Chaotic Sequence Derived from Bifurcation Dependency

Oluyemi E. Adetoyi, Solomon A. Adeniran

Abstract— In this paper, we show that logistic map exhibit sufficient dependence on bifurcation parameter and small perturbation of the bifurcation parameter can generate many sequences. Since there are dense islands of periodicity in the chaotic region of the map, Lyapunov exponent was employed to isolate the chaotic domains. Two-bit encoding was used, in other to reduce the quantization error. The threshold for encoding was determined by subjecting a training sequence to a compression algorithm, thus ensuring balanced sequence.

Index Terms— Bifurcation parameter, Chaotic sequences, Correlation, Initial condition, Logistic map.

1 Introduction

Generally, chaotic sequence exhibits sensitive dependence on initial condition through its non-converging and noise-like behaviour. This sensitive dependence on initial conditions was exploited in [1]-[7] for generation of chaotic sequences. Reference [5] stated that large number of uncorrelated, random-like, yet deterministic and reproducible signals can be generated by changing initial value. However, not all will have good correlation properties due to encoding applied to obtain binary sequence, thus a limit is imposed on the usable sequences. Reference [1],[4] and [5] shows that the use of chaotic sequences for spectral spreading in a direct-sequence spread spectrum system (DSSS) provides several advantages over conventional binary sequences, particularly pseudo-noise sequences which are frequently used in digital communication. In reference [6], it was suggested that the large size of the keyspace is an indication of strong candidature for cryptographic applications, especially for stream cipher cryptography.

2 Chaotic Sequences

Chaotic sequences are generated using discrete chaotic maps [8]. One-dimensional maps are common, although it is possible to generate sequences from two-dimensional or three-dimensional maps. The characteristic of the sequences is similar to that of random noise, even though the generation method is completely deterministic. Chaotic maps are initial condition sensitive. In theory, differing user code can be generated by assigning different initial condition. In practice, the choice of initial condition and method of generation should be carefully guided to avoid repeated codes. Due to non-binary output of chaotic sequences generator, some form of encoding is often required. Several schemes are proposed in [1], [2], [7], [9], [10], [11] and [12] on methods for generation of chaotic sequences. Some of these sequences have small family size; the Maximum Autocorrelation (M_{ac}) and the Maximum crosscorrelation (M_{cc}) are comparable to m-sequences and gold sequences or better in some cases. Reference [1] defines M_{ac} and M_{cc}, these are as shown in (1) and (2).

$$M_{ac}(\tau) = \max_i \max_{\tau \neq 0} |R_{ac}(\tau)| \quad (1)$$

$$M_{cc}(\tau) = \max_{i \neq j} \max_{\tau} |R_{cc}(\tau)| \quad (2)$$

where R_{ac} and R_{cc} are as defined by equation 3 and 4

$$R_{ac}(\tau) = \frac{1}{L}\sum_{n=0}^{L-1} b_i(n) b_i(n+\tau) \quad (3)$$

$$R_{cc}(\tau) = \frac{1}{L}\sum_{n=0}^{L-1} b_i(n) b_j(n+\tau) \quad (4)$$

for $0 \leq \tau \leq L-1$

The performance of these sequences can also be evaluated by Mean Square Aperiodic Auto-Correlation (MSAAC) and Mean Square Aperiodic Cross-Correlation (MSACC) measures defined in [13]-[15] as

$$MSAAC \equiv \frac{1}{M}\sum_{i=1}^{M}\sum_{\tau=1-N,\tau\neq 0}^{N-1} \left| r_{i,j}(\tau) \right|^2 \quad (5)$$

$$MSACC \equiv \frac{1}{M(M-1)}\sum_{i=1}^{M}\sum_{j=1,j\neq i}^{M}\sum_{\tau=1-N,\tau\neq 0}^{N-1} \left| r_{i,j}(\tau) \right|^2 \quad (6)$$

where,

$$r_{i,j}(\tau) = \frac{1}{N}\sum_{\tau=0}^{N-1} c_i(0) c_j(\tau) \quad (7)$$

3 Logistic Map

The dynamics of the logistic map is determined by the bifurcation parameter. The form of the discrete logistic map used is defined as

$$x_{n+1} = rx_n(1-x_n) \quad (8)$$

where r is the bifurcation parameter and lies between 0 and 4, x_n belongs to the open interval of 0 and 1, x_0 is the initial condition, u can takes any integer value and n can takes any integer value, including zero.

Reference [4] present four regions of the logistic map as defined by the bifurcation parameter. This is depicted in fig. 1 and shown as follows:

Case I ($0 \le r \le 1$)
The system always converges to x = 0

Case II ($1 \le r \le 3$)
It converges to different stable point given by the solution x = 1- 1 / r

Case III ($3 \le r \le 3.56$)
The attractor becomes unstable and period doubling occurs as the distance between successive bifurcations in the period doubling shrinks by Feigenbaum constant.

Case IV ($3.5669 \le r \le 4$)
Most values of r in this range produce chaos

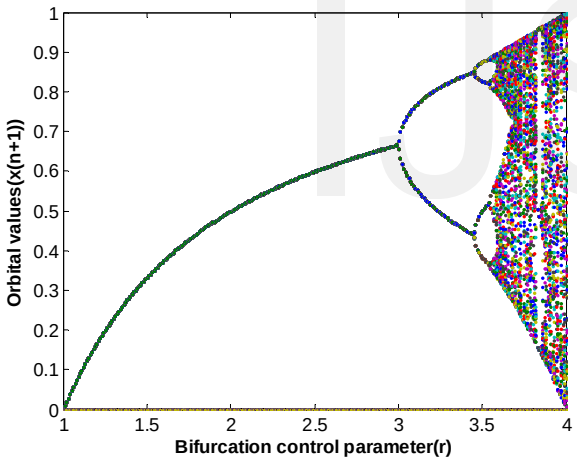

Figure 1: Bifurcation Diagram for Logistic Map

.

4 Generation of Real Chaotic Sequences

The generations of chaotic sequences in related works have been based on initial condition sensitivity. In the design of this code set, a preliminary investigation was carried out to determine the sensitivity of the logistic map to bifurcation parameter. The initial condition was fixed, the bifurcation parameter was perturbed to 10^{-3} degree; the trajectory shows marked difference after few iterations just like when the initial condition was perturbed and bifurcation parameter was fixed as shown in Figures 2 and 3. This was substantiated in [16] where distance between two sequences with slightly different parameters but same computational precision and same initial values was estimated. The work suggest that it is effective to modify the control parameter with slight difference if $r \approx 4$, since the two sequences are completely different from each other. However there is a slag in making sequence generation dependent on bifurcation parameter. In [4], it was observed that although most values beyond 3.57 exhibit chaotic behaviour, but there are still certain isolated values of r that shows non-chaotic behavior; these are sometimes called *islands of stability*, which are shown in figure 4 with negative Lyapunov exponent. For instance, around 3.82 there is a range of parameters r which show oscillation between three values, and for slightly higher values of r, oscillation between 6 values, then 12 etc. Since there are many dense periodic orbits in the chaotic region of interest, the approach is to break the chaotic region into equal interval chaotic domains. This is done by calculating Lyapunov exponent, which put a quantitative number to the chaoticity at different bifurcation parameter values. To calculate the Lyapunov exponent (λ), the method presented in [17], which depends on derivative of one orbit was used.The defining equation for it is:

$$\lambda = \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n} \ln\left| f'(x_i) \right| \quad (9)$$

It should be noted about the Lyapunov exponent as shown in Figure 4 that region with negative values exhibit periodicity, while region with positive values exhibit chaos. The larger the positive value, the greater the level of chaos. As such, chaotic region between r = 3.675 and r = 4 was used. After running the Matlab simulation of equation 10, ten domains (D1 – D10) are obtained having equal interval of 0.025.

Since the Lyapunov exponent increases with bifurcation parameter, the worst case scenario is D1 domain; the sequence generation was done in this domain and D7 for comparison. The sensitivity to bifurcation values taken at an accuracy of 10^{-4} was considered. It was discovered that the signals become uncorrelated after less than ten iterations. Subsequently, to generate real valued chaotic sequence of period N, the map was iterated N+10 times and the first ten discarded.

5 Chaotic Sequence Encoder

Since chaotic maps output are non- binary, there is need for encoding. The commonest method of encoding involves setting a threshold, and assigning a '1' or a '0' depending on whether the real chaotic value is greater or less than the threshold. The threshold for encoding was determined by passing a training sequence to Lloyd, A-law and Mu-law compression algorithms in turn. The effect of the compression algorithms on the encoded binary sequence can be seen in Tables 1-3. Since Lloyd shows best performance for odd number of real sequences, 2-bit and 4-bit encoding are investigated on it, as shown in Table 4. Although, performance improves with increasing quatization level, execution time is increased also. Therefore, 2-bit encoding offers a compromise between performance and execution time. Thus, the 2-bit encoding

corresponds to three partitions LT1, LT2 and LT3. Encoding of the real value sequence *x* is done according to the decision

$$x_i = \begin{matrix} 00 \\ 01 \\ 10 \\ 11 \end{matrix} if \begin{matrix} x_{n+1} \le LT1 \\ LT1 < x_{n+1} \le LT2 \\ LT2 < x_{n+1} \le LT3 \\ x_{n+1} > LT3 \end{matrix} \quad (10)$$

As stated in [5], there are usually some identical sequences that may be generated from different initial states, so these duplicates must be eliminated. It can be stated of this sheme that the possibility of repeated codes is approximately zero.

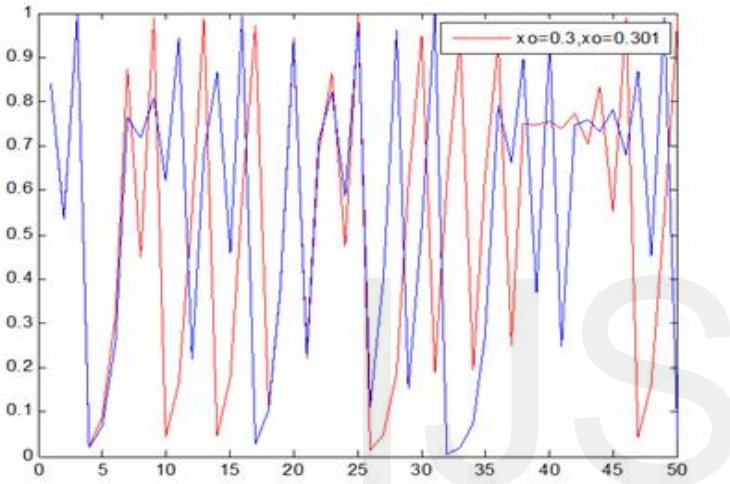

Figure 2: Time series produced from initial condition sensitivity taken to an accuracy of 10^{-3}

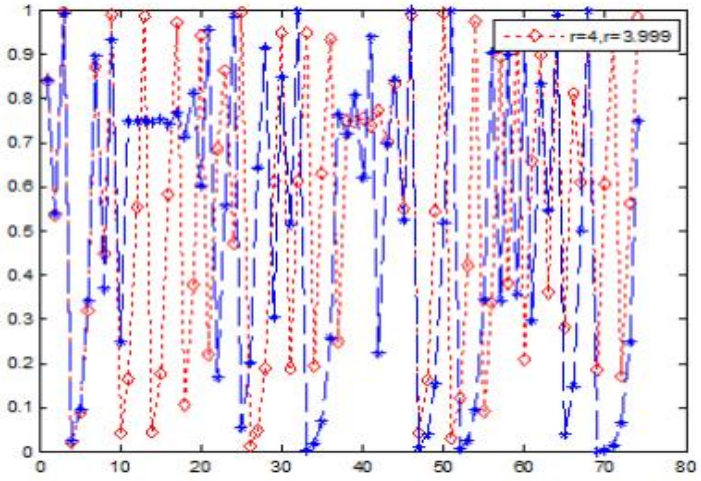

Figure 3: Time series produced from bifurcation parameter sensitivity taken to an accuracy of 10^{-3}

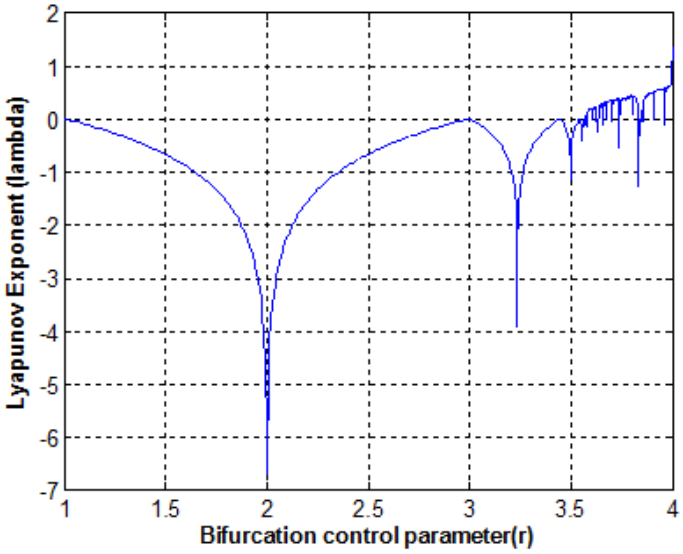

Figure 4: Lyapunov exponent measurement of Logistic map

TABLE 1
EFFECT OF LLOYD THRESHOLD ON CORRELATION MEASURES

Samples	MSAAC	MSACC	Size	Length
odd	5.0736	4.1486	26	63
even	7.5230	4.6783	26	62
even	7.4838	4.7111	26	64

TABLE 2
EFFECT OF A-LAW THRESHOLD ON CORRELATION MEASURES

Samples	MSAAC	MSACC	Size	Length
odd	5.2877	4.8101	26	63
even	6.7578	5.1321	26	62
even	6.7764	5.1673	26	64

TABLE 3
EFFECT OF MU-LAW THRESHOLD ON CORRELATION MEASURES

Samples	MSAAC	MSACC	Size	Length
odd	5.5584	5.0094	26	63
even	6.9614	5.2882	26	62
even	6.9911	5.3281	26	64

TABLE 4
EFFECT OF ENCODING LEVEL ON CORRELATION MEASURES USING LLOYD THRESHOLD

Encoding Type	MSAAC	MSACC	FOM	Size	Length
1-Bit (odd)	5.0736	4.1486	0.1971	26	63
1-Bit (even)	7.5230	4.6783	0.1329	26	62
1-Bit (even)	7.4838	4.7111	0.1336	26	64
2-Bit (odd)	2.1783	2.1069	0.4591	26	62
2-Bit (even)	3.1211	2.3951	0.3204	26	64
4-Bit (even)	1.6606	1.4699	0.6022	26	64
4-Bit (odd)	1.3045	1.3896	0.7666	26	68
4-Bit (odd)	1.2479	1.3137	0.8014	26	60

6 Proof of Bifurcation Sensitivity

One of the important indications of chaos is sensitive dependence on initial conditions. Lyapunov exponent is a quantitative measure of chaos that allows us to define exactly what is meant by chaos [18]. From the proof of chaos sensitivity to initial condition in [17], this can easily be extended to show chaos sensitivity to bifurcation parameter. Let the number of unique sequences to be generated be denoted by u. The one dimensional logistic map of Equation 8 on can be modified to account for the bifurcation sensitivity as $x_{n+1}=r_u x_n(1-x_n) = f_u(x)$ where u is the number of independent sequences and is an integer.

Let $\{a_1,a_2,a_3.....\}$ be orbit of $f_1(x)= r_1x_n(1-x_n)$ and $\{b_1,b_2,b_3.....\}$ be orbit of $f_2(x)= r_2x_n(1-x_n)$, where $a_1 = f_1(x_0)= r_1x_0(1-x_0)$ and $a_2 = f_1(a_1)$, $a_3 = f_1(a_2)= f_1^2(a_1)$, x_0 is the initial condition and it is fixed for all sequences. Similarly, $b_1 = f_2(x_0)= r_2x_0(1-x_0)$ and $b_2 = f_2(b_1)$, $b_3 = f_2(b_2)= f_2^2(b_1)$. Then the lyapunov number of orbit $\{a_1,a_2,a_3.....\}$ can be defined as

$$L(a)=\lim_{n\to\infty}\left| f_1'(a_1)\, f_1'(a_2)..... f_1'(a_n)\right| \tag{11}$$

If this limit exists and assuming that $f_1'(a_j) \neq 0$ for all j, the lyapunov exponent can be defined as

$$\lambda=\lim_{n\to\infty}\frac{1}{n}\sum_{i=0}^{n}\ln\left| f_1'(a_i)\right|\equiv \ln L \tag{12}$$

Where L(a) is the average separation rate for the orbit $\{a_1,a_2,a_3.....\}$ and a nearby orbit per iteration.

Now consider a few first iterations. Let $b_1 \approx a_1$ since x_0 is the same and f_1 and f_2 are chosen to be very close, $b_2 = f_2(b_1)$ and $a_2 = f_1(a_1)$, then $b_2 - a_2 \approx f_1'(a_1)(b_1 - a_1)$, which follows that $|b_2 - a_2| \approx |f_1'(a_1)|\,|(b_1 - a_1)|$ and $|f_1'(a_1)|$ is the multiplicative separation rate. After two iterations, we get $b_3 - a_3 \approx f_1'(a_2)(b_2 - a_2) \approx f_1'(a_2)f_1'(a_1)(b - a)$. Therefore, the multiplicative separation rate of two iterations is $|f_1'(a_2)f_1'(a_1)|$. From this, the average multiplicative separation rate per iteration can be defined as $A=|f_1'(a_2)f_1'(a_1)|^{1/2}$ and the separation rate for two iterations is A^2. Since the orbit involves infinite number of points, we define L(a) as above. If L(a) > 1, then nearby orbit will depart from the original orbit $\{a_1,a_2,a_3.....\}$. The condition L(a) > 1 implies that $\lambda > 0$. Therefore, a positive lyapunov exponent indicates that nearby orbits will depart from $\{a_1,a_2,a_3.....\}$. This implies sensitive dependence on bifurcation parameter.

7 Results

The number of sequences generated for any given length is greatly influenced by the degree of perturbation of the bifurcation parameter. For 62-bit length in the D1 domain, 26 sequences were generated with 10^{-3} perturbation degree as against 249 sequences when perturbation degree is 10^{-4}. The comparison of the sequence with 63-bit gold and m-sequence (Table 5), shows that their MSAAC and MSACC is also good; even for D1 domain, which is the worst case.

TABLE 5
CORRELATION COMPARISON

Sequence	MSAAC	MSACC	Code Set	Length
Maximal	0.0156	0.9908	6	63
Gold	0.9692	0.9841	65	63
Logistic (D1) Initial 0.7	2.4202	2.0025	249	62
Logistic (D7) Initial 0.7	1.0791	1.0247	251	62

7 CONCLUSION

In this paper, it has been shown that logistic map exhibit bifurcation sensitivity, which can be explored for generating chaotic sequences. The generating algorithm yield sequences with good correlation properties, such as can be used in DSCDMA and WCDMA. The large keyspace suggest difficult cryptanalysis in cryptography application. In future work, we intend to compare the performance of the bifurcation sensitive chaotic sequence in a CDMA environment.

ACKNOWLEDGMENT

The authors wish to thank Nigeria Tertiary Education Trust Fund (TETFund) and University of Ibadan. The staff training and development grant was made available by TETFund through the University of Ibadan.

REFERENCES

[1] C. Fatima and D. Ali, "New chaotic binary sequences with good correlation property using logistic maps," *IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)*, vol. 5, no. 3, pp. 59-64, 2013.

[2] B. N. Mahaseth and M.S. Anuradha, "Binary and Ternary Sequence Generation Using Improved Logistic Map," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 2, no. 8, pp. 3290-3294, August 2013.

[3] M. V. Mandi, R. Murali, and K.N. Haribhat, "Chaotic functions for generating binary sequences and their suitability in Multiple Access," in *Communication Technology, 2006. ICCT '06. International Conference on*, Guilin, 2006, pp. 1-4.

[4] V. H. Mankar, T. S. Das, and S. K. Sarkar, "Discrete Chaotic Sequence based on Logistic Map in Digital Communications," in *National Conference on "Emerging Trends in Electronics Engineering & Computing*, Nagpur, 2010, pp. 1017-1020.

[5] C. Vladeanu, I. Banica, and S.El. Assad, "Periodic chaotic spreading sequences with better correlation properties than convectional sequences-BER performances analysis," in *Signals,Circuits and Systems, 2003. SCS 2003.International Symposium on*, vol. 2, Iasi,Romania, 2003, pp. 649-652.

[6] M. Suneel, "Cryptographic pseudo-random sequences from the chaotic," *Sadhana*, vol. 34, no. 5, pp. 689-701, October 2009.

[7] N. K Pareek, V. Patidar, and K. K Sud, "A Random Bit Generator Using Chaotic Maps," *International Journal of Network Security*, vol. 10, no. No.1, pp. 32-38, 2010.

[8] K.R Raja,.M Revathi,.A Sampath, and.P Indumathi, "Secure Communication Using Chaos in Multiple Access Environment," in *Proceedings of the 8th WSEAS International Conference on Applied Electromagnetics, Wireless and Optical Communications*, pp. 15-19.

[9] P. Chengji and W. Bo, "Optimal Design and Performance Analysis for Chaotic Spreading," in *2012 4th International Conference on Signal Processing Systems (ICSPS 2012)*, vol. 58, Singapore, 2012, pp. 170-175.

[10] S. Liua, W. Sheng, X. Zhang, and Y He, "Digital Generating Scheme of Composite Discrete Chaotic Biphase Coded Signals," in *International Conference on Electronics, Information and Communication Engineering Lecture Notes in Information Technology*, vol. 11, 2012, pp. 105-109.

[11] K. Umeno and K Kitayama, "Spreading sequences using periodic orbits of chaos for CDMA," *Electronic Letters*, vol. 35, no. 7, pp. 545-546, April 1999.

[12] H. Zhang, J. Guo, H. Wang, R. Ding, and W Chen, "Oversample Chaotic Map Binary Sequences: Definition, Performance and Realization," in *Circuits and Systems, 2000. IEEE APCCAS 2000.*, Tianjin, 2000, pp. 618-621.

[13] M. P. Chawla, "A review comparison of different spreading codes for DS CDMA," *IJSRD - International Journal for Scientific Research & Development* |, vol. 2, no. 2, pp. 995-999, 2014.

[14] V. A. Kumar, Mitra A., and S. R. M. Prasanna, "On the Effectivity of Different Pseudo-Noise and Orthogonal Sequences for Speech Encryption from Correlation Properties," *International Journal of Information Technology*, vol. 4, no. 2, pp. 145-152, 2007.

[15] V. A. Kumar, A. Mitra, and S. R. M. Prasanna, "Performance Analysis of Different Pseudo Noise Sequences for Speech Encryption," *International Journal of Information and Communication Engineering*, 2008.

[16] S. Araki, K. Kakizaki, T. Miyazaki, and S. Uehara, "A study on distance between two sequences by the LogisticmMap over integers with slightly different parameters," in *Signal Design and Its Applications in Communications, The Sixth International Workshop on*, Tokyo, 2013, pp. 64 - 67.

[17] Y.Y. Lu. Introduction to dynamical systems and chaos. [Online]. http://math.cityu.edu.hk/~mayylu/ma4528/notes.pdf. 2016

[18] J. Bovy. (2004, September) Lyapunov exponents and strange attractors in discrete and continuous dynamical systems.