Journal of Information Hiding and Multimedia Signal Processing ©2016 ISSN 2073-4212
Ubiquitous International Volume **7**, Number **4**, July **2016**

Excellent Performances of The Third-level Disturbed Chaos in The Cryptography Algorithm and The Spread Spectrum Communication

Juan Wang[1,2] and Qun Ding[1]

[1]Electronic engineering institute,
Heilongjiang University,
Harbin, China
[2]Electronic and information engineering institute,
Heilongjiang University of science and technology,
Harbin, China
76115347@qq.com, qunding@aliyun.com

Received April, 2016; revised May, 2016

Abstract. *In this paper, a new logistic chaos was obtained by improving the traditional logistic chaos, and the second-level and the third-level chaoses were constructed in view of the ideas of cascade and disturbance. The performances of dynamic characteristics and statistical randomness were simulated and analyzed for the chaotic sequences at all levels, and the third-level disturbed chaotic sequence was proved to be more excellent. Consequently, when the third-level disturbed chaotic sequence is introduced into the cryptography algorithm and the spread spectrum communication, improved performance may be achieved.*
Keywords: Chaos; Cascade; Disturbance; Dynamic characteristic; Statistical randomness.

1. **Introduction.** Chaos is a deterministic and pseudo-random process produced by the nonlinear dynamic system. Chaos cannot be convergent but has bounds, it is aperiodic and sensitively dependent to the initial value [1]. Chaotic attractor has the characteristics of topological transitivity and miscibility and it is sensitive to the system parameter, as a result it fits for the confusion principle in cryptography design. Meanwhile, the divergence of trajectories and the sensitivity to initial value of chaos fit for the diffusion principle in cryptography design. Therefore, chaos has gradually become the focus of cryptography research [2]. On the other hand, chaos can provide numerous pseudo-random renewable signals, which are non-correlative and deterministic. When chaos is applied to the spread spectrum communication, the performances in anti-noise, anti-interference, anti-fading, anti-multipath and anti-decipher would be improved too [3, 4].

With the development of chaotic cryptography and chaotic communication technology, the requirements in the applications of chaotic sequences have been increasing. There are a series of disadvantages for the traditional logistic chaos, such as small surjective interval, narrow parameter range and low complexity, etc. In this paper, the traditional logistic chaos was improved and a new logistic chaos was obtained. In addition, the second-level and third-level chaoses were constructed in view of the ideas of cascade and disturbance. The performances of dynamic characteristics and statistical randomness were tested and analyzed for the chaotic sequences at all levels, and reached the conclusion that the

dynamic and pseudo-random characteristics of the third-level disturbed chaotic sequence are more excellent. When the third-level disturbed chaotic sequence is used as a key or a spread spectrum sequence, the cryptography algorithm and the spread spectrum communication would obtain better performance.

2. **The first-level chaos.** the discrete chaotic map is fast to iterate and easy to control, it has incomparable superiority compared with the continuous chaotic system [5]. At present, the application research of chaos is mostly focused on the discrete chaotic map, which can be described by difference equation.

2.1. **The first-level traditional chaos.** The equation of the first-level traditional logistic map is given to be,

$$x_{n+1} = \mu x_n(1 - x_n) \quad n = 1, 2, 3 \ldots \tag{1}$$

In Eq. (1), x_n is the value of being iterated n times where $x_n \in (0, 1]$, and x_{n+1} is the value of being iterated $n + 1$ times; the interval of system parameter is $\mu \in (0, 4]$, while when $\mu \in (3.569946, 4]$, the traditional logistic map should be in the chaotic state.

As a kind of chaos, the traditional logistic chaos has been widely researched and applied owing to its simple mathematical model. Although the traditional logistic chaos has preferable performances of randomness and correlation, and its circuit is easier to be implemented. the disadvantages of the traditional logistic chaos are also apparent, such as infinite fixed-point attractor, small surjective interval, narrow parameter range and low complexity, etc [6, 7, 8, 9]. When the system parameter is improperly chosen, the iteration results would tend to be a fixed-value or tend to be collectively distributed, the security of cryptography algorithm or the anti-interference of spread spectrum communication would be influenced to a certain extent. Therefore, the traditional logistic chaos is necessary to be improved.

2.2. **The first-level new chaos.** The equation of the first-level new logistic map is given to be,

$$x_{n+1} = \mu x_n(1-x_n^2)\mathrm{mod}1 \quad n = 1, 2, 3 \ldots \tag{2}$$

In Eq. (2), the interval of system parameter is $\mu \in (0, 4]$, the interval of initial value is $x_n \in (0, 1]$, and mod1 is the standard modulo 1 operation. From Eq. (2) we can see that $\mu x_n(1 - x_n^2)$ is greater than zero. In the operation of mod 1, When $\mu x_n(1 - x_n^2)$ is an integer, the value of x_{n+1} is zero; when $\mu x_n(1 - x_n^2)$ is not an integer, the value of x_{n+1} is a decimal. the original iteration values beyond the scope of the definition domain can be decreased, falling into the interval (0, 1] and iterated again. Although there is only a trivial improvement, the disadvantages in the traditional logistic chaos may be effectively ameliorated.

3. **The second-level chaos.** At present, there is not a possible theoretical framework on how to significantly improve the dynamic characteristics and pseudo-randomness of the discrete chaotic map [10]. Herein, based on the ideas of cascade and disturbance, we proposed several solutions in this paper.

3.1. **The second-level cascaded chaos.** The model of the second-level cascaded chaos is shown in figure 1. The first iteration output of new logistic map is input as the initial value into the traditional logistic map, and the first iteration output of traditional logistic map is input into the new logistic map for the next iteration. Such cycled process can produce the second-level cascaded chaotic sequence.

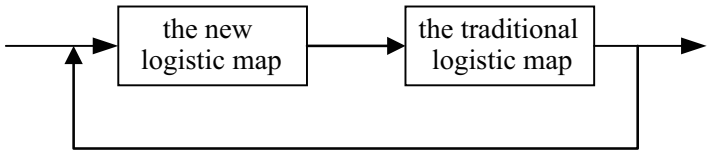

FIGURE 1. Model of the second-level cascaded chaos

Substituting x_n in Eq. (1) to be x_{n+1} in Eq. (2), The equation of the second-level cascaded chaos is given to be,

$$x_{n+1} = \mu x'_n(1 - x'_n) \quad n = 1, 2, 3 \ldots \tag{3}$$

In Eq. (3), the interval of system parameter is $\mu \in (0, 4]$; the initial value is given to be $x'_n = \mu x_n(1-x_n^2) \bmod 1$, where $x_n \in (0, 1]$.

3.2. **The second-level disturbed chaos.** The model of the second-level disturbed chaos is shown in figure 2, the system parameter of new logistic map is disturbed by the iteration output of traditional logistic map, and the iteration output of new logistic map is the second-level disturbed chaotic sequence.

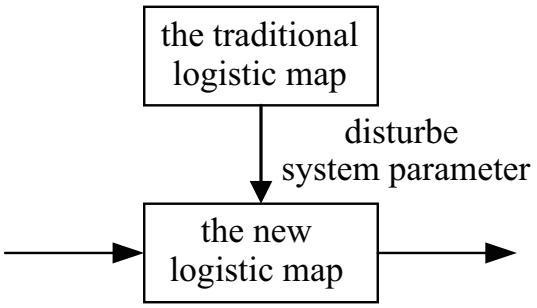

FIGURE 2. Model of the second-level disturbed chaos

Substituting μ in Eq. (2) to be $4x_{n+1}$, and x_{n+1} is in Eq. (1). The equation of the second-level cascaded chaos is given to be,

$$x_{n+1} = \mu' x_n(1-x_n^2) \bmod 1 \quad n = 1, 2, 3 \ldots \tag{4}$$

In Eq. (4), the interval of initial value is $x_n \in (0, 1]$; the system parameter is given to be $\mu' = 4\mu x_n(1 - x_n)$, where $\mu \in (0, 4]$.

4. **The third-level chaos.** In order to improve the complexity and the dynamics characteristics, achieve larger parameter and surjective interval for the discrete chaotic map, in this paper, the third-level chaos was constructed on the basis of the second-level chaos and the improved tent chaos.

4.1. **The third-level cascaded chaos.** The model of the third-level cascaded chaos is shown in figure 3, the new logistic map, the traditional logistic map and the improved tent map were cascaded to construct the third-level cascaded chaos, the equation of improved tent map is given to be [11],

$$x_{n+1} = 1 - abs(1 - \mu x_n) \quad n = 1, 2, 3 \ldots \tag{5}$$

In Eq. (5), the interval of initial value is $x_n \in (0, 1]$; the interval of system parameter is $\mu \in (0, 2]$, When $\mu \in [1, 2]$, the improved tent map should be in chaotic state.

Substituting x_n in Eq. (5) to be x_{n+1} in Eq. (3), The equation of the third-level cascaded chaos is given to be,

$$x_{n+1} = 1 - abs\left[1 - \mu_1\mu_2 x'_n(1 - x'_n)\right] \quad n = 1, 2, 3\ldots \tag{6}$$

In Eq. (6), μ_1 is the system parameter of improved tent map, where $\mu_1 \in (0, 2]$; μ_2 is the system parameter of the second-level cascaded chaos, where $\mu_2 \in (0, 4]$; the initial value is given to be $x'_n = \mu x_n(1-x_n^2)\text{mod}1$, where $x_n \in (0, 1]$.

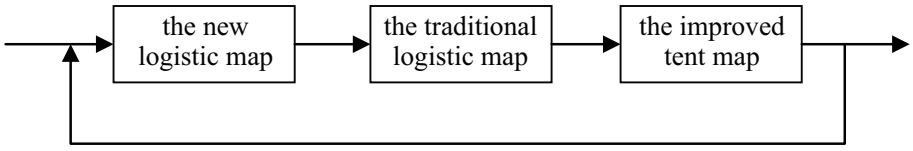

FIGURE 3. Model of the third-level cascaded chaos

4.2. **The third-level disturbed chaos.** The model of the third-level disturbed chaos is shown in figure 4, the system parameter of new logistic map is disturbed by the iteration output of traditional logistic map, and the iteration input of new logistic map is disturbed by the iteration output of improved tent map. Correspondingly, the iteration output of new logistic map is the third-level disturbed chaotic sequence.

Substituting x_n in Eq. (4) to be x_{n+1} in Eq. (5), The equation of the third-level disturbed chaos is given to be,

$$x_{n+1} = \mu' x'_n \left[1 - \left(x'_n\right)^2\right] \text{mod}1 \quad n = 1, 2, 3\ldots \tag{7}$$

In Eq. (7), the system parameter is given to be $\mu' = 4\mu x_n(1 - x_n)$, where $\mu \in (0, 4]$; the initial value is given to be $x'_n = 1 - abs(1 - \mu x_n)$, where $x'_n \in (0, 1]$.

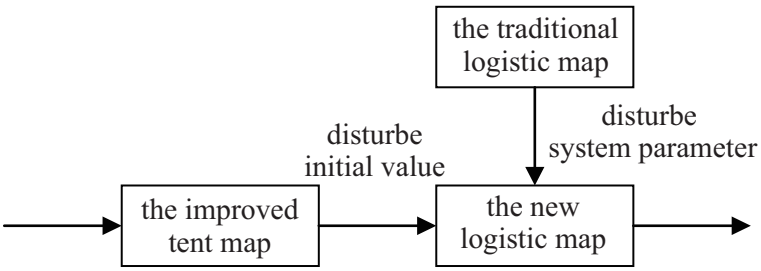

FIGURE 4. Model of the third-level disturbed chaos

5. **Performance analysis.**

5.1. **Performance of the Lyapunov exponent.** Lyapunov exponent may be adopted to quantitatively characterize the overall effect of approximation or separation between the trajectories generated by the nonlinear map. For the nonlinear map, the Lyapunov exponent represents the average exponent divergence rate of trajectories in the direction of each basic vector in n-dimensional phase space. When Lyapunov exponent is negative, the distance between the trajectories disappears exponentially, The motion state of the system corresponds to a periodic motion or fixed-point. When the Lyapunov exponent is positive, the trajectories which are adjacent in the initial state would separate exponentially, The motion of the system corresponds to chaotic state. When Lyapunov exponent is zero, the distance between the trajectories is constant, and the iteration point corresponds to the bifurcation point, i.e., the position where the period is doubled [12].

The Lyapunov exponents of chaos at all levels are shown in figure 5. As can be seen from the simulation, the Lyapunov exponent of traditional logistic chaos is positive only when $\mu > 3.57$, and the negative parameter points of Lyapunov exponent would emerge repeatedly in this range. For the new logistic and multi-level chaoses, the parameter range corresponds to a positive Lyapunov exponent is obviously enlarged. In particular, the Lyapunov exponent is larger and stable for the second-level and third-level disturbed chaoses. It may be seen in comparison that the third-level disturbed chaos is more sophisticated, more difficult to predict, and the trouble that the fixed and periodic points appear in the chaotic parameter range may be overcome effectively.

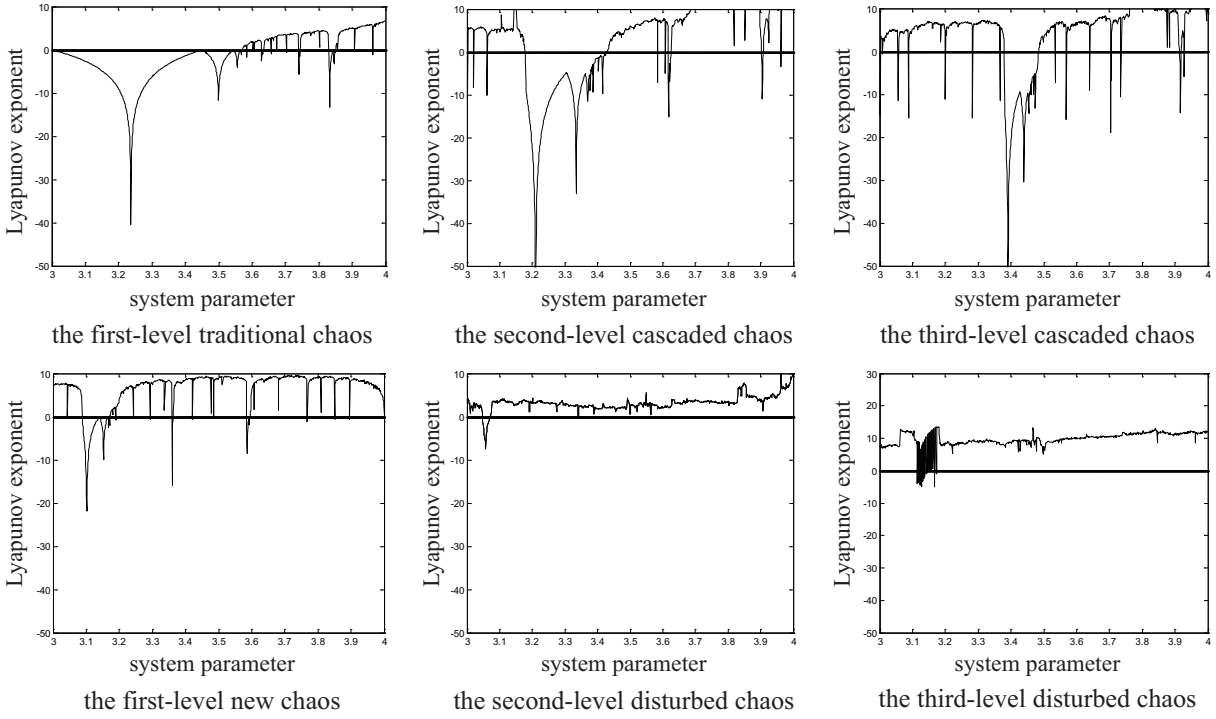

FIGURE 5. Lyapunov exponents of chaos at all levels

5.2. **Sensitivity of the initial value.** The randomness of chaotic sequences lies in the sensitivity of initial value. When two initial values which are very close are inputted into the chaotic map, after being iterated many times, the subsequent trajectories would be separated completely. The property that a tiny difference in initial value would lead to a large difference in output is referred to as initial value sensitivity [13].

The initial value sensitivities of chaos at all levels are shown in figure 6, in which two iteration sequences x1 and x2 are selected from each chaotic map, and the initial values of x1 and x2 are set to 0.600000 and 0.600001. When the iteration times are of the same, a large difference would emerge after being iterated many times, even though there is only a tiny difference between the initial value of x1 and x2. In particular, the second-level and the third-level chaoses are more sensitive to the initial value. As a result a large amount of chaotic sequences would be generated and the sequence space would be effectively enlarged, making the cryptanalysis more complicated.

5.3. **Performance of the bifurcation.** Bifurcation diagram is often used to intuitively reflect the two-dimensional relations between the system parameter and the numerical distribution of chaotic sequences. Based on the bifurcation diagram, the whole process of the chaotic map entering the chaotic state may be intuitively observed [14].

The bifurcation characteristics of chaos at all levels are shown in figure 7. As can be seen from the simulation, the iteration points of traditional logistic chaos would be mapped to the whole interval [0, 1] for a system parameter of $\mu = 4$, known as surjective map. With the increasing of the system parameter, the bifurcations of new logistic and multi-level chaoses become more and more intensive, and the parameter range of surjective map is gradually extended. In particular, the third-level disturbed chaos may completely enter into the chaotic state. As a result, the parameter selectivity of surjective map and the dynamic characteristics of chaotic sequence are simultaneously improved, and the problem of stable window is effectively solved.

5.4. **Performance of the attractor.** A group of trajectories in phase space is often referred to as an attractor, by which the overall system stability can be manifested. The structure and complexity of an attractor determine the dynamic characteristics of chaos, so it is an important way to study chaos [15].

Two-dimensional attractors of chaos at all levels are shown in figure 8. As can be seen from the simulation, the traditional logistic chaos has a helmet-shaped attractor, while the phase space distributions of new logistic and multi-level chaoses are more disorderly scattered, the difference between adjacent iteration values is larger, and the iteration may be effectively avoided tending to the same value. it is apparent that the attractor structure of the third-level disturbed chaos possesses a higher level of complexity, it does not have any regularities, effectively reducing the possibility of sequence being deciphered.

5.5. **Performance of the ergodicity.** Ergodicity indicates the randomness of chaotic sequence in the corresponding value range. The randomness and uniformity of chaotic sequence may be intuitively reflected by the distribution of chaotic sequence in the whole iteration interval [16].

Ergodicities of chaos at all levels are shown in figure 9, the system parameter and the initial value were set to be $\mu = 3.56$ and $x_0 = 0.1$, respectively. As can be seen from

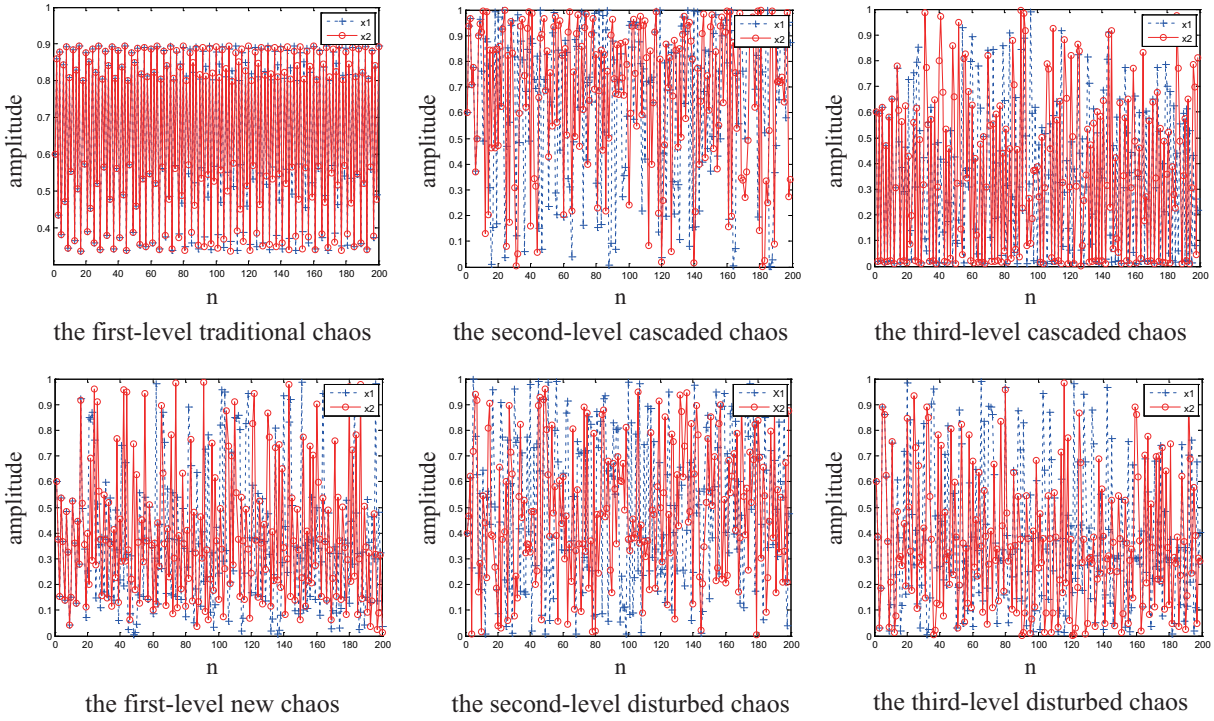

FIGURE 6. Initial value sensitivities of chaos at all levels

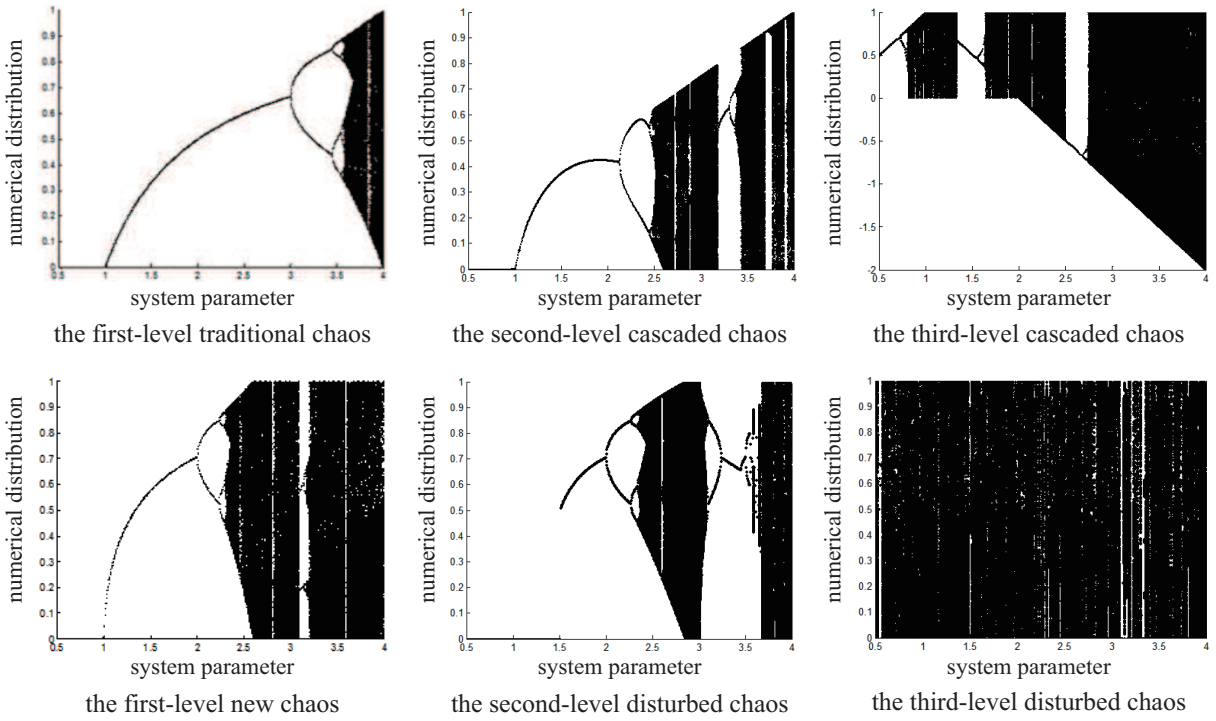

FIGURE 7. The bifurcation characteristics of chaos at all levels

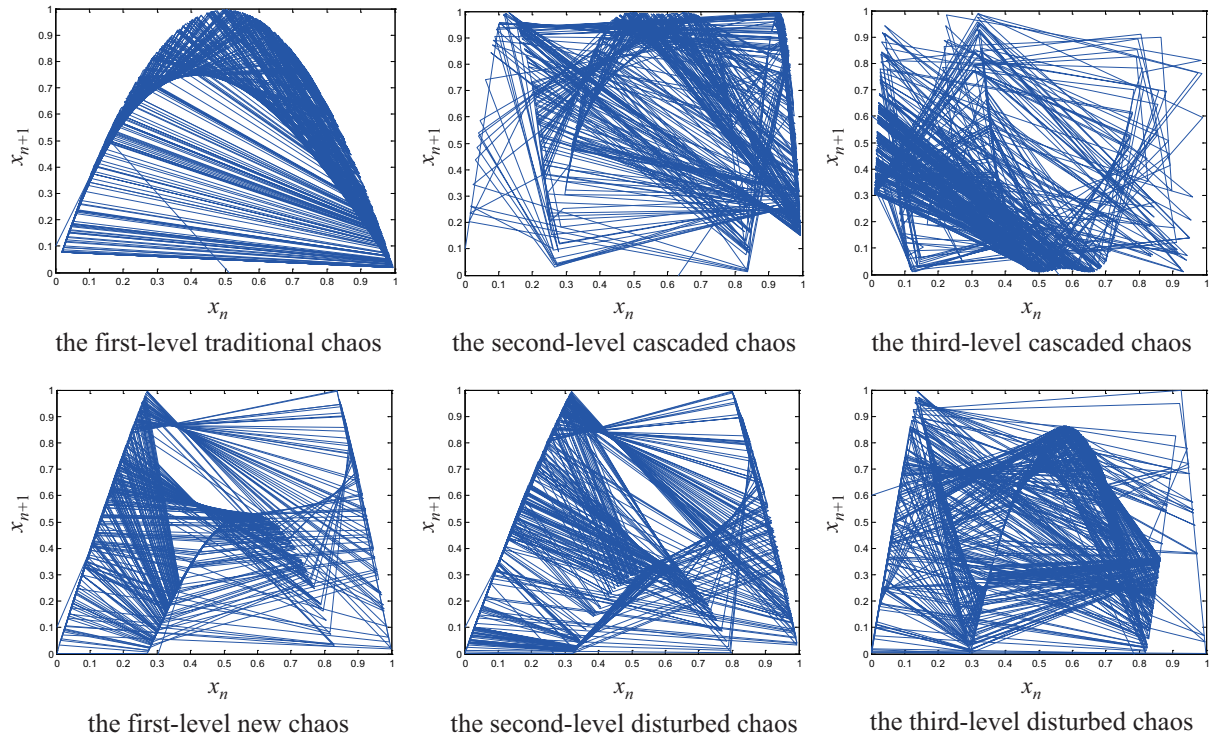

FIGURE 8. Two-dimensional attractors of chaos at all levels

the simulation, the iteration distribution of traditional logistic chaos is not uniform in the interval[0, 1]. When the chaos is improved and its level is increased, the values of x_n would entirely traverse the interval [0, 1] and its distribution would tend to be uniform. In contrast, the ergodicity of the third-level disturbed chaos is more ideal, indicating that it has better statistical randomness.

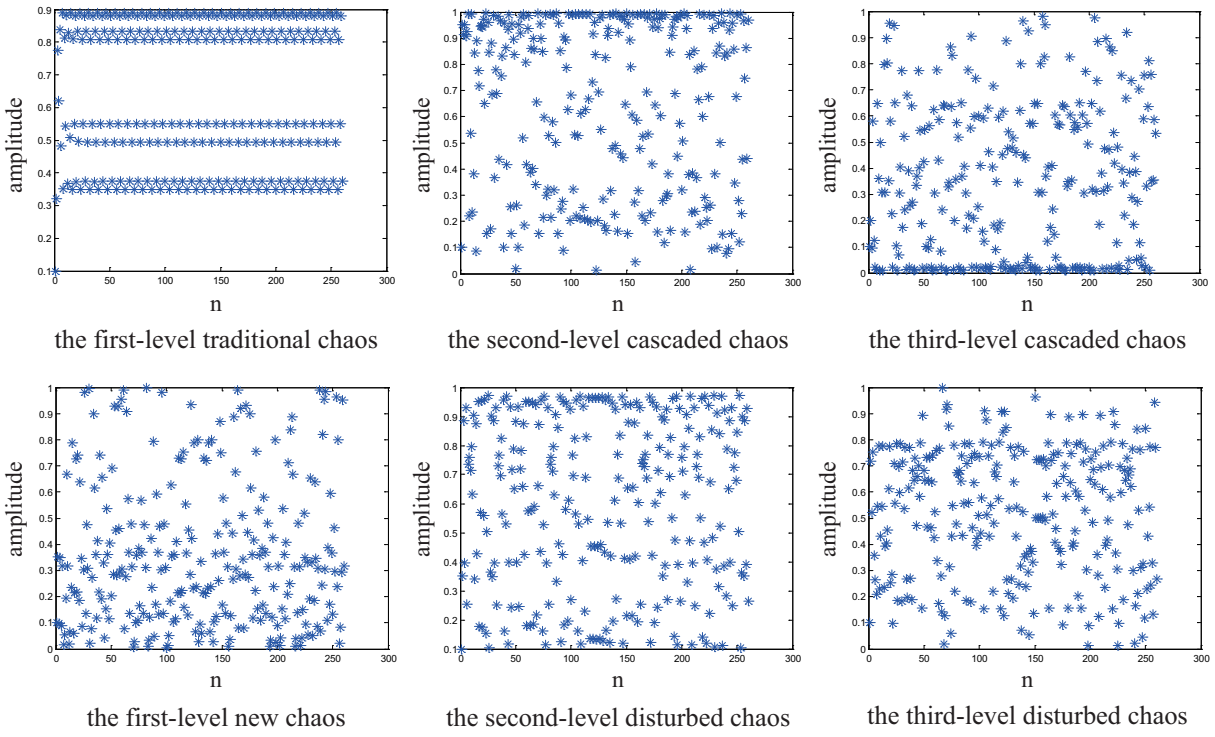

FIGURE 9. The ergodicities of chaos at all levels

5.6. **Performance of the histogram.** Histogram indicates the randomness of chaotic sequence in the corresponding value range. Histograms of chaos at all levels are shown in Figure 10, the system parameter and the initial value were set to be $\mu = 3.98$ and $x_0 = 0.1$, respectively. As can be seen from the simulation, the histogram become uniform when the chaos is improved and its level is increased. Comparatively speaking, the histogram of the third-level disturbed chaos is more ideal. This suggests that the third-level disturbed chaos has excellent statistical randomness to resist the statistical analysis attack.

5.7. **Performance of the correlation.** The relationship between the correlation performance of chaotic sequence and the security of cryptography algorithm or the anti-interference of the spread spectrum communication are compact. The expression of self-correlation function is given to be

$$R_x(m) = \frac{1}{N}\sum_{n=1}^{N} x_n x_{n+m} \tag{8}$$

Self-correlation performances of chaos at all levels are shown in Figure 11, the system parameter and the initial value were set to be $\mu = 3.56$ and $x_0 = 0.1$, respectively. When the chaos is improved and its level is increased, the iteration values are more randomly distributed in a larger scope and the sequence space would be enlarged. Among them, the self-correlation function of the third-level disturbed chaos is close to the ideal impulse function, which indicates the statistical randomness of the third-level disturbed chaos is excellent.

6. **Conclusion.** Based on the comparison and analysis of the dynamic characteristics indicated by the Lyapunov exponent, attractor, etc, we found that the third-level disturbed chaos has a larger surjective interval and higher complexity. In the application of the third-level disturbed chaos, the problems exist in traditional logistic chaos, such

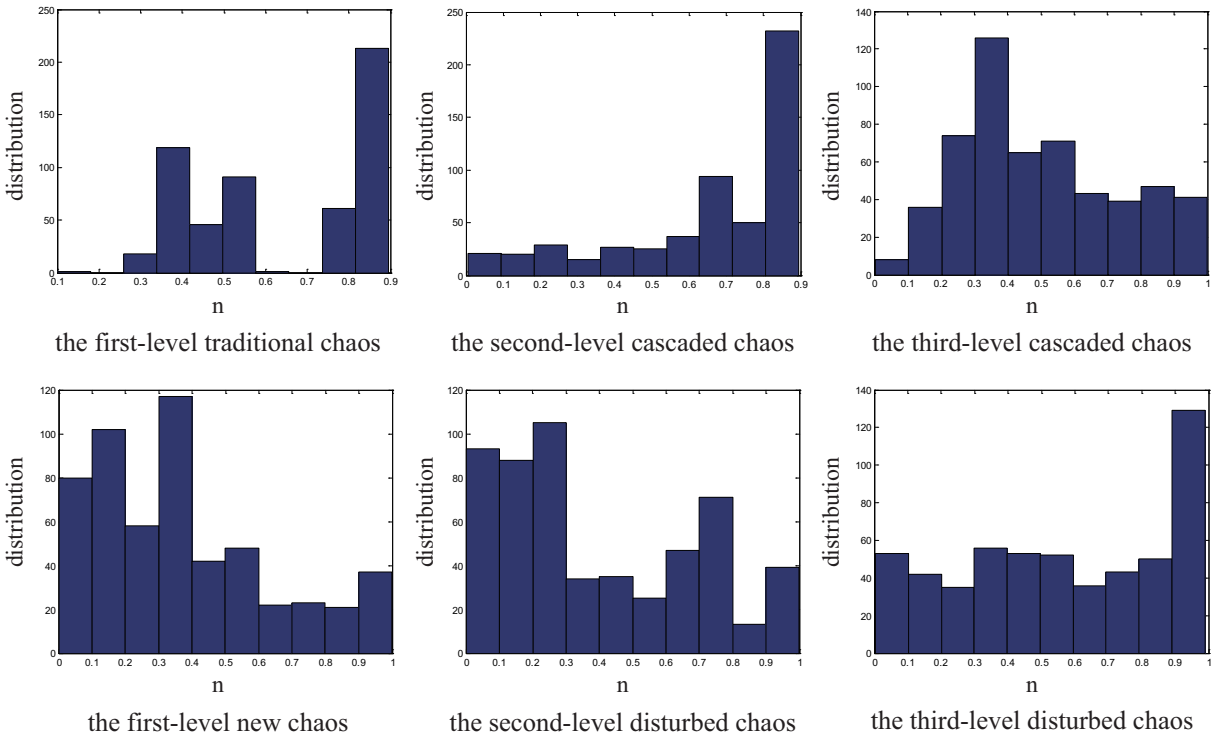

FIGURE 10. The histograms of chaos at all levels

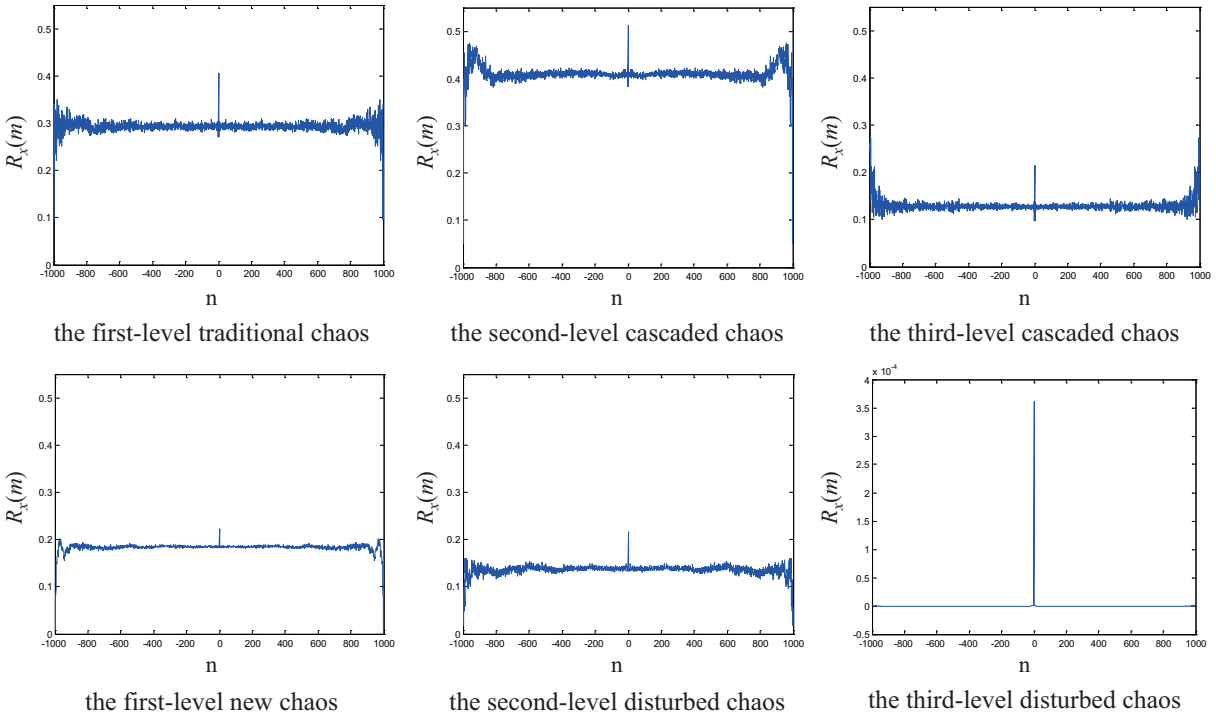

FIGURE 11. Self-correlation performances of chaos at all levels

as narrow stable window, the fixed-point, etc, were effectively solved. On the basis of the comparison and analysis of the statistical randomness indicated by the ergodicity, self-correlation, etc, we found that the third-level disturbed chaos has a better statistical randomness. Therefore, the third-level disturbed chaos proposed in this paper would

be more suitable to be applied in the cryptography algorithm and the spread spectrum communication.

Acknowledgment. This work is supported by the National Natural Science Foundation of China (no. 61471158) and doctor fund item of ministry of education (no. 2013230111 0004).

REFERENCES

[1] H. Wang, J. D. Hu, Improved Logistic-Map Chaotic Spreading Sequences, *Journal of Communication*, vol.8, pp. 71-77, 1997.

[2] P. An, M. Zanin, Image encryption with chaotically coupled chaotic maps, *[J]. Physica D,* vol. 237, pp. 2638-2648, 2008.

[3] B. Yu, L. H. Wang, Y. Q. Jia, Research and Simulation of Multi-User Chaotic Spread Communication System Based On Improved Chaotic Spread Sequences, *[J]. Application Research of Computers*, vol. 4, pp. 1161-1165, 2013.

[4] C. W. Rhodes, Interference to digital broadband communications and spread spectrum communications, *[J]. IEEE Transon Consumer Electronics*, vol. 58, no. 1, pp. 15-22, 2012.

[5] R. M. Yin, J. Yuan, X. M Shan, etc, Weak Keys Randomness Analysis of Chaotic Cryptographic System, *[J]. Science China, Information Sciences*, vol. 41, pp. 777-788, 2011.

[6] X. Y. Yang, G. Wang, X. T. Gu, Performance Analysis and Application Simulation of Logistic Chaotic Sequence, *[J]. Designing Techniques of Posts and Telecommunications*, vol. 46, no. 12, pp. 19-22, 2003.

[7] D. L. Zheng, G. Zhao, G. B Xu, Logistic Mapping Digital-flow Chaotic Strange Attractor and Its Parameter Analysis, *Journal of University of Science and Technology Beijing*, vol. 24, no. 3, pp. 350-352, 2002.

[8] Q. Lu, X. H. Lin, J. Li, etc., An Improved Design of Chaotic FH Sequence, *[J]. Data Acquision & Processing*, vol. 25, no. 1, pp. 122-125, 2009.

[9] W. Zhang, H.M. Xie, B. P. Wang, A New Algorithm of Spread Spectrum Communication Based on Segmented Logistic Chaos Spread, *[J]. Computer Science*, vol. 40, no. 1, pp. 59-62, 2013.

[10] M. l. Zheng, Research of Wireless Sensor Network Block Cipher Based Integer Chaos, *[D]. Master's Degree Theses of South China University of Technology* 2013.

[11] H. J. Wang, B. B. Song, Q. Liu, J. Pan, Q. Ding, FPGA Design and Applicable Analysis of Discrete Chaotic Maps, *International Journal of Bufication and Chaos*, vol. 24, no. 4, pp. 1-15, 2014.

[12] Y. Liu, Analysis of Communication Application Based On Chaos Theory, *[D]. Master's degree thesis of Xi'an Electronic and Science University* 2007

[13] G. Y. Wang, Y. Li, Reseach of Cascade Chaos and Its Dynamic Characteristics, *[J]. Chinese Journa of Physics*, vol. 62, no. 2, pp. 111-120, 2013.

[14] S. X. Li, C. WANG, G. P. LI, X. M. ZHANG, L. Y. YUE. Design and Analysis of New Two-Level Segmented Logistic Chaotic Map, *Journan of Northeast Normal University (Natural Science Edition)*, vol. 12, pp. 82-87, 2013.

[15] H. Xue, H. B. Zhao, Simulation and Analysis of Several Kinds of Chaotic Systems With Strange Attractors, *[J]. Journal of Binzhou College*, vol. 26, no. 6, pp. 66-70, 2010.

[16] B. Chen, G. H. Liu, J. Tang, et al, Research on chaotic sequence autocorrelation by phase space method, *Journal of University of Electronic Science arid Technology of China*, vol. 39, no. 6, pp. 859-863, 2010.