Hindawi
Mathematical Problems in Engineering
Volume 2019, Article ID 7685359, 10 pages
https://doi.org/10.1155/2019/7685359

Research Article

A New Two-Dimensional Mutual Coupled Logistic Map and Its Application for Pseudorandom Number Generator

Xuan Huang,[1] Lingfeng Liu ,[2] Xiangjun Li ,[2] Minrong Yu,[2] and Zijie Wu [2]

[1]*School of Software & Communication Engineering, Jiangxi University of Finance and Economics, Nanchang, 330013, China*
[2]*School of Software, Nanchang University, Nanchang, 330029, China*

Correspondence should be addressed to Lingfeng Liu; vatanoilcy@163.com and Xiangjun Li; lxjun_alex@163.com

Received 19 March 2019; Accepted 30 April 2019; Published 27 May 2019

Academic Editor: A. M. Bastos Pereira

Given that the sequences generated by logistic map are unsecure with a number of weaknesses, including its relatively small key space, uneven distribution, and vulnerability to attack by phase space reconstruction, this paper proposes a new two-dimensional mutual coupled logistic map, which can overcome these weaknesses. Our two-dimensional chaotic map model is simpler than the recently proposed three-dimensional coupled logistic map, whereas the sequence generated by our system is more complex. Furthermore, a new kind of pseudorandom number generator (PRNG) based on the mutual coupled logistic maps is proposed for application. Both statistical tests and security analysis show that our proposed PRNG has good randomness and that it can resist all kinds of attacks. The algorithm speed analysis indicates that PRNG is valuable to practical applications.

1. Introduction

Chaos is a popular phenomenon in the natural and social world. Some interesting nonlinear dynamical characteristics of chaotic system, including sensitivity to initial condition and parameter, topological transitivity, pseudorandomness, and wide spectrum,, leading the chaotic systems to be widely used in many different kinds of fields, such as spread spectrum communication, numerical simulation, error control coding, and cryptography [1–3]. In such applications, the pseudorandom number sequence (PRNS) with good security performances is necessary. Traditional methods for generating PRNS are mainly based on the linear congruential method or linear feedback shift registers. However, the inner-linear construction of these methods will make a greater risk by correlation attack [4] and algebraic attack [5]. Therefore, an improved method for generating PRNS is to use nonlinear source. The chaotic system is with rich nonlinear dynamics, which is regarded as an important pseudorandom source in the design of PRNG recently.

The first chaos-based PRNG was proposed by Oishi and Inoue in 1982 [6]. Since then, a large number of chaotic PRNGs have been proposed [7–18]. In [7], Szczepanski and Kotulski propose a chaotic PRNG by applying discrete chaotic dynamical systems, whose idea is exploiting the property of extreme sensitivity of trajectories to small changes of initial conditions. Li et al. propose a chaotic PRNG based on a coupled map lattice, which is adopted as a prototype of a spatiotemporal chaotic system [8]. Francois et al. proposed a secure PRNG three-mixer, whose principle of the method consists in mixing three chaotic maps produced from an input initial vector [9]. Hu et al. proposed a PRNG based on the Chen chaotic system by combining three coordinates of chaotic orbit [10]. In [11], a PRNG based on nonstationary logistic map, whose control parameter is driven by a dynamic algorithm, is proposed. Moreover, Wang et al. proposed a PRNG based on z-logistic map [12]; Kocarev et al. analyzed the application of a chaotic piecewise-linear one-dimensional map as RNG [13, 14]; Wang et al. proposed a PRNG by using piecewise logistic chaotic map [15]. Two PRNGs based on logistic chaotic maps intended for stream cipher applications are proposed in [16] and so forth.

Among all the chaos-based PRNGs, the one-dimensional chaotic map is most widely used, especially for logistic map. Logistic map is described by a simple mathematical function, which is quite easy to implement by both algorithm and circuits. However, some researches show that the sequences generated by logistic map are not secure with some weaknesses [19], including the following.

(1) Relatively small key space: logistic map has only one control parameter, and the state variable is one-dimensional, which makes the key space small.

(2) Uneven distribution: the distribution of the sequences generated by logistic map is "U" like, which is not uniform.

(3) Easily be attacked by phase space reconstruction: although the trajectory of logistic map looks complicated, once we reconstruct the trajectories into a space with higher dimension, the structure becomes simple and evident.

Therefore, logistic map cannot be used to construct PRNG before addressing all these weaknesses. In order to overcome these weaknesses, two kinds of method have been provided. References [20, 21] overcome the weaknesses by constructing parameter-varied logistic map. How to vary the parameter is the most important key to this kind of method. If the parameters are varying in a simple way, the parameter-varying chaotic map can still be predicted based on wavelet neural network and multiwavelets neural network [22]. Else, if the parameters are varying in a complicated way, the implement cost will be greatly increased. Another method is coupling multiple logistic maps. Reference [19] proposed three-dimensional coupled logistic maps to overcome the weaknesses of logistic map.

Motivated by [19], in this paper, we propose a new two-dimensional mutual coupled logistic map to overcome the weaknesses of logistic map. The experiment results show that this new map can enlarge the key space, can resist the phase space reconstruction attack, and has a uniform distribution. Our two-dimensional chaotic map is simpler than the three-dimensional coupled logistic map in [19], while the generated sequence of our system is more complex, which has been evaluated by using both approximate entropy (ApEn) and permutation entropy (PE). Furthermore, we propose a new kind of PRNG based on the mutual coupled logistic maps for application. Both statistical tests and security analysis show that our proposed PRNG is with good randomness and is capable of resisting all kinds of attacks. The algorithm speed analysis shows that the PRNG is valuable to practical applications.

The rest of this paper is organized as follows. The new two-dimensional mutual coupled logistic map and its dynamical performances are provided in Section 2. In Section 3, a new kind of PRNG is introduced. The statistical tests for PRNG are presented in Section 4. The security and algorithm speed analysis are presented in Section 5. Finally, Section 6 concludes the whole paper.

2. The New Mutual Coupled Logistic Map and Its Performances

To overcome the security weaknesses of logistic map, in this section, we construct the following mutual coupled logistic map, whose mathematical model can be described as

$$\begin{aligned} x_{i+1} &= a \cdot \left(10^3 - 1\right) \cdot \max\left\{x_i, y_i\right\} \cdot \left(1 - \max\left\{x_i, y_i\right\}\right) \\ y_{i+1} &= b \cdot \left(10^3 - 1\right) \cdot \sqrt{x_i y_i}\left(1 - \sqrt{x_i y_i}\right) \end{aligned} \quad (1)$$

$$\text{mod1}$$

where x_i and y_i are the state variables of maps X and Y, respectively. a and b are the control parameters of maps X and Y, respectively, $3.6 \le a, b \le 4$. By mutual coupling of two logistic maps, (1) becomes two-dimensional. This coupled model is proposed based on the following considerations.

(1) The subsystems of the coupled model should maintain the form of logistic map.

(2) Gain $10^3 - 1$ and modular operation are used to improve the distribution characteristics of the original logistic map.

(3) The coupled term $\max\{x_i, y_i\}$ and $(x_i y_i)^{1/2}$ are used to make the states of x_{i+1} and y_{i+1} be affected by both x_i and y_i, which can improve the complexity of the original logistic map.

Note that this coupled model is not irreplaceable. The gain $10^3 - 1$ can be replaced by another coefficient. Distribution characteristics are generally better for a larger gain. In addition, the coupled terms can also be replaced by other forms, e.g., $\min\{x_i, y_i\}$, $(x_i + y_i)/2$. Therefore, a more general model can be written as

$$\begin{aligned} x_{i+1} &= a \cdot k \cdot h_1\left(x_i, y_i\right) \cdot \left(1 - h_1\left(x_i, y_i\right)\right) \\ y_{i+1} &= b \cdot k \cdot h_2\left(x_i, y_i\right) \cdot \left(1 - h_2\left(x_i, y_i\right)\right) \end{aligned} \quad (2)$$

$$\text{mod1}$$

where k is the gain coefficient and $h_1(x_i, y_i)$ and $h_2(x_i, y_i)$ are two coupled functions. Although the coupled model appears simple, the weaknesses of the logistic map have been greatly improved. Next, we will show that the new two-dimensional chaotic map is with good dynamical and complexity performances. In the numerical analysis, the x-dimensional variable of (1) is selected. For the y-dimensional variable, similar results are omitted here to avoid redundancy.

2.1. Key Space Analysis. For the logistic map, only one parameter and one-dimensional initial condition can be selected as the secret key. Let the largest precision be 10^{-16}. The key space of the logistic map approximately equals $0.4 * 10^{32} \approx 2^{105}$, which is less than the secure requirement 2^{128} of cryptographic application. While for the mutual coupled logistic map described by (1), both parameters a, b and initial conditions x_0, y_0 can be selected as the secret key, with whose key space is about $0.16 * 10^{64} \approx 2^{210}$. Therefore, we can see that the key space of (1) has increased greatly, which is large enough to resist brute-force attack.

2.2. Distribution Diagram. As shown in Figure 1(a), the distribution of the sequences generated by logistic map is "U" like (not uniform) with a bad statistical property, and it can be attacked by some statistical analysis. Set $a = b = 3.999$, and the initial conditions x_0 and y_0 are randomly selected; the distribution of the generated sequences of our two-dimensional mutual coupled logistic map is shown in Figure 1(b). Evidently, Figure 1(b) indicates that the generated sequence by (1) is uniformly distributed. However, other two-dimensional logistic maps are not uniformly distributed. Figure 1(c) shows the histogram of the two-dimensional logistic map in [23]. The distribution of this map is obviously not uniform.

2.3. Trajectories and Phase Space. Let $a = b = 3.999$. Randomly choose the initial values of the logistic map and (1). Figure 2 shows the trajectories of these two chaotic maps. From Figure 2 we can find that these two trajectories are both disorganized with what appears as good randomness. However, once we reconstruct the trajectories into a space with an increased dimension, the structures differ. In the phase space reconstruction technology, delay time and embedding dimension are two key parameters. For the best reconstruction, in this experiment, we set delay time at 1 and the embedding dimension at 3 according to the autocorrelation function and false neighbor method. The reconstructed phase spaces are shown in Figure 3. From Figure 3(a) we have that the reconstructed phase space of logistic map has a significant structure, whereas the reconstructed phase space of mutual coupled logistic map is still disorganized without a significant structure. Therefore, our mutual coupled logistic map can resist the phase space reconstruction attack. Moreover, for other delay times and embedding dimensions, the phase space is still disordered without a significant structure for the mutual coupled logistic map, which we do not repeat here.

2.4. Complexity Analysis. In this section, the approximate entropy (ApEn) and permutation entropy (PE) are used to evaluate the complexity of the generated sequences. Comparisons to the generated sequences in [19] are also presented here. We set $a = b$ in these two tests.

2.4.1. ApEn Analysis. ApEn is a well-known complexity measure for time-series proposed by Pincus in [29]. The ApEn of the generated sequences by logistic map, (1) and the intertwining logistic map in [19] are shown in Figure 4. Figure 4 shows that our mutual coupled logistic map has the largest ApEn value with different parameters, which implies that our mutual coupled logistic map can significantly improve the complexity of the logistic map. Moreover, our system is also more complex than the intertwining logistic map in [19] in this sense, although with a lower dimension. The two-dimensional logistic map in [23] will be chaotic when the control parameter r is in the interval $[1.1, 1.19]$. The ApEn of this map ranges from 0.260919 to 0.626634 with the increase of parameter r, which is significantly much lower than our mutual coupled logistic map.

2.4.2. PE Analysis. PE is a natural complexity measure for time-series introduced in [30]. Furthermore, it is easier to implement and computationally much faster than other comparable methods, in addition to being robust to noise [31]. Figure 5 compares the PE of the logistic, mutual coupled logistic, and intertwining logistic maps in [19]. From Figure 5, we can conclude that our mutual coupled logistic map is more complex than the logistic and the intertwining logistic maps in [19] in this sense. Furthermore, the PE value of the mutual coupled logistic map is always larger than 0.99 with different parameter a, which indicates that the generated sequences have good randomness. Compared with the two-dimensional logistic map in [23], the PE of this map varies from 0.4674 to 0.8141 with the increase of parameter r, which is also lower than our mutual coupled logistic map.

Remark 1. Coupling multiple logistic maps is an effective method for improving the performances of a logistic map. For a good coupling strategy, the following three conditions should be satisfied.

(1) Performances. The coupled logistic maps should overcome the weaknesses mentioned in the Introduction and increase the dynamical complexity. As shown by the numerical experiments, our coupled logistic map can overcome such weaknesses, and it is more complex than the intertwining logistic map in [19] and the improved logistic map in [11].

(2) Costs. Coupling with more dynamical systems or a more complicated system generally increases dynamical complexity. However, it will also increase the implementation costs. Only two simple logistic maps are coupled in our model to improve its performance, which only requires much less implementation costs than other schemes, such as [11, 20].

(3) Universality. This paper proposed a general coupled logistic model. In this model, the gain coefficient and coupled functions are both variable, whereas only a specific model is proposed in other schemes.

In summary, compared with other recently proposed schemes, our mutual coupled logistic map has great advantages in performances, costs, and universality.

3. The New PRNG

As presented in Section 2, the mutual coupled logistic map (1) is with good performances. In this Section, a new kind of PRNG is proposed based on (1), which can be described as follows:

$$b_i = floor\left(256 \cdot x_i\right) \oplus floor\left(256 \cdot y_i\right) \tag{3}$$

where x_i and y_i are the state variables of (1), and sequence $\{b_i\}$ is the final bit sequence. According to (3), we can generate 8 bits for every one time of iteration, which can increase the productivity of random numbers. Some details will be analyzed in Section 5.4. The main frame of this kind of PRNG is shown in Figure 6, and Figure 7 depicts the mathematical model diagram of our PRBG.

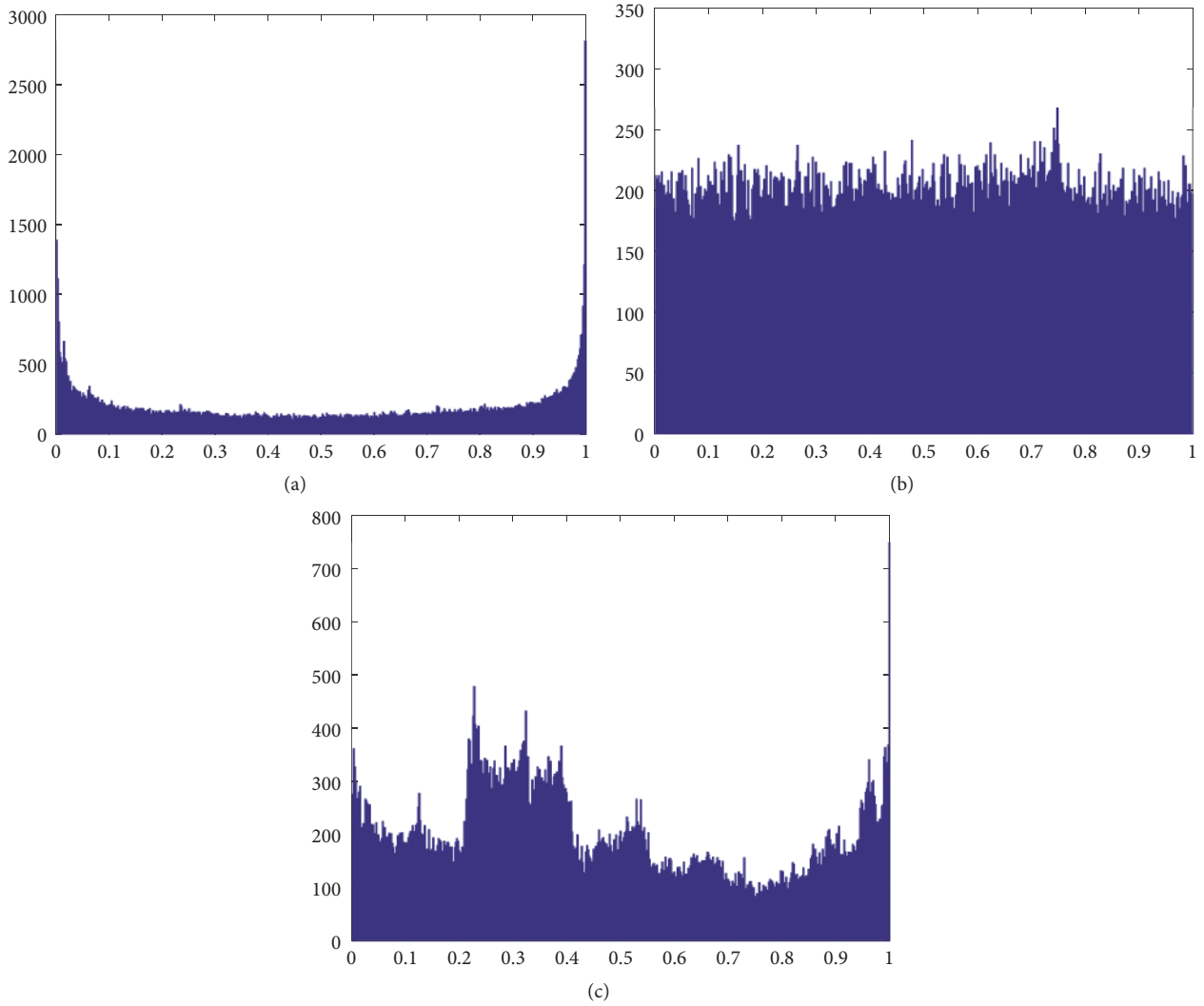

Figure 1: The distribution diagram for (a) logistic map; (b) mutual coupled logistic map; (c) two-dimensional logistic map in [23].

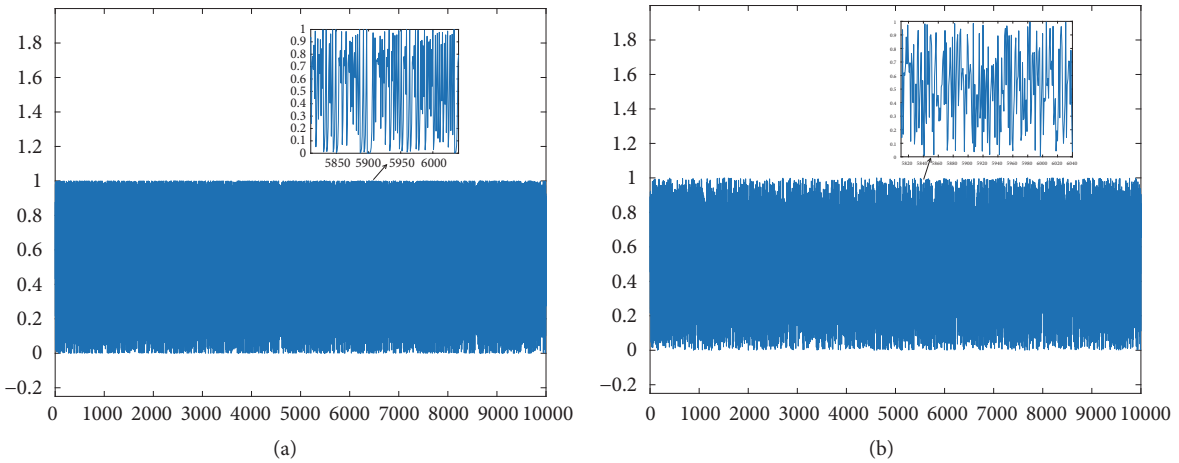

Figure 2: The trajectories of (a) logistic map; (b) mutual coupled logistic map.

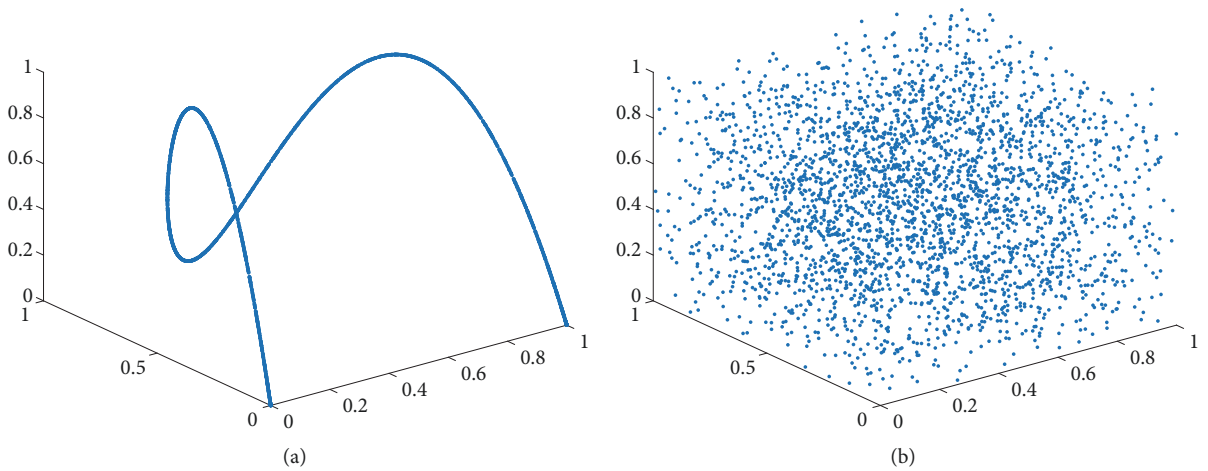

Figure 3: Phase space reconstruction for (a) logistic map; (b) mutual coupled logistic map.

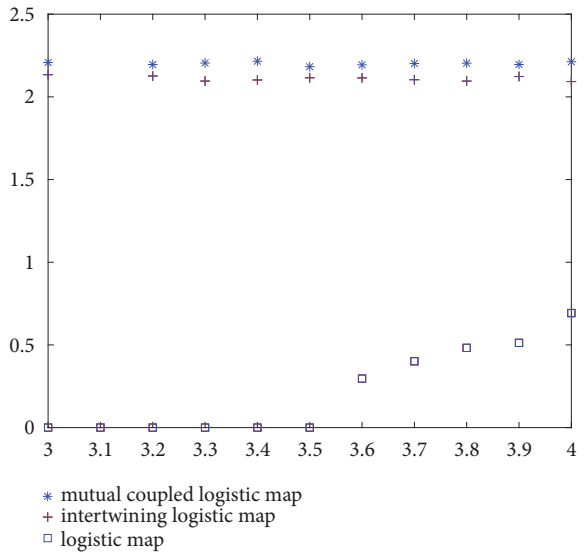

Figure 4: Approximate entropy comparison.

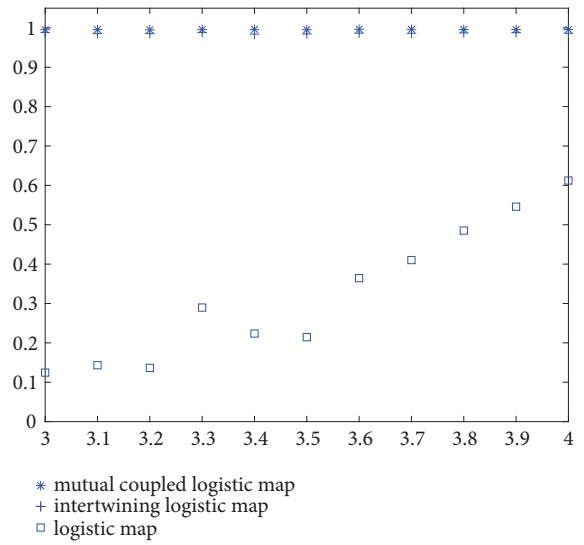

Figure 5: Permutation entropy comparison.

4. Statistical Tests

In this Section, several statistical tests are used to evaluate the randomness of sequences $\{b_i\}$. The parameters a and b are selected as $a = b = 3.999$ through the whole statistical tests.

4.1. Frequency Spectral Analysis. Frequency spectral analysis is used to test whether the center frequency exists or not in the bit sequence. If there is a center frequency in a sequence, it is periodic and cannot be regarded as ideal random sequence. The frequency spectrum of sequence $x(n)$ can be calculated by

$$x_p(n) = \sum_{n=1}^{N} x(n) e^{-j(2\pi/N)(k-1)(n-1)} \quad (4)$$

where N denotes the sequence length and k is the rank of harmonic, with $0 \le k \le N$.

Let the length of sequence be 20000. Randomly choose 2000 bits from the sequence. The frequency spectral analysis is shown in Figure 8. From Figure 8 we can see that there is no center frequency in the spectrum, which implies that the bit sequence $\{b_i\}$ is not periodic.

4.2. Beker and Piper's Statistical Tests. Beker and Piper's statistical test suite is a classical randomness test suite which includes frequency test, serial test, poker test, runs test, and autocorrelation test [32]. Set the confidence level of statistical tests to be 0.95. Randomly choosing the initial conditions, the test results are shown in Table 1 and Figure 9, where T in Table 1 refers to the threshold. As shown in Table 1, all the statistical values are smaller than T, which means that the bit sequence $\{b_i\}$ has passed all these four tests. Figure 8 shows that the autocorrelation and cross-correlation of sequence $\{b_i\}$ are delta function and zero function, respectively, which

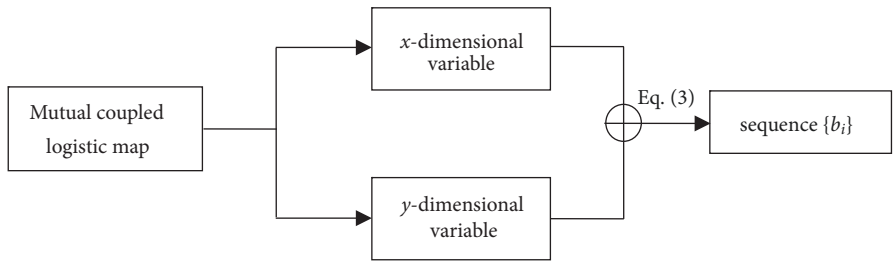

Figure 6: The main frame of our PRBG.

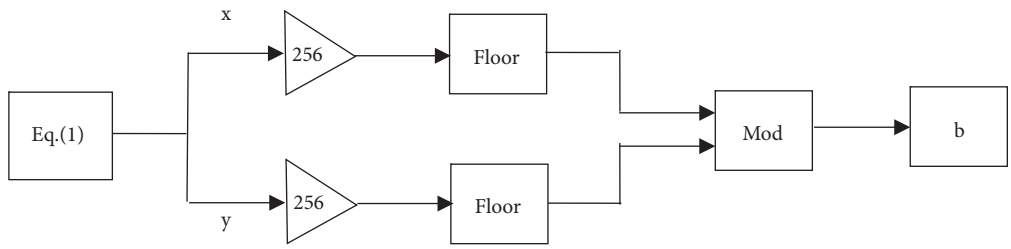

Figure 7: The mathematical diagram of the PRBG.

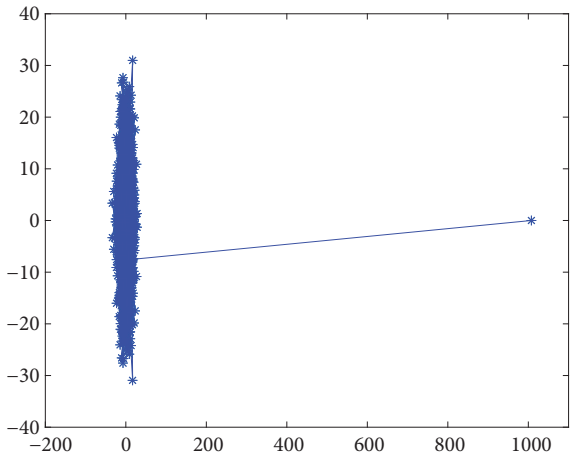

Figure 8: Frequency spectrum of sequence $\{b_i\}$.

are consistent with the ideal random sequences'. The results in Table 1 and Figure 9 indicate that sequence $\{b_i\}$ has good statistical characteristics and can be regarded as ideal random.

4.3. NIST Statistical Tests. NIST statistical test suite is stringent and also current industry norm for randomness testing, which is proposed in [33]. The well-known NIST test suite contains 16 different tests. The significance level of each test in NIST is set to 0.01. Sequences are said to pass a test if the calculated P_value > 0.01. In this numerical experiment, we generate 1000 groups of bit sequence with length as 10^6 by randomly choosing 1000 groups of initial condition. The passing ratio and means of P_value of each test are shown in Table 2. From Table 2 we can have that the bit sequence $\{b_i\}$ has passed all the tests, which implies that the sequence is with good statistical performances and can be regarded as true random.

4.4. TestU01 Statistical Tests. TestU01 statistical test suite [34] is stringent, as well as the current industry norm for randomness testing. This test suite contains three different crush type batteries: Small-Crush, Crush, and Big-Crush. In this test, we just use Small-Crush and Crush batteries based on the storage space of our computer. When the P-value is $[10^{-4}, 1 - 10^{-4}]$, it passes the test. The test results are shown in Table 3. From Table 3, we can obtain our generated bit sequences have passed all the TestU01 statistical test, which implies good randomness. While for the chaotic PRBGs in [24–26], there all are several failures through the TestU01 statistical test, which indicates that this PRBG is competitive in this sense.

5. Security and Algorithm Speed Analysis

Key space, key sensitivity, and linear complexity are some necessary conditions for a secure PRNG. Besides security, the algorithm speed is also important to the applicability of PRNG.

5.1. Key Space. Let the greatest precision be 10^{-r}. The control parameters a and b and initial conditions x_0 and y_0 can be selected as the secret key. As $3.6 \leq a, b \leq 4$, $0 < x_i, y_i < 1$, the key space size of our PRNG approximately equals $0.16 * 10^{4r}$. Let $r = 16$; the key space size is approximately equal to 2^{210}, which is large enough to withstand brute-force attack. Furthermore, the key space of our PRNG is also larger than some recently proposed chaotic PRNGs' under the same precision, such as 2^{188} in [27], which means that our PRNG is competitive in this sense.

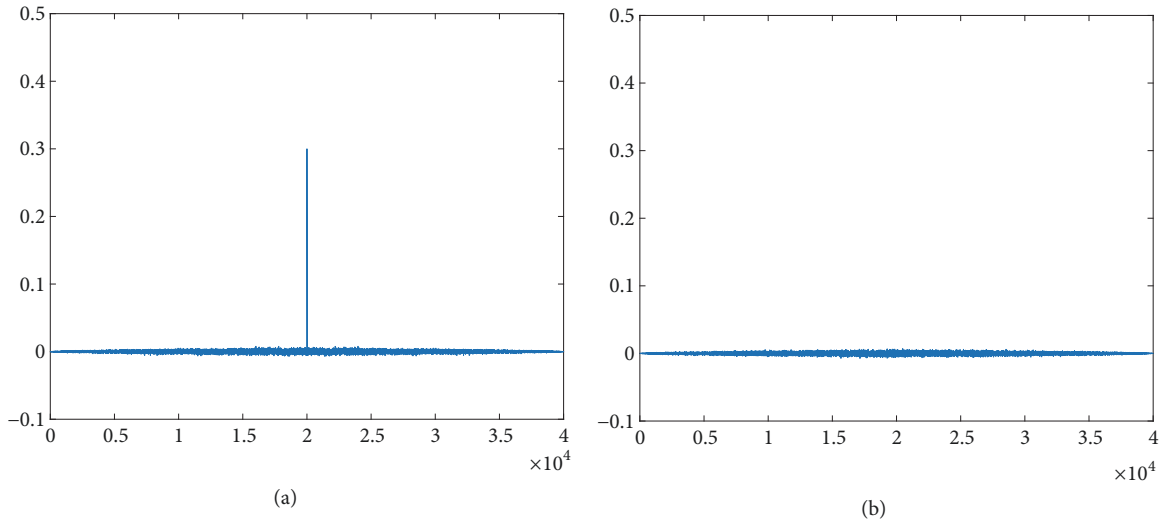

Figure 9: Correlation analysis: (a) auto-correlation; (b) cross-correlation.

Table 1: Statistical performances.

	Frequency test	Serial test	Poker test			Runs test
			$m = 2$	$m = 3$	$m = 4$	
25000 bits	0.62	2.61	2.69	7.24	14.19	1.58
50000 bits	0.33	2.55	2.33	8.03	10.53	1.31
75000 bits	0.29	1.93	1.74	5.99	8.62	1.34
100000 bits	0.07	1.04	1.01	4.20	6.45	1.03
T	3.84	5.99	7.81	14.07	26.00	1.96

Table 2: Results for NIST test suite.

Test Index	Passing Ratio	Means of P_value	Results
Approximate entropy	0.998	0.34973	Passed
Block frequency	0.999	0.33242	Passed
Cumulative sums	0.999	0.21495	Passed
FFT	0.997	0.41003	Passed
Frequency	0.999	0.42167	Passed
Linear complexity	0.999	0.51674	Passed
Random excursions	0.999	0.30147	Passed
Random excursions variant	0.998	0.29871	Passed
Longest runs of ones	0.996	0.25675	Passed
Overlapping template of all ones	0.998	0.31775	Passed
Rank	0.998	0.19306	Passed
Runs	0.999	0.24879	Passed
Serial	0.997	0.24198	Passed
Universal statistical	0.999	0.41029	Passed
Lempel-Ziv Compression Test	0.999	0.35497	Passed

Table 3: The number of failures in TestU01 test suite.

Battery	Parameters	Small-Crush	Crush
Our PRBG	Standard	0	0
Ref. [24]	Standard	3	15
Ref. [25]	Standard	2	12
Ref. [26]	Standard	3	19

Table 4: Sensitivity test for a.

Secret key a	3.999 and $3.999 + 10^{-16}$	$3.999 + 10^{-16}$ and $3.999 + 2\times10^{-16}$	$3.999 + 2\times10^{-16}$ and $3.999 + 3\times10^{-16}$
H	50.04%	50.04%	49.98%

Table 5: Sensitivity test for x_0.

Secret key x_0	0.164 and $0.164 + 10^{-16}$	$0.164 + 10^{-16}$ and $0.164 + 2\times10^{-16}$	$0.164 + 2\times10^{-16}$ and $0.164 + 3\times10^{-16}$
H	49.98%	50.02%	49.96%

Table 6: Speed comparison of different PRNG.

Different PRNG	Speed (Mb/s)
Our PRNG	3.8955
Ref. [27]	0.4844
Ref. [28]	0.2352

5.2. Key Sensitivity. Chaotic sequence is greatly sensitive to the initial condition and parameter. In this numerical experiment, we vary the secret keys by only 10^{-16} to generate new bit sequences and then compare them by each bit. Denote H as the number of differences. The key sensitivity test results for a and x_0 are shown in Tables 4 and 5, respectively. These two tables show that the variance ratios of each bit both approach 50%, which indicate that our PRNG is extremely sensitive to a and x_0. For secret keys x and y_0, the results are similar which we omitted here to avoid redundancy.

5.3. Linear Complexity. Linear complexity is one of the most important complexity measures for bit sequence. For an ideal random bit sequence with length n, the linear complexity should be close to the $n/2$ line. Figure 10 plots the linear complexity curve of the bit sequence generated by our PRNG, which indicates that the sequence is with ideal linear complexity since the curve is extremely close to the $n/2$ line.

5.4. Algorithm Speed Analysis. In this paper, the algorithms are experiment by Matlab R2014a on the computer with 3.3 GHz CPU and 4GB memory. The algorithm speed of our PRNG and other proposed chaotic PRNGs in [27, 28] are compared in Table 6. From Table 6 we have that the speed of our PRNG is about 3.8955 MB/s, which is much faster than the speed of PRNG in [24, 25] under the same running conditions. This result indicates that our PRNG is quite applicable for practical use.

6. Conclusions

In this paper, a new two-dimensional mutual coupled logistic map is proposed, which can overcome the several weaknesses of logistic map. Dynamical performances indicate that this new map has a larger key space, a uniform distribution, and can resist to the phase space reconstruction attack. Furthermore, the complexity performances show that the generated sequence of our system is more complex than the sequence generated by the three-dimensional coupled logistic map proposed in [19], together with a simpler mathematical model. For the application, we propose a new kind of PRNG based on the mutual coupled logistic map. Both statistical tests and security analysis show that our proposed PRNG is with good randomness and is capable of resisting all kinds of attacks. Moreover, the algorithm speed analysis indicates that the PRNG has a rather high generation efficiency, which is valuable to practical applications.

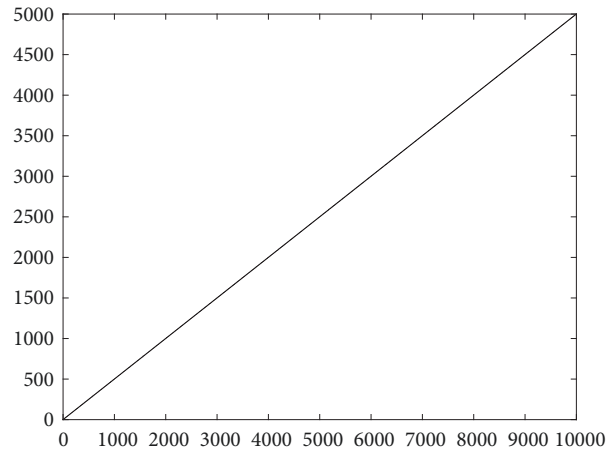

Figure 10: Linear complexity.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare no competing financial interests.

Authors' Contributions

Xuan Huang wrote the main manuscript text, Lingfeng Liu and Xiangjun Li did the numerical experiments, and Minrong Yu and Zijie Wu analyzed the results.

Acknowledgments

The contributions of this research are the following: the National Natural Science Foundation of China (No. 61862042, 61601215, 61762062, 61862044); Science

and Technology Innovation Platform Project of Jiangxi Province (No. 20181BCD40005); Major Discipline Academic and Technical Leader Training Plan Project of Jiangxi Province (No. 20172BCB22030); Primary Research & Development Plan of Jiangxi Province (No. 20181ACE50033, No. 20171BBE50064, 2013ZBBE50018, 20111BBE50008); Jiangxi Province Natural Science Foundation of China (No. 20171BAB202027, No. 20142BAB207011); Science & Technology Research Project of Education Department of Jiangxi Province (No. GJJ150104, GJJ161387).

References

[1] N. Kalouptsidis, *Signal Processing Systems*, Telecommunications and Signal Processing Series, Wiley, New York, NY, USA, 1996.

[2] T. Addabbo, M. Alioto, A. Fort, S. Rocchi, and V. Vignoli, "A feedback strategy to improve the entropy of a chaos-based random bit generator," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 53, no. 2, pp. 326–337, 2006.

[3] G. Alvarez, F. Montoya, M. Romera, and G. Pastor, "Keystream cryptanalysis of a chaotic cryprographic method," *Computer Physics Communications*, vol. 156, pp. 205–207, 2003.

[4] B. Zhang and D. Feng, "Improved multi-pass fast correlation attacks with applications," *Science China Information Sciences*, vol. 54, no. 8, pp. 1635–1644, 2011.

[5] N. T. Courtois and W. Meier, "Algebraic attack on stream ciphers with linear feedback," in *Proceedings of the EUROCRYPT '03*, vol. 2656 of *Lecture Notes in Computer Science*, pp. 345–359, Berlin, Germany, 2003.

[6] S. Oishi and H. Inoue, "Pseudo-random number generators and chaos," *Transactions of the Institute of Electronics and Communication Engineers of Japan E*, vol. E65, no. 9, pp. 534–541, 1982.

[7] J. Szczepański and Z. Kotulski, "Pseudorandom number generators based on chaotic dynamical systems," *Open Systems and Information Dynamics*, vol. 8, no. 2, pp. 137–146, 2001.

[8] P. Li, Z. Li, W. A. Halang, and G. Chen, "A multiple pesudorandom-bit generator based on a spatiotemporal chaotic map," *Physics Letters A*, vol. 349, no. 6, pp. 467–473, 2006.

[9] M. Francois, T. Grosges, D. Barchiesi, and R. Erra, "Pseudo-random number generator based on mixing of three chaotic maps," *Communications in Nonlinear Science and Numerical Simulation*, vol. 19, no. 4, pp. 887–895, 2014.

[10] H. P. Hu, L. F. Liu, and N. D. Ding, "Pseudorandom sequence generator based on Chen chaotic system," *Computer Physics Communications*, vol. 184, no. 3, pp. 765–768, 2013.

[11] L. Liu, S. Miao, H. Hu, and Y. Deng, "Pseudorandom bit generator based on non-stationary logistic maps," *IET Information Security*, vol. 10, no. 2, pp. 87–94, 2016.

[12] L. Wang, F. P. Wang, and Z. J. Wang, "Novel chaos-based pseudo-random number generator," *Acta Physica Sinica*, vol. 55, no. 8, pp. 3964–3968, 2006.

[13] T. Stojanovski and L. Kocarev, "Chaos-based random number generators – Part I: analysis," *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 48, no. 3, pp. 281–288, 2001.

[14] T. Stojanovski, J. Pihl, and L. Kocarev, "Chaos-based random number generators – Part II: practical realization," *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 48, no. 3, pp. 382–385, 2001.

[15] Y. Wang, Z. Liu, J. Ma, and H. He, "A pseudorandom number generator based on piecewise logistic map," *Nonlinear Dynamics*, vol. 83, no. 4, pp. 2373–2391, 2016.

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

[17] M. L. Sahari and I. Boukemara, "A pseudo-random numbers generator based on a novel 3D chaotic map with an application to color image encryption," *Nonlinear Dynamics*, vol. 94, no. 1, pp. 723–744, 2018.

[18] X. Lv, X. Liao, and B. Yang, "A novel pseudo-random number generator from coupled map lattice with time-varying delay," *Nonlinear Dynamics*, vol. 94, no. 1, pp. 325–341, 2018.

[19] X. Wang and D. Luan, "A novel image encryption algorithm using chaos and reversible cellular automata," *Communications in Nonlinear Science and Numerical Simulation*, vol. 18, no. 11, pp. 3075–3085, 2013.

[20] M. A. Murillo-Escobar, C. Cruz-Hernández, F. Abundiz-Pérez, R. M. López-Gutiérrez, and O. R. Acosta Del Campo, "A RGB image encryption algorithm based on total plain image characteristics and chaos," *Signal Processing*, vol. 109, pp. 119–131, 2015.

[21] Y. Wang, K.-W. Wong, X. Liao, T. Xiang, and G. Chen, "A chaos-based image encryption algorithm with variable control parameters," *Chaos, Solitons & Fractals*, vol. 41, no. 4, pp. 1773–1783, 2009.

[22] F. Xiao and X.-P. Gao, "An approach for short-term prediction on time series from parameter-varying systems," *Journal of Software*, vol. 17, no. 5, pp. 1042–1050, 2006.

[23] M. Machkour, A. Saaidi, and M. L. Benmaati, "A novel image encryption algorithm based on the two-dimensional logistic map and the latin square image cipher," *3D Research*, vol. 6, article 36, 2015.

[24] Y. Deng, H. Hu, W. Xiong, N. N. Xiong, and L. Liu, "Analysis and design of digital chaotic systems with desirable performance via feedback control," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 45, no. 8, pp. 1187–1200, 2015.

[25] X. Wang, X. Qin, 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.

[26] X.-Y. Wang and X. Qin, "A new pseudo-random number generator based on CML and chaotic iteration," *Nonlinear Dynamics*, vol. 70, no. 2, pp. 1589–1592, 2012.

[27] Y. Liu and X. J. Tong, "A new pseudorandom number generator based on complex number chaotic equation," *Chinese Physics B*, vol. 21, no. 9, article 090506, 2012.

[28] X. Tong and M. Cui, "Feedback image encryption algorithm with compound chaotic stream cipher based on perturbation," *Science China Information Sciences*, vol. 53, no. 1, pp. 191–202, 2010.

[29] S. M. Pincus, "Approximate entropy as a measure of system complexity," *Proceedings of the National Acadamy of Sciences of the United States of America*, vol. 88, no. 6, pp. 2297–2301, 1991.

[30] C. Bandt and B. Pompe, "Permutation entropy: a natural complexity measure for time series," *Physical Review Letters*, vol. 88, no. 17, Article ID 174102, 2002.

[31] J. P. Toomey and D. M. Kane, "Mapping the dynamic complexity of a semiconductor laser with optical feedback using permutation entropy," *Optics Express*, vol. 22, no. 2, pp. 1713–1725, 2014.

[32] H. Beker and F. C. Piper, *Cipher Systems: The Protection of Commnications*, Wiley, New York, NY, USA, 1982.

[33] A. Rukhin, J. Sota, J. Nechvatal et al., "A statistical test suite for random and pseudorandom number generators for cryptographic applications," Tech. Rep. NISTSpecial Publication 800-22, 2010.

[34] P. L'Ecuyer and R. Simard, "TestU01: a C library for empirical testing of random number generators," *ACM Transactions on Mathematical Software*, vol. 33, no. 4, pp. 1–22, 2007.