Research Article

Research on Generation Algorithm of Dynamic Multimapping Compound Chaotic Sequence

Mengjiao Quan,1,2 Weijia Cui,2 Bin Ba,2 Yuxi Du,2 and Hao Li2

1Zhengzhou University, Zhengzhou, Henan Province 450001, China
2National Digital Switching System Engineering & Technological Research Center, Zhengzhou, Henan Province 450001, China

Correspondence should be addressed to Mengjiao Quan; quanmengjiao2022@163.com

Received 15 April 2022; Revised 22 June 2022; Accepted 1 July 2022; Published 19 July 2022

Academic Editor: Jian Su

Copyright © 2022 Mengjiao Quan et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Aiming at the problems that the chaotic sequence is periodic due to the influence of calculation accuracy and the pseudorandomness of the sequence is not ideal, this paper proposes a dynamic multimapping compound (DMMC) chaotic sequence based on time of days (TOD) and several improved logistic mappings, which not only increases the key space, flexibility, and complexity of sequence generation but also improves pseudorandom performance. The sequence is composed of two new logistic maps with different initial values, which are then scrambled by the 2D-LICM sequence. In the whole process, the TOD is used to determine the system parameter and the selection of the scrambling sequence. After certain processing, it is connected in series with the original generated sequence to obtain the target chaotic sequence. The simulation analysis proves that the sequence generated by the algorithm proposed in this paper has good run length, correlation, and ideal balance and greatly improves the confidentiality of the system, which proves the effectiveness and reliability of the designed spread spectrum sequence.

1. Introduction

Chaotic sequences are gradually being widely used as pseudorandom sequences, especially in the field of spread spectrum communication. Direct sequence spread spectrum (DSSS) refers to the use of spread spectrum sequences to widen the frequency band of the signal, so that the information of the signal is hidden in the noise during the transmission process. The security performance of the system depends to a large extent on the performance of the selected spread spectrum sequence, so the spread spectrum sequence with good correlation and pseudorandomness is of great significance to the spread spectrum communication system. Theoretically, satisfying uniform distribution and independent of each other random sequences are the ideal spread spectrum sequence, but such sequences are difficult in the practical systems [1–3]. In response to this problem, people began to study pseudorandom sequences with noise-like properties and use them as spreading sequences. Most commonly used spread spectrum sequences use linear or nonlinear shift registers to generate pseudorandom sequences, such as $m$-sequence [4] and Gold sequence [5]. However, with the rapid development of spread spectrum communication, the limited number of spread spectrum sequences is no longer enough to meet the increasing user demands. On the other hand, the limited number of sequences and the fixed generation method also make the corresponding detection methods emerge endlessly, which finally poses a threat to the security of the spread spectrum communication system. Therefore, it is necessary to explore new concepts and discover new spreading sequences to meet users’ needs.

In recent years, the dynamics theory of chaos [6, 7] has been very mature. Some studies have applied chaotic sequences [8, 9] as pseudorandom sequences in DSSS communication, because the generation of chaotic signals only depends on iterative equations, initial values, and system parameters, which is beneficial to the reproduction and regeneration of signals. And it is very sensitive to initial conditions. Small changes in conditions can lead to completely uncorrelated signals in a chaotic system. That is, a large
number of uncorrelated sequences can be generated very conveniently. In addition, the initial value and parameters of the chaotic system cannot be derived from the sequence of limited length to achieve the effect of secure communication and enhance the security of the communication system. The chaotic sequence is aperiodic and has statistical properties close to Gaussian white noise, ideal correlation properties, strong anti-interference and confidentiality properties, and a large number of sequences, which is very effective for generating spread spectrum sequences with good performance. At present, some methods have improved many defects of traditional pseudorandom sequences, but these typical nonlinear mappings still cannot meet people's needs for communication [10–12]. Therefore, how further search for new chaotic spread-spectrum sequences with large numbers, strong robustness, good correlation characteristics, and convenient generation is still the direction of chaotic spread-spectrum communication efforts.

There are many methods for optimizing chaos. In [13], an improved spatiotemporal chaos model based on coupled tent mapping was proposed. A new pseudorandom sequence generator was designed based on this model, which can quickly generate multidimensional chaotic pseudorandom sequences. In [14], a single low-dimensional logistic sequence was combined with the Chebyshev sequence to propose a new chaos sequence, which has good balance, randomness, and correlation. In [15], based on the iterative concatenation of the improved logistic map and Chebyshev map, a new chaotic map was proposed, which effectively expands the key space of chaotic systems. In [16], a new piecewise logistic chaotic spread-spectrum communication algorithm was proposed and applied in spread-spectrum communication systems. In [17], this paper proposes a pseudo random number generator based on spatiotemporal chaos. In [18], an improved logistic chaotic map was constructed by introducing the sine-trigonometric function control term to meet the requirements of the value selection of the logistic chaotic map. In [19], a method for generating chaotic binary sequences based on compound mapping was proposed, and the balanced and correlated properties of chaotic binary sequences were screened and optimized. In [20], the sequence algorithm based on the improved logistic map, Chebyshev map, and Kent map is proposed, which overcomes the shortcomings of the limited number of sequences and fixed mechanism in direct sequence spread spectrum communication. A technique to enhance the randomness of binary sequences using nonlinear feedback systems was proposed in [21]. In [22], an effective extension sequence with high security was proposed, which consists of two logistic maps with different initial values, which is easy to implement with digital circuits, and has high system complexity and security. A new method for synchronous scrambler parameter estimation in direct sequence spread spectrum systems was proposed in [23]. [24] proposed a C-T coupled cascaded chaotic map as a spreading code generation algorithm, and the generated sequence has strong randomness.

The above methods are designed to design spreading sequences, so that better randomness can be achieved, more sequences can be obtained, and security can be improved. Inspired by these, we propose a dynamic multimapping composite (DMMC) algorithm based on time information. Unlike previous methods, our proposed method is not affected by computational accuracy and does not exhibit periodic features. At the same time, it has the advantages of good random performance and high security. Simulation results also confirm our sequential performance. Our major contributions are listed as follows:

1. We increase the flexibility of sequence generation by introducing time information as a parameter, so that the entire system of generating sequences is in dynamic change.
2. We improve the size of the key space and the difficulty of noncooperating parties to crack the sequence generation method by combining the methods of compounding and scrambling.
3. We achieve the ideal balance by inverting the polarity to avoid spectral leakage.

The rest of the paper is as follows: Section 2 introduces the logistic chaotic map, the new logistic chaotic map, and the 2D-LICM. Section 3 mainly discusses the specific steps of generating sequences and the related details involved. Section 4 mainly conducts a series of performance simulations on the generated sequences to verify the feasibility of the sequence generation algorithm and the security of quantitative analysis. Finally, some conclusions and discussions are given in Section 5.

2. Logistic Map and Its Improved Several Chaotic Sequences

2.1. Typical Logistic Map. Logistic map is a typical chaotic map, which is a dynamic system that has been widely studied because it exhibits chaotic phenomena. The mathematical equations are defined as follows:

\[ x_{n+1} = \mu x_n (1 - x_n) \quad x_0 \in (0, 1), \]

where \( \mu \) is the system parameter and \( 0 \leq \mu \leq 4 \), the initial value \( x_0 \in (0, 1) \); the relationship between the mapping state and the mapping parameter is shown in Figure 1.

Figure 1 shows that with the \( \mu \) change, the \( x \) dynamic range generated after several iterations also changes. When \( 3.5699 \leq \mu \leq 4 \), at that time, the system was in a chaotic state, and only when \( \mu = 4 \), the iteration result was mapped to the entire interval, which is called full mapping state.

2.2. New Logistic Mapping. The new logistic mapping [25] aims at the defect that the above mapping is full mapping only at one parameter point to propose a full mapping within a certain parameter interval. The mathematical equations are defined as follows:

\[ x_{n+1} = \frac{k^2}{2} x_n^2 + (k^2 - 2k) x_n + \frac{k^2}{2} - 2k + 1 \quad x_0 \in (-1, 1), \]

\[ 2 \text{ Wireless Communications and Mobile Computing} \]
where $k$ is the system parameter and $0 \leq k \leq 2$, the initial value $x_0 \in (-1, 1)$; the relationship between the mapping state and the mapping parameter is shown in Figure 1.

It can be seen from Figure 2 that the new logistic mapping has a full mapping relationship within a large range of parameters $k \in (1.53, 2)$. This kind of mapping greatly enhances the selectivity of the full mapping parameters and the dynamic characteristics of the chaotic sequence, so it is very suitable for application in the field of secure communication.

2.3. 2D Logistic ICMC Cascade Mapping. Two-dimensional logistic ICMC cascade map (2D-LICM) was proposed [26], which is generated by two one-dimensional chaotic maps, namely, logistic map and iterative map; the latter mathematical equation is defined as follows:

$$x_{n+1} = \sin \left( \frac{c}{x_n} \right).$$  \hspace{2cm} (3)

And $c \in (0, +\infty)$.

This new 2D logistic ICMC cascade map is defined as

$$\begin{cases} x_{n+1} = \sin \left( \frac{21}{(a(y_i + 3)kx_i(1 - kx_i))} \right), \\
y_{n+1} = \sin \left( \frac{21}{(a(kx_{i+1} + 3)y_i(1 - y_i))} \right). \end{cases}$$  \hspace{2cm} (4)
where \(a\) and \(c\) are system parameters and \(a \in (0,+\infty), k \in (0,+\infty)\). When \((a,k) = (0.6,0.8)\), the chaotic phenomenon is shown in Figure 3.

It can be seen from Figure 3 that the values generated by iteration are distributed evenly over the entire interval.

### 3. The Generation Algorithm of the Proposed Chaotic Sequence

The chaotic sequence generation algorithm proposed in this paper is from the perspective of improving the security of the spread spectrum communication system. By using compounding, scrambling, and other methods to increase the difficulty of noncooperating parties to estimate the composition of the system and introducing time information to dynamically affect the sequence generation, the entire sequence generation mechanism is more flexible. Based on the above ideas, three modules are proposed, namely, dynamic composite mapping module, dynamic scrambling module, and target sequence generation module.

#### 3.1. Dynamic Composite Mapping Module

In this module, the way we achieve dynamic is to use the constant change of time information to select different system parameter. In order to avoid selecting a nonfull mapping area, this paper fixes the dynamic change range of the system parameter to \([1.91, 2]\). The reason why we did not take a few more decimal places is that we found that the more decimal places, the more iterations are needed to have obvious differences, which limits the use of sequences. Then, we use the two determined initial values and the above selected system parameter to substitute into the new logistic mapping function formula to generate real-valued sequence 1 and real-valued sequence 2, respectively, which are represented by \(u\) and \(v\). Then, the two real-valued sequences are differentiated to generate a new complex chaotic sequence \(z\).

\[
z(n) = u(n) - v(n)
\]  

(5)

It should be noted that according to formula (2), the initial value must satisfy \(u_0 \neq v_0\); otherwise, \(\{u_n, v_n\}; \{z_n\}\) is always zero. Because the iterative sequences \(\{u_n\}\) and \(\{v_n\}\) have a value range of \((-1,1)\), the value range of \(\{z_n\}\) is expanded to \((-2,2)\). When \(k = 2\), the initial values of the new logistic map are 0.40000 and 0.40001, respectively; the generated complex chaotic sequence \(\{z_n\}\) diagram is shown in Figure 4.

In order to facilitate transmission by digital means, real-valued sequences are usually digitized. There are two ways to digitize real-valued sequences: binary quantization and multibit quantization. The binary quantization method is to perform \(L\)-bit 1,0 quantization on each real-valued sequence element \(x_n\) to obtain the sequence \(\tilde{x}_n\), where \(x_n = \sum_{i=1}^{L} x_{ni} 2^{-i}\). The multibit quantization rule is to perform \(L\)-bit quantization on each real-valued sequence element \(x_n\), and \(L\) sequence elements can be obtained for each \(x_n\), where

\[
x_n = \sum_{i=1}^{L} x_{ni} 2^{-i}\]  

The above quantization method is universal, so in order to improve the security as much as possible, the mapping method can be used; that is, each real-valued sequence element \(x_n\) is mapped to \(L\)-bit according to certain mapping rules, and the sequence \(\tilde{x}_n\) is obtained. Among them, the mapping rules have \(2^{L-1}\) possibilities. It can be seen that the more bits in the mapping, the higher the complexity and the better the confidentiality. For example, the abovementioned digitization of the
3.2. Dynamic Scrambling Module. In this module, we firstly use logistic ICMC cascade mapping to generate two-dimensional chaotic sequences and then perform quantization processing. At the same time, according to the established mapping rules, two discrete sequences $X$ and $Y$ are obtained, and they are used as the disturbance sequence set of composite chaotic sequences. In order to achieve the effect of dynamically selecting the scrambled sequence, the time information is used as a parameter, and an irrational number $\pi$ is introduced at the same time. Starting from the $n$th bit, the scrambled sequence $R$ is selected. The selection rules are as follows:

$$
R(i) = \begin{cases} 
X(i) & \text{if } p(i) = \text{odd} \\
Y(i) & \text{if } p(i) = \text{even} 
\end{cases} i = n, n + 1 \ldots (n > 2),
$$

(7)

Because the irrational number $\pi$ is random, this makes the choice of the scrambling sequence random. Because this module involves digital mapping rules, selection rules for disturbing sequences, and selection of irrational numbers, sequence security is increased from three dimensions. Finally, the sequence generated by the dynamic composite mapping module is XORED with the scrambled sequence generated above to obtain sequence $B$.

3.3. Target Sequence Generation Module. In the target sequence generation module, the sequence $B$ is first reversed to obtain $B^0$; that is, $B^0 = -B$, and then, the target sequence $C$ is obtained by concatenating the two sequences. The purpose of this is to obtain a perfectly balanced performance to prevent spectrum leakage when the chaotic sequences are used as spread spectrum sequences, resulting in poor carrier suppression and an obvious peak spectrum at the carrier frequency, thereby losing hidden feature and reducing the security of communication system.

3.4. Implementation Steps for Sequence Generation. The flowchart of the design sequence method formed by the above three modules is shown in Figure 5. The steps to generate the sequence are summarized as follows.

Step 1. Use time information to select a certain system parameter $k$ through the functional relationship (8) and mapping relationship (9) agreed by both parties.

$$
t = a * h + b * m + s,
$$

(8)

$$
\begin{cases} 
ds = f(s) & ds \in (1, 2, \ldots 9) \\
    k = 1.91 + 0.01 * ds,
\end{cases}
$$

(9)

where $a$ and $b$ are the coefficients.

In this process, we can use the constant change of time information to dynamically select system parameter. At the same time, according to the required transformation rate, the time information can be accurate to the second, millisecond, or even smaller level.
Step 2. Use the system parameters selected in Step 1 and two unequal initial values to be substituted into formula (2) to generate two real-valued sequences of equal length, $u$ and $v$, respectively.

\[
\begin{align*}
u_{n+1} &= \frac{k^2}{2} v_n^2 + (k^2 - 2k) v_n + \frac{k^2}{2} - 2k + 1, \quad v_0 = 0.4, \\
u_{n+1} &= \frac{k^2}{2} v_n^2 + (k^2 - 2k) v_n + \frac{k^2}{2} - 2k + 1, \quad v_0 = 0.4.
\end{align*}
\]

Step 3. Use the two sequences generated in Step 2 to perform differential operations at the corresponding positions to generate a complex chaotic sequence. Then, in order to facilitate digital transmission, the sequence is quantized to obtain the sequence $Z$.

\[
Z(n) = G(u(n) - v(n)),
\]

where $G$ represents the quantitative relationship.

Step 4. The 2D-LIMC sequence is used as the scrambling sequence set, and time information is introduced for...
dynamic selection as shown in equation (7), and the scrambling sequence $R$ is selected as $x$ or $y$.

**Step 5.** The composite sequence $Z$ of Step 3 and the scrambled sequence $R$ of Step 4 are XORed to generate sequence $B$.

$$B(n) = Z(n) \oplus R(n). \quad (13)$$

**Step 6.** Use the sequence $B$ generated in Step 5, reverse its polarity to get sequence $B'$, and then connect the above two sequences in series to obtain the target sequence $C$.

At this point, the length of sequence $C$ is twice the length of sequence $B$.

$$C = B \& B'.$ \quad (14)$$

### 4. Performance Simulation Experiment

Spread spectrum codes play a decisive role in the performance of spread spectrum communications. Anti-interference, antinoise, anti-interception, concealment, and confidentiality of information and data are all closely related to the design of spread spectrum codes. Next, the important characteristics of the spread spectrum sequence designed in this paper are simulated and analyzed to verify the feasibility of the design method.

#### 4.1. System Parameter

To increase the flexibility of sequence generation, the time parameter is introduced as an influencing factor. For the partner, time information, mapping rules, the type of chaotic sequence used, the number of iterations, and the quantization rules are known, and the receiver can restore the spread spectrum sequence of the sender. For noncooperating parties, only the information time is known, and the rest of the processing is invisible to noncooperating parties. It is very difficult to obtain the mapping of the entire system from simple time changes.

The value of the system parameter depends on the time parameter and the mapping rule. In practical application, the parameter of the independent variable can be changed according to the requirements. As shown in Figure 6, with the increase of time, the system parameters have been fluctuating up and down $[1.92,2]$ in the entire mapping interval and have randomness, which is determined by the nature of the selection of irrational numbers. As long as the input system parameters are different, when the initial values remain unchanged, the generated sequences are all different and independent. The sequence produced by this mapping method has no periodicity because it changes dynamically all the time, which adds randomness to the whole system.

Figure 7 is a histogram of the distribution of system parameters over 2000 seconds, which approximately obeys a uniform distribution, which is determined by the properties of the selected irrational numbers. On the one hand, although the system parameters are random, they conform to a uniform distribution as a whole, which avoids the high probability of a certain system parameter. On the other hand, the dynamic value of the system parameter adds one-dimensional information, which improves the security of the satellite communication waveform.

#### 4.2. Run

The run-length characteristic is an important feature to characterize the randomness of a pseudorandom sequence. In a pseudorandom sequence, a sequence of consecutive occurrences of the same number is called a run. The length of this sequence is called the run length. The run length is $i$, and the number of runs in a sequence should theoretically be $1/2^i$. For example, the number of runs with a run length of 2 should theoretically be 1/4. The run length of the spread spectrum sequence designed in this paper is simulated below.
Figure 8 is a simulation diagram of the number of runs changing with time when the initial value of the system is fixed, and the sequence length is 1, 2, and 3, respectively. The straight line is the ideal number of runs, and the line with jitter is the actual number of runs. When the number of runs of a pseudorandom sequence is closer to the theoretical value, its sequence distribution is more uniform, and the run characteristic is better. It can be seen from the figure that the run characteristics of the sequence change with time. Except when the run length is 1, the number of runs is relatively large, and the rest fluctuate around the ideal value and have good randomness.

Table 1 shows the run length performance comparison between the proposed DMMC sequence and several other sequences. It can be seen from the table that the proposed

<table>
<thead>
<tr>
<th>n</th>
<th>m</th>
<th>Logistic</th>
<th>Tent</th>
<th>C-T</th>
<th>DMMC</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.4933</td>
<td>0.4958</td>
<td>0.4756</td>
<td>0.5105</td>
<td>0.5237</td>
</tr>
<tr>
<td>2</td>
<td>0.3324</td>
<td>0.3240</td>
<td>0.3190</td>
<td>0.3202</td>
<td>0.2484</td>
</tr>
<tr>
<td>3</td>
<td>0.1421</td>
<td>0.1462</td>
<td>0.1344</td>
<td>0.1320</td>
<td>0.1209</td>
</tr>
<tr>
<td>4</td>
<td>0.0638</td>
<td>0.0744</td>
<td>0.0614</td>
<td>0.0618</td>
<td>0.0591</td>
</tr>
</tbody>
</table>
sequence is closer to the ideal value than the other four sequences when the run lengths are 2 and 3, but the run performance is slightly worse when the run lengths are 1 and 4. In general, the proposed sequence meets the run-length requirement of the spreading sequence.

4.3. Correlation. Theoretically, spread spectrum communication requires that the autocorrelation characteristic of the spread spectrum code must be peak-like at zero delays; the side lobes are infinitely close to 0. The value of the cross-correlation function should also be as close to 0 as possible. The reason is that the smaller the side lobe of the autocorrelation value, the less multipath interference, and the smaller the cross-correlation value of the two sequences, the lesser the multiple access interferences.

For the chaotic sequence, the corresponding autocorrelation function and cross-correlation function are:

$$R_x(k) = \frac{1}{N} \sum_{m=1}^{N-k} x(m)x(m+k),$$  \hspace{1cm} (15)

$$R_{xy}(k) = \frac{1}{N} \sum_{m=1}^{N-k} x(m)y(m+k).$$  \hspace{1cm} (16)

But in actual processing, it is more convenient to use the time average to find the correlation function. The autocorrelation function is

$$R_x(k) = \frac{1}{N} \sum_{m=1}^{N-k} x(m)x(m+k).$$  \hspace{1cm} (17)

The cross-correlation function is

$$R_{xy}(k) = \frac{1}{N} \sum_{m=1}^{N-k} x(m)y(m+k).$$  \hspace{1cm} (18)

Figure 9 is the autocorrelation characteristic curve of the designed sequence under the condition that the initial value is 0.40 and 0.41, and the system parameter is 1.98. It can be seen from the figure that it has a peak shape at zero delays, and other places are close to zero, so they have good autocorrelation. Therefore, the simulation result shows that the designed spread spectrum sequence has autocorrelation close to ideal conditions, which can meet the requirements of spread spectrum codes for autocorrelation.

Figure 10 is the cross-correlation characteristic curve of the two designed sequences when the system parameters are 2 and 1.98, respectively, and other conditions are the same. It can be seen from the figure that the absolute value of the cross-correlation value is very low. This shows that the sequences generated at different times have good cross-correlation. Figure 11 shows the cross-correlation characteristic curves of the two designed sequences when the initial values are 0.40 and 0.41 and 0.42 and 0.43, respectively, and other conditions are the same; the absolute value of the cross-correlation value does not exceed 0.05. From this, it can be seen that sequences generated by different initial values at the same time also have good cross-correlation.

It is proved by the above two simulations that there is an ideal cross-correlation between the dynamically generated sequences and between sequences with different initial values, which greatly increases the number of available spreading codes. The effect is that it can improve the confidentiality of spread spectrum communication and increase
the difficulty for noncooperating parties to decipher the information.

4.4 Balance. In spread spectrum communication, one of the requirements for spread spectrum sequences is to have a good sequence balance. Due to the imbalance of the spreading sequence, the leakage of the system carrier will become more extensive, and information error or loss is prone to occur. In practical applications, good balance can effectively

<table>
<thead>
<tr>
<th>Sequence</th>
<th>m</th>
<th>Logistic</th>
<th>Tent</th>
<th>C-T</th>
<th>DMMC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of 1</td>
<td>19912</td>
<td>9930</td>
<td>9546</td>
<td>9970</td>
<td>10000</td>
</tr>
<tr>
<td>Number of -1</td>
<td>10088</td>
<td>10070</td>
<td>10454</td>
<td>10030</td>
<td>10000</td>
</tr>
<tr>
<td>Difference</td>
<td>176</td>
<td>140</td>
<td>908</td>
<td>60</td>
<td>0</td>
</tr>
<tr>
<td>Balance</td>
<td>0.0088</td>
<td>0.007</td>
<td>0.0454</td>
<td>0.003</td>
<td>0</td>
</tr>
</tbody>
</table>

**Table 2: Sequence equilibrium comparison.**

![Cross-correlation characteristic simulation diagram.

**Figure 10:** Cross-correlation characteristic simulation diagram.

![Cross-correlation characteristic simulation diagram.

**Figure 11:** Cross-correlation characteristic simulation diagram.
suppress the carrier, reduce the transmit power, and be difficult to detect. On the contrary, if the sequence is unbalanced, it will destroy the confidentiality, anti-interference, and antidetection capabilities of the spread spectrum communication system. Therefore, it is necessary to pay attention to the balance of the spreading code.

The balance $E$ of the spreading sequence shows the difference in the number of $+1$ and $-1$ within a sequence:

$$E = \frac{A - B}{N},$$  \hspace{1cm} (19)

where $A$ and $B$ are the numbers of $+1$ and $-1$, respectively, and $N$ is the sequence length. Ideally, the balance $E$ of the pseudorandom sequence is 0, so as long as the chaotic sequence generated by statistical calculation is closer to 0, the sequence balance will be better.

In Table 2, the balance of the proposed DMMC sequence and the other four sequences is compared. It can be seen from the table that when the sequence lengths are the same, the balance of the other four sequences is close to 0 but not equal to 0, while the balance of the proposed sequence reaches 0. So the DMMC sequence designed in this paper has an ideal balance and is suitable for spread spectrum communication.

### 4.5. Key Space

The satellite secure communication waveform is closely related to the key size of the sequence. We divide the key space into two parts: the initial value key space and the system parameter key space.

Table 3 is the size comparison of the key space between the DMMC sequence and the other four sequences. The above results are calculated under the condition that the parameters of the DMMC scrambling sequence are fixed, and the calculation precision is 16 digits after the decimal point. Compared with the classical chaotic sequence, the key space of the proposed sequence has been greatly improved. And compared with the C-T sequence, there is also an order of magnitude improvement.

For the partner, as long as the agreed rules are followed, the same chaotic sequence as the sender can be generated. However, for noncooperating parties, the number of sequences is enormous and constantly changing. It takes a lot of time to decipher using the exhaustive method, which dramatically improves the security of satellite communication.

### 5. Conclusion

In this paper, two new logistic chaotic maps with different initial values are used to generate composite chaotic sequences, which effectively expand the initial key space and make the generated sequences more chaotic and unpredictable. Then, we use the 2D-LICM sequence scramble that sequences to increase the sequence generation complexity. It is worth noting that the flexibility of the sequence is improved because the entire process is dynamically influenced by time. It avoids the disadvantage of periodic characteristics caused by the influence of calculation accuracy, thereby reducing the security of wireless communication. It also increases the number of spreading sequences, so this design method increases the difficulty of the attacker predicting the state of the system. The simulation results also show that the designed DMMC sequence meets the requirements of pseudorandom sequences and has good statistical properties. Because of their high security, they are suitable for satellite security communications.

### Data Availability

The authors claim that the data used in this article are provided by our simulations and the data used to support the findings of this study are available from the corresponding author upon request.

### Conflicts of Interest

The authors declare that they have no conflicts of interest, and they confirm that the funding did not lead to any conflict of interests regarding the publication of this manuscript.

### Acknowledgments

The work is supported by the National Natural Science Foundation of China (grant No. 62171468).

### References


