Hindawi Publishing Corporation
Mathematical Problems in Engineering
Volume 2013, Article ID 769108, 10 pages
http://dx.doi.org/10.1155/2013/769108

Research Article

Study of a New Chaotic Dynamical System and Its Usage in a Novel Pseudorandom Bit Generator

Ana-Cristina Dăscălescu,[1,2] Radu Eugen Boriga,[1,2] and Adrian-Viorel Diaconu[1,3]

[1] *IT&C Department, Lumina-The University of South-East Europe, 021187 Bucharest, Romania*
[2] *Faculty of Informatics, University "Titu Maiorescu", 0400511 Bucharest, Romania*
[3] *ETTI Faculty, University Politehnica of Bucharest, 061071 Bucharest, Romania*

Correspondence should be addressed to Adrian-Viorel Diaconu; adrian.diaconu@lumina.org

Received 8 July 2013; Revised 14 September 2013; Accepted 16 September 2013

Academic Editor: Zhan Shu

A new chaotic discrete dynamical system, built on trigonometric functions, is proposed. With intent to use this system within cryptographic applications, we proved with the aid of specific tools from chaos theory (e.g., Lyapunov exponent, attractor's fractal dimension, and Kolmogorov-Smirnov test) and statistics (e.g., NIST suite of tests) that the newly proposed dynamical system has a chaotic behavior, for a large parameter's value space, and very good statistical properties, respectively. Further, the proposed chaotic dynamical system is used, in conjunction with a binary operation, in the designing of a new pseudorandom bit generator (PRBG) model. The PRBG is subjected, by turns, to an assessment of statistical properties. Theoretical and practical arguments, rounded by good statistical results, confirm viability of the proposed chaotic dynamical system and newly designed PRBG, recommending them for usage within cryptographic applications.

1. Introduction

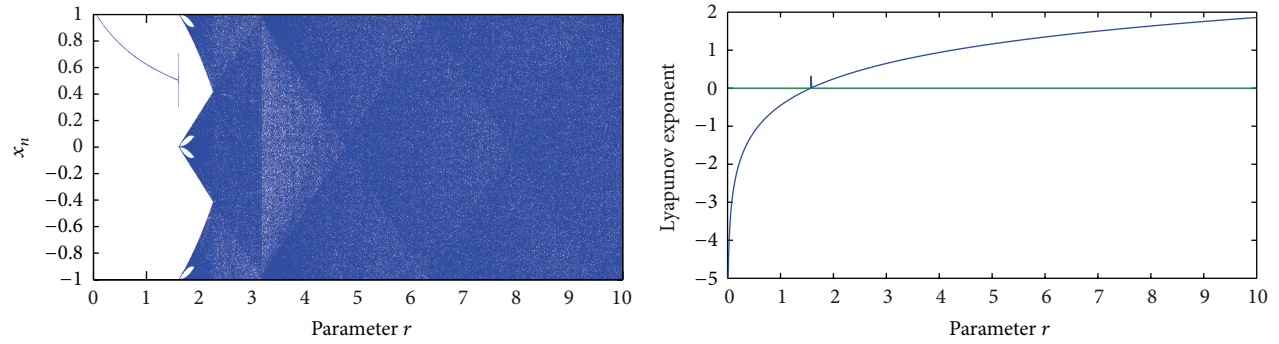
Nowadays, more and more, it appears that skilful genesis of chaos turns out to be a key issue in many technological application fields such as engineering, medicine, communications, information storage, and, with particular importance, cryptography [1–6].

Designing of dynamical systems, intended to be used as base of cryptosystems, must be done so as to ensure the use of a set of associated control parameters' values that leads to chaos [7–11]. Moreover, the ergodic [12–15] and randomness properties [16–19] must be confirmed, as a certainty of high security level of the chaotic dynamical system.

Since 1963, when Lorenz found the first chaotic attractor in a three-dimensional autonomous system while studying atmospheric convection [20], chaotification became a very attractive subject, leading to the development of new chaotic dynamic systems, for example, [21–25], and new chaos-based PRBGs, for example, [26–30], whose properties have been analyzed extensively and thoroughly in research or review articles and books, for example, [31–36].

Motivated by the extent of previous work, the present paper aims to present a new chaotic discrete dynamical system which, furthermore, may be included in the wide family of PRBGs through a simple, interesting, and yet complex new PRBG model, based on binary operation.

The rest of this paper is organized as follows. Section 2 presents the design of newly proposed dynamical system, including its chaotic behavior assessment (as a first step in system's evaluation process to establish its suitability within any cryptographic application). Section 3 showcases the detailed and comprehensive randomness' testing process of sequences generated by the new chaotic dynamical system (as a second step in system's evaluation process to establish its suitability within any cryptographic application). Section 4 presents the designing of a new PRBG scheme (based on binary operation, which uses previously designed and tested chaotic dynamical system), including the results of analysis performed using NIST suite in order to test the randomness and uniformity of values generated by the new PRBG. Finally, Section 5 concludes the work carried out.



(a) (b)

Figure 1: Bifurcation diagram of f_p map (a) and Lyapunov exponent of f_p map (b).

2. Proposed Discrete Dynamical System and Its Basic Properties

Newly dynamical system introduced in paper uses (1) [37, 38] as model for chaos generation. Here, whilst f represents a periodic real map (selected so as to ensure a large phase space), h represents a bounded real map (which, by an appropriate selection, restricts the phase space to a closed interval in which the dynamical system has good chaotic properties):

$$x_{n+1} = h\left(f\left(x_n\right)\right). \tag{1}$$

Therefore, the newly proposed one-dimensional discreet dynamic system, which is defined with respect to form (1), is given by (2) or (and), in a more detailed design, by (3). Here, r represents the control parameter of the resulted chaotic map, while arctg (i.e., arctangent function), and ctg (i.e., cotangent function), respectively, were chosen with respect to the above affirmations (i.e., the first one restricts the phase space to a close interval in which the dynamical system has good chaotic properties, while the second one ensures a large phase space):

$$x_{n+1} = f_p\left(x_n\right), \tag{2}$$

$$f_p : [-1, 1] \longrightarrow [-1, 1], \quad f_p\left(x\right) = \frac{2}{\pi}\operatorname{arctg}\left(\operatorname{ctg}\left(rx\right)\right). \tag{3}$$

In the following, dynamical behavior of newly proposed chaotic system is investigated, by both theoretical analysis and numerical simulation (e.g., by means of Lyapunov exponent, attractor's geometric shape and fractal structure, and system's ergodicity, i.e., Kolmogorov-Smirnov tests, etc.).

2.1. Sensitivity Level to Initial Conditions. The behavior of the proposed discrete dynamic system (3), in terms of its evolution over time domain, depends on both the control parameter r and the initial condition x_0. First of all, we propose stability analysis of fixed points in order to assess system's sensitivity level to initial conditions.

f_p map's fixed points are given by (4), and, according to the theorem of fixed points [39], x_k points are attractors if condition (5) is fulfilled, that is, if the control parameter r meets condition (6). Thus, taking into account the fact that f_p map is defined on the interval $[-1, 1]$, there exists only one fixed point, that is, (7), which is also an attractor:

$$t_k = \frac{\pi\left(2k + 1\right)}{2r + \pi}, \quad k \in \mathbb{Z}, \tag{4}$$

$$\left|f_p'\left(t_k\right)\right| < 1, \quad k \in \mathbb{Z}, \tag{5}$$

$$r < \frac{\pi}{2}, \tag{6}$$

$$t_0 = \frac{\pi}{2r + \pi}. \tag{7}$$

From the above equations, it can be noticed that for any $r \in (0, \pi/2)$, all trajectories that start at initial point x_0 converge, in time, to the attractor point t_0; for any $r > \pi/2$, fixed point t_0 loses its stability, and other instable fixed points appear. The aforementioned statements are also substantiated by the bifurcation diagram, namely, the one showcased in Figure 1(a), which emphasizes the stability of f_p's fixed points (i.e., for any values of parameter r, close to $\pi/2$, f_p has an instable behavior, and for any values of the parameter r, higher than $\pi/2$, the map enters into a complete chaotic regime). The road to chaos of the f_p map, with $r > \pi/2$, is not achieved through doubling process of the period, specific to some chaotic maps, but is induced by existence of a dense set of periodic orbits, whose periods are in the $[-1, 1]$ interval. Another tool used to assess f_p's sensitivity to the initial conditions is the Lyapunov exponent (8) and, taking into consideration the fact that orbit $\{x_1, x_2, \ldots, x_n\}$ is chaotic if this exponent is positive, (9) is derived (which is equivalent to $r > \pi/2$, meaning that for any $r \in (\pi/2, 10)$ f_p's orbits are chaotic). Lyapunov exponent, numerically computed [40] with respect to the parameter r within $(0, 10)$ interval, is shown in Figure 1(b). Consider

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

$$= \lim_{n\to\infty}\frac{1}{n}\sum_{i=1}^{n}\ln\left|\frac{-2r}{\pi\sin^2 rx\left(1 + \operatorname{ctg}^2 rx\right)}\right|$$

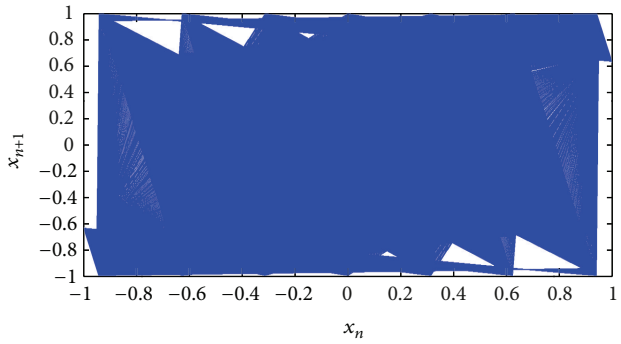


FIGURE 2: Attractor of f_p map, for $r = 7$.

$$= \ln \frac{2r}{\pi}, \tag{8}$$

$$\ln \frac{2r}{\pi} > 0. \tag{9}$$

2.2. Attractor's Geometric Shape and Fractal Structure. Analysis of dynamical system's attractor's shape can provide meaningful information about system behavior in time, for certain values of its parameters. The attractor of a dynamical system with a periodic behavior has a regular shape, while the one corresponding to a chaotic dynamical system has a complex structure, of fractal type, called strange attractor [39].

Figure 2 showcases f_p's attractor, for $r = 7$, where it can be observed that its shape is irregular, of fractal type, and complex shaped, in comparison with ones of, for example, tent or logistic maps (i.e., whose attractors exhibit a regular shape, i.e., triangle, resp., hyperbola shaped).

Fractal structure of an attractor is indicated by a fractional value of its fractal dimension, which is a ratio that provides a statistical index of complexity comparing how in detail a pattern changes with the scale at which it is measured or, alternatively, by a measure of the space-filling capacity of a pattern, telling how a fractal scale is different than the space in which it is embedded. There are several types of fractal dimensions, which can be theoretically and empirically estimated, such as Hausdorff dimension, Minkowski-Bouligand dimension, box-counting dimension, information dimension, and correlation dimension [41–44]. Using plots from Figure 3, we established that the attractor of the f_p map has a box-counting dimension $D_b = 0.97863$ and a correlation dimension $D_c = 0.97064$. Fractional values, of fractal dimensions previously estimated, allow us to conclude that the proposed map has a strange attractor which, by turns, indicates a chaotic behavior.

2.3. System's Ergodicity. In this subsection, using Birkhoff's theorem [5, 45] in conjunction with Kolmogorov-Smirnov test [46, 47], we intend to prove that the proposed dynamical system is ergodic for $r > \pi/2$ (i.e., long-term behavior of f_p's orbits is independent from the initial condition, and thus it may be subjected to a battery of statistical tests).

The Kolmogorov-Smirnov test is applied on two amounts of independent data $(x_1, x_2, \ldots, x_n)$ and $(y_1, y_2, \ldots, y_n)$, corresponding to the measurements of two random variables X and Y. Random variable X is obtained through an n-times iteration of f_p map, for a fixed parameter r and for a fixed initial condition x_0 (namely, $r > \pi/2$ and $x_0 \in [-1, 1]$). Second random variable, that is, Y, is obtained by selecting, at time k, the values generated by n orbits of the map, arising from n initial seeding points (belonging to $[-1, 1]$ interval) and same r parameter (previously fixed). Moment $k = 100$ is chosen from f_p's stationary zone, previously established using Kolmogorov-Smirnov test, as described in [46, 47].

Due to the fact that the random values X and Y correspond to time average of f_p and space average, respectively, the purpose of the test is to establish if the two experimental data sets derive from populations with the same distribution or not, with respect to Birkhoff's theorem. The analysis is based on distribution functions Fe_X and Fe_Y, associated with the experimental independent data sets X and Y.

Kolmogorov-Smirnov test is applied as follows:

(1) the maximum absolute difference between the two distribution functions δ is computed:

$$\delta = \max_u \left| \mathrm{Fe}_X(u) - \mathrm{Fe}_Y(u) \right|; \tag{10}$$

(2) for a significance level α, Δ_α is computed (α representing probability law's quantile, for the random value Δ); that is, $P(\Delta > \Delta_\alpha) = \alpha$,

$$\Delta_\alpha \cong \sqrt{\frac{n+m}{nm}} \sqrt{\frac{1}{2} \ln \frac{2}{\alpha}}; \tag{11}$$

(3) in case of $\delta \leq \Delta_\alpha$, the hypothesis H_0 is accepted (i.e., the two random variables X and Y have the same probability law; in other words, if the absolute maximum distance between the two distribution functions Fe_X and Fe_Y is lower than a certain accepted value Δ_α, then it will be decided that the two random variables X and Y have the same probability law); otherwise the test rejects H_0 hypothesis (i.e., for the chosen level, the two sets of experimental data come from random values with different probability laws).

Kolmogorov-Smirnov test was performed over a sequence of $n = m = 100.000$ samples, with a significance level set to $\alpha = 0.05$; the decision regarding system's ergodicity is based on Monte Carlo analysis (i.e., evaluating Kolmogorov-Smirnov test's ability to accept bad data as good data). The above experiment was repeated 500 times; at the end of each round, H_0 hypothesis's acceptance proportion (which belongs to $[0.93, 0.97]$ interval) was recorded.

Test's overall results are summarized in Table 1. One can observe that in case of all values selected for r parameter, with $r \in (\pi/2, 10)$, the acceptance proportion of H_0 hypothesis lies within the confidence interval. Thus, ergodicity of the proposed dynamical system is confirmed (over the entire interval of interest, for parameter r).

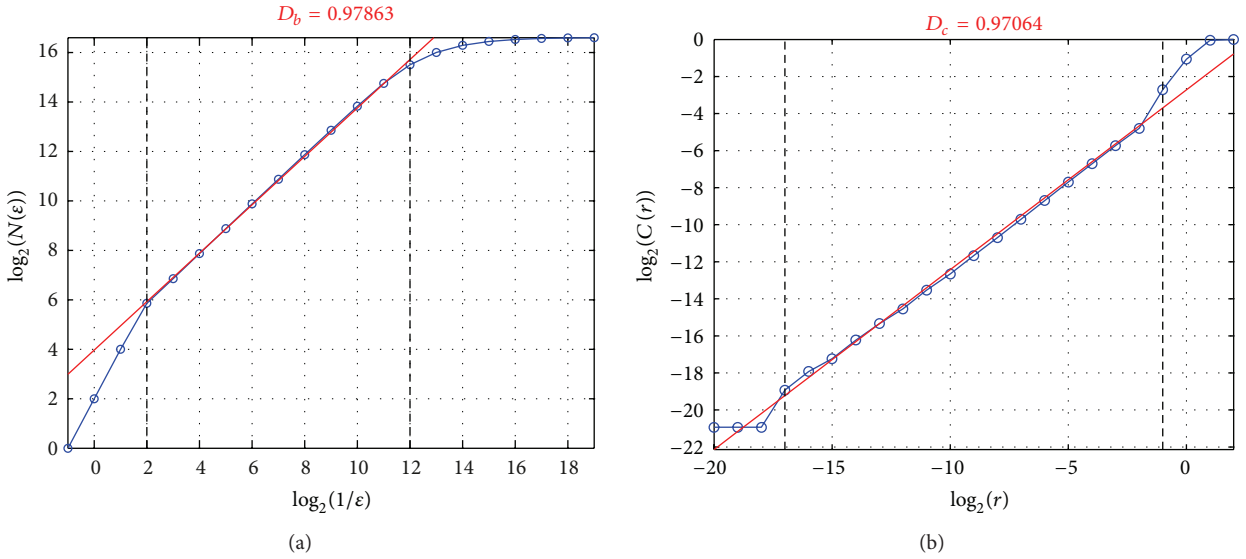


Figure 3: f_p's attractor's fractal dimensions: box-counting dimension (a) and correlation dimension (b).

Table 1: Results of f_p's ergodicity property testing.

Experiment iteration(s)	Parameter value	KS test value	Test result
1–49	—	$\in [0.93, 0.97]$	PASSED
50	2.805107703154233	0.956	PASSED
51–99	—	$\in [0.93, 0.97]$	PASSED
100	4.342554676193408	0.950	PASSED
101–149	—	$\in [0.93, 0.97]$	PASSED
150	5.352537126362448	0.950	PASSED
151–199	—	$\in [0.93, 0.97]$	PASSED
200	5.930260965351542	0.966	PASSED
201–249	—	$\in [0.93, 0.97]$	PASSED
250	6.547089923300568	0.940	PASSED
251–299	—	$\in [0.93, 0.97]$	PASSED
300	7.300182966818144	0.966	PASSED
301–349	—	$\in [0.93, 0.97]$	PASSED
350	7.710976298365504	0.960	PASSED
351–399	—	$\in [0.93, 0.97]$	PASSED
400	8.299998361920006	0.950	PASSED
401–449	—	$\in [0.93, 0.97]$	PASSED
450	9.127429903281719	0.964	PASSED
451–499	—	$\in [0.93, 0.97]$	PASSED
500	9.858890151572155	0.952	PASSED

Based on numerical results previously obtained, using instruments from the chaos theory, we can conclude that f_p map has a chaotic behavior, without intermittent scenarios, for any combination between the parameter $r \in (\pi/2, 10)$ and the initial seeding point $x_0 \in [-1, 1]$.

The chaotic behavior is a necessary but not sufficient condition to allow usage of the proposed dynamic system within cryptographic applications. System's security level, against some statistical cryptanalytic attacks, is assessed after a statistical analysis of the randomness of values generated. There are several options available for analyzing randomness of a newly developed pseudorandom bit generator (PRBG), as it will be revealed in the following section.

3. Randomness Analysis of the Proposed Chaotic Discrete Dynamical System

In order to assess PRBG's statistical properties (i.e., its true randomness and implicit suitability within cryptographic applications; see e.g., [48–52], etc.), different testing tools such as CrypTool and VRA (for basic statistical measures' quantification), respectively NIST [53] and DIEHARD [54] standard tests batteries (for high end quantitative and qualitative assessment) were used. Operating methodology, for each of the above tests, and obtained results are presented and discussed in the following subsections.

Chaotic cryptography deals with real numbers, so, in order to proceed and apply the battery of the statistical tests aforementioned, we have to apply a computational method to transform a chaotic sequence of real numbers into a bitstream. The discretization method that we used consisted in the extraction of the fractional parts of the generated subunitary real numbers.

3.1. CrypTool Analysis. CrypTool was used to compute the occurrence frequencies of any binary substring, composed of n symbols (i.e., the n-grams), over the flow of bits generated with the proposed PRBG. For true random bitstreams, it is expected that each entry within the n-gram has the same probability of occurrence. The n-gram statistics were performed over 1.000 randomly chosen binary sequences, each sequence being generated using different initial seeding

Table 2: PRBG's n-gram reports.

n-gram's order	Substring	Frequency (%)	$\lvert\Delta\rvert$
Histogram ($n = 1$)	0	50.0734	0.0734
	1	49.9266	0.0734
Digram ($n = 2$)	00	24.9605	0.0395
	01	24.9660	0.0340
	10	24.9660	0.0340
	11	25.1074	0.1074
Trigram ($n = 3$)	000	12.4899	0.0101
	001	12.4706	0.0294
	010	12.4293	0.0707
	011	12.5367	0.0367
	100	12.4705	0.0295
	101	12.4954	0.0046
	110	12.5367	0.0367
	111	12.5707	0.0707
4-gram ($n = 4$)	0000	6.2240	0.0260
	0001	6.2659	0.0159
	0010	6.2015	0.0485
	0011	6.2691	0.0191
	0100	6.2085	0.0415
	0101	6.2208	0.0292
	0110	6.2568	0.0068
	0111	6.2799	0.0299
	1000	6.2658	0.0158
	1001	6.2047	0.0453
	1010	6.2278	0.0222
	1011	6.2676	0.0176
	1100	6.2620	0.0120
	1101	6.2746	0.0246
	1110	6.2799	0.0299
	1111	6.2908	0.0408
12-gram ($n = 12$)	000000000000	0.0265	0.0020
	—	≈0.0244	≈0
	111111111111	0.0284	0.0039

points and of $i = 1.000.000$ bits in length; overall results are presented in Table 2.

It can be observed that the deviation from ideal value, of each n-gram's entry, is under 0.1%. Thus, PRBG's n-gram reports not only do not emphasize the dominant presence of any binary substring (i.e., in terms of frequency of use) [55, 56], but they also highlight a uniform system dynamics (i.e., in terms of the time evolution of f_p's trajectories). Positive results obtained at this point guide us to perform the next statistical analysis.

3.2. Visual Recurrence Analysis. A RP (i.e., Recurrence Plot) holds important insights into the time evolution of f_p's trajectories because typical patterns in RPs are linked to specific system behavior [57]. Yet, without proper settings of analysis' parameters, any RP is just a simple image, completely devoid of information. Thus, to obtain as much information, suitable embedding dimension and adequate time delay must be chosen. With the aid of AMI (i.e., Average Mutual Information) and FNN (i.e., False Nearest Neighbors) toolboxes (included in VRA's statistical test suite), these parameters can be correctly set to the optimal value [58]. AMI and FNN were performed on binary sequences, each of $i = 1.000.000$ bits in length (generated with 100 randomly chosen seeds); corresponding graphs are presented in Figures 4(a) and 4(b), respectively. Analyzing the two graphs, first AMI minimum and Optimal Global Embedding Dimension (OGED) are found: time delay $d = 3$ and embedding dimension $m = 3$. With these two parameters bitstream's RPI (i.e., Recurrence Plot Image) is computed, as shown in Figure 4(c).

Lack in clear patterns, within the RPI, indicates that consecutive samples in bitstream's structure are much far apart and uncorrelated. More than that, RPI's homogeneity along the major diagonal and its irregular distribution emphasizes a stationary, mostly stochastic behavior (i.e., intrinsically nondeterministic, nonintermittent, and sporadic), of the system that has generated the bitstream and, namely, a true random process (i.e., random binary strings).

VRA, through its embedded RQA (i.e., Recurrence Quantification Analysis) tool, also provides other additional measures (e.g., entropy, mean, percentage of recurrence and of determinism, etc.); some of them, the most important ones, are quantified in Table 3. One can notice that all the measures have values close to ideal [59].

Despite the fact that skewness has a negative value (i.e., indicating that the tail on the left side of the probability density function is longer than the right side and the bulk of the values lie to the right of the mean), being close to zero indicates that the values are relatively evenly distributed on both sides of the mean, typically (but not necessarily) implying a symmetric distribution [60]. At the same time, Kurtosis's high-level and negative value denotes a platykurtic distribution (i.e., data set with flatter peak around its mean, which causes thin tails within the distribution and low level of data fluctuation) [61].

Good general statistical properties revealed with the aid of VRA (either visually—evaluation of RPI's structural properties or through different specific measures evaluation—RQA), highlights randomness of bitstreams generated using the proposed PRBG function, thus allowing advancement to other statistical test suites.

3.3. NIST Statistical Testing. For the numerical experimentations of the proposed pseudorandom bit generator, we have generated $m = 2.000$ different binary sequences from 500 randomly chosen seeds, each sequence having a length of $n = 1.000.000$ bits, and we have computed the p-value corresponding to each sequence for all the 15 tests of the NIST suite. The significance level of each test in NIST is set to 1%, which means that 99% of test samples pass the tests if the random numbers are truly random. The acceptance region

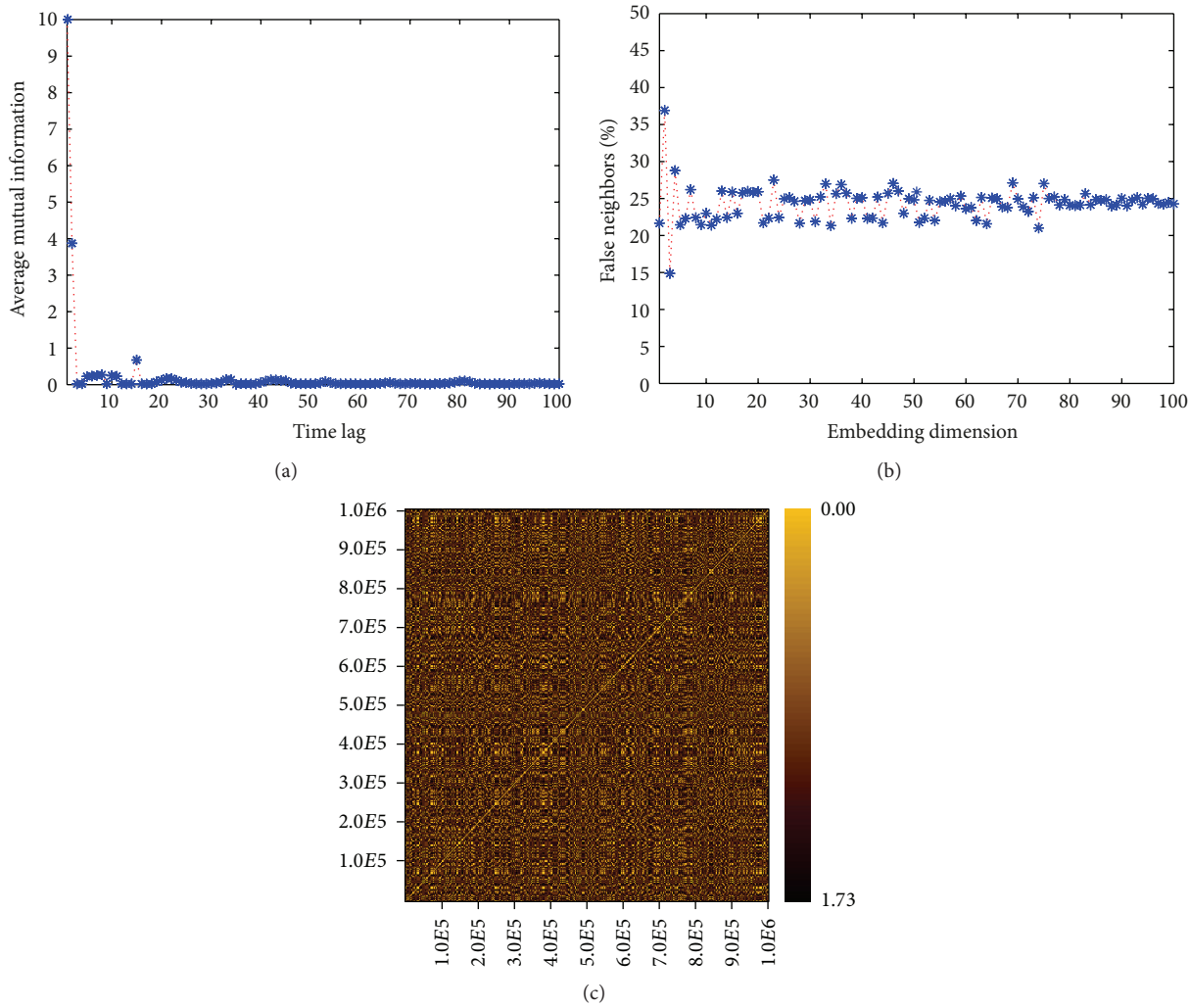


Figure 4: PRBG's visual recurrence analysis: AMI graph (a), FNN graph (b), and recurrence plot (c).

Table 3: PRBG's general statistics.

Mean	Variance	Standard deviation	Skewness	Kurtosis	Entropy
0.5007	0.2500	0.5000	−0.0029	−1.9999	0.9999

of the passing ratio is given by (12), where m represents the number of samples tested and $p = 1 - \alpha$ is the probability of passing each test:

$$\left[p - 3\sqrt{\frac{p(1-p)}{m}}, p + 3\sqrt{\frac{p(1-p)}{m}} \right]. \quad (12)$$

For $m = 2000$ and the probability $p = 0.99$ (corresponding to the significance level $\alpha = 0.01$), we obtained the confidence interval $[0.983, 0.996]$. In the second column of Table 4, we have summarized the results obtained after applying nonparameterized and parameterized tests of the NIST suite on the binary sequences produced by the proposed pseudorandom bit generator. The computed proportion for each test lies inside the confidence interval. Hence, the tested binary sequences generated by the proposed PRBG are random with respect to all tests of NIST suite. If tested sequences are truly random, then p-values are expected to appear uniform in the interval $[0, 1)$. NIST recommends to apply the χ^2-test in which the interval $[0, 1)$ is divided into 10 subintervals. Defining F_i as number of occurrences of the p-value in ith interval, then the χ^2 statistic is (13). NIST recommends setting its significance level to 0.01%, so the acceptance region of statistics has the value $\chi^2 \leq 33.72$. A p-value that corresponds to uniformity of p-values is calculated as in (14), so it must be greater than 0.0001

Table 4: NIST tests' results.

Test name	Passing ratio of the test	Uniformity p-value	Test result
Frequency	0.992	0.602803	PASSED
Block frequency	0.990	0.748891	PASSED
Cumulative sums	0.991	0.090388	PASSED
Runs	0.990	0.939005	PASSED
Longest run	0.989	0.592443	PASSED
Rank	0.991	0.840367	PASSED
FFT	0.989	0.242363	PASSED
Nonoverlapping template	0.983	0.761719	PASSED
Overlapping template	0.983	0.230755	PASSED
Universal	0.987	0.050629	PASSED
Approximate entropy	0.988	0.959347	PASSED
Random excursions	0.987	0.614382	PASSED
Random excursions variant	0.984	0.830939	PASSED
Serial	0.986	0.209392	PASSED
Linear complexity	0.989	0.764655	PASSED

to ensure that the p-values could be considered uniformly distributed. The results from the third column of Table 4 lead us to the conclusion that p-values, for each statistical test, are uniformly distributed:

$$\chi^2 = \sum_{i=1}^{10} \frac{\left(F_i - m/10\right)^2}{(m/10)}, \tag{13}$$

$$\text{igamc}\left(\frac{9}{2}, \frac{\chi^2}{2}\right). \tag{14}$$

The method to calculate the passing ratio of total test and the uniformity p-value of total test samples follows the same methodology described above. In this case, we considered the number of samples $m = 30.000$, so the acceptance region is $[0.988, 0.992]$. For the passing ratio of the total test we obtained the value 0.988, and the p-value corresponding to the uniformity of p-values from the total test was 0.294808, so the proposed map has perfect cryptographic properties.

4. Proposed PRBG and Its Statistical Testing

Most chaos-based PRNGs (and, implicitly, their subsequent PRBGs) are based on a single chaotic system (e.g., [25–29, 52]) and generate the random numbers (resp., the bitstreams) directly from its orbit. These types of PRNGs/PRBGs are potentially insecure, since the output values may expose some information about their underlying chaotic system [62]. To overcome this difficulty, a series of pseudorandom number (bit) generators based on a couple of chaotic system have been proposed (e.g., [63–67]). In the following, we present a novel PRNG/PRBG model, based on two chaotic maps coupled using a binary operation.

We consider two one-dimensional chaotic maps (e.g., as the previously designed model, i.e., (3)) defined as follows:

$$f_1 : [-1,1] \longrightarrow [-1,1], \quad f_1(x, r_1) = \frac{2}{\pi}\text{arctg}\left(\text{ctg}\left(r_1 x\right)\right),$$
$$f_2 : [-1,1] \longrightarrow [-1,1], \quad f_2(x, r_2) = \frac{2}{\pi}\text{arctg}\left(\text{ctg}\left(r_2 x\right)\right), \tag{15}$$

where x_0^1, x_0^2 are the initial conditions, r_1, r_2 are the control parameters, and x_i^1, x_i^2 are the two orbits obtained by recurrences $x_{i+1}^1 = f_1(x_i^1, r_1)$, $x_{i+1}^2 = f_2(x_i^2, r_2)$, for any $i \in \{0, 1, 2, \ldots\}$.

Also, we consider the binary operation given by the formula

$$a * b = \frac{a + b}{1 - a \cdot b}, \tag{16}$$

where $a, b \in [-1, 1]$.

The output $\{y_0, y_1, y_2, \ldots\}$ of the proposed PRNG is obtained applying the binary operation (16) to the chaotic maps f_1 and f_2 defined by (15); thus,

$$y_i = f_1\left(x_i^1, r_1\right) * f_2\left(x_i^2, r_2\right) = \frac{f_1\left(x_i^1, r_1\right) + f_2\left(x_i^2, r_2\right)}{1 - f_1\left(x_i^1, r_1\right) \cdot f_2\left(x_i^2, r_2\right)} \tag{17}$$

for any $i \in \{0, 1, 2, \ldots\}$ and $(x_0^1, r_1, x_0^2, r_2) \in [-1, 1] \times [1, 10] \times [-1, 1] \times [1, 10]$ is the seed of the proposed PRNG.

The real numbers obtained using the proposed PRNG were discretized extracting their fractional parts in order to apply the NIST statistical tests. For the numerical experimentations on the proposed pseudorandom numbers generator, we have generated 2.000 different binary sequences (sample size $m = 2.000$). Each sequence, with one million bits in length, has been generated from a randomly chosen seed

Table 5: NIST tests' results.

Test name	Passing ratio of the test	Uniformity p-value	Test result
Frequency	0.991	0.045971	PASSED
Block frequency	0.991	0.653773	PASSED
Cumulative sums	0.990	0.035876	PASSED
Runs	0.991	0.235589	PASSED
Longest run	0.987	0.937919	PASSED
Rank	0.994	0.221898	PASSED
FFT	0.988	0.160357	PASSED
Nonoverlapping template	0.986	0.036592	PASSED
Overlapping template	0.985	0.316808	PASSED
Universal	0.989	0.703417	PASSED
Approximate entropy	0.991	0.129620	PASSED
Random excursions	0.992	0.806491	PASSED
Random excursions variant	0.985	0.885727	PASSED
Serial	0.987	0.737475	PASSED
Linear complexity	0.990	0.325206	PASSED

(x_0^1, r_1, x_0^2, r_2), and for each we computed the p-value corresponding to the NIST tests. In Table 5 we have summarized the results obtained after implementing nonparameterized and parameterized tests of NIST suite on the binary sequences produced by the proposed pseudorandom numbers generator.

It can be seen that the computed proportion for each test lies inside the confidence interval; hence, the tested binary sequences generated by the proposed PRBG are random with respect to all the 16 tests of NIST suite.

5. Conclusions

Development of new chaotic dynamic systems, which meet the current demands of security, is a present research direction in the field of cryptography. The main objective is to obtain a large key space, induced by the control parameter and (or) initial conditions, for which the dynamic system is in chaotic regime, is ergodic, and has a uniform distribution of the values generated.

With respect to the aforementioned ideas, in this paper we have designed a new one-dimensional chaotic dynamic system that meets these requirements.

Moreover, a larger key space than the one of the known chaotic maps (e.g., logistic, tent, Hénon, etc.) was achieved, and, despite the fact that the implementation of trigonometric maps is little slower than the ones of other kinds of maps (e.g., polynomial, exponential, etc.), we consider that the advantage of a larger key space induced by their usage is a good compromise (i.e., a win-win situation).

Using specific mathematical and numerical tools from chaos theory and statistics, we proved that the proposed chaotic dynamic system has very good cryptographic properties. The proposed map was used in a new innovative way to design a new PRNG/PRBG model, based on a well-known binary operation.

We have performed an exhaustive testing process of the randomness of the generated binary sequences using the NIST suite to prove the viability of the proposed PRNG/PRBG.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

References

[1] M. S. Baptista, "Cryptography with chaos," *Physics Letters A*, vol. 240, no. 1-2, pp. 50–54, 1998.

[2] L. Kocarev, G. Jakimoski, G. Stojanovski, and U. Parlitz, "From chaotic maps to encryption schemes," in *Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS '98)*, vol. 4, pp. 514–517, Monterey, Calif, USA, May-June 1998.

[3] L. Kocarev, "Chaos-based cryptography: a brief overview," *IEEE Circuits and Systems Magazine*, vol. 1, no. 3, pp. 6–21, 2001.

[4] F. Huang and Z. H. Guan, "Cryptosystem using chaotic keys," *Chaos, Solitons & Fractals*, vol. 23, no. 3, pp. 851–855, 2005.

[5] A. Şerbănescu and C. I. Râncu, *Systèmes et Signaux Face au Chaos: Applications aux Communications*, Military Technical Academy Publishing House, Bucharest, Romania, 2008.

[6] L. Kocarev and S. Lian, Eds., *Chaos-Based Cryptography: Theory, Algorithms and Applications*, vol. 354 of *Studies in Computational Intelligence*, Springer, Berlin, Germany, 2011.

[7] D. Arroyo, G. Alvarez, S. Li, C. Li, and J. Nunez, "Cryptanalysis of a discrete-time synchronous chaotic encryption system," *Physics Letters A*, vol. 372, no. 7, pp. 1034–1039, 2008.

[8] D. Arroyo, J. M. Amigó, S. Li, and G. Alvarez, "On the inadequacy of unimodal maps for cryptographic applications," in *11 Reunión Española sobre Criptología y Securidad de la Información (RECSI '10)*, J. D. Ferrer, A. M. Ballesté, J. C. Roca, and A. S. Gómez, Eds., pp. 37–42, Universitat Rovira I Virgili, Tarragona, Spain, 2010.

[9] S. Li, X. Mou, B. L. Yang, Z. Ji, and J. Zhang, "Problems with a probabilistic encryption scheme based on chaotic systems," *International Journal of Bifurcation and Chaos*, vol. 13, no. 10, pp. 3063–3077, 2003.

[10] S. Li, X. Mou, Y. Cai, Z. Ji, and J. Zhang, "On the security of a chaotic encryption scheme: problems with computerized chaos in finite computing precision," *Computer Physics Communications*, vol. 153, no. 1, pp. 52–58, 2003.

[11] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *International Journal of Bifurcation and Chaos*, vol. 16, no. 8, pp. 2129–2151, 2006.

[12] J.-P. Eckmann and D. Ruelle, "Ergodic theory of chaos and strange attractors," *Reviews of Modern Physics*, vol. 57, no. 3, part 1, pp. 617–656, 1985.

[13] L.-S. Young, "Ergodic theory of chaotic dynamical systems," in *From Topology to Computation: Proceedings of the Smalefest*, pp. 201–226, Springer, New York, NY, USA, 1993.

[14] G. Álvarez, F. Montoya, M. Romera, and G. Pastor, "Cryptanalysis of an ergodic chaotic cipher," *Physics Letters A*, vol. 311, no. 2-3, pp. 172–179, 2003.

[15] R. M. Gray, *Probability, Random Processes, and Ergodic Properties*, Springer, New York, NY, USA, 2010.

[16] L. M. Berliner, "Statistics, probability and chaos," *Statistical Science*, vol. 7, no. 1, pp. 69–90, 1992.

[17] F. James, "Chaos and randomness," *Chaos, Solitons & Fractals*, vol. 6, pp. 221–226, 1995.

[18] J. A. González, L. I. Reyes, J. J. Suárez, L. E. Guerrero, and G. Gutiérrez, "Chaos-induced true randomness," *Physica A*, vol. 316, pp. 259–288, 2002.

[19] R. Lozi, "Emergence of randomness from chaos," *International Journal of Bifurcation and Chaos*, vol. 22, no. 2, Article ID 1250021, 15 pages, 2012.

[20] E. N. Lorenz, "Deterministic nonperiodic flow," *Journal of the Atmospheric Science*, vol. 20, no. 2, pp. 130–141, 1963.

[21] C. Zhang, W. K. S. Tang, and S. Yu, "A new chaotic system based on multiple-angle sinusoidal function: design and implementation," *International Journal of Bifurcation and Chaos*, vol. 19, no. 6, pp. 2073–2084, 2009.

[22] J. Lü and G. Chen, "A new chaotic attractor coined," *International Journal of Bifurcation and Chaos*, vol. 12, no. 3, pp. 659–661, 2002.

[23] C. Liu, T. Liu, L. Liu, and K. Liu, "A new chaotic attractor," *Chaos, Solitons & Fractals*, vol. 22, no. 5, pp. 1031–1038, 2004.

[24] G. Qi, G. Chen, S. Du, Z. Chen, and Z. Yuan, "Analysis of a new chaotic system," *Physica A*, vol. 352, no. 2, pp. 295–308, 2005.

[25] X. Zhao, F. Jiang, Z. Zhang, and J. Hu, "A new series of three-dimensional chaotic systems with cross-product nonlinearities and their switching," *Journal of Applied Mathematics*, vol. 2013, Article ID 590421, 14 pages, 2013.

[26] A. Luca, A. Ilyas, and A. Vlad, "Generating random binary sequences using tent map," in *Proceedings of the 10th International Symposium on Signals, Circuits and Systems (ISSCS '11)*, pp. 1–4, Iași, Romania, June-July 2011.

[27] N. K. Pareek, V. Patidar, and K. K. Sud, "A random bit generator using chaotic maps," *International Journal of Network Security*, vol. 10, no. 1, pp. 32–38, 2010.

[28] Q. Zhou, X. Liao, K. W. Wong, Y. Hu, and D. Xiao, "True random number generator based on mouse movement and chaotic hash function," *Information Sciences*, vol. 179, no. 19, pp. 3442–3450, 2009.

[29] X. Y. Wang and Y. X. Xie, "A design of pseudo-random bit generator based on single chaotic system," *International Journal of Modern Physics*, vol. 23, no. 3, 2012.

[30] A. Kanso and N. Smaoui, "Logistic chaotic maps for binary numbers generation," *Chaos, Solitons & Fractals*, vol. 40, no. 5, pp. 2557–2568, 2009.

[31] R. Gilmore, "Topological analysis of chaotic dynamical systems," *Reviews of Modern Physics*, vol. 70, no. 4, pp. 1455–1529, 1998.

[32] Y.-C. Lai and N. Ye, "Recent developments in chaotic time series analysis," *International Journal of Bifurcation and Chaos*, vol. 13, no. 6, pp. 1383–1422, 2003.

[33] W. Ditto and T. Munakata, "Principles and applications of chaotic systems," *Communication of the ACM*, vol. 38, no. 11, pp. 96–102, 1995.

[34] J. C. Sprott, *Chaos and Time-Series Analysis*, Oxford University Press, New York, NY, USA, 2003.

[35] Z. Liu, "Chaotic time series analysis," *Mathematical Problems in Engineering*, vol. 2010, Article ID 720190, 31 pages, 2010.

[36] M. Li, "Fractal time series—a tutorial review," *Mathematical Problems in Engineering*, vol. 2010, Article ID 157264, 26 pages, 2010.

[37] Z. Kotulski, J. Szczepanski, K. Górski, A. Górska, and A. Paszkiewicz, "On constructive approach to chaotic pseudorandom number generators," in *Proceedings of the Regional Conference on Military Communication and Information Systems*, vol. 1, pp. 191–203, 2000.

[38] Q. Z. Xu, S. B. Dai, W. J. Pei, L. X. Yang, and Z. Y. He, "A chaotic map based on scaling transformation of nonlinear function," *Neural Information Processing*, vol. 3, no. 2, pp. 21–29, 2004.

[39] K. T. Alligood, T. D. Sauer, and J. A. Yorke, *Chaos: An Introduction to Dynamical Systems*, Springer, New York, NY, USA, 1st edition, 1996.

[40] A. Wolf, J. B. Swift, H. L. Swinney, and J. A. Vastano, "Determining Lyapunov exponents from a time series," *Physica D*, vol. 16, no. 3, pp. 285–317, 1985.

[41] P. Grassberger and I. Procaccia, "Measuring the strangeness of strange attractors," *Physica D*, vol. 9, no. 1-2, pp. 189–208, 1983.

[42] J. D. Farmer, E. Ott, and J. A. Yorke, "The dimension of chaotic attractors," *Physica D*, vol. 7, no. 1–3, pp. 153–180, 1983.

[43] J. Theiler, "Efficient algorithm for estimating the correlation dimension from a set of discrete points," *Physical Review A*, vol. 36, no. 9, pp. 4456–4462, 1987.

[44] J. Theiler, "Estimating fractal dimension," *Journal of the Optical Society of America A*, vol. 7, no. 6, pp. 1055–1073, 1990.

[45] M. Ciuc and C. Vertan, *Prelucrarea Statistică a Semnalelor*, Matrix Rom Publishing House, Bucharest, Romania, 2005.

[46] A. Luca and A. Vlad, "On the statistical independence of two discrete random variables sampled from some chaotic signals," in *Proceedings of the 31st International Conference on Modern Technologies in the 21st Century*, pp. 163–166, Military Technical Academy, Bucharest, Romania, November 2005.

[47] W. J. Conover, *Practical Nonparametric Statistics*, John Wiley & Sons, New York, NY, USA, 1999.

[48] M. I. Mihăilescu and M. Pîrloagă, "New framework for biometric face recognition using visual cryptography," in *Proceedings of the 23rd DAAAM International Symposium*, vol. 23, pp. 163–166, Vienna, Austria, 2012.

[49] J. He, H. Qian, Y. Zhou, and Z. Li, "Cryptanalysis and improvement of a block cipher based on multiple chaotic systems," *Mathematical Problems in Engineering*, vol. 2010, Article ID 590590, 14 pages, 2010.

[50] Z. G. Xu, Q. Tian, and L. Tian, "Theorem to generate independently and uniformly distributed chaotic key stream via topologically conjugated maps of tent map," *Mathematical Problems in Engineering*, vol. 2012, Article ID 619257, 12 pages, 2012.

[51] W. Xingyuan, Q. Xue, and T. Lin, "A novel true random number generator based on mouse movement and a one-dimensional chaotic map," *Mathematical Problems in Engineering*, vol. 2012, Article ID 931802, 9 pages, 2012.

[52] J. Chen, J. Zhou, K.-W. Wong, and Z. Ji, "Enhanced cryptography by multiple chaotic dynamics," *Mathematical Problems in Engineering*, vol. 2011, Article ID 938454, 12 pages, 2011.

[53] A. Rukhin, J. Soto, J. Nechvatal et al., *A Statistical Test Suite for the Validation of Random Number Generators and Pseudorandom Number Generators for Cryptographic Applications*, Special Publication SP800-22, National Institute of Standards and Technology, 2010.

[54] http://www.stat.fsu.edu/pub/diehard/.

[55] S. Banerjee and T. Pedersen, "Design, implementation and use of n-gram statistics package," in *Proceedings of the 4th International Conference on Computational Linguistics and Intelligent Text Processing (CICLing '03)*, pp. 370–381, Mexico City, Mexico, February 2003.

[56] C. Muise, S. McIlraith, J. A. Baier, and M. Reimer, "Exploiting n-gram analysis to predict operator sequences," in *Proceedings of the 19th International Conference on Automated Planning and Scheduling (ICAPS '09)*, pp. 374–377, Thessaloniki, Greece, September 2009.

[57] N. Marwan, M. C. Romano, M. Thiel, and J. Kurths, "Recurrence plots for the analysis of complex systems," *Physics Reports*, vol. 438, no. 5-6, pp. 237–329, 2007.

[58] B. F. Jorge and C. Dulce, "Recurrence plots in nonlinear time series analysis: free software," *Journal of Statistical Software*, vol. 7, no. 9, pp. 1–18, 2002.

[59] C. E. Shannon, "A mathematical theory of communication," *Bell System Technical Journal*, vol. 27, no. 3, pp. 379–423, 1948.

[60] D. P. Doane and L. E. Seward, "Measuring skewness: a forgotten statistics?" *Journal of Statistics Education*, vol. 19, no. 2, pp. 45–63, 2011.

[61] L. T. DeCarlo, "On the meaning and use of kurtosis," *Psychological Methods*, vol. 2, no. 3, pp. 292–307, 1997.

[62] S. Li, X. Mou, and Y. Cai, "Pseudo-random bit generator based on couple chaotic systems and its applications in stream-cipher cryptography," in *Progress in Cryptology—INDOCRYPT 2001*, vol. 2247 of *Lecture Notes in Computer Science*, pp. 316–329, Springer, Berlin, Germany, 2001.

[63] D. Li and S. H. Wang, "Security analysis of a multiple pseudorandom-bit generator based on a spatiotemporal chaotic map," *Chinese Physics B*, vol. 19, no. 8, Article ID 080505, 2010.

[64] S. Ahadpour and Y. Sadra, "A pseudorandom bit generator based on chaotic coupled map lattices," *Journal of Theoretical Physics & Cryptography*, vol. 1, pp. 1–5, 2012.

[65] B. O. L. Amalia, A. M. Gonzalo, G. E. Alberto, P. D. Gerardo, R. G. Miguel, and M. V. Fausto, "Trident, a new pseudo random number generator based on coupled chaotic maps," in *Proceedings of the 3rd International Conference on Computational Intelligence in Security for Information Systems (CISIS '10)*, pp. 183–190, 2010.

[66] R. S. Katti, R. G. Kavasseri, and V. Sai, "Pseudorandom bit generation using coupled congruential generators," *IEEE Transactions on Circuits and Systems II*, vol. 57, no. 3, pp. 203–207, 2010.

[67] X. Wang, J. Zhang, and W. Zhang, "Chaotic keystream generator using coupled NDFs with parameter perturbing," in *Cryptology and Network Security*, pp. 270–285, Springer, Berlin, Germany, 2006.