Application of Chaotic Encryption Algorithm Based on Variable Parameters in RFID Security

Yi Guo
Center for Information Technology, Xi'an Technological University

Jianfang Yang
School of Computing Science & Engineering, Xi'an Technological University

Baolong Liu (liubaolongsin@126.com)
Xi’an Technological University

Research

Keywords: RFID system, segmented Logistic mapping, security mechanism, chaotic encryption algorithm

Posted Date: January 7th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-64820/v2

Version of Record: A version of this preprint was published at EURASIP Journal on Wireless Communications and Networking on July 14th, 2021. See the published version at https://doi.org/10.1186/s13638-021-02023-0.

Application of Chaotic Encryption Algorithm Based on Variable Parameters in RFID Security

Yi Guo[1], Jianfang Yang[2], Baolong Liu[*2]

(1 Centre for Information Technology, Xi'an Technological University)
(2 School of Computing Science & Engineering, Xi'an Technological University)

[*]Corresponding author, E-mail: liubaolongsin@126.com

Abstract: *In recent years, chaotic encryption has been applied in the field of cryptography by virtue of its unique characteristics, and it has received more and more attention in the security of RFID data transmission. Using the same key for encryption and decryption operations is a lightweight encryption algorithm. However, there are various problems in the application process of chaotic encryption: (1) nonlinear dynamic characteristics degradation and short-cycle cycle problems will occur under the influence of computer limited accuracy; (2) numerical conversion operations are required during application, to a certain extent It will affect the randomness of the iterative sequence; (3) During the iterative process, the iterative sequence cannot be spread over the entire value interval, and the randomness is poor. This paper proposes an improved segmented Logistic mapping encryption algorithm, uses the m-sequence to perturb initial value and sets a fixed step to change the control parameter value to generate a chaotic key stream sequence, and applies it to the RFID system data transmission security mechanism to encrypt the data. Experimental simulation and performance analysis show that the iterated chaotic sequence has good random distribution characteristics, unpredictability and traversability. Compared to the previous improvement, the key space is increased to reach the size of 10^{24} space and can meet the security needs, which improve RFID data security and can effectively avoid various security problems.*

Keywords: *RFID system; segmented Logistic mapping; security mechanism; chaotic encryption algorithm*

1 Introduction

RFID technology is a non-contact automatic identification technology using wireless radio frequency signals. It mainly uses inductive coupling and electromagnetic coupling to automatically identify surrounding identifiers. The process from searching for a target object using radio frequency signals to obtain relevant data information is done automatically, with no auxiliary equipment to intervene. The RFID system is mainly composed of a tag, a reader, and an information system [1]. Compared with other traditional automatic identification technologies, such as barcode identification, biometric identification, and magnetic stripe identification, RFID technology has a small size, low cost, and information storage. The advantages of large volume, long service life, high security, and rewrite ability have broad practical value in industrial automation, commercial automation, logistics management, medical health, and security inspection [2].

As an important way of information perception, RFID has a very important role in the application of the Internet of Things. However, due to the security problems brought about by the non-contact sensing of RFID systems, it has largely prevented the further development of RFID technology in applications. Data transmission seriously threatens the security and confidentiality of RFID data. With the rapid development of the Internet of Things, if the RFID security is not properly protected, it will easily lead to sensitive data leakage and the risk of various types of attacks, resulting in great economic losses. Therefore, the secure interaction of information and data has become a major problem that has to be faced. At present, the data transmission security of RFID has become a hot research direction of RFID.

At present, the problems of RFID have always been the biggest obstacle affecting and restricting the development of RFID in the Internet of Things, and have become a research topic of increasing concern. The problems that RFID needs to solve can be roughly summarized into the following aspects: (1) security certification and privacy protection issues; (2) anti-collision problems of readers and tags; (3) stable and accurate identification of target positions; (4) a large number Data storage issues; (5) Cost control issues. This article mainly discusses the wireless channel security problem that occurs in the information interaction between the reader and the tag. The transmitted data information is often exposed to the outside, and it is vulnerable to risks such as illegal eavesdropping, tampering, counterfeit attacks, privacy data leakage, and location tracking [3].

Chaos is a phenomenon appearing in deterministic systems that exhibits inherent randomness. It seems to be disordered, but has a complex ordered structure inside [4]. Chaotic systems have characteristics such as initial value-dependent dependency, unpredictability, pseudo-randomness, and ergodic properties. These characteristics make chaotic systems very suitable for encrypting and processing data information to achieve the purpose of chaos and diffusion. Iterative and initial conditions are achieved through chaotic mapping. And the encryption rules can get a key stream sequence for encrypting plaintext information.

At present, chaotic mapping in RFID security research is mainly used to encrypt data information and design security authentication protocols. Many researchers are based on the problems of chaotic mapping, and have adopted many improvements to improve chaotic performance, thereby improving data security. For example: (1) Use the segmented Logistic chaotic mapping iterative equations instead of the original Logistic chaotic mapping iterative equations [5-7]. Experiments have found that the segmented mapping can enter the chaotic state faster and more stable, and control when it is in the chaotic state. The parameter's desirable interval is larger; (2) The initial value and control parameters are continuously changed during the iteration process to change the process of each iteration [3,8-10]. The long-period behavior equation and m-sequence are used to disturb the initial value. A chaotic map or set a fixed step to change the value of the control parameter to solve the problem of single control parameter value and poor randomness of the sequence; (3) Hyperchaotic maps have good randomness and complexity. Hyperchaos maps are used to replace the traditional one. Dimensional Logistic mapping [11, 12]; (4) cascade operation of chaotic mapping, superimposing iterative sequences generated by two or more chaotic mappings [13-15], this scheme has a large amount of calculation and high complexity.

In this paper, based on the use of segmented Logistic map instead of traditional one-dimensional Logistic map, the chaotic map is improved by using the m-sequence perturbation initial value and the scheme of setting a fixed step to change the control parameter value. The m-sequence is shifted by linear feedback according to the encryption characteristics the register calculates that the change of the control parameter is calculated by the parameter change algorithm. Each iteration changes the control parameter to a different value. The purpose is to avoid the problem of single parameter value and small key space. Finally, through algorithm simulation and performance analysis to compare the relevant characteristics of the chaotic sequence before and after improvement achieve its application to the security mechanism of RFID.

This paper first analyzes and points out the problem of chaotic mapping. On this basis, an improved segmented Logistics mapping is proposed, and the improved algorithm is experimentally analyzed and applied to the RFID security mechanism. In this process, we refer to a large number of literature and research ideas, including doctoral dissertations, master's thesis and conference journal papers, focusing on the method of m-sequence disturbance initial value in the improved algorithm and the change process of control parameters in each iteration, and then The improved chaotic map is compared with the chaotic map that has been proposed in terms of the characteristics of the chaotic map. It mainly includes the sensitivity dependence analysis of the initial value, the comparison of the Lyapunov exponent, the random distribution comparison of the chaotic sequence, and the periodic analysis. When comparing the mapping, the control variable method is mainly used to compare and analyze, discussing the feasibility and safety of the improved chaotic mapping.

2 Chaos Mapping Analysis and Problems

Before applying chaotic mapping to RFID security, it is necessary to discuss its theory and the problems that arise in the process of use. On this basis, the problems that arise will be improved to meet the security requirements.

2.1 Traditional Logistic Mapping Analysis

Logistic mapping, as the most important research content in current chaotic systems, is often used in the field of information encryption. Generally speaking, the research on data encryption is based on the traditional Logistic mapping. The traditional Logistic mapping is a simple chaos. Mapping, in the ideal case, can produce complex chaotic behavior and is deterministic. Its mathematical expression is as follows:

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

In order to understand the relevant characteristics of Logistic mapping in detail, MATLAB software simulation is used. When the initial value x is 0.2 and the number of iterations n is 500, the logistic map bifurcation diagram is shown in the figure below. When the control parameters are changed within a certain range, complex nonlinear dynamic behavior can be generated. When the parameter value range is (3.5699, 4] and the iteration value is within (0, 1), the Logistic map is in a chaotic state.

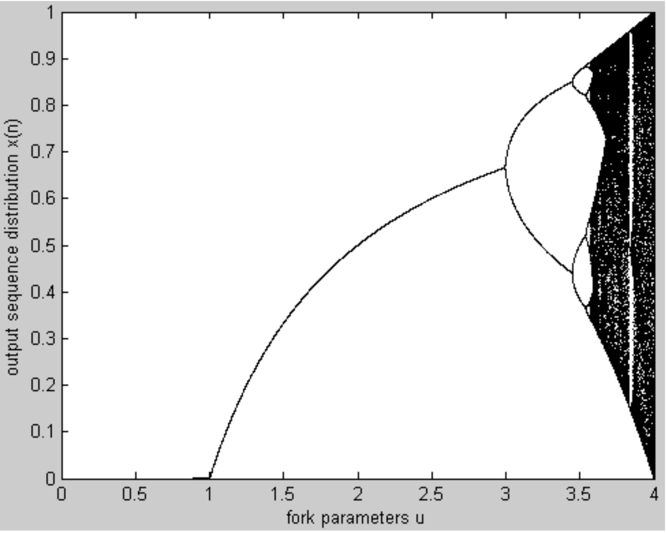


Fig 1 Traditional Logistic mapping bifurcation

Figure 1 show that when the control parameter is less than 4, the iterated value cannot be spread over the entire value interval [0, 1], only when the control parameter is equal to 4, the iteration sequence generated is spread over the [0, 1] interval Inside. Here is the distribution of the sequence of the traditional Logistic map with the control parameter μ equal to 3.9 and the number of iterations n equal to 1000 as shown in the Figure2. In the entire value range, if these problems are not improved well, it will inevitably have a certain impact on the encryption effect and performance.

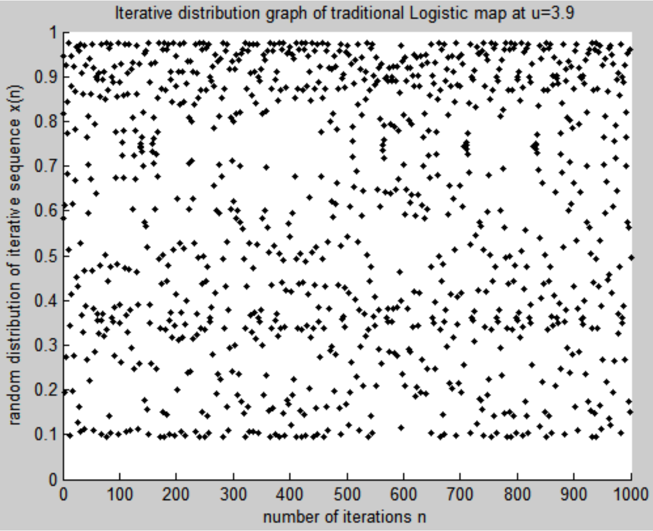


Fig 2 Iterative distribution graph with the control parameter 3.9

2.2 Problems of Chaotic Encryption

When applying Logistic mapping to data encryption, there will be some problems that need to be improved. These problems will affect the encryption effect, and are listed as the following aspects:

Due to the limited precision effect of the computer, when the chaotic encryption algorithm is applied in the RFID system, the mapping sequence period will be shortened [10], the dynamic characteristics will be sharply degraded and the generated trajectory distribution will be less different, which will affect the encryption strength and thus affect Information security of RFID system.

The application of chaotic encryption algorithm to RFID security has the problem of domain conversion. RFID data is expressed in binary domain in computer system storage, and the iterative numerical sequence of chaotic system is real domain value [16]. This requires a conversion mechanism between the binary and real domains. The conversion mechanism will affect the randomness of the iterative sequence to a certain extent.

When the value of the control parameter changes in the logistic map, the iteration value cannot be randomly distributed in the entire value interval, and which will affect the generated iteration sequence to a certain extent, and thus affect the effect of the key stream sequence using for encryption.

Before the improvement of chaotic mapping, if the same control parameters are used throughout the iteration process, there will be a problem that the control parameter has a single value and cannot obtain a good random performance chaotic sequence, which makes the iterated sequence less random, which will affect data encryption performance.

When Logistic mapping is applied to information encryption, due to the influence of the computer's limited precision effect, the encryption effect is not ideal and needs to be improved. This paper is mainly concerned with the security problems that occur during the transmission of RFID data to prevent the security risks faced by RFID data. The key stream sequence generated by the improved Logistic chaotic mapping is used to encrypt the RFID data to protect the RFID data during the transmission process. The improved chaotic encryption algorithm is to encrypt the generated key stream sequence and the plaintext information stream. The ciphertext information obtained is similar to the white noise sequence and has a good encryption effect.

3 Improved Algorithm Based on Segmented Logistic Mapping

In order to improve the various problems in the one-dimensional Logistic mapping mentioned above, this paper is based on the research of segmented Logistic mapping, and combines the initial value change and the control parameter change scheme in the iterative process to improve the segmented Logistic mapping. Under the influence of the finite precision effect of the computer, the nonlinear dynamic characteristic degradation problem and the short-cycle problem can be effectively controlled.

3.1 Segmented Logistic Mapping

For the chaotic sequence iterated by the traditional one-dimensional Logistic mapping cannot be randomly and uniformly distributed throughout the value interval, a segmented logistic mapping is used instead of the traditional one-dimensional Logistic mapping. Its mathematical expression is [17]:

$$x_{n+1} = \begin{cases} 4\mu(0.25 - x_n)^2, x_n \in (0,0.5] \\ 1 - 4\mu(0.75 - x_n)^2, x_n \in (0.5,1) \end{cases}$$

Among, $\mu \in (0,4]$, n is the number of iterations, $n = 0,1,2,\cdots$, $x_n \in (0,1)$.

In order to further understand the relevant characteristics of this segmented logistic mapping, analyze the value interval and distribution when it is in a chaotic state, use MATLAB software to simulate the experiment, and set it to generate when the initial value is $x_0 = 0.2$ and the number of iterations is 500. The bifurcation diagram of the iterative value distribution with the control parameters is shown in Figure 3.

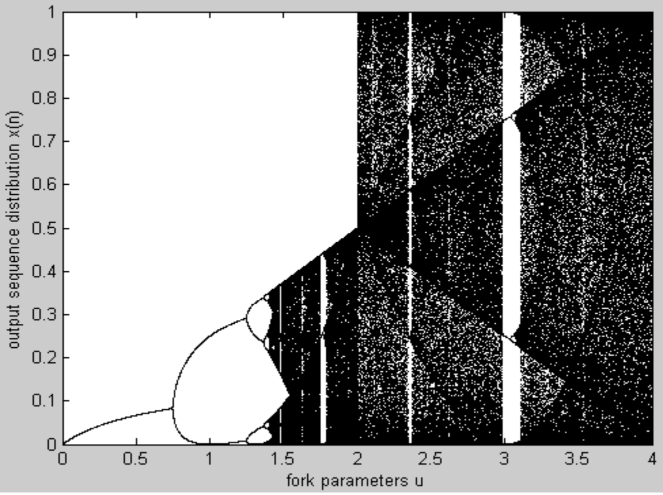


Fig 3 Bifurcation diagram of segmented Logistic mapping

It can be seen from the Figure 3 that when the control parameter $\mu > 1.42$, the segmented Logistic mapping begins to enter the chaotic state, but the chaotic sequences generated when the control parameter is in the range of $\forall \mu \in (2.01,2.98) \cup (3.11,4]$ and can all be in the interval $x \in [0,1]$. The injective state is reached within and the ergodicity is consistently satisfied. Therefore, in order to iterate the chaotic sequence to achieve better performance, the value of the control parameter is $(2.01, 2.98) \cup (3.11, 4]$.

From this analysis, it can be concluded that the segmental Logistic chaotic map satisfies the parameter μ corresponding to the interval traversal of [0, 1], and the range of the desirable interval of the parameter u is larger than that of the traditional Logistic chaotic map. In addition, the segmented Logistic map enters the chaotic state after that, no matter the control parameter takes any value, the iteration sequence can be spread over the entire value interval, and the ergodicity is better.

3.2 Changes in Initial Value

Under the influence of the digital environment, part of the track sequence will enter a short cycle loop sequence, which will seriously affect the encryption efficiency and quality when applied to encryption. It is proposed that the initial value change is based on the extreme sensitivity of the Logistic mapping system to the initial conditions [18]. The initial conditions are constantly changed to increase the periodic change of the chaotic mapping, which makes the motion trajectory more complicated. If the value has been changed, the motion trajectory also changed. Although the iteration value will partially overlap in this case, it will not fall into the loop. Here, an m-sequence with a long period property is used as an effective method to disturb the change of the initial value.

The m-sequence is the abbreviation of the longest linear feedback shift register sequence. The linear feedback shift register LFSR is used to generate the m-sequence. Its characteristic polynomial is:

$$f(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_n x^n = \sum_{i=0}^{n} c_i x^i$$

The original polynomial needs to be obtained before generating the m sequence. The primitive polynomial is the premise of generating the m sequence. It is defined as [19]:

(1) $f(\mathrm{x})$ cannot be factored, and polynomials can no longer be factored;

(2) $f(\mathrm{x})$ divisible by $\mathrm{x}^m + 1$, where $m = 2^n - 1$;

(3) $f(\mathrm{x})$ is not divisible by $\mathrm{x}^q + 1$, $q < m$;

Where $f(\mathrm{x})$ is the LFSR characteristic polynomial. The polynomial generated when the above conditions are true is the original polynomial. At this time, the original polynomial is an irreducible polynomial of order $2^{\mathrm{n}} - 1$, which is an m sequence with a maximum period of $2^{\mathrm{n}} - 1$. In addition, m sequence is the sequence of expression coefficients obtained by $1/f(\mathrm{x})$ long division.

The m sequence $\{a_i\}$ obtained from the above process is XOR with the initial value x_0 to obtain $x_0^{'}$, and $x_0^{'}$ is converted into a real number and substituted into the segmented Logistic mapping iterative equation for n times, and the obtained value is recorded as x_n .In this way, the initial value of each round is changed.

3.3 Control Parameter Changes

In order to deal with the problem of single control parameter value and small key space, to obtain a chaotic sequence with good random performance, the method of setting the control parameter change step size is used to change the value of the control parameter at each iteration, and a fixed step size method is used to The control parameters are changed slightly, so that the control parameters take different values during each iteration to generate iterative data. The result of the iteration basically maintains unrelated characteristics with the previous iteration. The generated data is random within the range of the interval distributed.

When the control parameter $\mu \in (2.01,2.98) \cup (3.11,4)$, the segmented Logistic mapping is in a chaotic state. During the change of the control parameter value, there are mainly three cases. When $\mu > 4$, the value range is exceeded. Therefore, the control parameter value is cycled to the beginning of the value When $2.98 < \mu < 3.11$, the value of the control parameter is in the window period, and the window period is not in a chaotic state, so the operation here directly assigns the value to $\mu = 3.11$, when the control parameter is less than the minimum value of the control parameter Assign directly to the minimum value m.

Here you need to set the control parameter change step to change the value of the control parameter. The specific pseudo code of the algorithm is as follows:

```
initialization    $x = x_0, \mu = \mu_0, \mathrm{m} \in (2.01, 2.01 + s), s = \frac{4-2.01}{n}$
while(condition<n){
    $\mu = \mu + s$;
If( $\mu > 4$ ) then
    $\mu = \mu - (4 - \mathrm{m})$;
end if
If( $2.98 < \mu < 3.11$ ) then
    $\mu = 3.11$;
end if
If( $\mu < m$ ) then
    $\mu = m$;
end if
}
```

Among, $x_0 \in (0,1)$, $\mu_0 \in (2.01, 2.98) \cup (3.11, 4)$ are the initial values and initial control parameters of the segmented Logistic map, $s = \frac{4-2.01}{n}$ is the step size of the control parameters, n is the number of iterations of the chaotic map, and $m \in (2.01, 2.01 + s)$ is the minimum value of the control parameters.

The control parameters are given different values during the iteration process, which solves the problem of a single value in each iteration. At the same time, the initial value is also dynamically changed during the iteration process, which reduces the impact of the computer's finite precision effect and short cycle Problem, expanding the key space.

3.4 Improved Algorithm Description

Based on the above discussion, this paper proposes an improved chaotic encryption algorithm, which uses a variable initial value and control parameters to iterate the chaotic sequence, which enhances the security and confidentiality of the algorithm. The corresponding encryption key is $Key(\mathrm{N}, \mathrm{i}, \mathrm{n}, \mathrm{s}, \mathrm{m})$ and contains The order of the m-sequence is N , the starting position i after the decimal point, the number of system iterations n , the control parameter change step s , and the minimum control parameter m , its structural model diagram and algorithm flow are shown in Figure 4 and Figure 5.

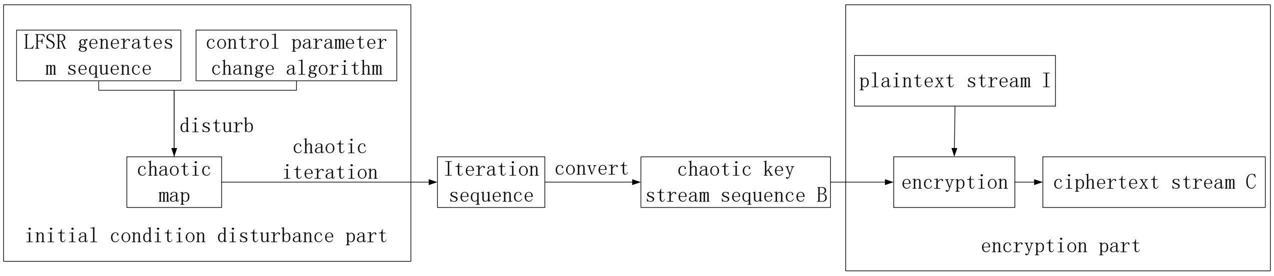

LFSR generates m sequence
control parameter change algorithm
disturb
chaotic map
chaotic iteration
initial condition disturbance part
Iteration sequence
convert
chaotic key stream sequence B
plaintext stream I
encryption
ciphertext stream C
encryption part

Fig 4 Structural model of the improved algorithm

Determine the initial value x_0, the control parameter μ_0, and the encryption key $Key(\mathrm{N,i,n,s,m})$, get $x_0^{'}$ by perturbation of x_0, change the small step size of the control parameter to $\mu = \mu + s$, substitute the value of $x_0^{'}$ and change the parameter into the mapping expression, and iterate n times to get x_n; Take the 3 consecutive digits after the i decimal point of x_n, convert the real value x_n to the integer value M, and take the remainder of M to 256 to convert to the chaotic encrypted byte B_k in binary form; finally, the chaotic encrypted byte and The XOR encryption operation of the plaintext information bytes yields the ciphertext bytes. Determine if the encryption is complete, if not, continue.

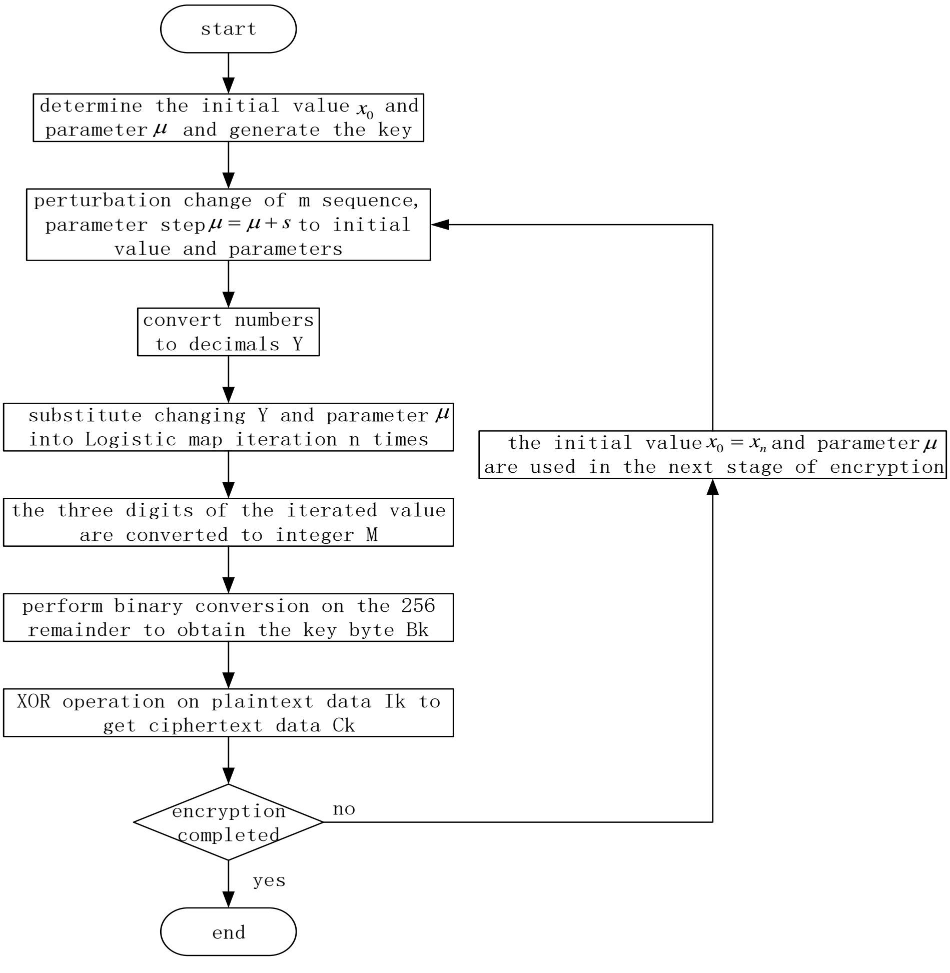

start
determine the initial value x_0 and parameter μ and generate the key
perturbation change of m sequence, parameter step $\mu=\mu+s$ to initial value and parameters
convert numbers to decimals Y
substitute changing Y and parameter μ into Logistic map iteration n times
the three digits of the iterated value are converted to integer M
perform binary conversion on the 256 remainder to obtain the key byte Bk
XOR operation on plaintext data Ik to get ciphertext data Ck
encryption completed
no
yes
end
the initial value $x_0=x_n$ and parameter μ are used in the next stage of encryption

Fig 5 Improved algorithm operation flowchart

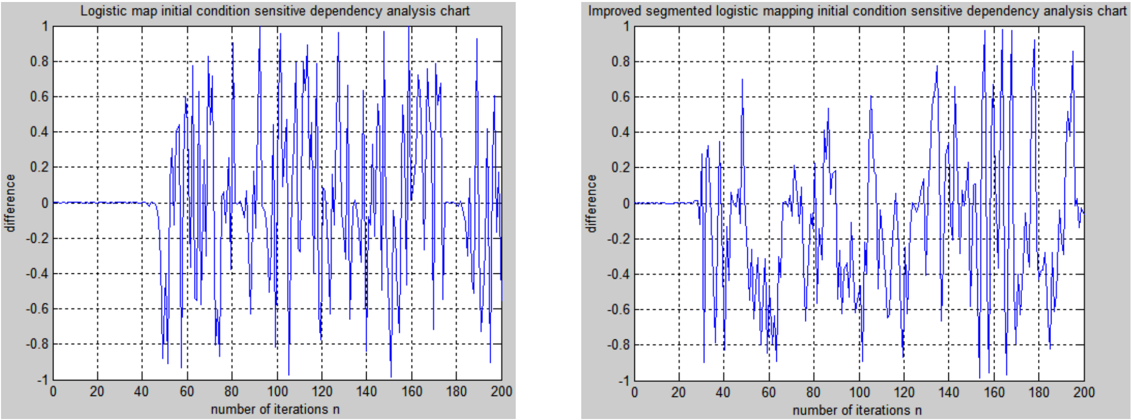
This improved algorithm has higher security than the previous chaotic encryption algorithm. The changes in the initial value and control parameters make the generated key stream sequence more random and unpredictable, increasing the key space and enhancing the confidentiality of the algorithm.

4 Results and Discussion

The algorithm simulation and performance analysis are important indicators to consider whether it meets the requirements. This paper uses MATLAB software and the method of theoretical analysis of data. The experimental conditions and specific settings are: MATLAB software, select the serial number on the label and generate it by the reader The random numbers are used as the initial value x_0 and the value of the control parameter μ , expressed in 16-bit binary form, set the number of iterations n =1000, the parameter change step size s is 0.002, the parameter minimum value $m \in (2.01,2.012)$, the starting bit after the decimal point i = 3 , The order $N = 2^{16} - 1$.

4.1 Initial Condition Sensitive Dependency Simulation

Initial value sensitive dependency analysis refers to the phenomenon that the chaotic sequence is extremely different when the initial value changes slightly. When the initial values are x0 = 0.656991000000000 and x1 = 0.656991000000001, the chaotic sequence iterations of the traditional logistic map and the improved segmented logistic map are shown in Figure 6.



(a) Traditional logistic mapping (b) Improved segmented logistic mapping

Fig 6 Logistic mapping under small initial value changes

It can be drawn from the Figure 6: 1) When the other conditions are consistent, the difference between the initial values of the two small differences (10^{-15}) is larger and larger with the increase of the number of iterations, and the improved segmented Logistic map is separated from the traditional Logistic map. Faster; 2) The improved segmented Logistic map has a stronger dependence on initial conditions than the traditional Logistic map, and its performance is more sensitive.

4.2 Lyapunov Exponent Simulation

Through the given calculation method, the Lyapunov exponent of the traditional one-dimensional logistic map and the segmented logistic map can be obtained [20]. The calculation result is:

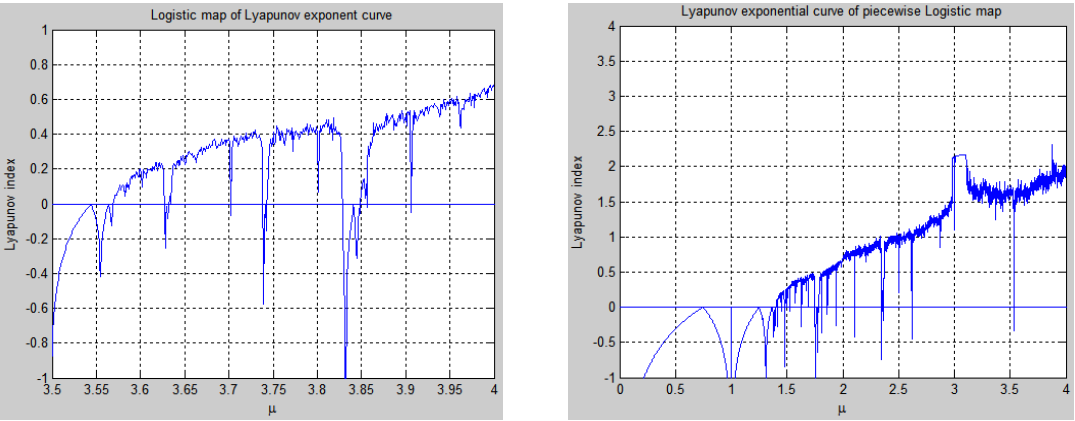
Traditional one-dimensional logistic mapping:

$$\lambda = \lim_{n \to \infty} \frac{1}{n} \sum_{i=1}^{n} \ln\left|\mu(1-2x_i)\right|$$

Segmented logistic mapping:

$$\lambda = \begin{cases} \lim\limits_{n\to\infty}\frac{1}{n}\sum\limits_{i=1}^{n}\ln\left|8\mu(x_i-0.25)\right|, x_i\in(0,0.5] \\ \lim\limits_{n\to\infty}\frac{1}{n}\sum\limits_{i=1}^{n}\ln\left|8\mu(0.75-x_i)\right|, x_i\in(0.5,1) \end{cases}$$

The curve analysis results of the Lyapunov exponent under different control parameters under the same conditions are shown in Figure 7.



(a) Traditional logistic mapping (b) Segmented logistic mapping

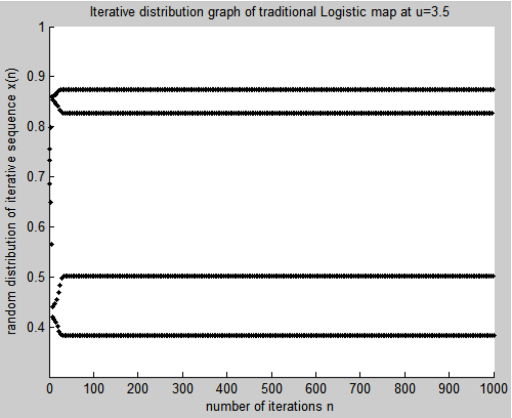
Fig 7 Lyapunov index analysis diagram

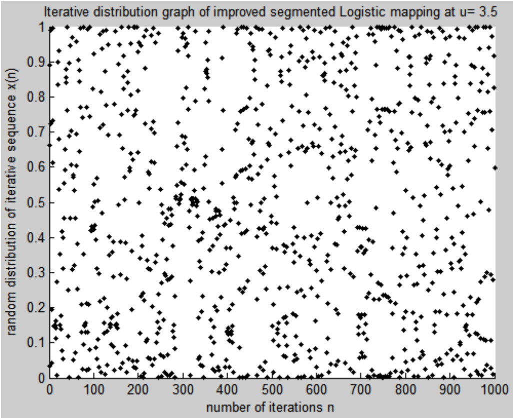
It can be seen from the above figure: 1) The segmented logistic map enters the chaotic state when the parameter is equal to 1.42, the control parameter value interval is relatively larger, plus the desirable interval when the full shot state is reached, the density is increased to a certain extent key space; 2) The segmented logistic map increases with the increase of control parameters, the Lyapunov exponent increases more obviously, and there are fewer periodic bifurcations and better stability.

4.3 Simulation of Random Distribution of Chaotic Sequence

In order to get a clearer understanding of the random distribution and related characteristics of the chaotic sequence iterated by the improved Logistic map, while keeping the number of iterations constant, we now compare the traditional Logistic map and the improved score when taking different values from the control parameters. The distribution of the segment Logistic map is shown in Figure 8.

When the control parameter $\mu = 3.5$ and the number of iterations n = 1000:

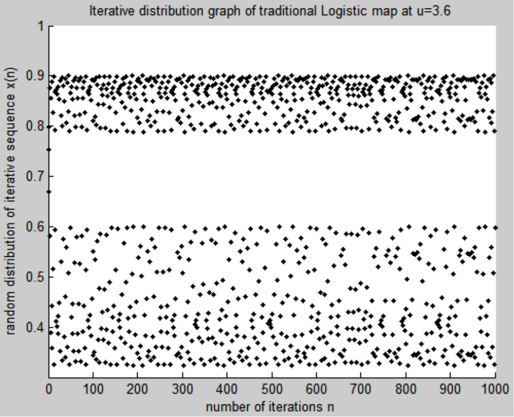


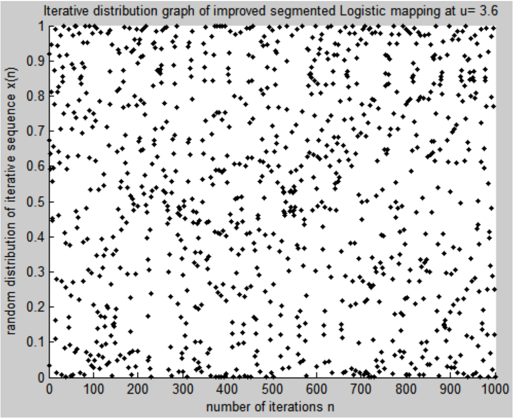


(a) Traditional logistic mapping

(b) Segmented logistic mapping

When the control parameter $\mu = 3.6$ and the number of iterations n = 1000:

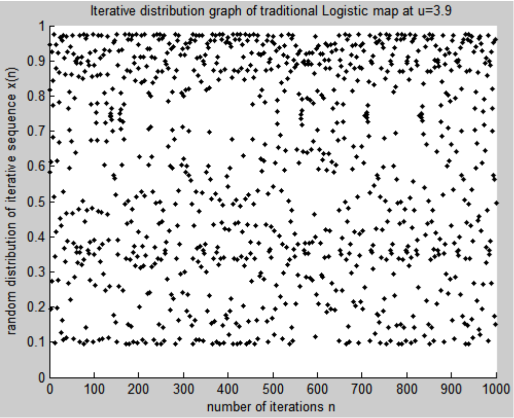


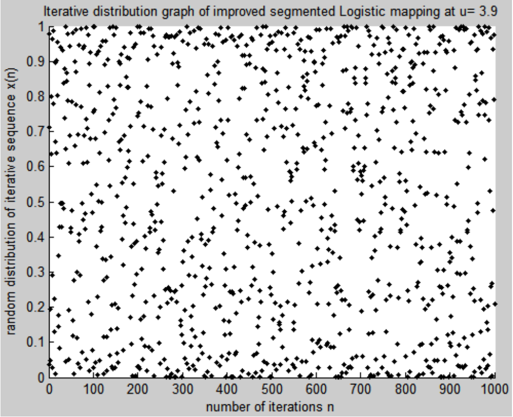


(b) Traditional logistic mapping

(d) Segmented logistic mapping

When the control parameter $\mu = 3.9$ and the number of iterations n = 1000:

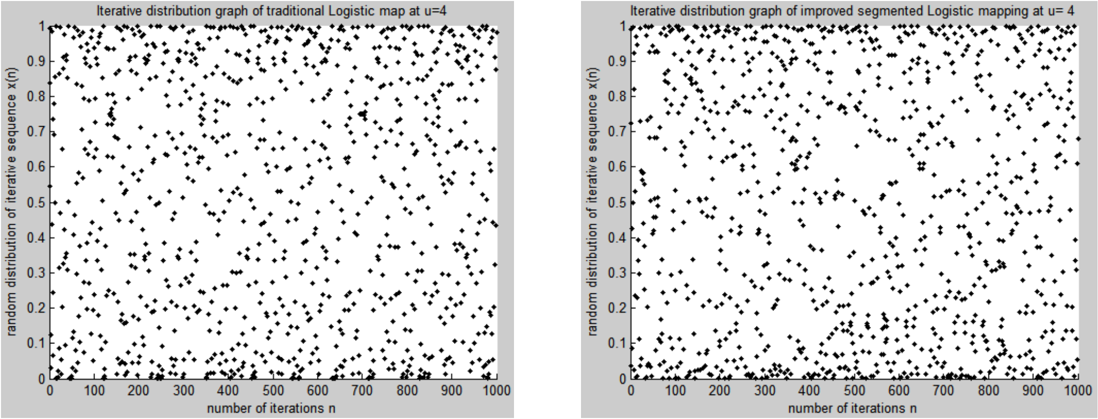




(e) Traditional logistic mapping

(f) Segmented logistic mapping

When the control parameter $\mu = 4$ and the number of iterations n = 1000:



(g) Traditional logistic mapping (h) Segmented logistic mapping

Fig 8 Distribution map of multiple groups of chaotic sequences

The following conclusions can be drawn from the above four groups of experimental analysis results:

When the control parameter is less than 4, the motion trajectory of the traditional Logistic map cannot meet the random distribution characteristic in the value interval. Only when the value is 4, it is randomly distributed in the entire value interval, and the improved segmented Logistic map takes any control parameter. At one value, the motion trajectory can be randomly distributed in the value interval;

From the simulation results, no matter the control parameter takes any value in $(2.01, 2.98) \cup (3.11, 4)$, the motion trajectory generated by the improved segmented Logistic map can be uniformly distributed irregularly in the value interval, and has good traversability.

4.4 Periodic Analysis

Under ideal conditions, the chaotic map iteration sequence is non-periodic and random, but under the influence of the limited precision effect of the computer, the chaotic key sequence will eventually become a short-period cyclic sequence during the iteration process. The sequence is periodically analyzed.

In the improvement scheme, the initial value perturbation and control parameter change step size are adopted. Therefore, these factors that affect the key space also need to be taken into account. Since the initial value change is perturbed by the m sequence, and the control parameter changes are also not affected by chaotic iteration, they are independent and unrelated to the iterative process. It can be drawn from the previous m-sequence analysis that the period of the m-sequence is $\mathrm{N} = 2^n - 1$, the initial value and control parameters are expressed in 16-bit binary form, assuming that the number of iterations is 1000, and the control parameter change step range is $(2.01, 2.98) \cup (3.11, 4)$, The minimum value of the parameter m is in the range $m \in (2.01, 2.012)$, and the value of the decimal point i is in the range $(0,15]$, then the size of the space of the encryption key Key (N, i, n, s, m) is roughly:

$$\mathrm{K} = (2^{16} - 1) \times (15 \times 10^{15}) \times 10^{3} \times (1.99 \times 10^{3}) \times 0.002 \approx 3.91 \times 10^{24}$$

It can be seen that the total size of the encryption key is large enough to meet the needs of current applications, and can resist the impact of exhaustive attacks and replay attacks. It also shows that this method is better than the previous one, which avoids chaotic iterative sequences becoming short-cycle cyclic sequences and improves the problem of period degradation.

5 Implementation Mechanism of Improved Chaotic Encryption Algorithm in RFID

Using the improved chaotic encryption algorithm discussed above, it is applied to the RFID security mechanism, so that the key sequence encryption operation generated by the RFID information and the unique serial number of the tag corresponds to ensure the security of RFID data transmission.

5.1 Data Conversion

When applying the improved chaotic encryption algorithm to RFID data encryption, since the iterated sequence of the chaotic map is a real sequence, and the RFID plaintext information flow in the computer corresponds to a binary sequence.Therefore, it is necessary to realize the mutual conversion between real value and binary value when performing encryption operations [20].

Conversion of real value to binary value: Since the range of chaotic iterative values is (0,1), the iterative value X_n can be expressed as a real number form $\mathrm{x}_n = 0.a_1a_2a_3\cdots a_n$, starting from the i decimal place and taking three significant digits together Make up the integer $\mathrm{M} = a_{i+1}a_{i+2}a_{i+3}$, the value range of M is (0,999), then use the three-digit number to take the remainder of 256 to get r, and the value range of r is (0,256), convert the obtained residue r to the corresponding binary form , To realize the conversion operation from iterative value to binary value[21].

Conversion of binary value to real value: When the RFID system information encryption uses 16-bit binary key stream sequence encryption, the range of binary conversion into decimal number is (0,65535), and the period of the m sequence used at this time is $2^N - 1 = 2^\wedge 16 - 1$, in the chaotic mapping process, the initial value x_0 ranges from (0,1), and the parameter μ_0 ranges from $\mu_0 \in (2.01, 2.98) \cup (3.11, 4)$. The initial value conversion process is: convert the binary number to the corresponding decimal number, and then divide by 65535 to get the real value of the initial value x_0, which is in the range of (0,1); the control parameter conversion process is: because there are two control parameters For different parameter value ranges, the corresponding conversion calculation factors need to be calculated separately: (2.98-2.01) /0.65535=1.480125, (4-3.11) /0.65535=1.358053, again convert the binary numbers corresponding to the parameters to decimal values, multiply The corresponding calculation factor is converted to a decimal (multiplied by 10^{-n}, n is determined by the calculation result) to form a decimal value plus the corresponding 2.01 / 3.11 as the real number corresponding to the parameter μ.

There are two operations for the conversion of the definition domains. The first one is to convert the mapping iterative real number sequence into a binary sequence used for encryption. This is to solve the problem of the XOR processing of the key stream sequence and the plaintext information sequence when encrypting the RFID data, which is to generated the key stream sequence after the mapping iteration; the latter is to calculate the initial value and the control parameter value during the initial iteration. It is necessary to convert the binary form of the sequence number and random number on the label to the real form. The initial value and control parameters are determined before the mapping iteration.

5.2 Security Authentication Mechanism Based on Chaotic Encryption

Based on the encryption framework of the improved chaotic encryption algorithm, an appropriate RFID security authentication mechanism needs to be proposed to ensure the legitimacy of the reader and tag. The security authentication process is as follows:

(1) The reader sends the query request information Query and the generated random number R to the tag;

(2) The tag performs an exclusive XOR operation on the random number R and the access password APW_t stored by itself to $E_t(\mathrm{R}) = APW_t \oplus R$, and transmits it to the reader;

(3) The reader will X-process the received $E_t(\mathrm{R})$ and the random number R to get $APW_{DS}{}' = E_t(\mathrm{R}) \oplus R$, and compare it with the APW_{DS} stored in the background system. If $APW_{DS}{}' = APW_{DS}$, it means the tag is a legal tag, otherwise the tag is illegal;

(4) The reader XOR the received $E_t(\mathrm{R})$ and random number R and the tag identifier ID_{DS} stored in the background system to obtain $E_{DS}(\mathrm{ID}) = \mathrm{E}_t(\mathrm{R}) \oplus R \oplus ID_{DS}$, and transmits the result to the tag;

(5) After receiving the result, the tag performs an XOR operation with the access password APW_t stored by itself, and obtains $ID_t{}' = E_{DS}(\mathrm{ID}) \oplus APW_t$, which is compared with its own identifier ID_t. If $ID_t{}' = ID_t$, it indicates that the reader is a legal reader, otherwise the reader is illegal;

(6) The tag transmits the stored encrypted data $\mathrm{C(x)}$ and key information $E_k(\mathrm{key})$ to the reader. After the reader receives the key information, it will decrypt the key information to obtain the relevant initial value(x_0), control parameter(μ)and key($Key(\mathrm{N,i,n,s,m})$), and after performing the decryption operation to encrypted data $\mathrm{C(x)}$,the result is $D(\mathrm{x})$.

The schematic diagram of the safety certification process is shown in Figure 9.

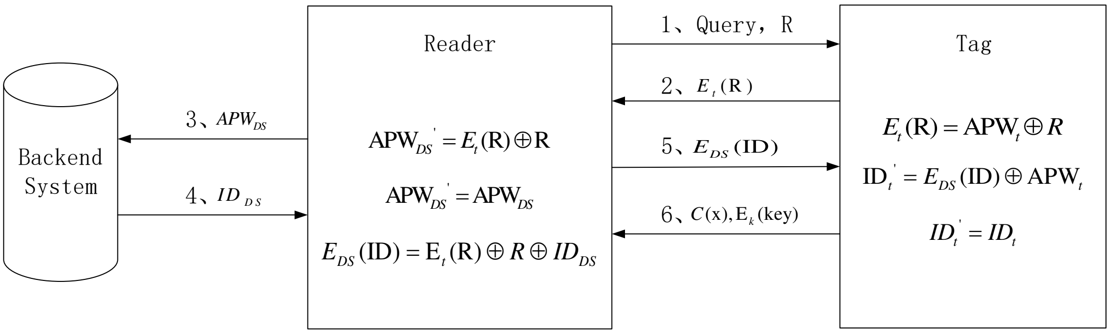

Backend
System
3、APW_{DS}
4、ID_{DS}
Reader
$\mathrm{APW}_{DS}{}' = E_t(\mathrm{R}) \oplus \mathrm{R}$
$\mathrm{APW}_{DS}{}' = \mathrm{APW}_{DS}$
$E_{DS}(\mathrm{ID}) = \mathrm{E}_t(\mathrm{R}) \oplus R \oplus ID_{DS}$
1、Query，R
2、$E_t(\mathrm{R})$
5、$E_{DS}(\mathrm{ID})$
6、$C(\mathrm{x}), \mathrm{E}_k(\mathrm{key})$
Tag
$E_t(\mathrm{R}) = \mathrm{APW}_t \oplus R$
$\mathrm{ID}_t{}' = E_{DS}(\mathrm{ID}) \oplus \mathrm{APW}_t$
$ID_t{}' = ID_t$

Fig 9 Security certification process diagram of tag and reader

When the key and security encryption mechanism are not known, the illegal intruder cannot speculate and parse out the plaintext data information even if the part of the data information are intercepted, and cannot decrypt it correctly. This shows that the RFID system based on the improved chaotic encryption algorithm has a good ability to resist various attacks after data encryption, which ensures the security and confidentiality of the RFID system. And the increase of the key space makes the unpredictability and pseudo-randomness of the generated chaotic sequence more obvious, and accordingly improves the security of encryption.

6 Conclusions

Based on the think about of chaotic mapping, this paper proposes a progressed chaotic encryption algorithm based on the degradation of dynamic characteristics and short-cycle problems under the influence of finite precision effects. This algorithm uses segmented logistic mapping. At the same time, the initial value and control parameters are ceaselessly changed during the iteration. The m-sequence is used when the initial value is changed. Perform disturbance processing, and set a parameter of change step s when the control parameter changes. Due to the chaotic characteristic of the segmented Logistic map, conditions for the change of control parameters are created and the key space is enlarged. It is verified by MATLAB software simulation that the made improved chaotic encryption algorithm can generate a great pseudo-random sequence, which encompasses a great uniform distribution and traversal within the value interval. The change of the initial value and control parameters before each iteration avoids the short Periodic cycle sequence.

List of Abbreviations

Query：The query request information sent by the reader to the tag.

t : tags，r : reader，ID_t : The unique identifier of the tag stored in the tag as the initial value of the chaotic map, ID_{DS}： The tag's unique identifier stored in the background system as the initial value of the chaotic map，APW_t：Tag storage access password，APW_{DS}：Tag access password stored in the background system，x_0：Chaos map initial value，μ：Chaos mapping control parameters，R：The random number generated by the reader is used as the chaotic mapping control parameter，N : Order of M sequence，i : Start of decimal point，n：Number of iterations，s：Control parameter change step，m：Minimum value of control parameter，$Key(\mathrm{N,i,n,s,m})$: Chaotic map encryption key，$\oplus$: XOR，$E()$: Encryption operation，$C()$: Chaotic mapping function，$\mathrm{D}()$：Decryption operation.

Declarations

The declaration part of this paper mainly includes the following aspects.

Competing interests

None.

Funding

This work was partially supported by Science & Technology Program of Shaanxi Province under project 2017GY-196.

Author’s contributions

B. Liu conducted the research design and analysis, and coordinated the revision of the entire manuscript. Y. Guo conducted research on chaotic encryption algorithm and applied it to RFID security mechanism, and participated in the conception and writing of the manuscript. J. Yang supported this research and participated in its analysis and coordination.

Acknowledgments

Special thanks to the Shaanxi Provincial Department of Science and Technology for the support of the science and technology project funds, and also thank all the laboratory staff for their help and support.

References

[1] Xin Jin,Guohui Shu.An RFID security model for Internet of Things based on ECC information implantation [J]. Journal of Jixi University,2016:1672-6758.

[2] Fanyue Kong. Research on Anti-collision Algorithm and Security Authentication Protocol of RFID System [D].

Master Degree Thesis of Jilin University,2019.

[3] Jiali Tian.Research on ECC-based RFID system security authentication protocol [D]. Beijing: Beijing Jiaotong University, 2015.

[4] Genhua Zhao. Research on the Confidentiality of RFID System Based on Chaos Theory [D]. Master Degree Thesis of Hunan University, 2011.

[5] Hailan Pan,Yongmei Lei,Chen Jian.Research on digital image encryption algorithm based on double logistic chaotic map[J].EURASIP Journal on Image and Video Processing,2018:142.

[6] Yue Wu, Gelan Yang.Image Encryption using the Two-dimensional Logistic Chaotic Map[J].Journal of Electronic Imaging,2012:10.1117.

[7] Shuangxin Li, Chi Wang.A new type of two-level segmented Logistic chaotic map and its performance analysis [J] .Journal of Northeast Normal University, 2013: 1000-1832.

[8] Tao Xie. Application Research of Logistic Mapping in Cryptography [D]. Master Degree Thesis of Xiangtan University, 2014.

[9] Jinjie Xu, Guangyi Wang, Dapeng Wang.Improved dynamic characteristics of Logistic mapping [J] .Journal of Hangzhou Dianzi University, 2014: 1001-9146.

[10] You Tang, Yuanyuan Lu.Chaotic dynamic disturbance algorithm based on RFID system [J] .Computer Applications, 2012: 32 (6) 1001-9081.

[11] Yuqing Hu. FPGA implementation of pseudo-random sequence generator based on hyperchaos [D]. Master degree thesis of Tianjin University of Technology, 2018.

[12] Qin Zhang, Da Lin, Li Xu.Design of pseudo-random sequence generator of CNN hyperchaotic system [J] .Journal of Sichuan University of Science and Engineering, 2017: 1673-1549.

[13] Xueqin Fan.Compound chaos encryption algorithm combined with m-sequence disturbance [J] .Computer Engineering and Science, 2009: 1007-130X.

[14] Mengting Li, Zemao Zhao. A new method for generating chaotic pseudo-random sequences [J] .Computer Application Research, 2011: 1001-3695.

[15] Mingsheng LIU,Yan WANG, RFID System Information Security Based on Chaotic Encryption [C].IEEE International Conference on Multimedia Information Networking and Security,2011.

[16] Mustapha Benssalah,Mustapha Djeddou,Karim Drouiche. Security enhancement of the authenticated RFID security mechanism based on chaotic maps [J]. Security and communication networks, 2014, 7(12):2356-2372.

[17] Bing Liu. Binary sequence scrambling encryption algorithm based on improved Logistic map [J] .Journal of West China Normal University, 2017: 1673-5072.

[18] Guodong Zhu. RFID encryption algorithm and security authentication protocol based on super prime numbers and chaos [D]. Master Thesis of Hefei University of Technology, 2018.

[19] Lingfeng Liu,Bocheng Liu.Reducing the Dynamical Degradation by Bi-Coupling Digital Chaotic Maps[J].International Journal of Bifurcation and Chaos, 2018:10.1142.

[20] Mete Akgun,M.Ufuk Caglayan.Vulnerabilities of RFID Security Protocol Based on Chaotic Maps[C].IEEE International Conference on Network Protocols, 2014.

[21] Yan Wang. Application Research of Chaos Technology in RFID Security Authentication Protocol [D]. Master Thesis of Hebei University of Engineering, 2012.

Figure:

Fig.1. Traditional Logistic Mapping Bifurcation Diagram

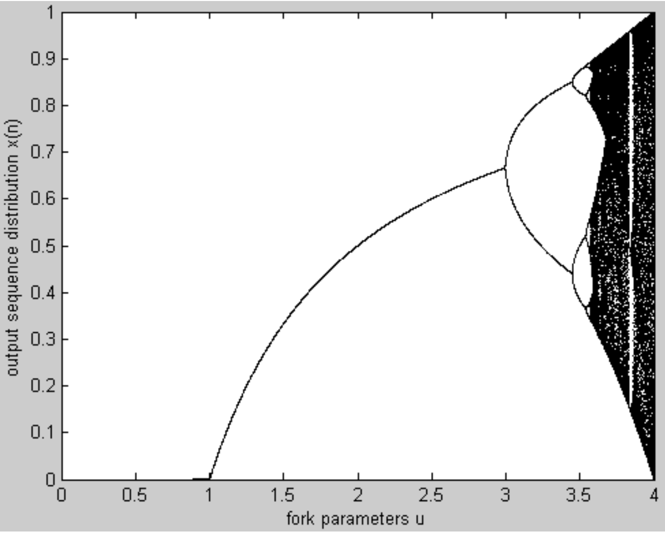


Fig.2. Iterative distribution graph with the control parameter 3.9

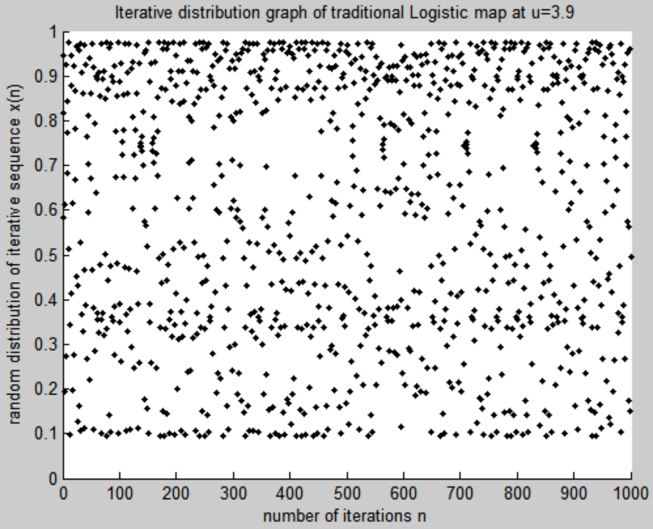


Fig.3. Bifurcation diagram of segmented Logistic mapping

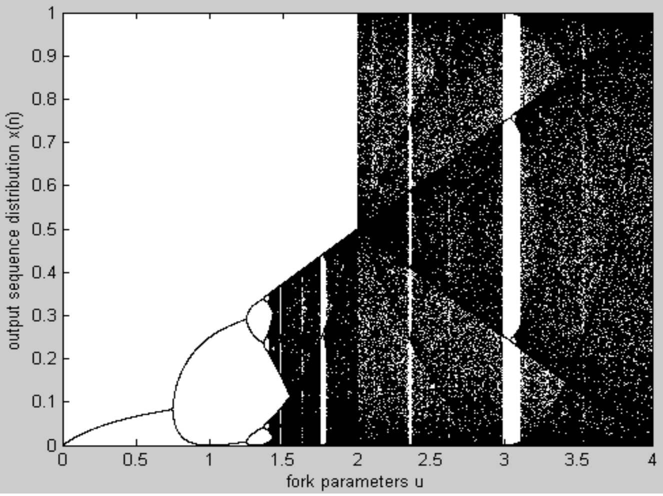


Fig.4. Structural Model of the Improved Algorithm

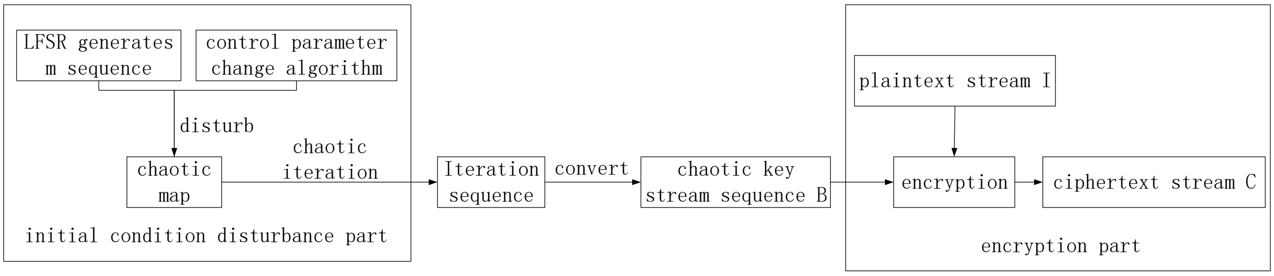

LFSR generates m sequence
control parameter change algorithm
disturb
chaotic map
chaotic iteration
Iteration sequence
convert
chaotic key stream sequence B
initial condition disturbance part
plaintext stream I
encryption
ciphertext stream C
encryption part

Fig.5. Improved Algorithm Operation Flowchart

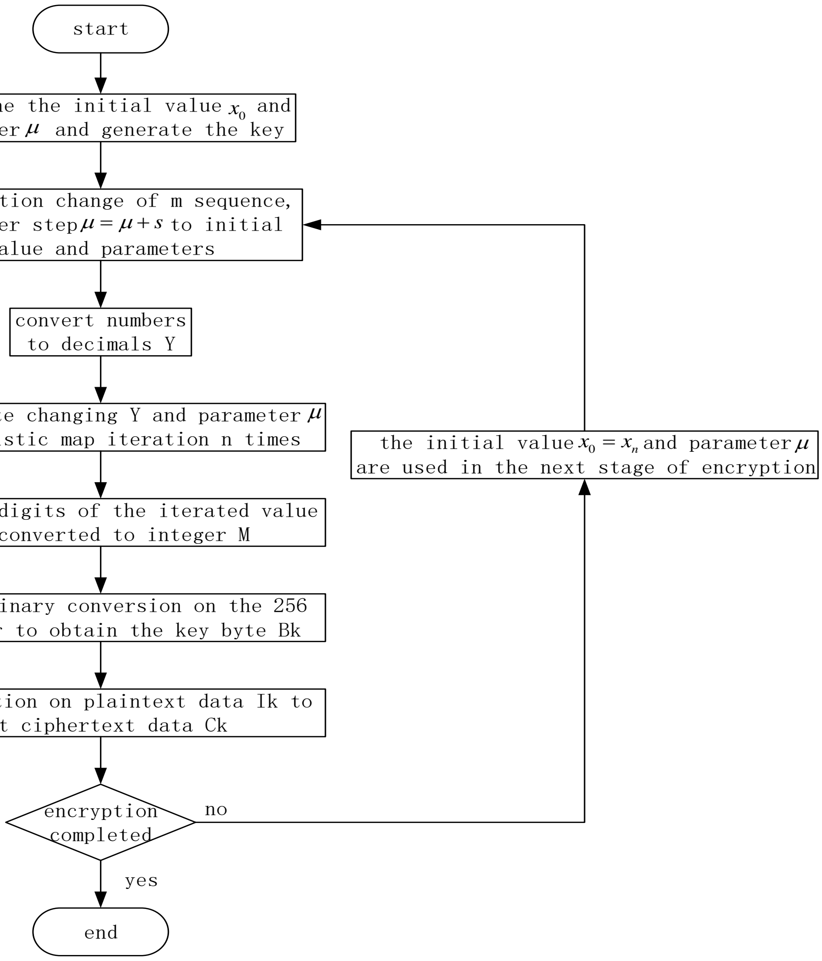
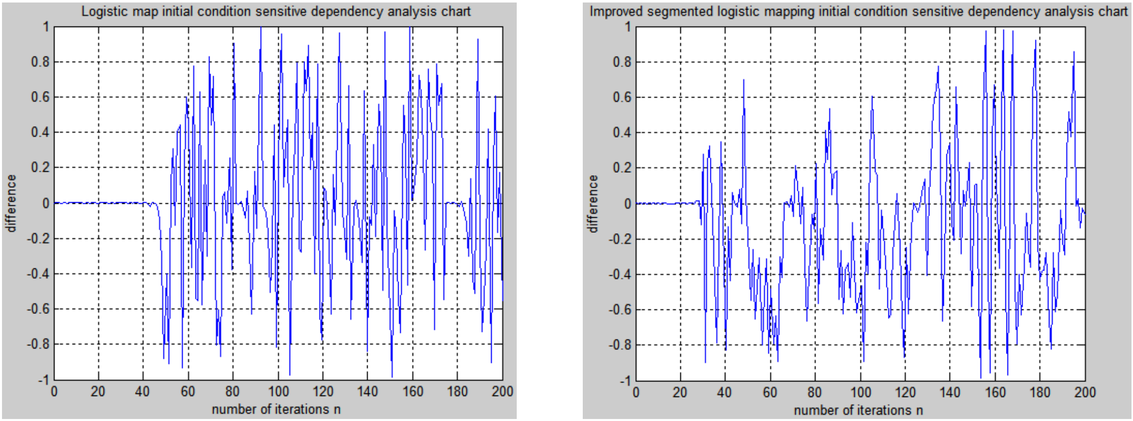

start
determine the initial value x_0 and parameter μ and generate the key
perturbation change of m sequence, parameter step $\mu=\mu+s$ to initial value and parameters
convert numbers to decimals Y
substitute changing Y and parameter μ into Logistic map iteration n times
the three digits of the iterated value are converted to integer M
perform binary conversion on the 256 remainder to obtain the key byte Bk
XOR operation on plaintext data Ik to get ciphertext data Ck
encryption completed
no
yes
end
the initial value $x_0=x_n$ and parameter μ are used in the next stage of encryption

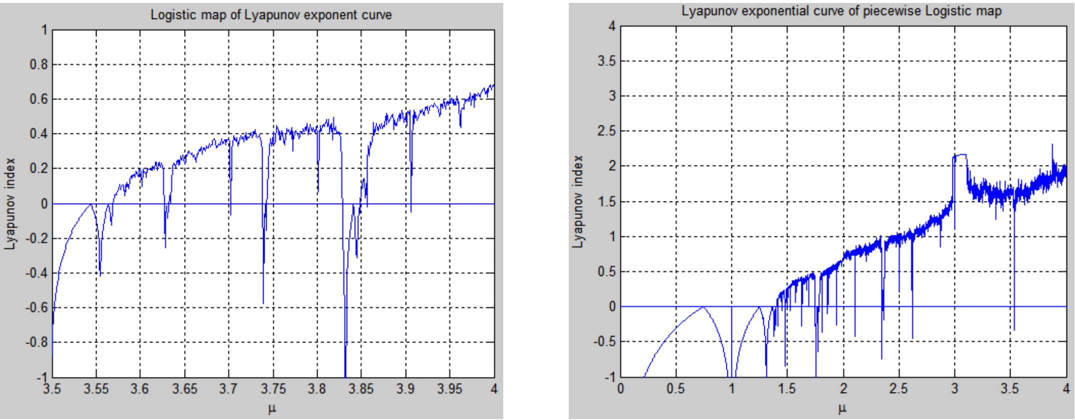
Fig.6. Logistic mapping under small initial value changes



(a)traditional logistic mapping

(b)improved segmented logistic mapping

Fig.7. Lyapunov index analysis diagram

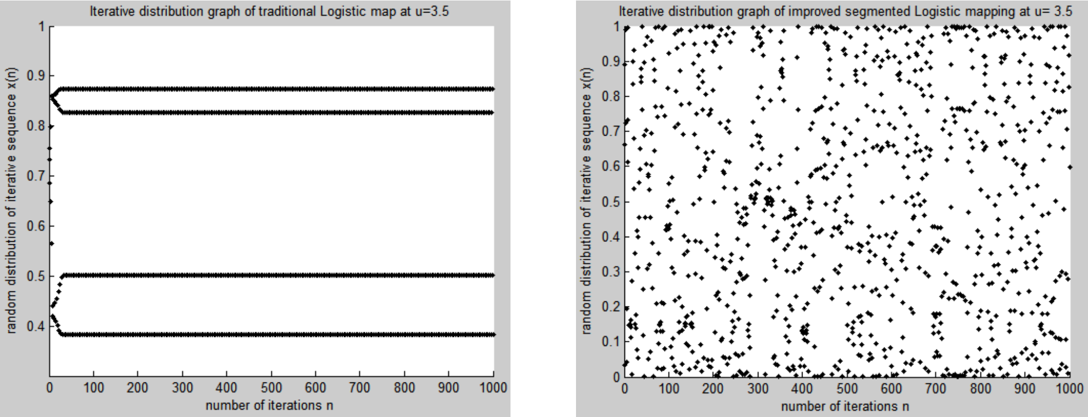


(a)traditional logistic mapping

(b)segmented logistic mapping

Fig.8. Distribution map of multiple groups of chaotic sequences

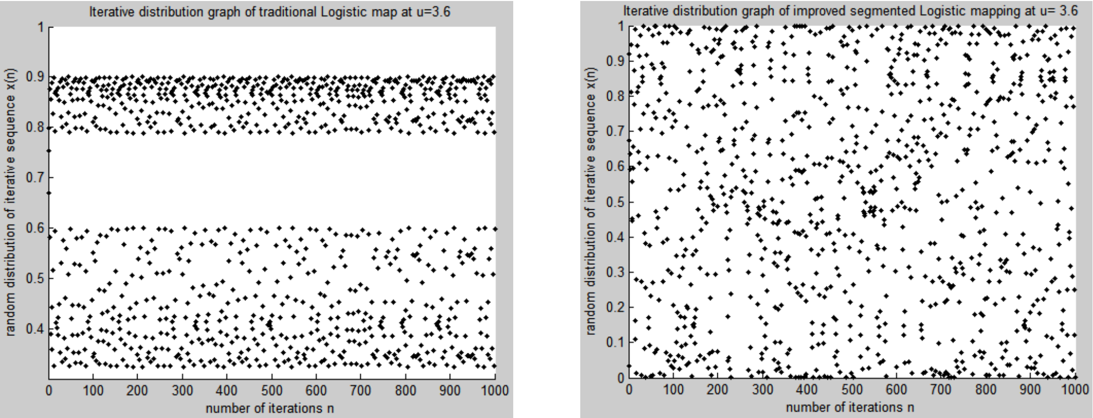
When the control parameter $\mu = 3.5$ and the number of iterations n = 1000:



(a)traditional logistic mapping

(b)segmented logistic mapping

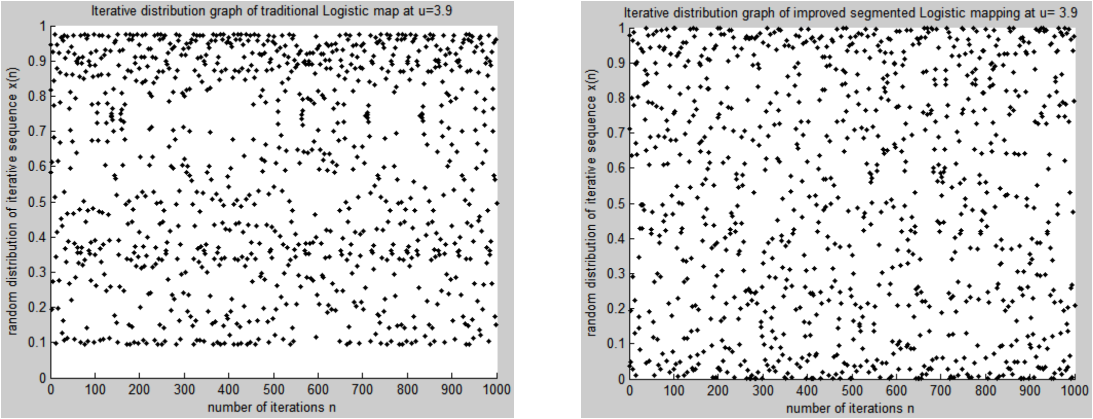
When the control parameter $\mu = 3.6$ and the number of iterations n = 1000:



(c)traditional logistic mapping

(d)segmented logistic mapping

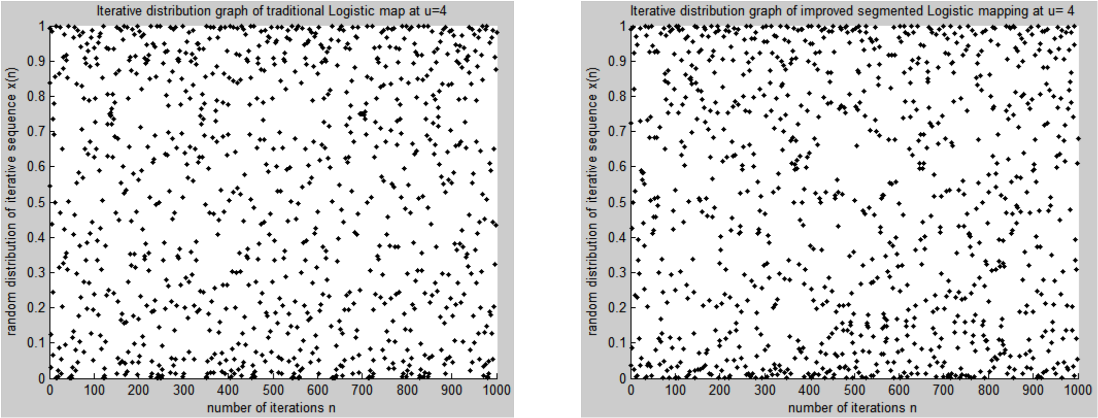
When the control parameter $\mu = 3.9$ and the number of iterations n = 1000:



(e)traditional logistic mapping

(f)segmented logistic mapping

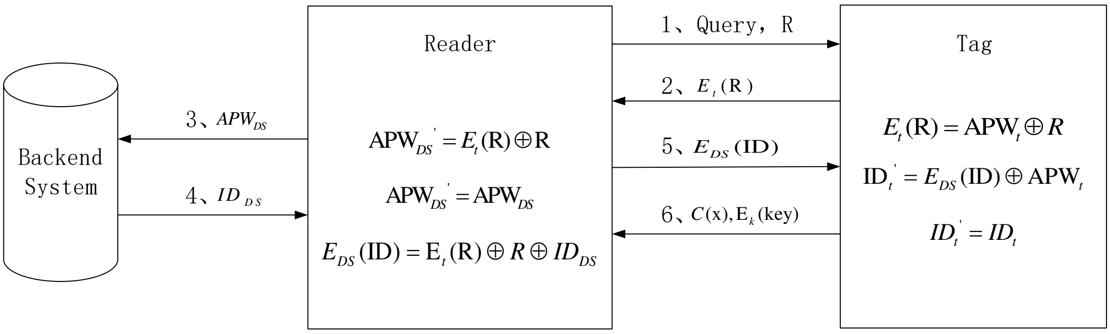
When the control parameter $\mu = 4$ and the number of iterations n = 1000:



(g)traditional logistic mapping

(h)segmented logistic mapping

Fig.9. Security Certification Process Diagram of Tag and Reader


Backend System
Reader
Tag
1、Query，R
2、E_t(R)
3、APW_{DS}
4、ID_{DS}
5、E_{DS}(ID)
6、C(x), E$_k$(key)
$\mathrm{APW}_{DS}{}' = E_t(\mathrm{R}) \oplus \mathrm{R}$
$\mathrm{APW}_{DS}{}' = \mathrm{APW}_{DS}$
$E_{DS}(\mathrm{ID}) = \mathrm{E}_t(\mathrm{R}) \oplus R \oplus ID_{DS}$
$E_t(\mathrm{R}) = \mathrm{APW}_t \oplus R$
$\mathrm{ID}_t{}' = E_{DS}(\mathrm{ID}) \oplus \mathrm{APW}_t$
$ID_t{}' = ID_t$

Figures

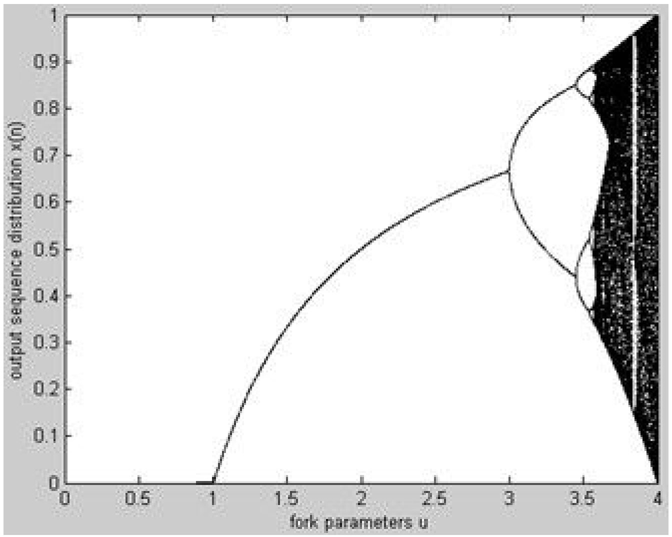


Figure 1

Traditional Logistic Mapping Bifurcation Diagram

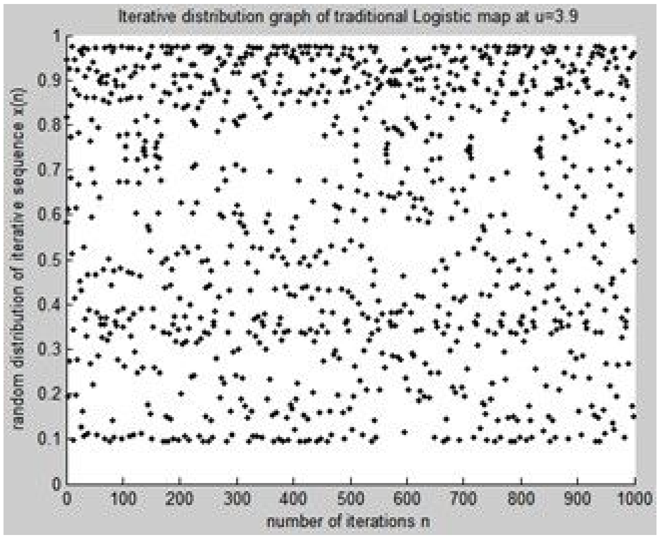


Figure 2

Iterative distribution graph with the control parameter 3.9

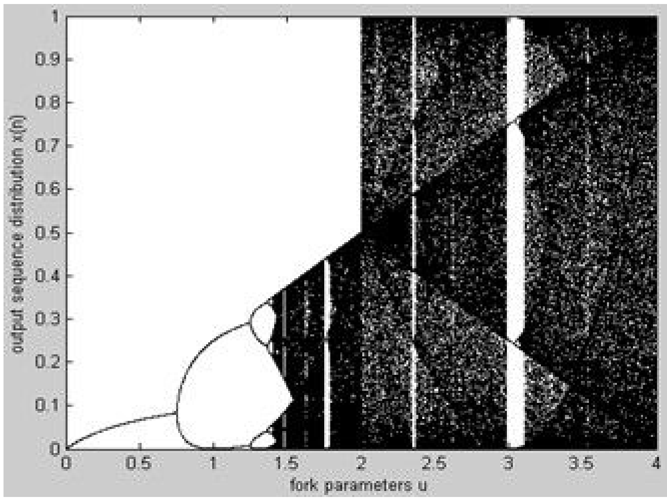


Figure 3

Bifurcation diagram of segmented Logistic mapping

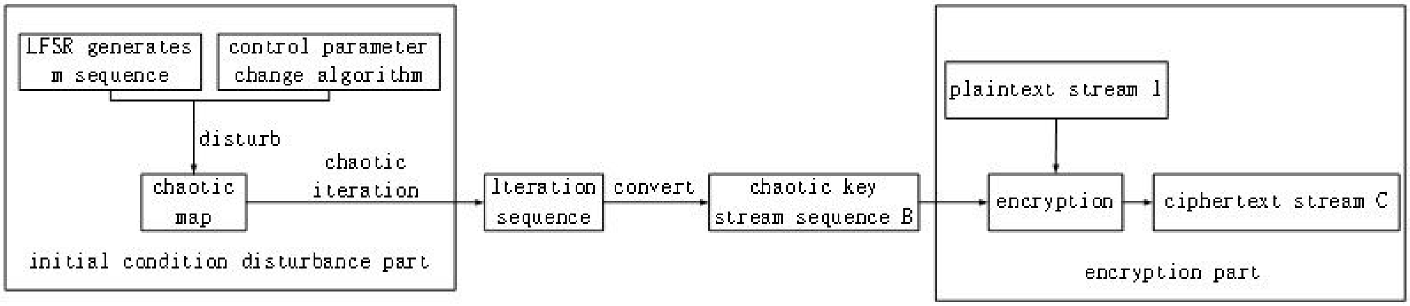

LFSR generates m sequence
control parameter change algorithm
disturb
chaotic map
chaotic iteration
initial condition disturbance part
Iteration sequence
convert
chaotic key stream sequence B
plaintext stream 1
encryption
ciphertext stream C
encryption part

Figure 4

Structural Model of the Improved Algorithm

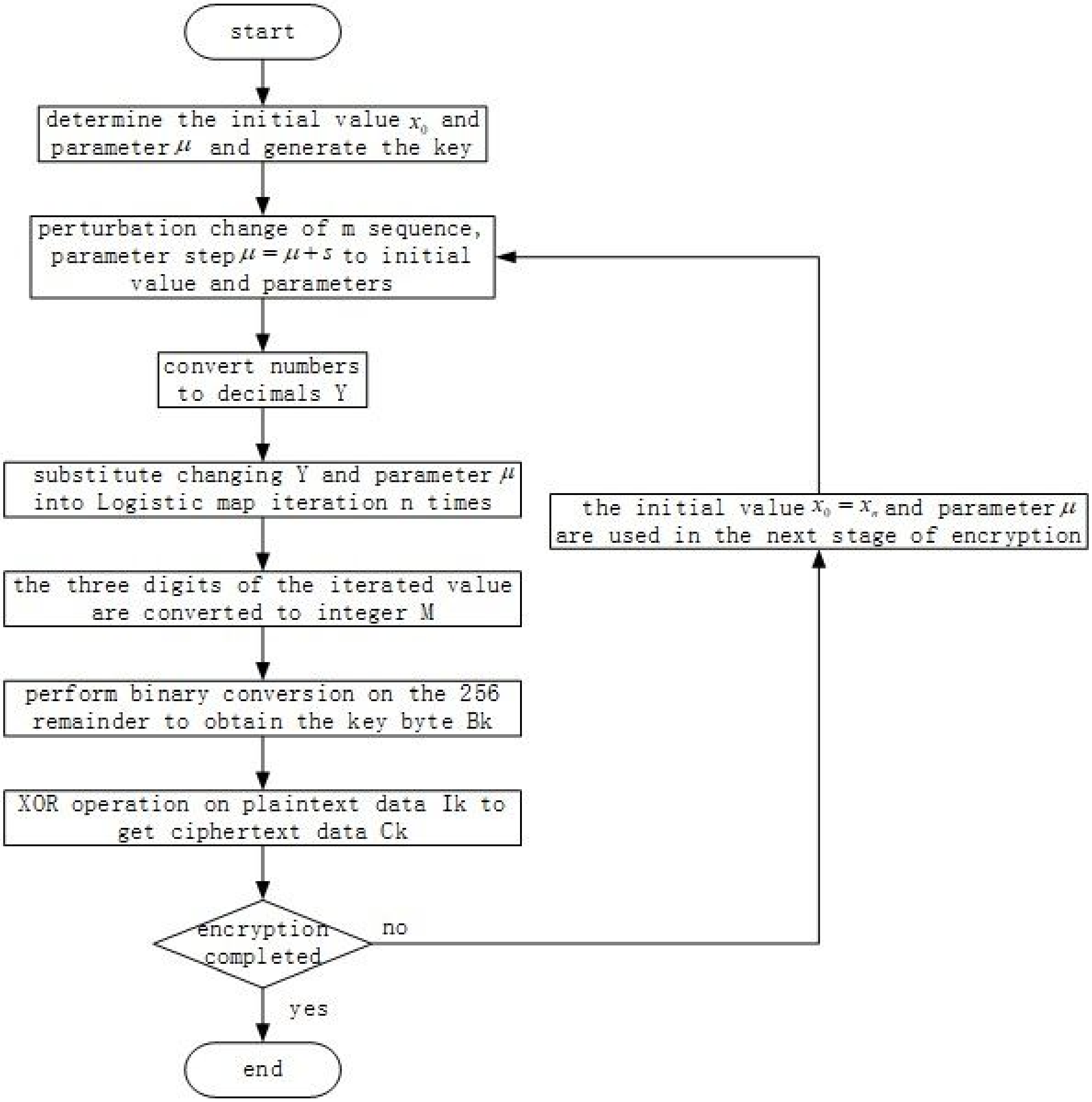
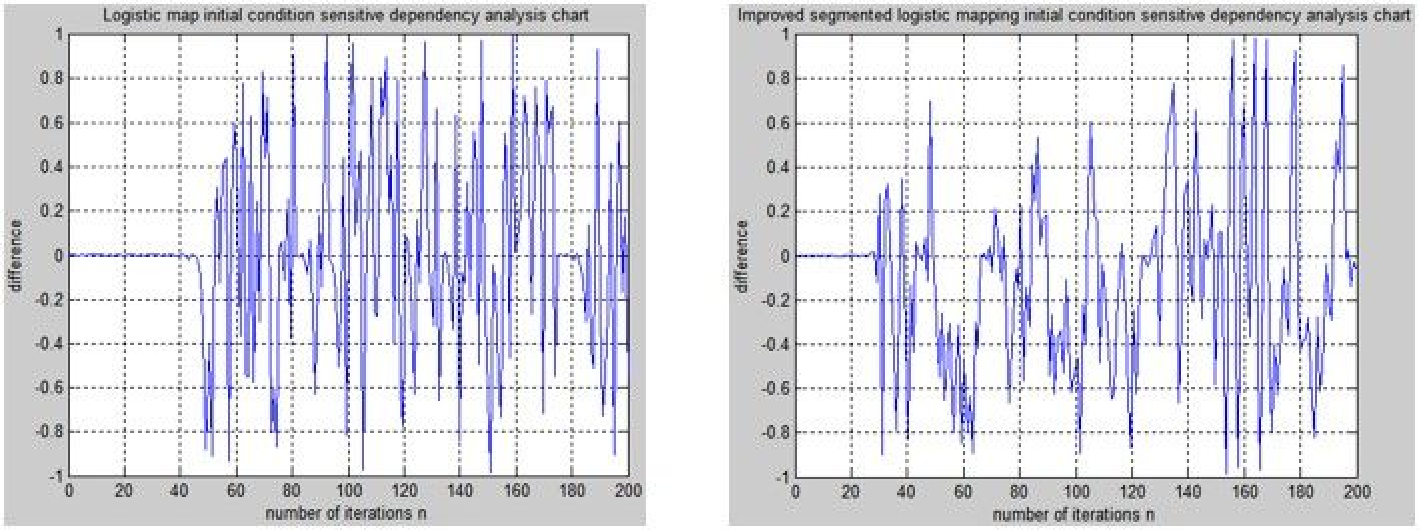

start
determine the initial value x_0 and parameter μ and generate the key
perturbation change of m sequence, parameter step $\mu = \mu + s$ to initial value and parameters
convert numbers to decimals Y
substitute changing Y and parameter μ into Logistic map iteration n times
the three digits of the iterated value are converted to integer M
perform binary conversion on the 256 remainder to obtain the key byte Bk
XOR operation on plaintext data Ik to get ciphertext data Ck
encryption completed
no
yes
end
the initial value $x_0 = x_n$ and parameter μ are used in the next stage of encryption

Figure 5

Improved Algorithm Operation Flowchart

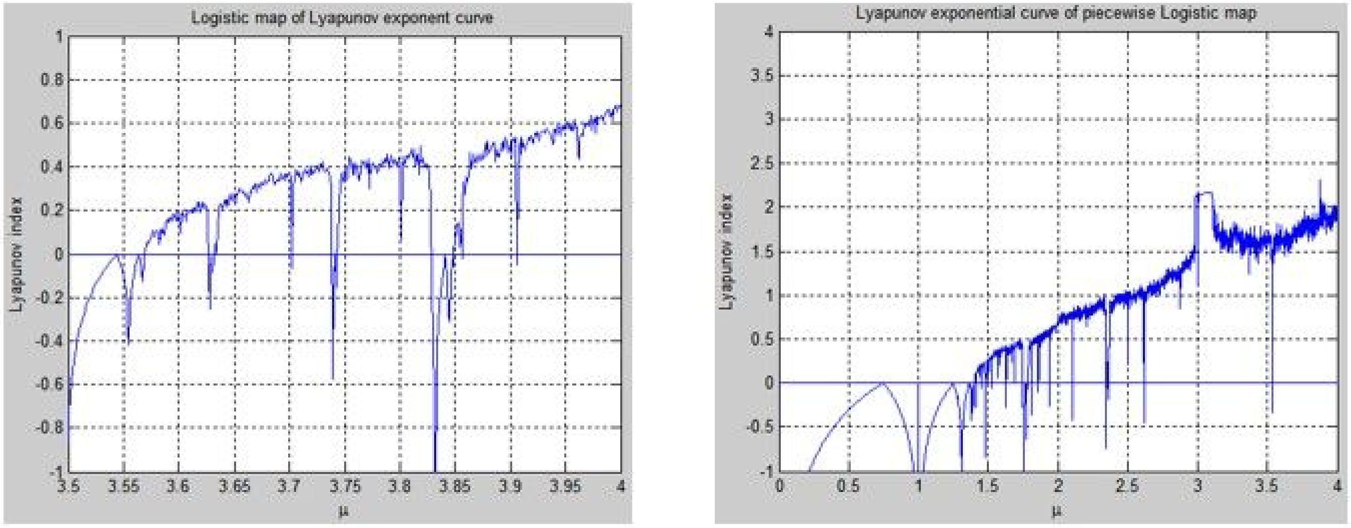


(a)traditional logistic mapping

(b)improved segmented logistic mapping

Figure 6

Logistic mapping under small initial value changes

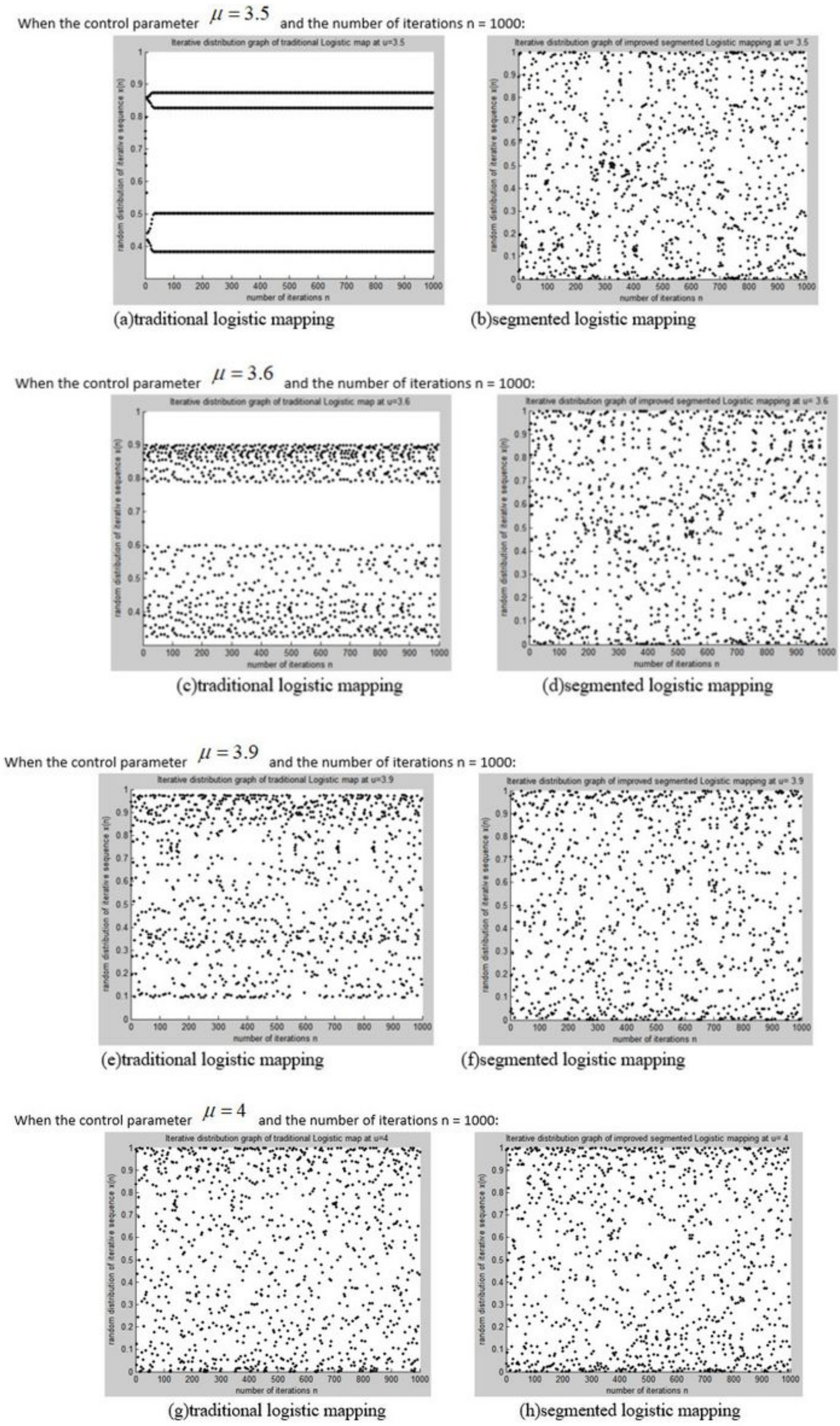


(a)traditional logistic mapping

(b)segmented logistic mapping

Figure 7

Lyapunov index analysis diagram


When the control parameter $\mu = 3.5$ and the number of iterations n = 1000:

(a)traditional logistic mapping (b)segmented logistic mapping

When the control parameter $\mu = 3.6$ and the number of iterations n = 1000:

(c)traditional logistic mapping (d)segmented logistic mapping

When the control parameter $\mu = 3.9$ and the number of iterations n = 1000:

(e)traditional logistic mapping (f)segmented logistic mapping

When the control parameter $\mu = 4$ and the number of iterations n = 1000:

Iterative distribution graph of traditional Logistic map at u=4
Iterative distribution graph of improved segmented Logistic mapping at u= 4
random distribution of iterative sequence x(n)
number of iterations n
0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0.9
1
0
100
200
300
400
500
600
700
800
900
1000

(g)traditional logistic mapping (h)segmented logistic mapping

Figure 8

Lyapunov index analysis diagram

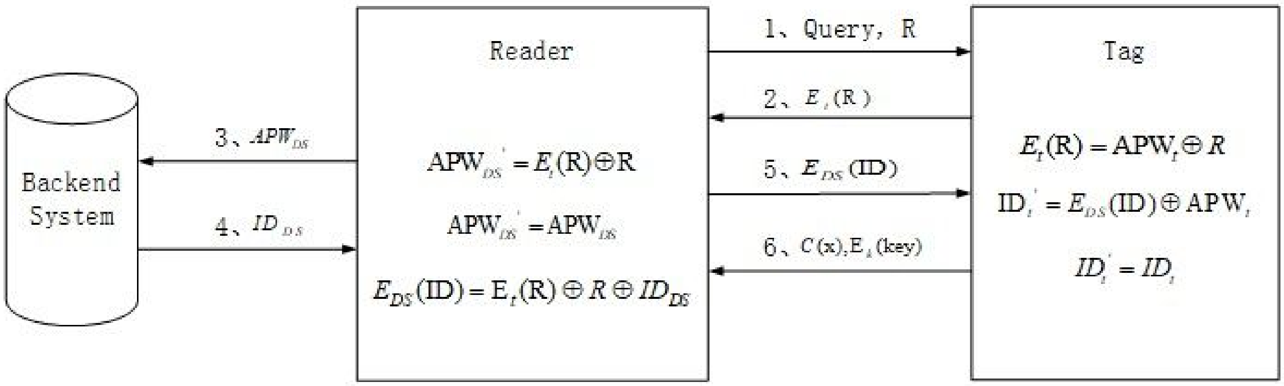


Figure 9

Security Certification Process Diagram of Tag and Reader