International Journal of Future Generation Communication and Networking
Vol. 9, No. 11 (2016), pp. 327-336
http://dx.doi.org/10.14257/ijfgcn.2016.9.11.30

Design of Integer Chaotic Key Generator for Wireless Sensor Network

[1,2]Juan Wang, [2]Taiheng Yang, [2]Yuhang Li and [1]Qun Ding

[1] Electronic engineering institute Heilongjiang university Harbin, China, 150001.
[2]Electronic and information engineering institute Heilongjiang university of science and technology Harbin, China, 150022
76115347@qq.com, qunding@aliyun.com

Abstract

In the block encryption algorithm of wireless sensor network, the chaotic map is used as a key generator conform to the application requirements of security and efficiency. Due to the one-dimensional discrete chaotic map would appear the degradation of dynamic characteristics after integer quantization, the cascaded and disturbed integer chaotic key generator 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 cascaded and disturbed integer chaotic sequences, and the disturbed integer chaotic sequence whose disturbance position for 1-8 bits was proved to be more excellent, and it can not only meet the encryption requirements of wireless sensor network, but also reduce the computing power and hardware resources overhead of the processor.

Keywords*: Wireless sensor network, Key generator, Integer chaos, Dynamic characteristics, Statistical randomness*

1. Introduction

With the flourishing development of wireless sensor network, the information security has become a key problem that restricts its application in many occasions[1]. If the monitoring information of wireless sensor network is military deployment, security protection, personal privacy, *etc*. the information encryption is an indispensable part of security mechanism of wireless sensor network. On the one hand, wireless sensor network is facing huge security challenges; on the other hand, due to the characteristics of limited node resources, low computing power and less energy, which make the traditional encryption algorithms based on complex operation are inapplicable[2]. Therefore, lightweight symmetric cryptography has gradually become a hot research topic in this field [3].

Block encryption algorithm is one of the most widely used lightweight symmetric cryptography, a key part for its design and application is how to generate the random sequence as key or encryption parameters [4-5]. Due to the characteristics of unpredictability, high nonlinear, pseudo randomness and parameters sensitivity, *etc*. Chaos provides an opportunity to break through the bottleneck of arbitrary length random sequences generation. In particular, the discrete chaotic maps are fast to operate and easy to control, which provide the theoretical basis for the application of block encryption algorithm in wireless sensor network. The efficient and lightweight integer chaotic key generators based on one-dimensional discrete chaotic tent map is proposed in this paper, which provide the necessary guarantee for the design and realization of block encryption algorithm of wireless sensor network.

ISSN: 2233-7857 IJFGCN

2. Integer Quantization

For cost, volume and other considerations, the nodes of wireless sensor network usually use embedded processors, which cannot directly process floating point, division and other complex operations [7]. Due to the amplitude of chaotic map is continuous, the idea of chaotic integer quantization was first proposed in literature, so that it would suitable for the node operations of wireless sensor network [8].

2.1. Quantization Principle

The iterative values of tent map are evenly distributed in surjective map interval, when it is applied to the encryption system has the inherent advantages. The difference iterative equation of tent map is given to be,

$$\begin{cases} x_{n+1} = \mu x_n & 0 \le x_n < 1/2 \\ x_{n+1} = \mu(1-x_n) & 1/2 \le x_n \le 1 \end{cases} \tag{1}$$

As shown in the equation (1), the tent map is a piecewise linear system. study shows that when 1<μ<2, the tent map is in a chaotic state.

Through the further generalization, a new class of linear piecewise tent map proposed in literature [9] is given to be,

$$x_{n+1} = \begin{cases} x_n / \mu & 0 \le x_n < \mu \\ x_n - \mu / 0.5 - \mu & \mu \le x_n < 0.5 \\ 1 - x_n - \mu / 0.5 - \mu & 0.5 \le x_n < 1 - \mu \\ 1 - x_n / \mu & 1 - \mu \le x_n \le 1 \end{cases} \tag{2}$$

According to the method of integer quantization proposed in literature [10], both sides of equation (2) multiplied by a simultaneously, $\mu = 1/4$, $t_n = ax_n$, then the equation of integer tent map is given to be,

$$t_{n+1} = \begin{cases} 4t_n & 0 \le t_n < a/4 \\ 4t_n - a & a/4 \le t_n < a/2 \\ 3a - 4t_n & a/2 \le t_n < 3a/4 \\ 4a - 4t_n & 3a/4 \le t_n \le a \end{cases} \tag{3}$$

In literature [11], the improved tent map is given to be,

$$x_{n+1} = 1 - |1 - \mu x_n| \qquad \mu \in [0,2] \quad x_n \in (0,1] \tag{4}$$

Substituting t_n in equation (3) to be x_n in equation (4), converts t_{n+1} into an integer ,then the equation of integer tent map is given to be,

$$T_{n+1} = \begin{cases} \lfloor 4T_n \rfloor & 0 \le T_n < 1/4a \\ \lfloor 4T_n - a \rfloor & 1/4a \le T_n < 1/2a \\ \lfloor 3a - 4T_n \rfloor & 1/2a \le T_n < 3/4a \\ \lfloor 4a - 4T_n \rfloor & 3/4a \le T_n < a \end{cases} \tag{5}$$

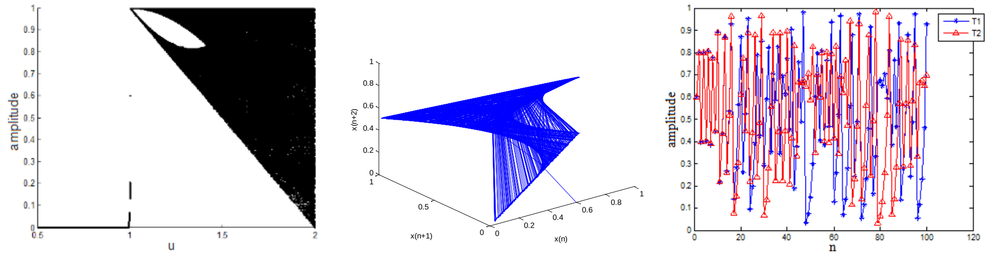
In equation (5), the word length of processor is assumed to be n bits, and $T_{n+1} \in [0, 2^n - 1]$. For example, if the word length of processor is assumed to be 16 bits, that is $a = 2^{15}$, and $T_{n+1} \in$ [0, 65535],which just corresponds to the unsigned integer range of 16 bits binary numbers representation . In this way, the real operation of tent map can be equivalent converted to integer operation. $4T_n$ mean the left shift two bits of T_n, so the integer tent map only need to do addition, subtraction, shift and other simple operations.

As a result, the integer tent map not only suitable for the node operation of wireless sensor network, but also can reduce the computing capability of processor and the resource costs of hardware.

2.2. Performance Analysis

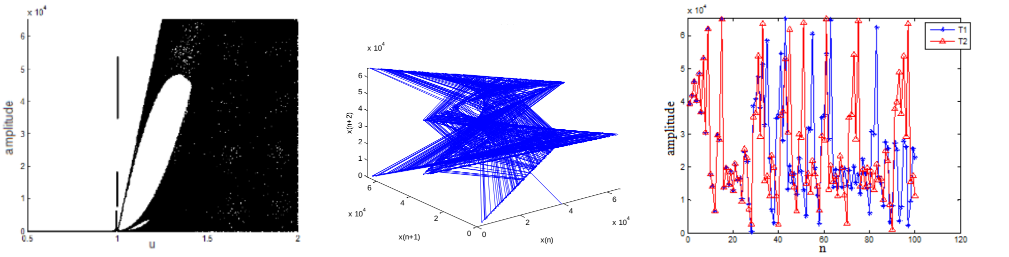
Although after integer quantization the integer tent sequences are more suitable for node operation of wireless sensor network, it is necessary to detect its basic characteristics such as complexity, randomness, periodicity, *etc*. Through the analysis, it can be concluded that whether the integer tent map would appear the degradation of dynamic characteristics, whether it would have an impact on the cryptographic security.

As shown in figure 1-2, on the basis of the comparison and analysis of attractor, bifurcation diagram and initial value sensitivity, we found that the integer tent map can inherit the original folding and stretching properties of tent map, and the nonlinear nature and non reversibility of tent map will still exist in a finite integer set. Although the integer tent map has more complex attractor and larger surjective map interval, its initial value sensitivity decreased significantly, so it is necessary to compensate the chaotic characteristics of the integer tent map.



(a) bifurcation diagram (b) attractor (c) initial value sensitivity

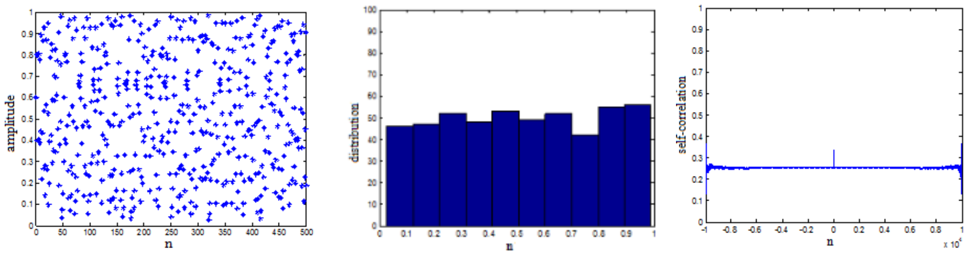
Figure 1. Chaotic Characteristics of Tent Map



(a) bifurcation diagram (b) attractor (c) initial value sensitivity

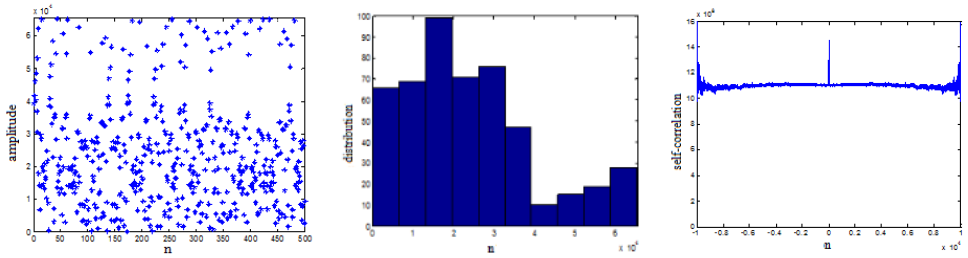
Figure 2. Chaotic Characteristics of Integer Tent Map

As shown in figure 3-4, on the basis of the comparison and analysis of ergodicity, histogram and self-correlation, we found that if the tent map is entered into the chaotic region, the points on the orbit traverse the whole phase space with the same probability, and the orbital period becomes infinite. After integer quantization the uniform distribution characteristics of tent map in the real domain would be destroyed. Due to the short cycle and uneven distribution of the integer tent map, it is easy to decipher through the way of probability statistics, *etc*. Therefore, the performance characteristics of integer tent map are not enough to meet the security requirements of key generator.



(a) ergodicity (b) histogram (c) self-correlation

Figure 3. Statistical Randomness of Tent Map



(a) ergodicity (b) histogram (c) self-correlation

Figure 4. Statistical Randomness of Integer Tent Map

3. The Integer Chaotic Map

In this paper, in order to achieve the ergodicity and increase the complexity, under the same precision the integer tent map would be improved and optimized to obtain the ideal security performance.

3.1. The Cascaded Integer Chaos

The cascaded integer chaotic key generator is shown in Figure 5 the difference iterative equation of logistic map is given to be,

$$x_{n+1} = \mu x_n(1-x_n) \qquad \mu \in (0,4] \quad x_n \in (0,1] \tag{6}$$

In equation (6), when $\mu = 4$, the logistic map is in the surjective state.

The iteration output of logistic map is input as the iteration input into the tent map, that is Substituting x_n in equation (4) to be x_{n+1} in equation (6), then the iteration output of tent map is given to be,

$$x_{n+1} = 1-\left|1-4\mu x_n\left(1-x_n\right)\right| \qquad x_n \in [0,1] \quad \mu \in (0,2] \tag{7}$$

The iteration output of tent map is input as the iteration input into the logistic map, such cycled process can produce the cascaded chaotic sequence, then the integer cascaded chaotic sequences can be obtained by integer quantization. Owing to each iteration result of the cascaded integer chaos is determined by two chaotic maps, which make the iteration mode is more complex.

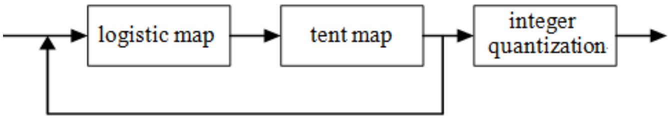


Figure 5. The Cascaded Integer Chaotic Key Generator

3.2. The Disturbed Integer Chaos

If the chaotic state variables are disturbed at the fixed interval which is less than the period length of chaotic sequence, the chaotic state can be effectively changed to avoid the periodicity. Disturbance strategy is mainly divided into the disturbance to input sequence, the disturbance to output sequence, and the disturbance to input and output sequence simultaneously [13]. In this paper, the output sequence of integer tent map would be disturbed by the logistic chaotic sequence.

The disturbed integer chaotic key generator is shown in Figure 6.If the wireless sensor network node is a 16-bits processor, the integer tent sequence T(n) would be expressed as a 16-bits binary number. Due to the iteration output of logistic map is in the interval [0,1], the iteration output of logistic map is amplified by 10 times and divided by 256,the mod of which L(n) is 8-bits pseudo-random sequence as a disturbance sequence. Meanwhile, the integer tent sequence T(n) is also divided by 256 and the mod of which M(n) is 8 bits pseudo-random sequence. The L(n) is used to disturb the M(n) in the form of XOR operation, then being OR operation with 10000000 to generate sequence P(n). Finally, using P(n) to replace the 8-bits binary number of integer tent sequence T(n), so as to complete the output disturbance of the integer tent map.

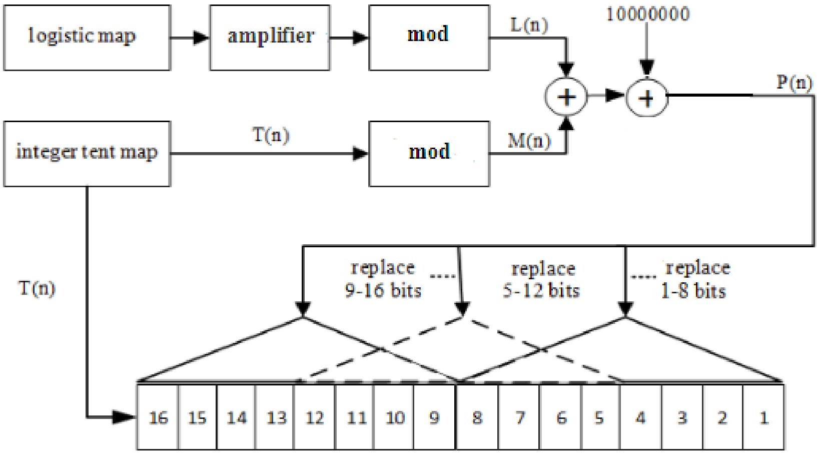
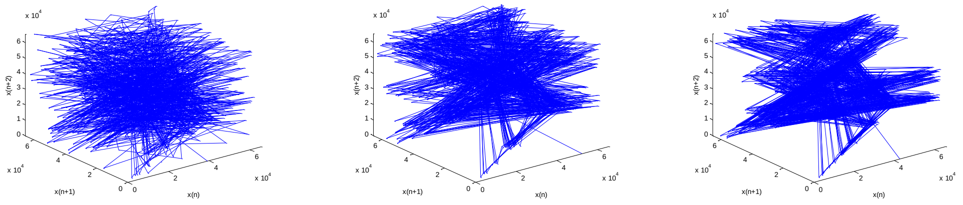


Figure 6. The Disturbed Integer Chaotic Key Generator

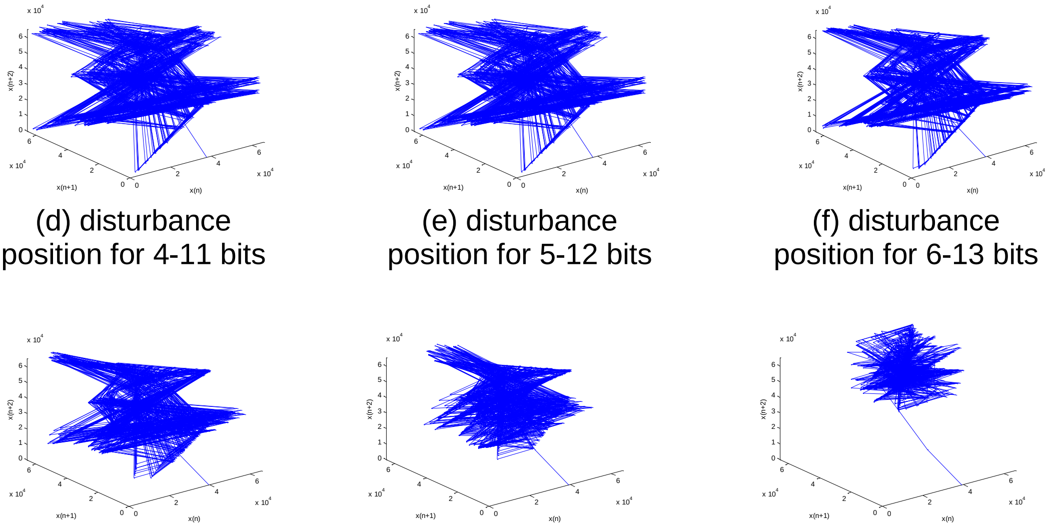
The influence of different disturbance position on the key performance is shown in Figure 7-8. Through the simulation analysis it can be seen that the position of the disturbance sequence has great impact on the chaotic and random characteristics of the integer tent map, and better performance would be obtained if the position of the disturbance sequence P(n) moves forward. The best disturbance effect can be achieved when the position of the disturbance sequence P(n) is exactly corresponds to the 1-8bits of integer tent sequence T(n).



(a) disturbance position for 1-8 bits

(b) disturbance position for 2-9 bits

(c) disturbance position for 3-10 bits



(d) disturbance position for 4-11 bits

(e) disturbance position for 5-12 bits

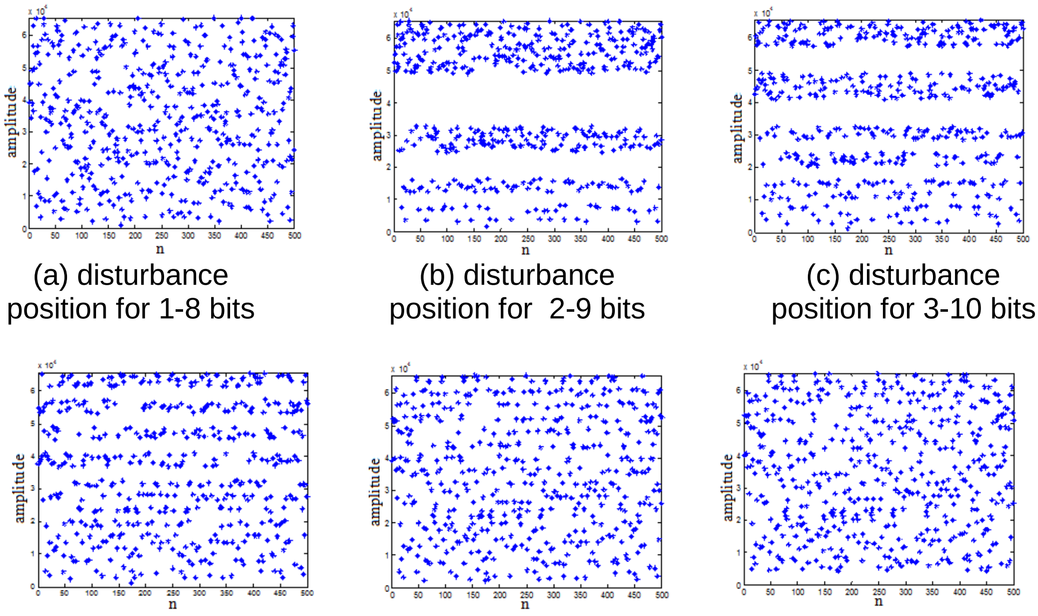
(f) disturbance position for 6-13 bits

(g) disturbance position for 7-14 bits

(h) disturbance position for 8-15 bits

(i) disturbance position for 9-16 bits

Figure 7. Chaotic Characteristics of Different Disturbance Position on Integer Tent Map



(a) disturbance position for 1-8 bits

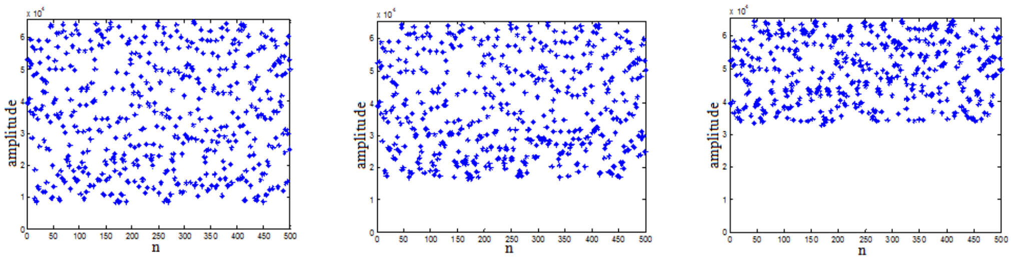
(b) disturbance position for 2-9 bits

(c) disturbance position for 3-10 bits

(d) disturbance position for 4-11 bits

(e) disturbance position for 5-12 bits

(f) disturbance position for 6-13 bits



(g) disturbance position for 7-14 bits

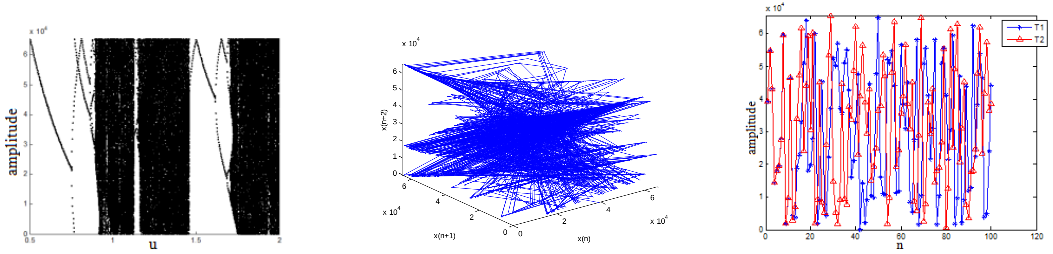
(h) disturbance position for 8-15 bits

(i) disturbance position for 9-16 bits

Figure 8. Random Characteristics of Different Disturbance Position on Integer Tent Map

3.3. Performance Analysis

As shown in Figure 9-10, the cascaded and disturbed integer chaos not only extend the surjective map interval, but also have more complex dynamic characteristics, more dispersed and disorderly phase space distribution, which can effectively solve the problem of stable window. The greater difference between adjacent iterative values would avoid iterations tend to be same value, it can effectively reduce the possibility of decipher sequence through the way of phase space inversion, *etc*. Even if the same chaotic system has a tiny initial value difference, it will produce a completely different state after several rounds of iterations, which shows that it has extremely strong initial value sensitivity.

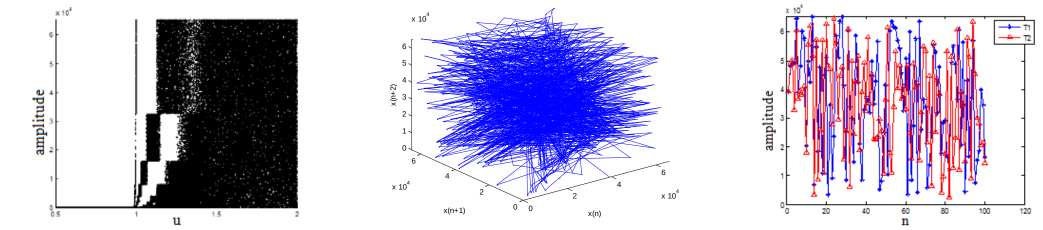


(a) bifurcation diagram

(b) attractor

(c) initial value sensitivity

Figure 9. Chaotic Characteristics of Cascaded Integer Chaos



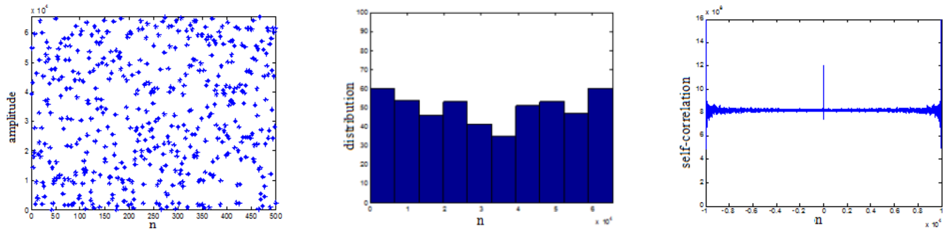
(a) bifurcation diagram

(b) attractor

(c) initial value sensitivity

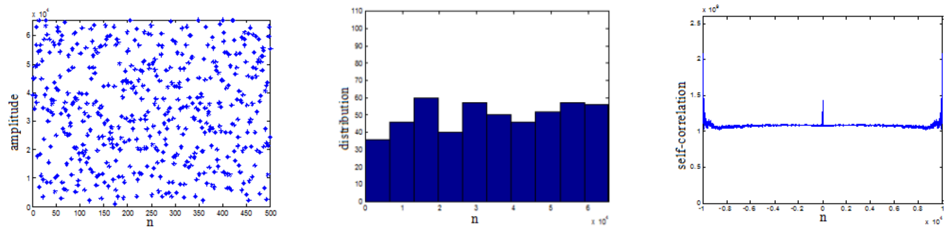
Figure 10. Chaotic Characteristics of Disturbed Integer Chaos

As shown in Figure 11-12, With respect to the integer tent map, both distribution uniformity and self-correlation of cascaded and disturbed integer tent map have been greatly improved, and the period of chaotic sequence have been effectively extended too. Therefore, the cascaded and disturbed integer chaotic key generators can meet the requirements for random, and it is difficult to be deciphered by attackers.



(a) ergodicity (b) histogram (c) self-correlation

Figure 11. Statistical Randomness of Cascaded Integr Chaos



(a) ergodicity (b) histogram (c) self-correlation

Figure 12. Statistical Randomness of Disturbed Integer Chaos

Through the comparison we can find that the cascaded and disturbed integer chaos not only inherit the str*etc*hing and folding characteristics of tent map, but also overcome the problems of uneven distribution and short period , and the dynamic characteristics has also been significantly enhanced. In contrast, the disturbed integer chaos has bigger surjective interval, more complicated attractor structure. Furthermore, cascade different chaotic map will bring more complex calculations. Therefore, the disturbed integer chaos is more suitable for application in wireless sensor network block encryption algorithm.

4. Conclusion

In this paper, according to the characteristics of the wireless sensor network, based on the relevant theory of chaos and block encryption, aimed at dynamic degradation and short period of the integer chaotic map, the integer chaotic key sequence generators were constructed in view of the ideas of cascade and disturbance. Through comparing and analyzing the performances of two key generators, it can be concluded that the disturbed integer chaos has larger key space and higher complexity, and the generated key sequences have excellent characteristics of uniform distribution and pseudo-randomness. Moreover, it only needs to carry out addition and shift operation when implemented in computer, which can reduce hardware resources and improve operational speed. Therefore, the integer chaotic key sequence generators can not only guarantee the operation of wireless sensor network node, also can further strengthen the safety and efficiency of the encryption algorithm, very suitable for the application of encryption algorithm in wireless sensor networks.

Acknowledgment

This work is supported by the National Natural Science Foundation of China (no.61471158) and doctor fund item of ministry of education (no.20132301110004).

References

[1] Z. Lai, M. Wang and J. Yin, "Survey on Security of Wireless Sensor Networks", Electronic Measurement Techniques, vol. 33, no. 12, **(2010)**, pp. 72-78.

[2] C. Wang, G. Hu and H. Zhang, "Lightweight Security Architecture for Wireless Sensor Networks", Journal of Communication, no. 02, **(2012)**, pp. 30-35.

[3] W. J. Huo and Z. L. Liu, "Secure Encryption Embedded Processor Design for Wireless Sensor Network Application", vol. 17, no. 1, **(2011)**, pp. 75-79.

[4] Y. Tan, "A Chaotic Block Cipher Used in WSN", University of Electronic Science and Technology, **(2010)**.

[5] K. Zuo, "Research on Text Block Encryption Based on Chaos in Wireless Sensor Networks", Harbin Institute of Technology, **(2011)**.

[6] K. Yang, "Research on the Application of Chaotic Block Cipher in Wireless Sensor Networks", Beijing University of Chemical Technology, **(2012)**.

[7] S. Chen, "Research on Chaos Encryption Theory and Key Technology of Wireless Sensor Networks", ChongQing University, **(2006)**.

[8] X. Tong, K. Zuo and Z. Wang, "A New Block Encryption Algorithm Based on Mixed Chaos for Wireless Sensor Network", Journal of Physics, no. 03, **(2012)**, 030502-1-11.

[9] S. Chen and R. Shu, "Block Permutation Cipher in Chaos with Feistel Structure for Wireless Sensor Networks", Advances in Intelligent and Soft Computing, vol. 105, **(2011)**, pp. 391-296.

[10] L. Yuan, "Application Research of Communication Based on Chaos Theory", Xian University of Electronic Science and Technology, **(2007)**.

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