x_{i+k} \text{ where } k = 0,1,\dots,N-1 \quad (18)$$

Where $r(k)$ is the auto-correlation function of the sequence $x(k)$, and N is the length of the sequence.

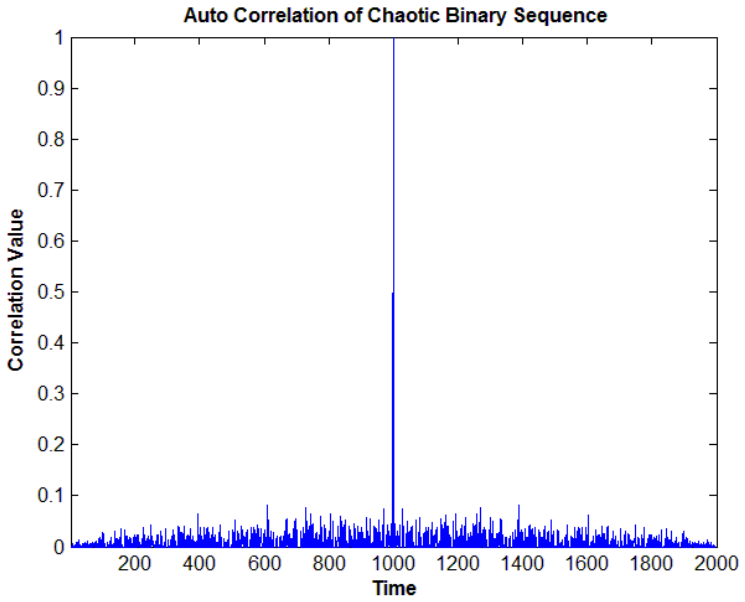

Fig. 6. The autocorrleation function of the chaotic binary sequence genration.

The impulse like shape 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. It is clear from Fig. 6 that the sequence generated by the proposed generator has a moderate auto-correlation function form.

The American National Institute of Standards and Technology (NIST) is proposed a Federal Information Processing Standard (FIPS) 140-2, that is described four tests named as follow: monobit, poker, runs, and long runs test to verify the randomness of pseudorandom bit sequences (Min et al., 2013). These tests can be described as:

1. The monobit test: The sequence is random if the number of one in bits stream generated by tested algorithm lie in range (9654-10346).
2. The poker test: the 20,000 bits stream generated by tested algorithm is divided into 5,000 contiguous 4 bit segments. The values of each 4 bit segments are determined and occurrences of each of the 16 possible 4 bit segment values are counted and stored in $f(i), \text{where } 0 < i < 15$, as the number of each 4 bit value. Then, we evaluate the following:

$$x = \left(\left(\frac{16}{5000}\right)\left(\sum_{i=0}^{15} f(i)^2\right)\right) - 5000 \quad (19)$$

If $1.03 < x < 57.4$ then the test is passed and the sequence is random.

3. The runs test: The run can be defined as the repeated of the same bit in contiguous bits. The tested algorithm can pass this test if the number of runs of length 1, 2, 3, 4, 5, and longer than 5 lies in specified limits described in Table (1) (Min et al., 2013).

Table 1. The runs test interval required under FIPS 140-2

Length of Run	Required Interval
1	2315-2685
2	1114-1386
3	527-723
4	240-384
5	103-209
6+	103-209

4. The long run test: The tested algorithm can pass this test if there is no run of length equal to or greater than 34 bit.

The results of all tests are reported in Table (2). One could notice the proposed chaotic algorithm passing these tests, and the sequence produced is random sequences.

Table 2. Randomness test of the proposed chaotic algorithm

Algorithm Test	Monobit Test	Poker Test	Runs Test						Long Runs Test
			L=1	L=2	L=3	L=4	L=5	L=6	
Acceptance* Range	9,725-10,275	2.16-46.17	2,315-2,685	1,114-1,386	527-723	240-384	103-209	103-209	0
Test Results	10168	12.9632	2453	1268	585	314	171	150	0

6. CONCLUTIONS

In this paper, a new quadratic map has been proposed to generate a chaotic binary sequence. The stability of chaotic maps and their basic properties are discussed. Simulation results showed that the proposed generator has many advantages over the stability of chaotic binary sequence generated, such as broadband, difficult to predict, and noise-like sequence. Finally, this proposed algorithm is easy to realize using simple pc program.

7. REFERENCES

Azou, S, Burel, G, and Pistre, C (2002), "A Chaotic Direct-Sequence Spread-Spectrum System for Underwater Communication", IEEE-Oceans'2002, Biloxi, Mississippi, USA.

Chua, L. O. et al., (1993), "a Universal Circuit for Studying and Generating Chaos-Part I: Routes to Chaos", IEEE Transaction on Circuits and Systems, Vol.40, No10, pp.732-744.

Das, S and Mandal, S (2013), "Performance Analysis of Chaotic Spreading Sequence in WCDMA Downlink System", Workshop Proceedings of "Advanced Wireless Communication and Networking" Under TEQIP-II, Organized by ECE Dept. of NIT Durgapur.

Diks, C (1999), "Nonlinear Time Series Analysis: Methods and Applications", Word Scientfic Publishing Co. Pte. Ltd., pp. 27-31.

Hirsch, M. W., Smale, S., and Devaney, R. L., (2004), "Differential Equations, Dynamical Systems, and an Introduction to Chaos", Elsevier, India, Second Edition.

Mandi, M, Haribhat, K, and Murali, R (2010), "Generation of Large Set of Binary Sequences Derived From Chaotic Functions Defined Over Finite Field GF (28) With Good Linear Complexity and Pairwise Cross Correlation Properties", Inter. Jour. of Distributed and Parallel systems, Vol.1, No.1, pp. 93-112.

Min, L., Chen, T., and Zang, H., (2013), "Analysis of FIPS 140-2 Test and Chaos-Based Pseudorandom Number Generator", Chaotic Modeling and Simulation (CMSIM), Vol. 2, pp. 273–280.

Pratt, S (2008), "Bifurcations Are Not Always Exclusive", An International Journal of Complexity and Education, Vol. 5, No. 1, pp. 125-128.

Sajic, S and et al (2013), "Random Binary Sequences in Telecommunications", Jour. of Electrical Engineering, Vol. 64, Issue. 4, pp. 230–237.

Seventline, J. B., Rani, D, and Raja Rajeswari, K (2010), "Ternary Chaotic Pulse Compression Sequences." Radio Engineering Vol. 19, No.3, pp. 415-420.