JOURNAL OF THEORETICAL PHYSICS & CRYPTOGRAPHY

www.IJTPC.org/Publications

A Pseudorandom Bit Generator based on Chaotic Coupled Map Lattices

Sodeif Ahadpour, Yaser Sadra

Department of Physics, University of Mohaghegh Ardabili, Ardabil, IRAN

Accepted: 10th August, 2012

ABSTRACT

In this paper, we discuss the properties of making a deterministic algorithm suitable to generate a pseudo random sequence of numbers: high value of Kolmogorov-Sinai entropy, high dimensionality of the parent dynamical system, and very large period of the generated sequence. We propose the chaotic coupled map lattices as a pseudo random number generator. We show what chaotic features of the coupled map lattices are useful for generating pseudo random numbers and investigate numerically which of them survive in the discrete state version of the map. To evaluate the randomness of the bit sequences generated by the RNGs, the NIST suite tests were performed. The proposed RNGs can be used in many applications requiring random bit sequences and also in the design of secure cryptosystems.

Keywords

Chaotic function, Pseudorandom sequence, Ergodic theory, Invariant measure, Coupled map lattice, NIST test.

1. INTRODUCTION

Random number generators can be classified into three classes which are true random number generators, pseudo random number generators and hybrid random number generators. Pseudo random number generators (PRNG) use deterministic processes to generate a series of outputs from an initial seed state [1,2,3]. Chaotic maps have the following stochastic properties: ergodicity, mixing, sensitive dependence on initial conditions which follows from the positivity of the Lyapunov exponent, and local divergence of all trajectories which follows from the positivity of the Kolmogrov-Sinai (KS) entropy. These properties resemble certain properties of randomness. In this paper, we present PRNG's based on an ensemble of hierarchy of one-parameter families $\Phi=(\alpha,x)$ of maps of interval [0, 1] with an invariant measure and analyze the requirements for a good PRNG with respect to our scheme [4]. An interesting property of these chaotic maps is their ability in simultaneous production and consumption of entropy. To ensure that a random number generator is secure, its output must be statistically unpredictable and indistinguishable from a true random sequence [1]. Extremely important is the application of random number generator in cryptography for generation of cryptographic keys, and random initialization of certain variables in cryptographic protocols. A good random number generation helps to improve the cryptographic security [5,6].

2. COUPLING OF ONE-DIMENSIONAL MAPS

Coupled map lattices are arrays of states whose values are continuous, usually within the unit interval, or discrete space and time. The applications of 2D chaotic maps as a random number generator are widely investigated [6,7]. In this paper we propose the coupled map as a two-dimensional dynamical map defined as:

$$\Phi(x,y)=\begin{cases} X=\Phi(x,y) \\ Y=\Phi(y,x) \end{cases}$$

As it will be shown in section 3, by an appropriate choice of the function $\Phi(x,y)$ we may have a two-dimensional dynamical system with the property of having an invariant measure in invariant sub-manifolds x=y and x= -y (if we have $\Phi(-x,y)=\Phi(x,-y)$) On the other hand, almost most of linearly or non-linearly symmetric coupled maps can be considered as a symmetric two-dimensional map of the form given by Eq. (1). The following a generic symmetric non-linearly coupled map is an example of the point:

$$\Phi_{coupled}(x,y)=\begin{cases} X=\Phi(x,y)=(1-\epsilon)\Phi_1(x)+\epsilon\Phi_2(y) \\ Y=\Phi(y,x)=(1-\epsilon)\Phi_1(y)+\epsilon\Phi_2(x) \end{cases} \quad (1)$$

where, ε the strength of the coupling, and the functions Φ_1,Φ_2 are two arbitrary one-dimensional maps. We introduce chaotic trigonometric map ensemble $\{\Phi\}$, based on the one-parameter families of chaotic maps $\tilde{\Phi}_N(x,\alpha)$ of the interval [0, 1] with an invariant measure, which can be

defined as the ratio of polynomials of degree N [4]. We first review one-parameter chaotic maps which can be used in the construction of chaotic trigonometric maps. The one-parameter chaotic maps [4] are defined as the ratio of polynomials of degree N:

$$\tilde{\phi}_N^1(x,a)=(1+(-1)^N\,{}_2F_1(-N,N,\frac{1}{2},x))\times \frac{a^2}{(a^2+1)+(a^2-1)(-1)^N\,{}_2F_1(-N,N,\frac{1}{2},x)}$$

$$=\frac{a^2(T_N(x^{\frac{1}{2}}))^2}{1+(a^2-1)(T_N(x^{\frac{1}{2}})^2)}$$

and

$$\tilde{\phi}_N^2(x,a)=(1-(-1)^N\,{}_2F_1(-N,N,\frac{1}{2},(1-x)))\times \frac{a^2}{(a^2+1)-(a^2-1)(-1)^N\,{}_2F_1(-N,N,\frac{1}{2},x)}$$

$$=\frac{a^2(U_N((1-x)^{\frac{1}{2}}))^2}{1+(a^2-1)(U_N((1-x)^{\frac{1}{2}})^2)}$$

where N is an integer greater than one. Also,

$${}_2F_1(-N,N,\frac{1}{2},x)=(-1)^N\cos(2N\arccos(x^{\frac{1}{2}}))$$

$$=(-1)^N T_{2N}(x^{\frac{1}{2}})$$

is the hypergeometric polynomials of degree N and $T_N(U_n(x))$ are chebyshev polynomials of type I (typeII), respectively. The chaotic trigonometric maps are their conjugate maps which are defined as:

$$\begin{cases}\phi_N^1(x,a)=h\circ\tilde{\phi}_N^1(x,a)\circ h^{-1}\\ =\frac{1}{a^2}\tan^2(N\arctan(x^{\frac{1}{2}})),\\ \phi_N^2(x,a)=h\circ\tilde{\phi}_N^2(x,a)\circ h^{-1}\\ =\frac{1}{a^2}\cot^2(N\arctan(x^{-\frac{1}{2}})).\end{cases}$$

Conjugacy means that invertible map $h(x)=\frac{1-x}{x}$ maps I =[0, 1] into [0,∞) [8]. In order to simplify the calculation in this paper, we denote the chaotic trigonometric maps $(\phi_N^1(x,a),\phi_N^2(x,a))$ with $\Phi_1(x,a),\Phi_2(x,a)$ respectively. Therefore, the chaotic trigonometric maps are as follows:

$$\begin{cases}\Phi_1(x_n,a_1)=\frac{1}{a_1^2}\tan^2(N_1\arctan(x_{n-1}^{\frac{1}{2}})),\\ \Phi_2(x_n,a_2)=\frac{1}{a_2^2}\cot^2(N_2\arctan(x_{n-1}^{-\frac{1}{2}})).\end{cases}\quad (2)$$

Obviously, We have a two-dimensional dynamical system associated with the coupled map with the property of possessing an invariant measure at synchronized state.

3. SYNCHRONIZATION

The word "synchronization" comes from Greek, which means "share time". Today, in science and technology, it comes to be considered as the time coherence of the different processes. Synchronization of two (or more) chaotic dynamical systems (starting with different initial conditions) means that their chaotic trajectories remain in step with each other during the temporal evolution. In this field, the key concept of complete synchronization refers to a state where the trajectories of dynamical systems approach each other [8,9]. In this study we introduce the system has fast speed and robust synchronization properties.

3.1 INVARIANT MEASURE AT SYNCHRONIZED STATE

Studying the existence of absolutely continuous invariant measures is a main problem in ergodic theory and its applications. Ergodicity claims that it is very hard to predict the actual position of a point from its initial position [10,11]. Dynamical systems, even apparently simple dynamical systems which are described by maps of an interval, can display a rich variety of different asymptotic behavior. On theoretical level, these types of behavior are described by Sinai-Ruelle-Bowen (SRB) measure [12]. The probability measure μ for the symmetric two-dimensional map $\Phi(x,y)$ given in Eq.(1) fulfills the following formal Frobenius-Perron (FP) integral equation [12,13]:

$$\mu(X,Y)=\int dx\int dy\delta(X-\Phi(x,y))\times\delta(Y-\Phi(y,x))\times\mu(y,x),$$

the corresponding FP equation can be written as:

$$\mu(X,Y)=\sum_{(x_k,y_\ell)\in\Phi^{-1}_{coupled}(X,Y)}\mu(x_k,y_\ell)J(x_k,y_\ell)\quad k,\ell=1,2,...,\tilde{M}\quad (3)$$

where x_k and y_l be roots of Eq. (2) and the jocobian J is defined as:

$$J^{-1}(x_\ell,y_k)=\left|\det\begin{pmatrix}\frac{\partial\Phi(x_k,y_\ell)}{\partial x_k} & \frac{\partial\Phi(x_k,y_\ell)}{\partial y_\ell}\\ \frac{\partial\Phi(x_k,y_\ell)}{\partial x_k} & \frac{\partial\Phi(x_k,y_l)}{\partial y_\ell}\end{pmatrix}\right|\quad (4)$$

By considering the one-dimensional maps with invariant measure $\mu(y)$, one can prove that, at synchronized states, the invariant measure of coupled maps may take the following form:

$$\mu(x,y)=\delta(x-y)\mu(y),\quad (5)$$

we insert $\mu(x,y)=\delta(x-y)\mu(y)$ in Eq.(3), after using the Dirac delta function, we get:

$$\sum_k\frac{\mu(x_k)}{|h_1(x_k)+h_2(x_k)|}\times\sum_\ell\frac{\delta(x_k-y_\ell)}{|h_1(x_k)-h_2(x_k)|}\quad k,\ell=1,2,....,\tilde{M}$$

We have used $h_1(x)=\left.\frac{\partial\Phi(x,y)}{\partial x}\right|_{x=y}$ and $h_2(x)=\left.\frac{\partial\Phi(x,y)}{\partial y}\right|_{x=y}$. For a given root x_k, the last term of sum is reduced to:

$$\sum_{\ell}\frac{\delta(x_k-y_\ell)}{|h_1(x_k)-h_2(x_k)|}=\sum_{\ell}\delta(\Phi(x_k,y_\ell)-\Phi(y_\ell,x_k))$$

$$=\delta\left(\Phi(x_k,y)-\Phi(y,x_k)\right)=\delta(X-Y),$$

where two last equalities result from the fact $x_k\in\Phi^{-1}_{coupled}(x,y)$, i.e., x_k is one of the roots of the map Eq.(1) for a given set of {X,Y} and the expansion of $\delta(\Phi(x_k,y)-\Phi(y,x_k))$ (by considering y as the variable). Substituting the obtained results in Eq.(3), we obtain:

$$\mu(X,Y)=\delta(X-Y)\mu(X)=\delta(X-Y)\sum_{x_k\in\Phi^{-1}(X,X)}\frac{\mu(x_k)}{|h_1(x_k)+h_2(x_k)|}$$

which implies that $\mu(X)$ should satisfy:

$$\mu(X)=\sum_{x_k\in\Phi^{-1}(X,X)}\frac{\mu(x_k)}{|h_1(x_k)+h_2(x_k)|}$$

$$=\sum_{x_k\in\Phi^{-1}(X,X)}\left|\frac{d\Phi(x_k,x_k)}{dx_k}\right|^{-1}\mu(x_k)\qquad(6)$$

which is the same as PF equation of one-dimensional map $X=\Phi(x,x)$. The required condition for the presentation of the invariant measure of the synchronized coupled map is choosing a one-dimensional map with an invariant measure as introduced in our previous work [4].

3.2 STABILITY ANALYSIS

This section introduces the KS-entropy for hierarchy of coupled maps with dynamical parameter. We try to calculate Lyapunov exponent as another tool to study the stability [12,13]. KS-entropy or metric entropy measures how chaotic a dynamical system is and it is proportional to the rate at which information about the state of dynamical system is lost in the course of time or iteration. Therefore, it can also be defined as the average rate of loss of information for a discrete measurable dynamical system (Φ,μ). People believed that, after determining the KS-entropy of a data sequence, one would know the true nature (deterministic or stochastic) of the law generating the series. By considering the very large KS-entropy the true (deterministic) nature of the PRNG becomes apparent only at a very high resolution [14,15]. By introducing a partition $\alpha=A_c(n_1,...,n_\gamma)$ of the interval [0,1] into individual laps A_i, one can define the usual entropy associated with the partition by [11]:

$$h(\mu,\gamma)=-\sum_{i=1}^{n(\gamma)}m(A_c)\ln m(A_c),$$

where $m(A_c)=\int_{n\in A_i}\mu(x)dx$ is the invariant measure of A_i. Defining a n-th refining $\gamma(n)$ of γ:

$$\gamma^n=\bigcup_{k=0}^{n-1}(\Phi)^{-(k)}(\gamma)$$

then an entropy per unit step of refining is defined by :

$$h(\mu,\Phi,\gamma)=\lim_{n\to\infty}\left(\frac{1}{n}H(\mu,\gamma)\right),$$

now, if the size of individual laps of $\gamma(n)$ tends to zero as n increases, the above entropy reduces to well known as KS-entropy, that is $h(\mu,\Phi)=h(\mu,\Phi,\gamma)$. KS-entropy is actually a quantitative measure of the rate of information lost in the refining process. It can be written as:

$$h(\mu,\Phi)=\int dx\int dy\,\mu(x,y)\ln\left|\frac{\partial(X,Y)}{\partial(x,y)}\right|$$

$$=\int dx\int dy\,\mu(x,y)\times\left|\det\begin{pmatrix}\frac{\partial\Phi(x,y)}{\partial x} & \frac{\partial\Phi(x,y)}{\partial y}\\ \frac{\partial\Phi(y,x)}{\partial x} & \frac{\partial\Phi(y,x)}{\partial y}\end{pmatrix}\right|.$$

The measurable dynamical system (μ,Φ) is chaotic for $h(\mu,\Phi)>0$ and predictive for $h(\mu,\Phi)=0$. At synchronized state we have:

$$h(\mu,\Phi_{syn})=\int dx\int dy\,\delta(x-y)\left|\frac{\partial\Phi(x,y)}{\partial x}\frac{\partial\Phi(y,x)}{\partial y}-\frac{\partial\Phi(y,x)}{\partial x}\frac{\partial\Phi(x,y)}{\partial y}\right|=\int dx\mu(x)\ln|h_1^2(x)-h_2^2(x)|$$

$$=\int dx\mu(x)\ln|h_1(x)+h_2(x)|+\int\mu(x)dx\ln|h_1(x)-h_2(x)|$$

$$h(\mu,\Phi_{syn})=h(\mu,X=\Phi(x,x))$$

$$+\int dx\mu(x)\ln|h_1(x)-h_2(x)|,\qquad(7)$$

where $h(\mu,X=\Phi(x,x))$ is the KS-entropy of one-dimensional map $X=\Phi(x,x)$ with invariant measure $\mu(x)$. The transition from chaotic synchronization (spatial order with temporal chaos) to non-synchronized states with positive KS-entropy (spatial and temporal disorder) occurs.

The stability of the coupled map can be assessed by computing its lyapunov exponent spectrum [12,13]. A spectrum of all the lyapunov exponents with respect to the synchronization solution can be evaluated in a fashion similar to that of one dimensional local maps. At synchronized state, the lyapunov exponents $\Lambda_\pm$ of two-dimensional dynamical system described by the map Eq. (1) are defined as:

$\lim_{n\to\infty}\frac{1}{n}|\lambda_\pm(x_n)|$, where $\lambda_\pm=h_1(x)\pm h_2(x)$ are eigen states of the following matrix:

$$\begin{bmatrix}\frac{\partial\Phi(x,y)}{\partial x}|_{x=y} & \frac{\partial\Phi(x,y)}{\partial y}|_{x=y}\\ \frac{\partial\Phi(y,x)}{\partial x}|_{x=y} & \frac{\partial\Phi(y,x)}{\partial y}|_{x=y}\end{bmatrix}=\begin{bmatrix}h_1(x) & h_2(x)\\ h_2(x) & h_1(x)\end{bmatrix}\qquad(8)$$

in the case of ergodic one-dimensional map $X = \Phi(x, x)$, the Lyapunov exponents can be written as:

$$\Lambda_{\pm,\,\mathrm{syn}} = \lim_{n\to\infty} \frac{1}{n} \ln|\lambda_{\pm}(x_n)|$$
$$= \lim_{n\to\infty} \frac{1}{n} \ln|\lambda_{\pm}(\overbrace{\Phi(\Phi o \Phi o..\Phi}^{n}(x_0, x_0))|$$
$$= \lim_{n\to\infty} \frac{1}{n} \sum_{k=0}^{n} \ln|h_1(x_k) \pm h_2(x_k)|$$
$$= \int dx \mu(x) \ln|h_1(x) \pm h_2(x)| \qquad (9)$$

where $x_n = \overbrace{\Phi o \Phi o ... \Phi}^{n}(x_0, x_0)$. Finally, by comparing the KS-entropy Eq. (7) with the sum of $\Lambda_{\pm}$, we have:

$$h(\mu, \Phi_{\mathrm{syn}}) = \Lambda_{+}(\Phi_{syn}) + \Lambda_{-}(\Phi_{syn})$$

According to Pessin's theorem [12,13], the ergodicity of one-dimensional map implies the ergodicity of symmetric two-dimensional map Eq. (1) at unstable synchronized state (synchronized state is stable for negative critical exponent Λ_{-}). Obviously the non-ergodic choice of one-dimensional map will lead to the non-ergodicity at synchronized state.

4. THE PROPOSED PRNG AND RANDOMNESS ANALYSIS

In this section, we introduce the proposed pseudorandom number generators based on the generalized threshold function and then their randomness is discussed. To consider a one-dimensional chaotic system which is defined as follows: $x_n = f(x_{n-1}) \quad n = 0,1,2,...$ that $f : I \to I \ (I = [0,1])$ is a nonlinear map. In this method, we divided the interval of I=[0,1] into 2^{k-1} blocks and then divided each block into 2 boxes by threshold function (i.e., c). Consequently, we have 2^{k} boxes in the interval of I=[0,1]. Width of boxes are $(c \times \frac{1}{2^{k-1}})$ and $((1-c) \times \frac{1}{2^{k-1}})$, respectively. In this case, the pseudorandom bit sequence $\{z_n\}_{n=0}^{\infty}$ is defined as follows :

$$z_n = \begin{cases} 0 & [x_n \times 2^{k-1}] \le c \\ 1 & \text{other wise} \end{cases} \qquad (3)$$

where symbol of [] is the fractional part. With this way, randomness of the PRNG is increased, because, this method decreased periodic effect of the chaotic maps in randomness of the PRNG. With regard to the above contents, we can be redefined this method in two-dimension. For this purpose, to consider a two-dimensional chaotic system which is defined as follows:

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

$y_n = g(y_{n-1}) \quad n = 0,1,2,...$

that f and $g : I \to I \ (I = [0,1])$ are nonlinear maps $(\Phi_1(x,a), \Phi_2(x,a))$. Threshold functions of the $\{x_n\}_{n=0}^{\infty}$ values and the $\{y_n\}_{n=0}^{\infty}$ values are c and c', respectively. Therefore, the pseudorandom bit sequence $\{z_n\}_{n=0}^{\infty}$ is defined as follows :

$$z_n = \begin{cases} 0 & (\text{A or B}) \\ 1 & \text{other wise} \end{cases} \qquad (4)$$

Where,

$$A \equiv ([x_n \times 2^{k-1}] \le c \text{ and } [y_n \times 2^{k-1}] \le c')$$
$$B \equiv ([x_n \times 2^{k-1}] > c \text{ and } [y_n \times 2^{k-1}] > c')$$

and symbol of [] is the fractional part. We have survey the randomness and uniformity of the several bit sequences of large size, generated by the proposed PRNGs for different sets of control parameter and initial conditions of the chaotic maps. Here, we show the results for 2^{20} sized bit sequences corresponding to the following parameter values of the four sets:

$$\begin{cases} A = (0.12, 0.69, 2, 1.5, 3, 2, 3) \\ B = (0.53, 0.23, 1.6, 2.5, 4, 7, 4) \\ C = (0.24, 0.78, 8, 3.5, 8, 6, 5) \\ D = (0.62, 0.37, 3.2, 4, 7, 10, 7). \end{cases}$$

For convenience, these four sets are designated as:

$$\{A, B, C, D = (x, y, \alpha_x, \alpha_y, N_x, N_y, k)$$

that A and B are related control parameter values of the PRNG based on segmentation and C and D are related control parameter values of the PRNG based on self-similarity. We have used MATLAB 7.10.0 (R2010a) running program in a personal computer with a Core i3 3.1GHz intel, 4GB memory and 500GB hard-disk capacity. The average time used for generating random bit sequences with size of 2^{20} bits is shorter than 0.1 s. We discuss in the following paragraph of this Section the result and conclusions of our study of the different statistical tests to observe the randomness and uniformity of the bit sequences generated by the proposed PRNG. The US NIST statistical test suite provides 15 statistical tests to detect deviations of a bit sequence from randomness. A statistical test is formulated to test a null hypothesis which states that the sequence being tested is random. There is also an alternative hypothesis which states that the sequence is not random. For each test, there is an associated reference distribution (typically normal distribution or χ^2 distribution), based on which a P-value is computed from the bit sequence. If the P-value is greater than a predefined threshold α which is also called significance level, then the sequence would be considered to be random with a confidence of $1-\alpha$, and the sequence passes the test successfully. Otherwise, the sequence fails this test. A P-value of zero indicates that the sequence appears to be completely non-random, and the larger the P-value is, the closer a sequence to a perfect random sequence. In our experiment, we set α to its default value 0.01, which means a sequence passed the test is considered as random

with 99% confidence. Before presenting the test results of our proposed three approaches, we would first introduce all 15 statistical tests briefly as follows. A more detailed description for those tests could be found in [2].

The frequency test (FT), the runs test (RT) and the cumulative sum test (CST) are recommended that each sequence to be tested consist of a minimum of 10^2 bits (i.e., $n \geq 10^2$). The frequency Test within a Block (FTB) is recommended that each sequence to be tested consist of a minimum of $M \times N$ bits (i.e., $n \geq MN$). The block size M should be selected such that $M \geq 20$ and $N < 10^2$. The discrete fourier transform test (DFTT) is recommended that each sequence to be tested consist of a minimum of 10^3 bits (i.e., $n \geq 10^3$). The approximate entropy test (AET) is recommended that each sequence to be tested consist of a minimum of 2^{12} bits (i.e., $n \geq 2^{12}$). The test for the longest run of ones in a block (LROBT) is recommended that each sequence to be tested consist of a minimum of 6272 bits for M=128. The binary matrix rank test (BMRT) is recommended that each sequence to be tested consist of a minimum of 10^5 bits (i.e., $n \geq 10^5$). The non-overlapping template matching test (NTMT), the overlapping template matching test (OTMT), the maurer's universal statistical test (MUST), the linear complexity test (LCT), the serial test (ST), the random excursions test (RET) and the random excursions variant test (REVT) are recommended that each sequence to be tested consist of a minimum of 2^{20} bits (i.e., $n \geq 2^{20}$).

The NIST suite tests were performed on four bit sequences, each containing 2^{20} bits. The P-value as well as final results obtained from the NIST suite for four different sets are given in Table 1. The proposed PRNGs successfully pass all randomness tests of NIST suite. According to [1], we can conclude that the data generated by these PRNGs are random.

Table 1. The results obtained from NIST suite for 15 tests.

NIST Tests	A	B	C	D
FT	0. 12810	0. 50959	0. 73877	0.50402
FBT	0.81849	0. 41964	0. 60238	0.92002
RT	0. 77196	0.98864	0.87415	0. 34100
LROBT	0. 72801	0.04134	0.71471	0. 80442
RBMRT	0. 69567	0. 67702	0. 42659	0. 26585
DFTT	0. 75011	0.44084	0. 83971	0. 93605
ATMT	PASS	PASS	PASS	PASS
PTMT	0. 13424	0. 83774	0. 97694	0. 87069
MUST	0. 26139	0. 34621	0. 39409	0. 75311
LCT	0. 91286	0. 91698	0. 87837	0. 72932
ST (P1) (P2)	0. 79047 0. 80494	0. 19241 0. 90443	0. 76171 0.48004	0. 55015 0. 12033
AET	0. 41219	0. 37636	0.87768	0. 91856
CST (FORWARD) (REVERSE)	 0. 65193 0. 65008	 0. 28879 0. 38809	 0. 55974 0. 85388	 0. 85364 0. 83570
RET	PASS	PASS	PASS	PASS
REVT	PASS	PASS	PASS	PASS

5. CONCLUSIONS

We discuss the properties making a deterministic algorithm suitable to generate a pseudo random sequence of numbers: high value of KS-entropy, high dimensionality of the parent dynamical system, and very large period of the generated sequence. Here, in this work by introducing a symmetric two-dimensional map with the property of possessing invariant measure in its diagonal and anti-diagonal sub-manifolds, we have tried to challenge the chaotic synchronization of some coupled maps of non-linear types. We choose the system because it has fast speed and robust synchronization properties. We show that chaotic features of this map are useful for generating pseudo random numbers and investigate numerically which of them survive in the discrete state version of the map. It should be mentioned that a very general class of statistical defects of PRNG's can be improved by an ergodic stationary source with finite memory as it was introduced in this paper. Also these chaotic maps is suggested in serious applications that require a high level of security.

6. REFERENCES

[1] Rukhin A., Soto J., Nechvatal J., Smid M., Barker E., Leigh S., Levenson M., Vangel M., Banks D., Heckert A., Dray J., VoA S., 2010. NIST special publication, 5-125.

[2] Fernandez J.F., Criado C., 1999. Phys.Rev.E 60, 3361.

[3] Vattulainen I., Ala-Nissila T., Kankaala K., 1995. Phys.Rev.E 52, 3205.

[4] Jafarizadeh M.A., Behnia S., Khorram S., Nagshara H., 2001. J.Stat.Phys. 104, 1013.

[5] Behnia S., Akhshani A., Mahmodi H., Akhavan A., 2008. Chaos, Solitons & Fractals, 35, 408.

[6] Behnia S., Akhshani A., Ahadpour S., Mahmodi H., Akhavan A., 2007. Physics Letters A, 366, 391.

[7] Wang K., Pei W., Xia H., Cheung Y., 2008. Physics Letters A, 372, 4388.

[8] Shabunin A., Astakhov V., 2005. Phys.Rev.E 72, 016218.

[9] Shu Y., Zhang A., Tang B., 2005. Chaos,Solitons and Fractals, 23, 563.

[10] Eckman J.P., Ruelle D., 1985. Rev.Mod.Phys. 57, 617.

[11] Cornfeld I.P., FominS.V., Sinai Ya.G., 1982. ErgodicTheory. Springer-Verlag, Berlin.

[12] Ott E., 1993. Chaos in dynamical system, 51, Cambidge university press, Canada.

[13] Dorfman J.R., 1999. An Introduction to chaos in Nonequilibrium Statistical Mechanics, Cambrige.