Improved Chaotic Sequence Generation Method Based on Direct Spread Spectrum

Fang Liu, Shiyao Jia, Xiaodan Xu, Minghao Tian
School of Information Science and Engineering, Shenyang Ligong University, Shenyang 110159, China
zhqing1019@163.com

Abstract. Aimed at the shortcomings of one-dimensional chaotic sequences as spread spectrum address codes in DS/SS(Direct Sequence Spread Spectrum) communication system, such as low complexity, simplicity of generation and easy to be estimated backwards, etc, an improved chaotic sequence is proposed, which is composed of two one-dimensional chaotic maps and the fractal parameter of one map is controlled to control the fractal parameter of another map in a certain mathematical form. Then the performance analyses of the sequence are carried out from the angles of complexity, correlation, randomness and anti-interference ability. The results of simulation show that the improved chaotic sequence not only improves the complexity obviously, but also has good correlation and randomness, and the anti-interference ability in DS/SS communication is more prominent.

1. Introduction
With the maturity of the research on chaos theory, the application of chaos has gradually infiltrated into various fields, including the application in direct sequence spread spectrum communication. Chaotic mapping is sensitive to initial values and controlled by system parameters, so a large number of signals with good correlation, high complexity can be produced and regenerated easily. The randomness of chaos manifests itself in the irregularity of the chaotic map itself. This unity of certainty and uncertainty is precisely the characteristic that traditional random motion does not possess. This inherent nature of chaotic non-linear system is not affected by the outside world, which makes chaotic non-linear system possess many unique and excellent characteristics. Therefore, more and more researchers put their eyes on chaotic pseudo-random spread spectrum sequence above[1].

With the in-depth study of chaotic pseudo-random spread spectrum sequences, it is found that the traditional one-dimensional chaotic sequences have some limitations after truncation. The excellent performances of them are weakened to a certain extent, such as low complexity, poor randomness, too simple to be produced. Besides, their parameters are easy to be cracked. At present, there are many methods of estimating fractal parameters[2]. Therefore, how to improve the performance of chaotic pseudo-random sequences has become the focus of this research field in recent years[3]. In the view of this, an improved chaotic sequence based on parameter control is proposed, and its complexity, correlation, randomness and anti-interference ability in DS/SS communication are analyzed. The simulation results show that the performance of the improved chaotic sequence is improved in these aspects.

2. Typical One-Dimensional Chaotic Maps
At present, the typical one-dimensional chaotic maps with good statistical performance are mainly
composed of the following kinds, their expressions and the range of initial values and fractal parameters are as follows:

1) The expression of the a-order Chebyshev map is:

\[
    x_{n+1} = \cos(a \cos^{-1} x_n) \quad -1 \leq x_n \leq 1
\]  

(1)

The range of initial value \(x_n\) is \([-1,1]\), \(x_{n+1}\) is the iterative result. When the fractal parameter \(a \geq 2\), the chaotic map is in chaotic state, and when \(a \geq 4\), the chaotic map reaches full mapping state[4].

2) The expression of the Kent map is:

\[
\begin{align*}
    x_{n+1} &= (1 - x_n)/(1 - a) , \quad a < x_n < 1 \\
    x_{n+1} &= x_n/a , \quad 0 < x_n \leq a
\end{align*}
\]  

(2)

The range of initial value \(x_n\) is \((0,1)\), \(x_{n+1}\) is the iterative result. When the fractal parameter \(a\) is in the interval \((0,1)\), the chaotic map is in chaotic state, according to literature[4], when \(a = 0.4997\), the chaotic state is the best[5].

3) The expression of the Piecewise logistic map is:

\[
\begin{align*}
    x_{n+1} &= 1 - 4a(x_n + 1/2)^2 , \quad -1 \leq x_n \leq 0 \\
    x_{n+1} &= 4a(x_n - 1/2)^2 - 1 , \quad 0 \leq x_n \leq 1
\end{align*}
\]  

(3)

The range of initial value \(x_n\) is \([-1,1]\), \(x_{n+1}\) is the iterative result. When the fractal parameter \(a\) is in the interval \((0,2)\), the chaotic map is in chaotic state, experiments show that when \(a \in (1.8,2)\), the chaotic map reaches full mapping state[6].

3. An Improved Method for Generating Chaotic Sequence

Based on the shortcomings of typical one-dimensional chaotic maps as pseudo-random sequences of spread spectrum, such as simplicity, low complexity and poor randomness, etc, an improved chaotic sequence is proposed. Its generating principle is that the change trajectory of fractal parameter is controlled by mathematical representation. Using Kent map as controlling map and Chebyshev map as controlled map, the fractal parameter of Chebyshev map is controlled by the iteration output value of Kent map through mathematical transformation, so that the fractal parameter of Chebyshev map contain the changes of Kent map. Then, the result is fed back by the optimization strategy, and the improved chaotic sequence which meets the optimization condition is obtained.

The principle block diagram is shown in Fig.1.

![Fig.1 Block diagram of improved chaotic sequence](image)

Its mathematical expression is as follows:

The input and output of expression (2) of the Kent map are expressed by \(y_n\) and \(y_{n+1}\) and its fractal parameter is set to 0.4997. The expression is as follows:

\[
\begin{align*}
    y_{n+1} &= (1 - y_n)/(0.5003) , \quad 0.4997 < y_n < 1 \\
    y_{n+1} &= y_n/0.4997 , \quad 0 < y_n \leq 0.4997
\end{align*}
\]  

(4)
\( y_{n+1} \) is mathematically transformed into the fractal parameter of Chebyshev map, and the expression is as follows:

\[
a = 4 + 4y_{n+1}
\]  

From the range of \( y_{n+1} \), the range of fractal parameter of Chebyshev map is (4,8). In this range, the chaotic system reaches the full mapping state.

The expression of improved chaotic map is obtained by substituting fractal parameter into Chebyshev map:

\[
x_{n+1} = \cos [4 + 4y_{n+1}) \cdot \cos^{-1} x_n] - 1 \leq x_n \leq 1
\]  

The specific process of implementation is as follows:

1. Giving the fractal parameter of Kent map and the initial value of Chebyshev map, the initial value of Kent system is set as a variable to generate a sequence \( f \) with a length of 255.
2. The fractal parameter of Chebyshev map is \( a = 4 + 4f \), which controls the change of Chebyshev map and binarizes the sequence.
3. Then, the optimal selection strategy is used to determine the balance of sequence, the size of autocorrelation sidelobe and the maximum peak value of cross correlation. The limit of determination is set by referring to the corresponding results of the traditional gold code under the length of 255 sequence. The limit value of balance is set to 0.01; the maximum value of autocorrelation sidelobe is less than 0.15; and the limit value of the maximum value of cross correlation is set to 0.2. Then it can get the improved chaotic sequence. Its initial value is 0.52 and the fractal parameter is 0.4997.

4. Performance Analysis of Improved Chaotic Sequence

As Pseudo-Random Spread Spectrum sequence in DS/SS communication system, it must have good performances. These performances are mainly reflected in complexity, correlation, randomness and anti-interference ability\[7-8\]. Therefore, based on the theoretical analysis, the complexity, correlation, randomness and anti-interference ability of the sequence are tested by using MATLAB language based on the simulation software of MATLAB 2015a.

4.1. Analysis of complexity

The complexity of sequence will affect the randomness and uncertainty of the sequence. The higher the complexity, the better the randomness and uncertainty are. The complexity of sequence can be measured by ApEn (approximate entropy) \[9-10\]. The effects of different length of sequence on the complexity and the complexity of different chaotic sequences are shown in Table 1.

| Length of sequence | Chebyshev | Kent | Piecewise logistic | Improved chaotic sequence |
|--------------------|-----------|------|-------------------|---------------------------|
| 1000               | 1.2276    | 0.6452 | 1.1284            | 1.6028                    |
| 2000               | 1.2839    | 0.6499 | 1.2073            | 1.6819                    |
| 3000               | 1.2970    | 0.6726 | 1.2285            | 1.6976                    |

As can be seen from Table 1, the complexity of chaotic sequence increases obviously with the increase of length of chaotic sequence, and the improved chaotic sequence has the largest ApEn value under the same sequence length, that is, its complexity is the highest. The improved chaotic sequence shows better uncertainty.

4.2. Analysis of correlation

As a pseudo-random sequence, chaotic sequence must have good correlation performance. The autocorrelation value should be approximated to the delta function to facilitate the detection and synchronization of spread spectrum code, while the cross-correlation value should be close to 0, so as to effectively suppress the interference between different spread spectrum codes. This is very
important for multiple address application in communication[11].

If the length of the improved chaotic sequence \( S \) is \( N \), then the autocorrelation function is[12]:

\[
R(n) = \sum_{k=0}^{N-1} S(k) \times S(k+n)
\]

(7)

In the formula, \( k \) is the sequence point, \( n \) is the offset point, and \( R(n) \) is the autocorrelation peak.

The maximum of autocorrelation peak value is[12]:

\[
R_{\text{max}} = \max\{R(n)\} \quad n = 0,1, \cdots N - 1
\]

(8)

In the formula, \( n \) is the offset point and \( R_{\text{max}} \) is the maximum of autocorrelation peak.

The maximum of autocorrelation secondary peak value is[12]:

\[
R_{\text{max,1}} = \max\{R(n)\} \quad n = 1, \cdots N - 1
\]

(9)

In the formula, \( n \) is the offset point, \( R(n) \) is the phase peak and \( R_{\text{max,1}} \) is the maximum of autocorrelation secondary peak.

If the length of chaotic sequence \( S_1 \) and \( S_2 \) is \( N \), then the cross-correlation function is[12]:

\[
C(n) = \sum_{k=0}^{N-1} S_1(k) \times S_2(k+n)
\]

(10)

In the formula, \( k \) is the sequence point, \( n \) is the offset point, and \( C(n) \) is the cross-correlation peak.

The maximum of cross-correlation peak value is[12]:

\[
C_{\text{max}} = \max\{C(n)\} \quad n = 0,1, \cdots N - 1
\]

(11)

In the formula, \( n \) is the offset point, \( C(n) \) is the correlation peak, and \( C_{\text{max}} \) is the maximum of the correlation peak.

Fig.2 and Fig.3 are the autocorrelation and cross-correlation diagrams of the improved chaotic sequence when the sequence length is 5400, respectively.

From the overall trend of Fig.2, it can be seen that the improved chaotic sequence has the similar property of delta-like, its autocorrelation function has sharp autocorrelation maximum peak value, and the autocorrelation secondary peak value is almost zero. So, the improved chaotic sequence shows good autocorrelation.

From Fig.3, it can be seen that the improved chaotic sequence has no obvious cross-correlation peak value and the cross-correlation function values are close to zero. So the cross-correlation performance of the improved chaotic sequence is good[12].
4.3. Analysis of random

In addition to the performance test described above, as a pseudo-random sequence, it is also necessary to test its own randomness. In DS/SS system, the randomness of spread spectrum sequence will affect the security of the system. The better the randomness, the more difficult it will be to be cracked by non-communicators, and the more secure the information of the system will be. Therefore, it is necessary to analyze the randomness of the improved chaotic sequence[13].

At present, there are many tools of testing random, such as NIST(National Institute of Standards and Technology) test, semi-numerical algorithm and so on. The most commonly used tool is NIST test. The tool has 16 statistical tests. The p-value of each test is used as the statistical results of the sequence. When the p-value is greater than 0.01, it is random. In terms of sequence generated by the deterministic system and algorithm, the most important tests are include frequency test, block frequency test, runs test, FFT(Fast Fourier Transformation)test and approximate entropy test[14]. According to the requirement of NIST test, in order to ensuring the reliability and accuracy of test results, the length of each measured sequence should be $10^3$ ~ $10^7$. Therefore, the length of each sequence is $10^6$[15].

Table 2 shows the results of randomness test of chaotic sequences.

| Sequence          | Frequency test | Block frequency test | Runs test | FFT test | Approximate entropy test |
|-------------------|----------------|----------------------|-----------|----------|--------------------------|
| Chebyshev         | 0.0179         | 0.3504               | 0.3504    | 0.3504   | 0.1223                   |
| Kent              | 0.5341         | 0.5341               | 0.3504    | 0.1223   | 0                        |
| Piecewise logistic| 0.3504         | 0                    | 0.1223    | 0.5341   | 0.3504                   |
| Improved chaotic sequence | 0.5341 | 0.9914               | 0.1223    | 0.0668   | 0.2133                   |

From Table 2, it can be seen that some test items of piecewise logistic map and Kent map are failed, but the improved chaotic sequence not only passes these tests completely, but also its each value of test is very high. So the randomness of the improved chaotic sequence is very good.

4.4. Analysis of anti-interference abilitys

In DS/SS communication, anti-interference ability is an important reflection of system performance. The common interference signals are include broadband interference and FM(Frequency Modulation) comb interference[16-17]. The improved chaotic sequence as a spread spectrum sequence in DS/SS communication system is necessary to have good anti- interference ability. Therefore, the improved chaotic sequence’s anti-broadband interference and anti-FM comb interference ability should be tested separately, and compared with anti-interference ability of gold sequence at the same condition. The length of sequence is set to 5400, and the ISR(Interference/Signal Ratio) is set to 15-40dB.

Fig.4 shows the anti-broadband interference comparison diagram between improved chaotic sequence and gold sequence under the same ISR condition.
It can be seen from Fig.4 that under the same ISR condition, the overall trend is that with the increasing of ISR, the capture peak ratio decreases gradually. In addition, it can be clearly seen that under the same ISR, the capture peak ratio of the improved chaotic sequence is higher than that of the gold sequence, which shows that the anti-broadband interference ability of the improved chaotic sequence is better than that of the gold sequence.

Fig.5 shows the anti-FM comb interference comparison diagram between improved chaotic sequence and gold sequence under the same ISR condition.

It can be seen from Fig.4 that under the same ISR condition, the overall trend is that with the increasing of ISR, the capture peak ratio decreases gradually, and the capture peak ratio of the improved chaotic sequence is significantly higher than that of the gold sequence, which shows that the anti-FM comb interference ability of the improved chaotic sequence is better than that of the gold sequence.

5. Conclusion
Aimed at the shortcomings of low complexity, poor randomness and easy estimation of typical one-dimensional chaotic pseudo-random sequences in DS/SS communication system, this paper proposes an improved chaotic sequence based on parameter control. Compared with one-dimensional chaotic sequences, the improved chaotic sequence not only improves the complexity and randomness of the sequence, but also retains the good correlation performance of the sequence. In the anti-interference test, its anti-interference ability is also very outstanding compared with the traditional
gold sequence. It shows good spread spectrum performance.

Acknowledgments
This work is supported by National Natural Science Foundation of China (No.61501309), the National Defense Basic Scientific Research Planed Project (2018).

References
[1] Jovic B, et al, "A robust sequence synchronization unit for multi-user DS-CDMA chaos-based communication systems," Signal Processing, vol. 87(7), 2007, pp. 1692-1708.
[2] F. Benedetto, G.Giunta, and S. Bucci, "A Unified Approach for Time-Delay Estimators in Spread Spectrum Communications," IEEE Transactions on Communications, vol. 59(12), 2011, pp. 3421-3429.
[3] Talebi, Siamak, and N. Rahnama, "Performance comparison of chaotic spreading sequences generated by two different classes of chaotic systems in a chaos-based direct sequence-code division multiple access system," IET Communications, vol.7(10), 2013, pp. 1024-1031.
[4] Rahnama, Nazila, and S. Talebi, "Performance comparison of chaotic spreading sequences generated by 1D and 3D chaotic systems in a chaos-based DS-CDMA system," International Symposium on Telecommunications IEEE, 2013.
[5] Yang Dixiong, Z. Liu, and J. Zhou, "Chaos optimization algorithms based on chaotic maps with different probability distribution and search speed for global optimization," Communications in Nonlinear Science & Numerical Simulation, vol. 19(4), 2014, pp. 1229-1246.
[6] Tavazoei, Mohammad Saleh, and M. Haeri, "Comparison of different one-dimensional maps as chaotic search pattern in chaos optimization algorithms," Applied Mathematics & Computation, vol.187(2), 2007, pp. 1076-1085.
[7] Yin Y, Zhou F, Qiao G, et al, "Burst Mode Hybrid Spread Spectrum Technology for Covert Acoustic Communication," Oceans. IEEE, vol. 155(2), 2014, pp. 1-8.
[8] Kodovsky J, Fridrich J, Holub V, "Ensemble Classifiers for Steganalysis of Digital Media," IEEE Transaction on Information Forensics and Security, vol. 7(2), 2012, pp. 432-444.
[9] Wang Ling, Y. Xu, and L. Li, "Parameter identification of chaotic systems by hybrid Nelder–Mead simplex search and differential evolution algorithm," Expert Systems with Applications, vol. 38(4), 2011, pp. 3238-3245.
[10] Gu Junrong, et al, "Analysis of an Interleaved Chaotic Spread Spectrum Sequence," International Conference on Wireless Communications IEEE, 2008.
[11] Shi P, Qi D, Li M, et al, "Robustness of Fractional Order for FRFT-OFDM systems," IEEE International Conference on Communication Software and Networks. IEEE, vol. 91(9), 2015, pp. 241-244.
[12] Drakakis K, Gow R, Rickard S, et al,"On the Maximal Cross-Correlation of Algebraically Constructed Costas Arrays," IEEE Transactions on Information Theory, vol. 57(7), 2011, pp. 4612-4621.
[13] Zhang Kexue, X. Liu, and W. C. Xie,"Impulsive Control and Synchronization of Spatiotemporal Chaos in the Gray–Scott Model," Interdisciplinary Topics in Applied Mathematics, Modeling and Computational Science. Springer International Publishing, 2015.
[14] Rukhin, Andrew L., et al, "SP 800-22 Rev. 1a. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications," Applied Physics Letters vol. 22(7), 2010, pp.1645-179.
[15] Khan, M. K., and J. Zhang," [IEEE 2006 IEEE International Conference on Engineering of Intelligent Systems - Islamabad, Pakistan (22-23 April 2006)] 2006 IEEE International Conference on Engineering of Intelligent Systems - Investigation on Pseudorandom Properties of Chaotic Stream Ciphers," 2006, pp. 1-5.
[16] Rhodes, Charles W.,"Interference to digital broadband communications and spread spectrum communications," IEEE Transactions on Consumer Electronics, vol. 58(1), 2012, pp.15-22.
[17] Lichtman, Marc, et al, "A Communications Jamming Taxonomy," IEEE Security & Privacy, vol. 14(1), 2016, pp. 47-54.