Conducting Digitized Chaotic Time Series with a Guaranteed Enhanced Period

Chuanfu Wang and Qun Ding

Electronic Engineering College, Heilongjiang University, Harbin 150080, China

Correspondence should be addressed to Qun Ding; qunding123@163.com

Received 23 April 2019; Revised 31 May 2019; Accepted 3 July 2019; Published 22 December 2019

Academic Editor: Quanmin Zhu

Copyright © 2019 Chuanfu Wang and Qun Ding. 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.

When chaotic systems are realized in digital circuits, their chaotic behavior will degenerate into short periodic behavior. Short periodic behavior brings hidden dangers to the application of digitized chaotic systems. In this paper, an approach based on the introduction of additional parameters to counteract the short periodic behavior of digitized chaotic time series is discussed. We analyze the ways that perturbation sources are introduced in parameters and variables and prove that the period of digitized chaotic time series generated by a digitized logistic map is improved efficiently. Furthermore, experimental implementation shows that the digitized chaotic time series has great complexity, approximate entropy, and randomness, and the perturbed digitized logistic map can be used as a secure pseudorandom sequence generator for information encryption.

1. Introduction

Chaotic time series are widely used in information fields for their initial sensitivity, nonlinearity, aperiodicity, and randomness. These chaotic behaviors are consistent with the “confusion” and “diffusion” in Shannon’s information theory [1], which provides a basis for chaotic pseudorandom sequence generator, chaotic secure communication, and other information fields [2–8]. However, when chaotic systems are realized in digital circuits, chaotic behavior will degenerate [9]. For the finite precision effect in digital systems, chaotic systems will eventually collapse in finite fields, and digitized chaotic time series will show short periodic behavior. In this paper, degraded chaotic systems in digital circuits are called digitized chaotic systems, and their time series are called digitized chaotic time series.

Short periodic behavior brings hidden dangers to the application of digitized chaotic time series [8, 10–15]. A large period is the basic security indicator of a pseudorandom sequence with encryption ability. Pseudorandom sequences with short periods cannot be used as key streams to encrypt information. Key streams repeated in a short time can be easily broken without initial keys. The period of a pseudorandom sequence with encryption ability should be at least greater than $2^{80}$ and does not have a weak key. The weak key is the initial key that will lead to a pseudorandom sequence with a short period. Therefore, the period of digitized chaotic time series needs to be exactly determined or given a low bound to satisfy the basic security indicator.

In order to improve the short periodic behavior of digitized chaotic time series, some methods have been put forward: (1) Using higher precision [6, 17]. The period of digitized chaotic time series can be increased by improving the precision. However, the rate of period rises slowly with the increase of precision. (2) Using higher dimension [18, 19]. Compared with low-dimensional chaotic systems, high-dimensional chaotic systems have more variables and can support larger state space after being digitized. However, for dense periodic orbits in a chaotic system, short periodic behavior of digitized chaotic time series cannot be fully eliminated. (3) Using multiple cascading chaotic systems [20, 21]. The cascading chaotic system with two logistic maps is the classical method. However, it is difficult to counteract the short periodic behavior of digitized chaotic time series. If two digitized logistic maps are both in short periodic orbits, then the final output digitized chaotic time series will show short periodic behavior. (4) Perturbing the chaotic system [9, 22–25]. Perturbation sources can be introduced in variables and...
parameters. However, there are potential dangers in perturbing parameters, because chaotic systems are sensitive to the parameters. Chaotic systems can show chaotic behavior only under certain parameters; for example, parameter $\mu = 4$ for chaos in a logistic map [26] and parameters $\sigma = 10$, $r = 30$, $b = 8/3$ for chaos in the Lorenz equation [27]. It is difficult to preserve chaotic behavior when these parameters are changed according to random perturbation sources. (5) Transforming into different finite fields [28, 29]. Due to the influence of the finite precision effect, chaotic systems will eventually collapse in finite fields. Different finite fields have different impacts on digitized chaotic time series. In [28], the digitized logistic map in fields $\mod p$ is proposed, where $p$ is a prime number. However, the short periodic behavior of output chaotic time series was not improved efficiently. In [29], the digitized logistic map in field $\mod 3$ is proposed, and the upper bound of output chaotic time series is studied in detail. However, only the low bound of output chaotic time series could guarantee secure encryption. Therefore, we should find the lower bound rather than the upper bound. In addition, some novel methods have also been proposed. To counteract the degradation of chaotic systems, the ciphertext sequence is chosen as the pseudorandom sequence to perturb the digitized chaotic system and the coefficients of the dynamic feedback control scheme [30]. In [31], a coupled chaotic model is proposed to reduce the dynamical degradation. In this model, the state variable of one digitized chaotic map is used to control the parameter of the other digitized map. In [32], a new delay coupled chaotic model is proposed to reduce the dynamic degradation of digitized chaotic maps. In this model, the delay state variable is introduced in digitized map, and the state variable of one map is used to change the control parameters of another map. In [33], the State Mapping Networks (SMN) structure of chaotic maps is used to counteract the degradation of chaotic behavior. The randomness of sequences can be improved efficiently by introducing SMN structure. These novel methods improve the short periodic behavior to a certain extent. However, it is difficult to determine the exact length of periodic orbits in digitized chaotic systems. Therefore, the short periodic behavior in digitized chaotic systems has not been completely resolved.

This paper studied the period of digitized chaotic time series generated by a digitized logistic map and provides a perturbation method to enhance the period. In addition, complexity, entropy, and randomness were used to analyze the security of digitized chaotic time series. The randomness of digitized chaotic time series was tested by the National Institute of Standards and Technology (NIST) randomness test suite and proved by computational complexity in mathematical theory.

Thereafter, this paper is organized as follows. The digitized logistic map and its complex period behavior are analyzed in Section 2. Section 3 analyzes two perturbation methods, then a concrete scheme to enhance the period of digitized chaotic time series is proposed. Section 4 analyzes the security of digitized chaotic time series, including complexity, entropy, and randomness. Finally, Section 5 concludes the paper.

### 2. Time Series Analysis of Digitized Logistic Map

A logistic map is a widely used one-dimensional chaotic map in information encryption. A logistic map over the real number field is defined as [26]:

$$x(n + 1) = \mu x(n)(1 - x(n)), \quad n = 0, 1, 2, 3, \ldots,$$

where $x(n) \in [0, 1]$, $x(0)$ is the initial value, $\mu$ is a parameter, and $n$ acts as the $n$-th iteration. A bifurcation diagram of the logistic map is shown in Figure 1.

When the logistic map is realized in a digital circuit, it will degenerate into a digitized logistic map. The digitized logistic map is defined as

$$x(n + 1) = \left[\frac{4x(n)(2^N - x(n))}{2^N}\right] \mod 2^N, \quad n = 0, 1, 2, 3, \ldots$$

![Bifurcation diagram of logistic map: (a) when $\mu \in [0, 4]$; (b) when $\mu \in [3.9, 4]$.](image)
where $\lceil \cdot \rceil$ is the integer-valued function, and $N$ represents the precision of digital physical devices. In a digital system, under precision $N$, the term $(2^N - x(n))$ is equal to $(\sim x(n) + 1)$, where $\sim$ means "not operation" bit by bit. The optimized map of (2) is defined as

$$x(n + 1) = \left\lfloor \frac{4x(n)(\sim x(n) + 1)}{2^N} \mod 2^N \right\rfloor, \quad n = 0, 1, 2, 3, \ldots, \tag{3}$$

where $x(n) \in \{0, 2^N - 1\}$. For the finite precision effect in digital physical devices, the chaotic behavior of the logistic map degenerates. The digitized logistic map shows short periodic behavior. Taking $N = 4$ as an example, the whole time series of the digitized logistic map is shown in Figure 2.

There are three periodic cycles in Figure 2, and two of them have the same length. The relationship between the initial value $x(0)$ and the length of periodic cycle $T$ under $N = 4$ is shown in Table 1.

For a logistic map over the real number field, different initial values have different time series, and the chaotic time series is aperiodic. However, in the digitized logistic map, all the time series are periodic, and different initial values may lead to the same time series. Through traversal searching, when $N = 4, 8, 9, 10\ldots19$, the periodic orbits of digitized Logistic map are shown in the Appendix. The time series with a maximum period in the digitized logistic map is very small, which provides hardly any security for information encryption. The time series with a small period presents hidden danger to the security of chaos-based encryption. The period of pseudorandom sequence with encryption ability should be at least greater than $2^{80}$ and does not have a weak key. Through traversal searching, we find that the digitized logistic map has many weak keys.

### 3. Digitized Logistic Map with Introduced Perturbation Sources

#### 3.1. Existing Perturbation Method

Introducing perturbation sources is an effective method of resisting the short periodic behavior of digitized chaotic time series. "Perturbation" means the pseudorandom number generated by perturbation sources are operated with system variables or control parameters. Suppose the perturbation sources is the pseudorandom number generator, and its output pseudorandom number is $P(n)$, the diagram of perturbed digitized logistic map is shown in Figure 3. In Figure 3(a), perturbation sources $P(n)$ are operated with system variable $x(n)$. In Figure 3(b), the parameter $\mu$ is generated by perturbation sources $P(n)$, that is $\mu = P(n)$.

When $\mu = 4$, the logistic map is ergodic in $[0, 1]$. Therefore, the parameter $\mu$ is set as 4 in Figure 3(a). From Figure 3(a), we know that the variable is perturbed by perturbation sources directly. Therefore, the output sequence is related to the perturbation source. The periodic behavior of the digitized logistic map can be well controlled by the perturbation sources. When parameter $\mu$ is generated by perturbation sources, the block diagram is shown in Figure 3(b). For chaotic systems, they are sensitive to parameters. For the logistic map, if parameter $\mu$ is changed arbitrarily, the map may not be a chaotic system. For example, when $\mu = 4$, the logistic map is chaotic. When $\mu \in [3.75, 3.85]$, from Figure 1(a), we can see that the bifurcation diagram of the logistic map has lots of period windows. When $\mu \in [3.9, 4]$, from Figure 1(b), there are still many periodic windows. Periodic windows mean that the logistic map is no longer chaotic. Therefore, parameter $\mu$ cannot be changed arbitrarily. Parameters are very important for chaotic systems. When parameters are perturbed by perturbation sources, maintaining chaotic behavior is key.

### 3.2. The Digitized Logistic Map with Introduced Parameter

Although the method of introducing perturbation sources in parameters has many advantages, it is difficult to maintain chaotic behavior under arbitrary parameters. From Figure 1, it is obvious that the original parameter $\mu$ cannot be arbitrarily changed. Therefore, a new parameter $t$ is introduced to overcome the drawback of introducing the perturbation source in original parameter $\mu$. 

![Figure 2: Time series of digitized logistic map when $N = 4$.](image)

**Table 1: Initial values and cycle lengths.**

<table>
<thead>
<tr>
<th>$x(0)$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
<th>15</th>
</tr>
</thead>
<tbody>
<tr>
<td>$T$</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
</tbody>
</table>
Theorem 1. A parameter $t$ introduced in the quadratic term of the logistic map can maintain chaotic behavior. The controlled map is

$$x(n+1) = 4x(n)(1-tx(n)).$$

Proof. Let $x(n) = u(n)/t$ and $t \in (0,1]$, and the resulting system,

$$u(n+1) = 4u(n)(1-u(n)),$$

is identical to (1).

From Theorem 1, we know that map (4) is still a chaotic system when $t \in (0,1]$. For a certain parameter $t$, the map is a certain chaotic system. Therefore, we can perturb the map (4) by randomly changing the parameter $t$ in the interval $(0,1]$.

For a certain parameter $t_n$ and initial value $x(0)_n$, we can obtain an output number $x(1)_n$. Then for an another certain parameter $t_{n+1}$ and initial value $x(0)_{n+1}$, we can obtain an another output number $x(1)_{n+1}$. For $n = 0, 1, 2, 3...$, we can get a pseudorandom sequence ($x(1)_n$) made up of multiple chaotic systems (map (4) with different parameter $t_n$) through one iteration. The pseudorandom sequence ($x(1)_n$) can be described by Eq. (6).

$$x(1)_n = 4x(0)_n(1-S(n)).$$

where $S(n) = t_n x(0)_n$. For easier hardware implementation, let $x(0)_n \in [0,1]$. Then, for a certain $t_n$ we can find a corresponding $x(0)_n$ such that $S(n) \in [0,1]$. After being digitized in digital circuits, map (6) can be transformed into

$$x(1)_n = \left\lfloor \frac{4x(0)_n(1-S(n)+1)}{2^N} \right\rfloor \mod 2^N, \quad n = 0, 1, 2, 3...,$$

where $x(n), S(n) \in [0, 2^N-1]$.

3.3. Pseudorandom Sequence Generator based on Perturbed Digitized Logistic Map. In this paper, the m-sequence generator is used as a perturbation source. Under precision $N$, the m-sequence is the periodic sequence generated by a linear function with a period of $2^N-1$. The m-sequence generator can generate a periodic pseudorandom sequence, which is made up of numbers from 1 to $2^N-1$. Compared with other pseudorandom sequences, the structure of the m-sequence is simpler and occupies less hardware logic resources.

In this paper, $S(n)$ and $x(0)_n$ are generated by different improved m-sequences. Suppose variable $x(0)_n$ is generated by the improved m-sequence $m_1(n) \in [0, 2^N-1]$, that is $x(0)_n = m_1(n)$. Suppose $S(n)$ is generated by the improved m-sequence $2m_1(n) \mod 2^N \in [0, 2^N-1]$, then $S(n)$ is an even number and $S(n) = 2m_1(n) \mod 2^N$. Thus, parameter $t_n$ is generated by the quotient of two improved m-sequences, that is $t_n = S(n)/(x(0)_n)^{-1} \mod 2^N$. The pseudorandom sequence generator based on map (7) is

$$w(n) = \left\lfloor \frac{4m_1(n)(2m_1(n)+1)}{2^N} \right\rfloor \mod 2^N,$$

where $n = 0, 1, 2, 3...$, $w(n) = x(1)_n$. In view of binary numbers, for simpler hardware implementation, map (8) can be transformed into

$$w(n) = \left\lfloor \frac{4m_1(n)(m_1(n)+1)}{2^N} \right\rfloor \mod 2^N, \quad n = 0, 1, 2, 3...,$$

where $2m_1(n)+1 = m_2(n)||1$, $m_1(n) \in [0, 2^N-1]$, $m_2(n) \in [1, 2^N-1]$, “||” is the connector in field $F_2^N$, and $N$ represents the precision of digital physical devices. For example, suppose $m_1(n) = 5$; its binary representation in field $F_2^N$ is 3 bits, “101.” Then $m_2(n)||1 = 11$, and its binary representation in field $F_2^N$ is 4 bits, “10111.” The improved m-sequence $m_1(n)$ has one more number 0 than the m-sequence. Since the period of the m-sequence is $2^N-1$, the period of $m_2(n)$ is $2^N$. The specific steps for constructing the improved m-sequence $m_2(n)$ are as follows:

**Step 1.** Select two $N$ bit variables $a \in [0, 2^N-1]$ and $b \in [0, 2^N-1]$, in which $a$ is the initial key of m-sequence $m(n)$.

![Diagram of perturbed digitized logistic map](image)
Step 2. Initial: \( m_s(0) = m(0) = a, i = 0 \). Then, for \( i = i + 1 \) do

(If \( m(i) = b \) then

\[
m_s(i) = b,
\]

\[
m_s(i + 1) = 0,
\]

\[ i = i + 1, \]

else

\[ m(i) = m_s(i) \]

Through several transformations of variable \( x(0)_n \) and parameter \( S(n) \), we obtain a pseudorandom sequence generator with very simple structure. From the structure of the equation, we can see that Eq. (3) is equivalent to Eq. (9). They both contain multiplication and division. In digital circuits, connector operation does not consume any hardware resources. Therefore, compared with Eq. (3), the hardware for implementing Eq. (9) does not require too much additional resource consumption. Compared with other methods, such as using a higher-dimensional chaotic map [18, 19], multiple cascading chaotic systems [20, 21], transforming into different finite fields [28, 29], or perturbing the chaotic systems [9, 22–25], the proposed method has a simpler structure. The Lorenz chaotic system is used in [9] to perturb the logistic map, whereas in this paper, the m-sequence is used to perturb the logistic map. Compared with the Lorenz chaotic system, the m-sequence has a simpler structure and less hardware resource consumption. In [15], the perturbation method is switching multiple chaotic systems. Implementing multiple chaotic systems undoubtedly increases the consumption of hardware resources. The perturbation sources all have complex structures in [13, 16, 17]. Therefore, compared with other methods, Eq. (9) has a simpler structure and less resource consumption for hardware implementation.

4. Security Analysis of Digitized Chaotic Time Series

4.1. Period Analysis. Before analyzing the digitized chaotic time series generated by map (9), let us take a special quadratic map \( Q(x) = x(ax + 1) \mod 2^N \) into consideration.

Lemma 1. The quadratic map \( Q(x) = x(ax + 1) \mod 2^N \) is a one-to-one mapping when \( a \) is even.

Proof. Suppose \( f(x_1) = f(x_2) \), where \( x_1 \) and \( x_2 \) are two different numbers. Then, \( f(x_1) - f(x_2) = (x_1 - x_2) [a(x_1 + x_2) + 1] \mod 2^N = 0 \). When \( a \) is even, the term \( a(x_1 + x_2) + 1 \) is odd. Therefore, \( x_1 - x_2 \) must be a multiple of \( 2^N \). Since \( x_1, x_2 \in (0, 2^N - 1) \), the term \( x_1 - x_2 \) must be zero, that is, \( x_1 = x_2 \).

Then, let us take the quadratic map

\[
P(x) = \left[ \frac{4x(ax + 1)}{2^N} \right] \mod 2^N
\]

into consideration. For an integer \( b \in [0, 2^N - 1] \), \( b \) can be represented by \( N \)-tuple binary numbers. The transforming equation between integer \( b \) and \( N \)-tuple binary numbers \( (b_{N-1}, b_{N-2}, ..., b_0) \) is

\[
b = \sum_{i=0}^{N-1} b_i 2^i.
\]

Theorem 2. When an even \( a \) is perturbed by period \( T \), the periods of low significant bit \( P(x)_0 \) and \( P(x)_1 \) in map (10) are also \( T \).

Proof. In binary numbers, the product of two \( N \)-bit binary numbers are \( 2N \) bits. From map (11), the \( N \)-tuple binary numbers of \( Q(x) \) and \( P(x) \) have the relationship that low significant bit \( P(x)_0 = Q(x)_{N-2} \) and \( P(x)_1 = Q(x)_{N-1} \).

From Lemma 1, \( Q(x) = x(ax + 1) \mod 2^N \) is a one-to-one mapping. For the characteristic of one-to-one mapping, if \( a \) is perturbed by period \( T \), the periods of low significant bit \( P(x)_0 \) and \( P(x)_1 \) in map (10) are also \( T \).

Theorem 3. Suppose the period of \( m_s(n) \) is \( T_s \), and the period of \( m_l(n) \) is \( T_l \). If \( \gcd (T_s, T_l) = 1 \), the periods of low significant bit \( w(n)_0 \) and \( w(n)_1 \) in map (9) are both \( T_s T_l \).

Proof. Since \( 2m_s(n) \mod 2^N \) is the even number in \( [0, 2^N - 1] \), we can always find an even number \( a \) such that \( am'_s(n) = 2m_l(n) \).

From Lemma 1, for a fixed \( m_l(n) \), map (8) is a one-to-one mapping. From Theorem 2, when \( m_s(n) \) is perturbed by period \( T_s \), the periods of low significant bit \( P(x)_0 \) and \( P(x)_1 \) in map (8) are also \( T_s \). Suppose the period of \( m_l(n) \) is \( T_l \) and \( \gcd (T_s, T_l) = 1 \), then the period of \( w(n) \) is \( T_s T_l \). Since map (9) is the equivalent transformation of map (8), the periods of low significant bit \( w(n)_0 \) and \( w(n)_1 \) in the map (9) are both \( T_s T_l \). Under precision \( N \), the period of \( m_s(n) \) is \( 2^N \) and the period of \( m_l(n) \) is \( 2^{N-1} \). The number \( 2^N \) only has a prime factor of 2. Since the number \( 2^{N-1} - 1 \) is odd, it cannot have a prime factor of 2. Therefore, \( \gcd (2^N, 2^{N-1} - 1) = 1 \). The periods of low significant bit \( w(n)_0 \) and \( w(n)_1 \) in the map (9) are both \( 2^N (2^{N-1} - 1) \).

In this paper, the period of proposed digitized chaotic time series can be determined definitively. To the best of the authors’ knowledge, the period of digitized chaotic time series in chaos-based encryption has not been fully considered. In [29], the upper bound period of digitized chaotic time series generated by a digitized logistic map was analyzed in detail. However, the security of the digitized chaotic time series depends on the low bound of the period. The upper bound of the period cannot guarantee the security of the digitized chaotic time series. In chaos-based encryption, it is not secure to use a digitized chaotic time series without knowing how large the period is. For digitized chaotic systems, degeneration of the period cannot be avoided. The period of digitized chaotic time series with encryption ability should be at least greater than \( 2^{64} \) and not have a weak key. The period of pseudorandom sequence with encryption ability, such as a standard stream cipher, is generally greater than \( 2^{128} \). In this paper, when \( N > 64 \), the period of the proposed digitized chaotic time series is larger than \( 2^{128} \).

4.2. Balance Analysis. In a pseudorandom sequence generator, balance is necessary to resist correlation attacks [36]. When
the precision of a digital physical device is \( N \) bits, \( m_s(n) \) is an integer number made up of \( N \) bits, \( m_0(n) \) is an integer number made up of \( (N - 1) \) bits, and \( w(n) \) is an integer number made up of \( N \) bits. Therefore, in the view of binary numbers, the number of input bits in map (9) is equal to \((2N - 1)\) and the number of output bits is equal to \( N \). Then, map (9) can be regarded as a mapping from \( F_2^{2^{2N-1}} \) to \( F_2^N \). For each output bit in map (9), there exists a mapping \( f \) from \((2N - 1)\) input bits to a corresponding output bit. In view of the vector function, \( F_2^{2^{2N-1}} \) is the set of \((2N - 1)\)-tuples in the field \( F_2 \). Then, map (9) can be regarded as a vector function \( F = \{ f_0, f_1, ..., f_{2^N-1} \} \), which is the mapping from \( F_2^{2^{2N-1}} \) to \( F_2^N \). The function \( f_i \) is the mapping from \( F_2^{2^{2N-1}} \) to \( F_2 \) for \( 0 \leq i \leq 2^N - 1 \). For map (9), function \( f_0 \) is the mapping from \( F_2^{2^{2N-1}} \) to \( w(n)_0 \), and function \( f_1 \) is the mapping from \( F_2^{2^{2N-1}} \) to \( w(n)_1 \). A balance function means the numbers of elements 0 and 1 in the output time series are equal. For the properties of the \( m \)-sequence, the inputs \( m_1(n) \) and \( m_0(n) \) are balanced. From Lemma 1, the quadratic map \( Q(x) = x(ax + 1) \bmod 2^N \) is a one-to-one mapping when \( a \) is even. From Theorems 2 and 3, \( w(n)_1 \) and \( w(n)_0 \) in map (9) preserve the properties of one-to-one mapping. Therefore, \( w(n)_1 \) and \( w(n)_0 \) are balanced.

### 4.3. Nonlinearity Complexity Analysis

As a nonlinear function in digital systems, the nonlinearity complexity of the digitized logistic map with introduced perturbation sources should be analyzed. The Walsh cycle transform is a useful tool to analyze the nonlinearity complexity [36]. The Walsh cycle transform is defined as \( WT_f(\alpha) = \sum_{x=0}^{2^N-1} (-1)^{f(x) \cdot \phi_\alpha(x)} \), where \( \phi_\alpha(x) = \alpha_N x_N \cdot \alpha_{N-1} x_{N-1} + \alpha_N x_{N-2} x_{N-3} + ... + \alpha_0 x_0 \). Nonlinearity complexity is a vital indicator used to measure the strength of the cryptosystem to resist linear attack [36]. Suppose \( f(x) : F_2^N \rightarrow F_2 \) then the nonlinearity complexity of function \( f(x) \) is

\[
N(f) = 2^{2N-1} \left( 1 - \frac{1}{2^N} \max_{w \in F_2^N} |S_f(w)| \right)
\]  

(12)

For the Walsh cycle transform, the computational complexity of computing the Walsh spectrum is \( \bigO(N2^N) \), which increases exponentially with input bits \( N \). Therefore, it is difficult to compute the nonlinearity complexity of map (9) under large bits \( N \). The nonlinearity complexity of functions \( f_0 \) and \( f_1 \) when \( N = 4, 5, ..., 12 \) is shown in Table 2.

If the precision of a digital physical device is \( N \) bits, then \( m_s(n) \) is \( N \) bits, \( m_0(n) \) is \( (N - 1) \) bits, and all input bits in map (9) are \((2N - 1)\) bits. Although we cannot compute the nonlinearity complexity with high precision, the nonlinearity complexity of functions \( f_0 \) and \( f_1 \) increases exponentially with precision \( N \). For large precision \( N \), the nonlinearity complexity of functions \( f_0 \) and \( f_1 \) is very large.

### 4.4. Security Randomness Analysis

Cryptographic security is the most important characteristic of the randomness pseudorandom sequence. A pseudorandom sequence that can be used to encrypt information must prove cryptographic security. However, the existing information encryption based on chaotic systems does not give the cryptographic security of digitized chaotic time series in mathematical terms. The concept of cryptographic security is that the security of a cipher should rely on the secrecy of the initial key only. With this fundamental premise, there are only three methods of proving cryptographic security [37]:

1. **Unconditional security.** A cryptosystem is unconditionally secure if it cannot be broken, even with infinite computational resources.

2. **Computational security.** A cryptosystem is computationally secure if the best known algorithm for breaking it requires at least \( N \) operations, where \( N \) is some specified very large number.

3. **Provable security.** A cryptosystem is provably secure if it is as difficult to break as solving some well-known and supposedly difficult, such as subset sum problem, traveling salesman problem, integer factorization, and so on.

In this paper, the cryptographic security of the proposed chaotic pseudorandom generator is proved by provable security, and the secure proof is based on integer factorization problem.

**Theorem 4.** The outputs of the digitized chaotic time series \( w(0), w(1), ..., w(n) \) and \((w(0)_0, w(1)_0, ..., w(n)_0) \) have secure randomness.

**Proof.** Secure randomness is equal to unpredictability [38]. Suppose we can efficiently generate a reverse direction digitized chaotic time series from \((w(n)_0, w(n)_1) \) and from \((w(n)_1, w(n-1)_0) \) to \((w(n-1)_0, w(n-1)_1) \). Let \( D(n) = m_s(n) m_0(n) || 1 \), where \( D(n) \) is a \( 2N \)-bit integer. First, from the known bits \((w(n)_0, w(n)_1) \), we must determine the complete integer \( D(n) \). Since \( D(n) \) is a \( 2N \)-bit integer, there are \( 2^{2N-2} \) different combinations to reconstruct it. Then, integer \( D(n) \) needs to be factorized into the specific multiplication form \( m_s(n) m_0(n) || 1 \) to recover the initial key \( m_s(n) \) and \( m_0(n) \) to predict the reverse direction digitized chaotic time series \((w(n-1)_0, w(n-1)_1) \). However, integer factorization is an NP problem [39]. It is difficult to factorize integer \( D(n) \) into the product of \( m_s(n) \) and \( m_0(n) || 1 \). Therefore, the outputs of digitized chaotic time series \((w(0)_0, w(1)_0, ..., w(n)_0) \) are unpredictable.

<table>
<thead>
<tr>
<th>Precision</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input bits</td>
<td>7</td>
<td>9</td>
<td>11</td>
<td>13</td>
<td>15</td>
<td>17</td>
<td>19</td>
<td>21</td>
<td>23</td>
</tr>
<tr>
<td>( f_1 )</td>
<td>48</td>
<td>192</td>
<td>864</td>
<td>3680</td>
<td>15264</td>
<td>62496</td>
<td>254496</td>
<td>1029792</td>
<td>4147168</td>
</tr>
<tr>
<td>( f_0 )</td>
<td>32</td>
<td>192</td>
<td>768</td>
<td>3456</td>
<td>13104</td>
<td>61056</td>
<td>249984</td>
<td>1017984</td>
<td>4119168</td>
</tr>
</tbody>
</table>

**Table 2: Nonlinearity complexity of functions \( f_1 \) and \( f_0 \).**
The NIST test suite, a method of measuring randomness, is published by US National Institute of Standards and Technology [40]. It focuses on many kinds of molds of nonrandomness regarding sequence. It includes many approximate independent statistical tests, such as linear complexity, approximate entropy, and so on. In statistics, approximate entropy is a technique used to quantify the amount of regularity and unpredictability of fluctuations over time series data. The main idea of approximate entropy is to use a nonnegative value to quantify the complexity and irregularity of the time series, and the value increases with increased sequence complexity [41–43]. Table 3 shows the results of the NIST test regarding the P-values of the digitized chaotic time series from map (9) when N = 12.

If the P-value for a test is determined to be equal to 1, then the sequence appears to have perfect randomness, and a P-value less than 0.01 indicates that the sequence appears to be completely nonrandom. From Table 3, we can see that the digitized chaotic time series have good random characteristics. However, it should be noted that the NIST test suite is a statistical analysis. Many information encryption schemes based on chaotic systems use the NIST test suite as the only pseudorandom sequence generator. However, the NIST test suite is local statistical testing and cannot guarantee that all random sequences have great randomness. The documentation of the NIST test suite states: “These tests may be useful as a first step in determining whether or not a generator is suitable for a particular cryptographic application. However, no set of statistical tests can absolutely certify a generator as appropriate for usage in a particular application, i.e., statistical testing cannot serve as a substitute for cryptanalysis” [40]. Thus, the NIST test suite cannot provide complete security of a pseudorandom sequence.

<table>
<thead>
<tr>
<th>Test</th>
<th>(P(w(n)_i, N = 12))</th>
<th>(P(w(n)_o, N = 12))</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency</td>
<td>1.000000</td>
<td>1.000000</td>
</tr>
<tr>
<td>Block frequency (BL = 128)</td>
<td>0.596179</td>
<td>0.805613</td>
</tr>
<tr>
<td>Cumulative sums</td>
<td>0.846848</td>
<td>0.861024</td>
</tr>
<tr>
<td>Runs</td>
<td>0.905980</td>
<td>0.397491</td>
</tr>
<tr>
<td>Longest run</td>
<td>0.942394</td>
<td>0.873752</td>
</tr>
<tr>
<td>Rank</td>
<td>0.412787</td>
<td>0.681544</td>
</tr>
<tr>
<td>FFT</td>
<td>0.927277</td>
<td>0.065952</td>
</tr>
<tr>
<td>Nonoverlapping template (BL = 9)</td>
<td>147/147</td>
<td>147/148</td>
</tr>
<tr>
<td>Overlapping template (BL = 9)</td>
<td>0.075027</td>
<td>0.851665</td>
</tr>
<tr>
<td>Universal</td>
<td>0.585344</td>
<td>0.080354</td>
</tr>
<tr>
<td>Approximate entropy (BL = 10)</td>
<td>0.794921</td>
<td>0.143161</td>
</tr>
<tr>
<td>Random excursions variant</td>
<td>8/8</td>
<td>8/8</td>
</tr>
<tr>
<td>Serial (BL = 16)</td>
<td>0.455423</td>
<td>0.516985</td>
</tr>
<tr>
<td>Linear complexity (BL = 500)</td>
<td>0.648535</td>
<td>0.203704</td>
</tr>
</tbody>
</table>

It is proved that the simple multiplication is hard to invert. The function of inverting the multiplication \(x = ab \in F_2^N\) \((x \in \{0, 1\}^N)\) into \(N/2\)-bit multiplier number \(a\) and \(N/2\)-bit multiplicand number \(b\) is believed to be one-way. Inverting simple multiplications is known as the integer factorization problem [39].

Definition 3. Let \(G : \{0, 1\}^n \rightarrow \{0, 1\}^n\) be a polynomial-time computable function. Let \(\ell : \mathbb{N} \rightarrow \mathbb{N}\) be a polynomial-time computable function such that \(\ell(n) > n\) for every \(n\). We say that \(G\) is a secure pseudorandom generator of stretch \(\ell(n)\) if \(G(x) = \ell(|x|)\) for every \(x \in \{0, 1\}^*\) and for every probabilistic polynomial-time \(A\) there exists a negligible function \(\epsilon : \mathbb{N} \rightarrow [0, 1]\) such that

\[
\Pr_{x \in \{0, 1\}^n, y \leftarrow f(x)} \left[A(G(x)) = 1\right] - \Pr_{U \leftarrow \mathbb{U}_{\ell(n)}} \left[A(U_{\ell(n)}) = 1\right] < \epsilon(n) \tag{14}
\]

for every \(n \in \mathbb{N}\).

Theorem 5. Map (9) is a secure pseudorandom generator that can be used to encrypt information.

Proof. From map (9), we can see that output \(w(n)\) is the multiplication of integer \(m_1(n)\) and integer \(\langle m_1(n)\rangle\). Therefore, inverting map (9) is the integer factorization problem, and it is a one-way function. If one-way functions exist, then for every \(\epsilon \in \mathbb{N}\) there exists a secure pseudorandom generator with stretch \(\ell(n) = n'\) [44].

The secure pseudorandom sequence generator BBS is also based on the integer factorization problem [45], which is a
4.5. Key Space Analysis. It is proved that the $2^{100}$ key space is sufficiently large to resist attacks by existing computers [46]. Therefore, the precision length $N$ need only be greater than 34 for map (9). The key space of map (9) is $2^{2^{N}-1}$.

5. Conclusions
In this paper, a new method that enhances the period of digitized chaotic time series based on a digitalized logistic map with introduced perturbation sources is proposed. Experimental implementation shows that, under precision $u_1D441$, the period of digitized chaotic time series in this paper is $2^{u_1D441}(2^{u_1D441}-1)$. Through some security analysis, the digitized chaotic time series is strictly balanced and has large nonlinearity complexity, linear complexity, and approximate entropy. Through secure randomness analysis, the proposed digitized logistic map is a secure pseudorandom generator for information encryption.

Appendix
In Table 4, the number $N$ is the length of precision, $iv$ is the number of initial value, $M$ is the period of M-sequence, $m$ is the period of m-sequence, $T$ is the appen period of the sequence generated by digital Logistic map with an initial value, $k$ means $k$ different initial values lead to the same period $T$, $T_{max}$ is the maximum period sequence generated by digital Logistic map. For example, when $N = 15$, there are 32768 initial values, 44 of them lead to period-1 sequences, 46 of them lead to period-6 sequences, 56 of them lead to period-9 sequences, 6770 of them lead to period-20 sequences, 14398 of them lead to period-91 sequences, 11454 of them lead to period-127 sequences. Through statistical analyses on the sequences with the same period and precision, all the sequences with maximum period is the same or just in different phases. In addition to the maximum period sequence, there are a small amount of different sequences with other same period and precision, and these different sequences period is too small. From Table 4, $M$ and $m$ increase as the increasing of $N$ exponentially. But the behavior of $T_{max}$ is more complex than $M$ and $m$ as the increasing of $N$. Although $T_{max}$ is gradually increased in general, some local scopes are on the decline as the increasing of $N$. For example, when $N = 15$, $T_{max} = 127$, and when $N = 16$, $T_{max} = 119$.

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

Conflicts of Interest
The authors declare that they have no conflicts of interest.
**Acknowledgments**

This work is supported financially by the National Natural Science Foundation of China (No. 61571181).

**References**


