ON THE COMPLEXITY OF A DIGITIZED LOGISTIC MAP

[1]RAKIYA MK ADAMU, [2]ALIYU DANLADI HINA, [3]ISA YAHAYA

[1,2,3]Dept. of Mathematics & Statistics, The Federal Polytechnic, Bauchi, Bauchi State.

ABSTRACT

A topologically conjugate map that is equivalent to the well known logistic map $f(x) = ax(1-x)$ *with* $x \in [0,1]$ *and* $\alpha \in [0,4]$ *is constructed. This constructed map's domain is defined to be the integer domain [0,* 2^n*). This domain has a one to one correspondence to the points in the interval [0, 1] with n-bits precision. The topological conjugacy of the two maps and the dynamics of the constructed map were found to define the same dynamics as that of the logistic map with very similar lyapunov exponents. With a view to be applied in cryptography as a Pseudo-Random number generator (PRNG), the complexity of the constructed map as a source of randomness is determined using both the Permutation entropy (PE) and the Lempel-Ziv (LZ-76) complexity measures, and the results are compared with numerical simulations.*

Keywords: *Leveling Network, LSE, MATLAB, Weighted, Unweighted.*

INTRODUCTION

One of the basic ingredients of cryptography is the Random Number generators (RNG) used in generating the pseudo-random key streams mentioned above. The realization of (RNG) using chaotic maps cannot be said to be truly random since the maps are deterministic thus the name Pseudo-Random Number generators (PRNG).

Discrete-valued sequences generated from chaotic systems have received considerable attention in the field of cryptography (Stojanovski and Kocarev, 2001; Shuai, et al. 2010), spread-spectrum (Heidari-Bateni and McGillem, 1994), communication and coding (Hayes, S., Grebogi, and Ott, 1993), Pseudo-Random Number Generators (PRNG) (Kocarev et al. 2003) etc. If designed carefully, sequences of independent and identically distributed random variables will be produced by certain one-dimensional (1D) chaotic systems, e.g., the tent map and the logistic map. We considered sequences generated from one dimensional (1D) discrete time dynamical systems.

There are basically two ways of designing digital chaotic ciphers that has received attention in literature:

1) The use of chaotic systems to generate pseudo-random key stream, which is used to mask the plaintexts;
2) Iterating a chaotic systems a multiple number of times to obtain ciphertext using the plaintext and/or the secret key(s) as the initial conditions and/or control parameters.

In the topology of a digital (PRNG) Fig. (1), the state forming logic is a digital nonlinear map (a map taking integer values) which serves a source of entropy that gives the generated sequence the required randomness. This state forming map is defined a map of the form $g : \Omega \rightarrow \Omega$ on an integer phase space $\Omega = [0, 2^{n-1}]$ for a given precision 2^n. At this precision, a one to one correspondence with the real phase space $I = [0, 1] \subset \mathbb{R}$ is realized. The candidacy of chaotic maps as random number generators despite being deterministic is dependent on their characteristics such as aperiodicity with a positive lyapunov exponent, sensitivity to initial conditions. We will be considering a discrete time dynamical system where the future state depends only on the current state.

The use of chaotic maps in the construction of PRNGs has received considerable attention from researchers (Lagarias, 1990; Chien and Liao, 2005; Addabbo et al., 2007a; Addabbo et al., 2007b; Xie and Han, 2010). Inability to compute complexities (probabilities and entropy) of the RNG, Reliance by authors on the assumed randomness of a physical process among other factors renders most of the PRNGs inefficient. In this paper, we focused our attention on the complexity of the sequence generated, it is obvious that the randomness of the sequence of pseudo-random numbers (PRN) generated cannot be more than that of the input of the state forming map (Cicek, et al., 2014). The difficulty to find, and the criteria for the construction of a good (RNG) has been suggested in (Park and Miller, 1988). Researchers have therefore converged to the fact that the quality of a PRNG depends on the complexity measure of the nonlinear map generating the input states.

The quantity defining the complexity of a system gives an in-depth knowledge into the mechanisms governing the processes. This quantity is determined by the measure of entropy, early works in classical entropy includes, the Shannon entropy (Segal, 1960), Kolmogorov-Sinai entropy (Collet et al., 1983), topological entropy (Smital, 1986). Classical approaches to entropy computation are characterized by the requirement of a long sequence thus making them computationally expensive. As a solution to this shortcoming, Bandt and Pompe (2002) came up with a new approach to entropy measure which they called permutation entropy (PE) which was successful in addressing the identified lapse of the earlier methods, e.g. Kolmogorov-Sinai measure. Canovas et. al. (2013) computed the topological and Shannon permutation entropies of interval maps, a measure of randomness for chaotic binary series was implemented in (Liu et al., 2015). As a result of wide ranges of applications of PE in

diverse areas of research, we choosed to adopt it in this article as a measure for complexity. The Lempel Ziv complexity is also implemented, based on the comparison of the two methods in (Lempel and Ziv, 1976), we equally compared the two results.

For the purpose of this paper we will be considering a family of one parameter family of one dimensional maps which we denote by $\boldsymbol{F}$. If we define a one dimensional (1D) map $f \in \boldsymbol{F}$ by:

$$x_{n+1} = f(x_n) = \alpha * x_n * (1 - x_n), \qquad x_n \in [0,1], \quad \alpha \in [0,4], \quad n = 0, 1, \ldots \qquad (1)$$

where $a * b$ denotes the algebraic product of a and b and $f : I \to I$, $f(0) = f(1) = 0$, is a nonlinear unimodal mapping which has two preimages, and I is the interval [0,1].

The logistic map is known to have the probability density function (PDF) of $\frac{1}{\pi\sqrt{x(1-x)}}$ [22] and that of the tent map is given by $\frac{1}{b-a}$ [23]. While the PDf of the tent map is uniform that of the logistic map is non uniform A unimodal map f(x) is a one-dimensional function $f : \mathbb{R} \to \mathbb{R}$ defined on an interval $I \in \mathbb{R}$ with a monotonically increasing (or decreasing) branch, a critical point $x_c$for which $f(x_c)$ attains the maximum (minimum) value, followed by a monotonically decreasing (increasing) branch. With unimodal maps, the interval is stretched and folded only once, with at most two points mapping into a point in the refolded interval. Maps with multiple critical points in the interval I are called Multi-modal maps. System may depend on many parameters, for one dimensional maps, it is sufficient to study one parameter family of maps since using more parameters does not bring about a different phenomena. A suitably chosen one parameter map, will go through all possible spectrum of orbits, the map under study (1) falls into this category of maps.

Chaotic sequences are by computation periodic; this is due to the limitation in memory of the computing machine. All chaotic algorithms operated on the limited precision machine producing chaotic sequence does not completely have chaotic characteristics since they are found to degrade dynamically (Lasota and Mackey, 2013). Periodicity is an inherent characteristic of chaotic sequences generated from such mediums with as low periods as less than 500. This therefore raises alot of concerns as to the viability of their uses in cryptographic protocols. The chaotic sequence will inevitably evolve into a sequence with period under the approximate operation results, which will make encryption algorithm based on chaos theory to be cracked ultimately. Chaotic maps being deterministic, makes iterates depend on one another as the orbit moves forward in time. This dependency creates correlation between elements of the sequence generated by the chaotic map, with the correlation decreasing down the sequence. This implies that the correlation between two adjacent elements is much higher that any

two that are further apart. We studied the issue of correlation within chaotic sequence that are obviously periodic, with short periods, thus very inappropriate for cryptographic applications. This is done through the use of a transformation called Karhunen - Loeve Transform (KLT). This transform is found to be a better method in eliminating correlation than both the Discrete Cosine Transform (DCT) and the Discrete Fourier Transform (DFT).

It is an optimal transform which can as well increase the period and complexity of the digital chaotic sequence. Karhunen - Loeve Transform takes a given collection of data (an input collection) and creates an orthogonal basis (the KLT basis) for the data. We will be considering a univariate time series generated from a one dimensional map.

(A univariate time series is a sequence of measurements of the same variable collected over time. Most often, the measurements are made at regular time intervals).

All simulations are conducted with a precision of 2^{16} extending to other precisions of choice follows with memory availability on the machine of implementation.

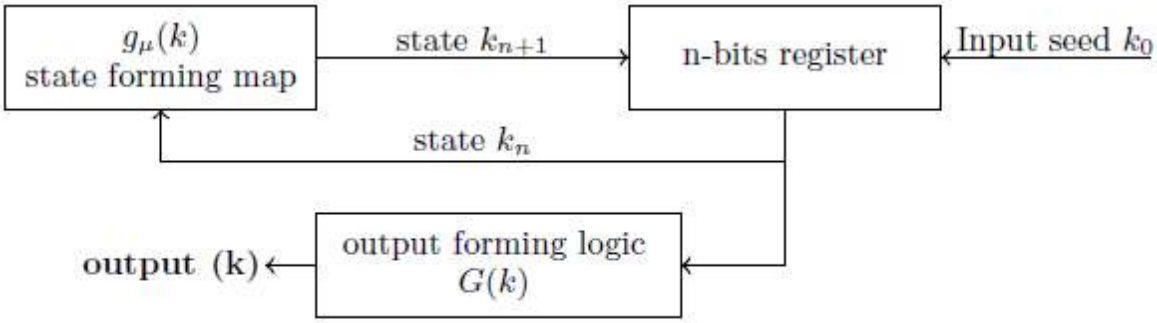

Fig. 1. A typical topology for PRNG

2.0 Constructing the Digital Map

As we have mentioned above that the state forming map of the PRNG is a digitized variant of the map f, we will thus digitize the map f into its equivalent with integer input. Given the map (1) with $x_i \in I = [0, 1]$, the state x_i is given by a rational number represented with an infinite binary representation $x_i = 0.b_1b_2b_3 \ldots b_n \ldots$ where each $b_i = \{0, 1\}$.

Due to the finite precision of the computing machine, the infinite binary number will be truncated a particular position depending on the precision of the machine. We highlight, before we continue that: $XmodY = X - floor\left(\frac{X}{Y}\right)Y$XmodY, and the floor function is the smallest integer less than or equal to x. Let the approximated state of the system be $\tilde{x}_i = 0.b_1b_2b_3 \ldots b_n$ (assuming a precision of 2^n) is a set of rationals of

the form $\tilde{x}_i = \frac{k_i}{2^n}$ where $k_i, 2^n \in \mathbb{N}$. This therefore makes $\tilde{x}_i$ assume rational values in $I \subset \mathbb{R}$ as defined below:

$$\tilde{x} = (0.b_1 b_2 b_3 \ldots b_n)_2 = \sum_{j=1}^{n} b_j 2^{-n}, \quad b_j = \{0, 1\} \tag{2}$$

where b_1 and b_n are the most significant bit (MSB) and the least significant bit (LSB) respectively. Its obvious to observe that each bit string represents a unique discretized state $\tilde{x}_i$, thus each $\tilde{x}$ can be related to an integer number $k_i = 2^n * \tilde{x}_i \in \mathbb{Z}, \quad 0 \leq k_i \leq 2^n - 1$.

The discretized map can therefore be expressed as

$$\tilde{x}_{n+1} = \tilde{f}_a(\tilde{x}_n)_{t,r} \tag{3}$$

where a is the control parameter and the subscripts t and r account for the truncation and rounding off approximation strategy used for evaluating $\tilde{f}_a$ to the required precision. Suppose the truncation is effected to the precision 2^n, the (3) becomes:

$$\tilde{f}(\tilde{x}) = floor(2^n * a * \tilde{x}_n * (1 - \tilde{x}_n) mod\ 2^n) * 2^{-1} \tag{4}$$

One will observe to see that there is a one - one correspondence between $\tilde{I}$ and the set $\mathcal{K} = \{k \in \mathbb{N}: 0 \leq k \leq 2^n - 1\}$. We can therefore define a conjugate map $g: \mathcal{K} \to \mathcal{K}$. Thus, there exist a homeomorphism $h: I \to \mathcal{K}$ such that $h \circ f(k) = g \circ h(k)$ with $h(k) = 2^n \tilde{f}(\frac{k}{2^n})$. Through the transformation h(k) we define the conjugate map $g: \mathcal{K} \to \mathcal{K}$ by:

$$g(k) = floor\left(2^n * a * \frac{k}{2^n} * \left(1 - \frac{k}{2^n}\right)\right) mod\ 2^n$$

$$k_{n+1} = g(k) = floor(2^{-n} * a * k * (2^n - k_n) mod 2^n \tag{5}$$

The expression (5) describes the same dynamics as (1). It is therefore the digitized version of (1) with integer inputs. For value of s = 4, (5) is simplified to

$$k_{n+1} = g(k) = floor(2^{2-n} * a * k * (2^n - k_n) mod 2^n \tag{6}$$

with k is restricted to the space $\Omega = [0, 2^n - 1]$.

We are considering the value of a within the range $3.57 \leq a \leq 4$, we have to consider other values of a other than a = 4. Let $3.57 \leq a \leq 4$, thus it can be written as $a = a_I + a_f$ where a_I is the integer part of a and a_f is the corresponding fractional part, (5) can therefore be expressed as:

$$k_{n+1} = g(k) = floor(2^{2-n} * (a_I + a_f) * k * (2^n - k_n) mod 2^n \quad (7)$$

$$k_{n+1} = g(k) = floor(2^{2-n} * [(k * a_I) + (k * a_f)] * (2^n - k_n) mod 2^n \quad (8)$$

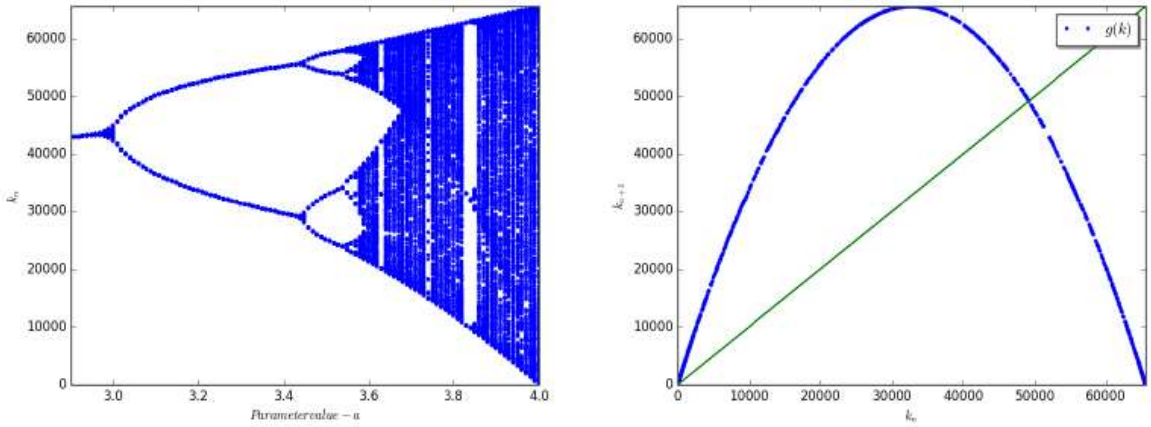

Fig. 2. Bifurcation of the Digitized map and its Dynamics

Due to the modular operation embedded, it will just be sufficient to consider the integer part of 8, which reduces it to:

$$k_{n+1} = floor\left(2^{-n} * [(k * a_I) + floor(k * a_f)] * (2^n - k_n)\right) mod 2^n \quad (9)$$

Where a_I is necessarily equal to 3 and a_f is of the form 2^{-t} for t > 0.

Figure (2) describes the bifurcation of the digitized map along the parameter axis showing the period 3 window at the appropriate location as is obtained in the classical map. The dynamics is on a precision of 2^n defining similar trajectory. All dynamical properties of (1) are also defined on (5) at the corresponding location on the discretized phase space Ω.

3.0 Complexity

In the last two decades, complexity theory grew out of chaos theory and largely supplemented it as an analytic frame for social systems. Complexity draws on similar principles but in the end is a very different beast. The comparison between chaotic and random time series is usually undertaken by the measure of the complexity of the systems. Tools used for the determination of complexity includes among others, entropy, lyapunov exponents and fractal dimensions, there inter relationship enables the computation of one from the other. The relationship between complexity and

entropy on the description of the information of a discrete ergodic source was first mentioned by Shannon, although without a precise definition of the second quantity called complexity. Kolmogorov (Kolmogorov et al., 1965) later gave a detailed definition of the concept on a finite word. The works (Lempel and Ziv, 1976; Bandt and Pompe, 2002; Riedl, et al., 2013) and many more provides rich insight into the area. Lempel and Ziev [21] proposed a method that uses the gradual build-up of new patterns along the sequence of interest thereby constructing random like sequence. The use of permutation entropy as a measure of complexity was reported in the works of Bandt and Pompe (2002), and Bandt, Keller and Pompe (2002). The presence of observational noise has little or no effect on the complexity chaotic time series without the need for pre-processing and fine tuning of parameters.

3.1 Entropy of the Map

The dynamical complexity of a measure-preserving system f_α can be quantified by its metric entropy. The metric entropy measures the uncertainty of the forward evolution of the system when the initial condition is not exactly known the higher the uncertainty, the greater the complexity.

3.1.1 The Permutation Entropy

As a complexity measure for the given map, we had used the permutation entropy approach in the sense of Bandt and Pompe (2002). Computing for interval maps was implemented in (Bandt et al., 2002). The explicit use of partitions as required in the topological case is not necessarily the case in permutation entropy. As an ingredient we take the following definition. An exclusive review on the use of PE with considerations on the dependent parameters is given in (Amigó, et al., 2004). An important concept in the definition of permutation entropy is the Ordinal patterns.

Definition 2: Let $x \in I$ and let σ_L be the set of permutations $\{0, 1, 2, \dots, L-1\}$ of length L. Given an interval map $f: I \to I$ we can associate to $\{f^t(x): 0 \le t \le L-1\}$ its order pattern $\pi(x) = [\pi(0), \pi(1), \dots \pi(L-1)]$ if: $f^{\pi(0)} < f^{\pi(1)} < f^{\pi(2)} < \cdots < f^{\pi(L-1)} \in \sigma_L$, x is therefore said to have defined the order pattern $\pi = \pi(x)$.

Let P_π be the set of points for which their orbits defined the pattern π by:

$P_\pi = \{x \in I: x_0 < x_1 < \cdots < x_{L-1}\}, \quad for\ L \ge 2$. for L = 4, the table below gives the 24 possible permutations $\pi \in \sigma_4$.

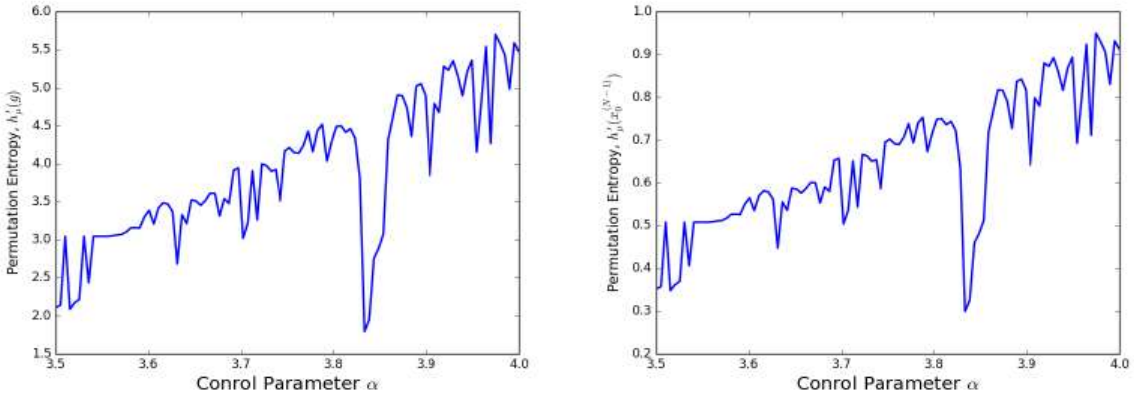

Fig. 4. Permutation entropy of the map (left) and the per symbol permutation entropy (right)

Order Patterns of length four, $P_\pi : \pi \in \sigma_4$							
$\pi(i)$	$P_{\pi(i)}$	$\pi(i)$	$P_{\pi(i)}$	$\pi(i)$	$P_{\pi(i)}$	$\pi(i)$	$P_{\pi(i)}$
0	[0, 1, 2, 3]	7	[1, 0, 3, 2]	14	[2, 1, 0, 3]	21	[3, 1, 2, 0]
1	[0, 1, 3, 2]	8	[1, 2, 0, 3]	15	[2, 1, 3, 0]	22	[3, 2, 0, 1]
2	[0, 2, 1, 3]	9	[1, 2, 3, 0]	16	[2, 3, 0, 1]	23	[3, 2, 1, 0]
3	[0, 2, 3, 1]	10	[1, 3, 0, 2]	17	[2, 3, 1, 0]		
4	[0, 3, 1, 2]	11	[1, 3, 2, 0]	18	[3, 0, 1, 2]		
5	[0, 3, 2, 1]	12	[2, 0, 1, 3]	19	[3, 0, 2, 1]		
6	[1, 0, 2, 3]	13	[2, 0, 3, 1]	20	[3, 1, 0, 2]		

Table 1. Order Patterns of length four, $P_\pi : \pi \in \sigma_4$

An ordinal pattern can be allowed or forbidden pattern of the map g depending on the cardinality of P_π. It is allowed if $P_\pi \neq 0$ otherwise it is forbidden. We define the intervals defined by the permutation $P_\pi \neq 0$ by the relation $g^{\pi(i)}(k) = g^{\pi(i+1)}(k)$ $for\ i = 1, 2, \dots L-2$. We considered both the Metric and Topological aspects of the permutation entropy.

Permutation Entropy Let μ be an $f-$ invariant measure, from the notion of Shannon's entropy of information source, and let there be a finite sequence of length N such that the relative frequency of the pattern π is given by:

$$p(\pi) = \frac{\{t\,; 0 \leq t \leq N-w, (x_{t+1}, x_{t+2}, \dots, x_{t+w}),\quad of\ type\ \pi\}}{N-w+1}$$

We define from [35],

$$h'_\mu(g) = -\lim_{L\to\infty} \frac{1}{L} \sum_{\pi\in\sigma} \mu(p(\pi)) log\mu(p(\pi)) \qquad (20)$$

if the limit exist, where $\mu p(\pi)$ is the probability for the ordinal L-pattern π occurring as defined above. For the Topological Permutation Entropy, one counts the number of distinct allowed patterns

$$h'_T = -\lim_{L\to\infty}\frac{1}{L}\log|\{P_\pi \neq \emptyset : \pi \in \sigma_L\}| \quad (21)$$

However, [30] states in their result that for a piecewise monotone map g, $h'_\mu(g)$ converges to $h_\mu(g)$ and similarly $h'_T(g)$ converges to $h_T(g)$. Given the set P_π as defined above, let $f : I \to I$ defined on $I \in \mathbb{R}$ Have an invariant measureμ, Let P_L be a partition of I, define P_L as $P_\pi = \{P_\pi \neq \emptyset : \pi \in \sigma_L\}$. The topological permutation entropy of order $L \geq 2$ is defined as $H^L_{Top}(f) = \frac{1}{L}\log |P_L|$. If there is a finite partition of I into intervals, such that f is a continuous and monotone on each of those intervals, then:

$$\lim_{L\to\infty} H^L_{Top}(f) = h_T(f) \quad (22)$$

If L is finite, (22) estimates h_T in fact it holds only when it is finite and monotone [35]. It follows that: $|P_L| = |\{P_\pi \neq \emptyset : \pi \in \sigma_L\}|$. It can be shown that, $|P_L| \propto e^{Lh_{Top}(f)}$ indicating that the number of allowed L-patterns for f grows exponentially with L.

Proposition 1 For a map f defined on the unit interval I, there exist $\pi \in \sigma_L$ and $L \geq 2$ such that $P_\pi = \emptyset$.

Figure (4) shows the permutation entropy of the digitized map with a pattern length of 6 for both the map (left) and the per symbol computation (right). It can be observed that the peaks of the two computations coincide, implying that the entropy per symbol is nothing but the entropy of the map confine within the interval [0; 1].

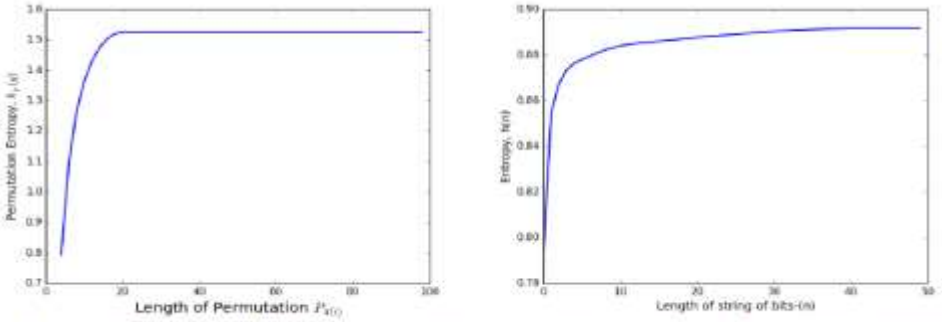

Fig. 5. Asymptotic Convergence of the Permutation entropy and Shannon Entropy at L = 12 along the parameter axis

Figure 5 above indicates existence of the limit in (20) which converges to the value *1.5247471457695274* for the permutation entropy. Thus the entropy of digitized logistic map (9) converges to a limit (as claimed by [30]) for increasing N-the length

of the sequence. The similarity of the graphs in Figure (4) with that of the lyapunov exponents Figure (3) tells us that one can be computed from the other.

3.2 Lempel-Ziv Complexity

This complexity measure was given birth to my A. Lempel and J. Ziv in the years 1976 and 1978 giving rise to the notations LZ - 76 (Ziv & Lempel, 1976) and LZ - 78 (Ziv & Lempel, 1978) for the two algorithms. Hence thereafter, a lot of researchers have found the schemes worthwhile for wide range of applications due to close relation of its growth rate with that of the entropy rate of an ergodic source. In this paper we considered the LZ-76 algorithm because of its faster convergence than the LZ-78 (Ziv & Lempel, 1978).

Let the number of a distinct word (patterns) generated from the sequence $x_1^N = (x_1, x_2, \dots x_N)$, the exhaustive history of the sequence x_1^N, $E(x_1^N)$ is defined by:

$E(x_1^N) = x(i, v_1)x(v_1 + 1, v_2) \dots x(v_{m-1} + 1, N)$

With $x(i, j) = x_i x_{i+1} \dots x_j$, thw complexity of x_1^N denoted $C(x_1^N)$ is the number of factors $E(x_1^N)$. As an example, for a sequence x $= 1011101000011$, the exchaustive history of the sequence x is x $=$ E(x) $= 1|0|111|010|000|11$ where each factor is delimited by '|' thus the LZ-76 complexity of E(x) is C(x) $= |$E(x)$|$, implying that C(x) $= 6$.

From [21], for a string of length N the complexity is bounded from above by:

$$C(x_1^N) < \frac{(N)}{(1 - \epsilon_N) log_s(N)} \quad (23)$$

where s the total number of symbols in the sequence and $\epsilon \to 0$ as $N \to \infty$ decays slowly with increasing N and Its given by:

$$\epsilon(N) = 2\frac{1 + log_s log_s SN}{log_s N} \quad (24)$$

Nunes et. al [33] showed that for a binary sequence the value $\epsilon(N) = 0.1$ is achieved for as large value of N as $N = 10^{50}$. Taking limits, lets

$$\lim_{N\to\infty} C(x_1^N) = \frac{(N)}{log_s(N)} = B(N).$$

The normalized complexity $\mathcal{N}(x_1^N)$ via $B(N)$ Measures the rate of generation of new patterns along x_0^N. $\mathcal{N}(x_1^N)$ is defined by:

$$\mathcal{N}(x_1^N) = \frac{C(x_1^N)}{B(N)} \quad (25)$$

Given an ergodic source X of the string of bits with entropy rate h(X) in information theoretical definition, it was proved in [29] that:

$$h(X) = \lim sup_{N\to\infty} \frac{C(x_1^N)}{B(N)} \quad (26)$$

Equation (26) which reflects the rising rate of new patterns in the sequence, implies that random sequences, similar to those outputted from a $(\frac{1}{2},\frac{1}{2})$-Bernoulli process, reach the highest possible $C(x_0^N)$ value for an infinite length sequence.
However this does not limit the attainment of the bound by only random sequences.
We noted that for an ergodic source holds in the limit of infinite length sequences, however, h(X) always holds a value less than 1 and lim $sup_{N\to\infty} \frac{C(x_1^N)}{Nlog_s(N)}$ takes in values greater than 1 even for an infinitely long finite sequences.
From figure (6), The distribution of LZ-76 across the parameter axis (left) showing much similarity with that of the PE. One will therefore conclude that in the context of the map under discussion, complexity measure using the two different approaches are similar. The figure at the right shows the inability of LZ-76 to attain the bound defined in (23) for increasing length of the sequence N.

5.0 Conclusion

The complexity of a sequence is an important index to quantify the performance of chaotic sequences in cryptographic applications. The higher the complexity of a sequence is, the minimal the chance of recovery.

Table 2. Comparison between original and transformed Sequences

	Original Sequence		Transformed Sequence	
Precision	16	32	16	32
Period	583	4967296	Non	Non
Entropy	0.212757	0.234259	0.233437	0.234907
Complexity	91	97	114	114

We have shown that typical random sequences of finite length fall short of the maximum Lempel-Ziv complexity. We observed significant drop in the complexity of the map at parameter values corresponding to periodic windows in the parameter axis. The effect of such windows affects the randomness and statistical performance of the map. The complexity measure of the map using the two methods considered shows an agreeing pattern for an increasing length of the sequence. Despite the improvement through the KL transform, the source complexity and the information hidden in the generated sequence does not meet the requirement of high security cryptographic

application. Thus, the suitability or otherwise of the digitized map depends on the area of application, the authors are of the opinion that it will not be a good candidate for cryptographic applications without further enrichment in the form of; reducing periodicity and removing correlation through the use of post-processing functions (Algebraic or Dynamic).

References

Stojanovski, T. and Kocarev, L., 2001. Chaos-based random number generators-part I: analysis [cryptography]. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, *48*(3), pp.281-288.

Shuai, R., Jing, W. and Zhang, X., 2010, October. Research on chaos partheno-genetic algorithm for TSP. In *2010 International Conference on Computer Application and System Modeling (ICCASM 2010)* (Vol. 1, pp. V1-290). IEEE.

Heidari-Bateni, G. and McGillem, C.D.,1994. A chaotic direct-sequence spread-spectrum communication system. *IEEE Transactions on communications*, *42*(234), pp.1524-1527.

Hayes, S., Grebogi, C. and Ott, E., 1993. Communicating with chaos. *Physical review letters*, *70*(20), p.3031.

Kocarev, L., Jakimoski, G. and Tasev, Z., 2003. Chaos and pseudo-randomness. In *Chaos Control* (pp. 247-264). Springer, Berlin, Heidelberg.

Lagarias, J. C. (1990). in Cryptography and Number Theory. *Cryptology and computational number theory*, *42*, 115.

Chien, T.I. and Liao, T.L., 2005. Design of secure digital communication systems using chaotic modulation, cryptography and chaotic synchronization. *Chaos, Solitons & Fractals*, *24*(1), pp.241-255.

Addabbo, T., Fort, A., Rocchi, S. and Vignoli, V., 2007, August. On the generation of pseudo-random sequences exploiting digitized chaotic systems. In *2007 18th European Conference on Circuit Theory and Design* (pp. 639-642). IEEE.

Addabbo, T., Alioto, M., Fort, A., Rocchi, S. and Vignoli, V., 2007, May. Maximum-Period PRNGs Derived From A Piecewise Linear One-Dimensional Map. In *2007 IEEE International Symposium on Circuits and Systems* (pp. 693-696). IEEE.

Xie, Q. and Han, Z., 2010. Chaotification of nonlinear discrete systems via sliding mode control. *Journal of Computational Information Systems*, *6*, pp.4951-4958.

Cicek, I., Pusane, A.E. and Dundar, G., 2014. A novel design method for discrete time chaos based true random number generators. *INTEGRATION, the VLSI journal*, *47*(1), pp.38-47.

Park, S.K. and Miller, K.W., 1988. Random number generators: good ones are hard to find. *Communications of the ACM*, *31*(10), pp.1192-1201.

Segal, I.E., 1960. A note on the concept of entropy. *Journal of Mathematics and Mechanics*, pp.623-629.

Collet, P., Crutchfield, J.P. and Eckmann, J.P., 1983. Computing the topological entropy of maps. *Communications in Mathematical Physics*, *88*(2), pp.257-262.

Smital, J., 1986. Chaotic functions with zero topological entropy. *Transactions of the American Mathematical Society*, *297*(1), pp.269-282.

Bandt, C. and Pompe, B., 2002. Permutation entropy: a natural complexity measure for time series. *Physical review letters*, *88*(17), p.174102.

Cánovas, J.S., Rodrıguez, J.M. and Marın, M.R., 2013. Computing permutation entropy of interval maps. *International Journal of Pure and Applied Mathematics*, *82*(2), pp.163-178.

Liu, L., Miao, S., Cheng, M. and Gao, X., 2015. Permutation entropy for random binary sequences. *Entropy*, *17*(12), pp.8207-8216.

Lempel, A. and Ziv, J., 1976. On the complexity of finite sequences. *IEEE Transactions on information theory*, *22*(1), pp.75-81.

Lasota, A., & Mackey, M. C. 2013. *Chaos, fractals, and noise: stochastic aspects of dynamics* (Vol. 97). Springer Science & Business Media.

Baranovsky, A., & Daems, D. 1995. Design of one-dimensional chaotic maps with prescribed statistical properties. *International journal of bifurcation and chaos*, *5*(06), 1585-1598.

Kay, S. 1995. Asymptotic maximum likelihood estimator performance for chaotic signals in noise. *IEEE Transactions on signal processing*, *4*(43), 1009-1012.

Kay, S., & Nagesha, V. 1995. Methods for chaotic signal estimation. *IEEE Transactions on signal processing*, *43*(8), 2013-2016.

Wang, S., Yip, P. C., & Leung, H. 1999. Estimating initial conditions of noisy chaotic signals generated by piecewise linear Markov maps using itineraries. *IEEE transactions on signal processing*, *47*(12), 3289-3302.

Xiaofu, W., & Songgeng, S. 1999. A general efficient method for chaotic signal estimation. *IEEE Transactions on signal processing*, *47*(5), 1424-1428.

Kolmogorov, AN, Novoe v Zhizni, Nauke, Tekhn, Ser. Matem. Kibern 1, (1965) 24 - 29

Ziv, J., & Lempel, A. 1978. Compression of individual sequences via variable-rate coding. *IEEE transactions on Information Theory*, *24*(5), 530-536.

Bandt, C., Keller, G., & Pompe, B. 2002. Entropy of interval maps via permutations. *Nonlinearity*, *15*(5), 1595.

Riedl, M., Müller, A., & Wessel, N. 2013. Practical considerations of permutation entropy. *The European Physical Journal Special Topics*, *222*(2), 249-262.

Amigó, J. M., Szczepański, J., Wajnryb, E., & Sanchez-Vives, M. V., 2004. Estimating the entropy rate of spike trains via Lempel-Ziv complexity. *Neural Computation*, *16*(4), 717-736.