TSINGHUA SCIENCE AND TECHNOLOGY
ISSN 1007-0214 28/49 pp156-161
Volume 12, Number S1, July 2007

Extended Logistic Chaotic Sequence and Its Performance Analysis*

ZHANG Xuefeng (张雪锋)[1,2,**], FAN Jiulun (范九伦)[1]

1. Department of Information and Control, Xi'an Institute of Posts and Telecommunications, Xi'an 710061, China;
2. School of Electronic Engineering, Xidian University, Xi'an 710071, China

Abstract: In order to improve performance and security of image encryption algorithm effectively based on chaotic sequences, an extended chaotic sequence generating method is presented based on logistic chaotic system using Bernstein form Bézier curve generating algorithm. In order to test the pseudorandom performance of the extended chaotic sequence, we also analyze random performance, autocorrelation performance, and balance performance of the extended chaotic sequence. Simulation results show that the extended chaotic sequence generated using our method is pseudorandom and its correlation performance and balance performance are good. As an application, we apply the extended chaotic sequence in image encryption algorithm, the simulation results show that the performance of the encrypted image using our method is better than that using logistic chaotic sequence.

Key words: logistic system; Bézier curve; Bernstein function; correlation performance; balance performance; image encryption

Introduction

In the last decades, digital information, such as digital images and digital video, has been widely used in many fields. Anyone may have the possibility to freely access multimedia sources, so the problem of the digital information's copyright protection from any kind of unauthorized manipulation is becoming more and more important.

Discrete chaotic dynamical systems have nonlinear dynamic behavior. The sequence generated by using chaotic dynamical system is pseudorandom, sensitive to the initial conditions and can generate highly complicated signals by a simple recursive procedure. Because of the good properties of the chaotic sequence, chaotic system is widely used in communications, cryptology, optimization, control and image processing, etc.[1-5] In 1989, Matthews firstly used discrete chaotic dynamical systems in cryptography[6]. He derived a one-dimensional chaotic map, which is used to generate a sequence of pseudorandom numbers, and used the one-dimensional chaotic sequence in cryptograph. In 1991, Habutsu et al. developed a cryptosystem based on a piecewise linear chaotic system—tent map[7]. In Habutsu's cryptosystem, the parameter of the tent map is used for a secret key of the encryption algorithm and the chaotic sequence generated by forward iteration of the chaotic tent map. The efficiency of the algorithm is good but the cryptosystem can be easily broken by using a 'chosen ciphertext attack' and 'known plaintext attack'. Zhang and Wang [8] presented a new image encryption algorithm based on permutation transform and chaotic systems. The first step of the algorithm dealed with the image using technique of permutation transform. Then, two-dimensional nonlinear map was utilized to circularly iterate gray value of pixels. The algorithm validly solves the problem of encryption owing to the self-similarity. But the chaotic sequence

Received: 2007-02-01
* Supported by the National Natural Science Foundation of China (No. 60572133) and the Scientific Research Fund of Education Department of Shaanxi Province (No.06JK193)
** To whom correspondence should be addressed.
E-mail: zhangxuefeng3@163.com; Tel: 86-29-85383400

generating method is not safe because its key-space is not enough.

This paper proposes an extended one-dimensional chaotic sequence generating method based on logistic systems and Bernstein function. Simulation results show that the sequence generated by this method is pseudorandom. We analyze random performance, correlation performance, and balance performance of the extended chaotic sequence. In addition we present an application of the extended chaotic sequence in image encryption algorithm.

1 Algorithm Principles

1.1 Logistic chaotic system

One-dimensional logistic chaotic system is widely used in communications, cryptology, optimization, control, and image processes because its expression is simple and the computation process is easy. Logistic chaotic system has two different expressions, one is

$$a_{n+1} = F(a_n) = \mu \cdot a_n \cdot (1 - a_n), \quad 0 < a_n < 1,\ n = 1,2,\ldots \tag{1}$$

where $3.57 \leqslant \mu \leqslant 4$, $a_0 \in (0,1)$, and the sequence generated by using formula (1) is distributed in $(0,1)$. The other is

$$a_{n+1} = F(a_n) = 1 - 2 \cdot a_n^2,\ -1 < a_n < 1,\ n = 1,2,\ldots \tag{2}$$

where $a_0 \in (0,1)$ and the sequence generated by using formula (2) is distributed in $(-1,1)$. We will present an extended chaotic sequence generating method based on the above two logistic system and also analysis random performance, correlation performance, and balance performance of the extended chaotic sequence and the corresponding logistic sequence thereinafter.

1.2 Chaotic sequence generating mothod

CAD/CAM mathematical problems have generated many solutions, each adapted to specific aspects of development. In 1971, Bézier presented a curve generating method based on Bernstein function and control points[9]. The method is widely used in computer aided geometric design (CAGD) because of its good properties. The method is described as follows:

Suppose $P_i = (x_i, y_i, z_i),\ i = 0,1,\ldots,n,$ are control points, where $P_i \in \mathbf{R}^3$. Then the n-rank Bézier curve generated by these n+1 points is defined as follows:

$$P(u) = \sum_{i=0}^{n} P_i \cdot B_{i,n}(u),\ u \in [0,1] \tag{3}$$

here $B_{i,n}(u) = \mathrm{C}_n^i \cdot (1-u)^{n-i} \cdot u^i$ is called Bernstein basic function. When the parameter u changes from 0 to 1, we can get a curve generated by formula (3), which is inside the polygon constituted by control points. The curve is called Bézier curve generated by the control polygon.

The main properties of Bézier curve is presented as follows[9]:

(1) **Affine invariance** Bézier curve is invariant under affine maps.

(2) **Convex hull property** For $u \in [0,1]$, Bézier curve lies in the convex hull of the control polygon.

(3) **Endpoint interpolation** Bézier curve passes through P_0 and P_n.

(4) **Symmetry** Bézier curve defined by control polygon $P_0 P_1 \ldots P_n$ is the same as the curve defined by control polygon $P_n P_{n-1} \ldots P_0$, they only differ in the direction in which they are traversed.

In the above processing of generating Bézier curve, the control points $P_i \in \mathbf{R}^3$ are all geometric points in three-dimensional space, and the curve $P(u)$ is in the polygon generated by control points. Now let us consider an extended situation. If the control points are nonobjective numeral points, then the points on the curve generated by formula (3) will also be nonobjective numeral points, and we can get a nonobjective numeral curve generated by formula (3) which is inside the nonobjective numeral polygon constituted by the nonobjective numeral control points. When the control points are random, we can get a random curve generated by the random control points.

Now we present the extended chaotic sequence generating method based on the above analysis. Set $\{a_1^i, a_2^i, \ldots, a_n^i, \ldots\}$, $i = 0, 1, 2, \ldots, K$ are K+1 one-dimensional logistic sequences generated by formula (1) or (2) and $\{t_1, t_2, \ldots\}$ is a one-dimensional logistic sequence generated by formula (1) (Because the sequence generated by formula (1) is distributed in $(0,1)$). Based on the above chaotic sequences, we can generate an extended logistic chaotic sequence as follows:

$$a_n = \sum_{i=0}^{K} a_n^i \cdot B_{i,n}(t_n),\ n = 1,2,\cdots \tag{4}$$

Using formula (4), we can generate an extended

chaotic sequence based on known chaotic sequences $\{a_1^i, a_2^i, \ldots, a_n^i, \ldots\}$ and $\{t_1, t_2, \ldots\}$, $i = 0,\ 1,\ 2,\ \ldots, K$.

Now we propose the extended chaotic sequence computing formula of $K = 1, 2, 3$, here $\{a_1^i, a_2^i, \ldots, a_n^i, \ldots\}$, $i = 0, 1, 2, 3$ and $\{t_1, t_2, \ldots\}$ are known one-dimensional chaotic sequences:

$$a_n = (1-t)\cdot a_n^0 + t\cdot a_n^1,\ n = 1,\ 2,\ \ldots \tag{5}$$

$$a_n = (1-t)^2\cdot a_n^0 + 2\cdot(1-t)\cdot t\cdot a_n^1 + t^2\cdot a_n^2,\ n = 1, 2, \ldots \tag{6}$$

$$a_n = (1-t)^3 a_n^0 + 3(1-t)^2 t a_n^1 + 3(1-t)t^2 a_n^2 + t^3 a_n^3,\quad n = 1, 2, \ldots \tag{7}$$

Because there is de Casteljau algorithm for generating Bézier curve in CAGD, the efficiency of generating an extended chaotic sequence is better. And from formula (4) we can know that the extended chaotic generating system's key space is larger than formula (1) or (2) because there are *K*+2 parameters for generating an extended chaotic sequence, so the extended method is more secure.

2 Performance Analysis

Expanded frequency sequence is widely used in expanded frequency communication, and the sequence is binary sequence defined in $\{-1,1\}$. We can generate expanded frequency sequence by using chaotic sequence[10]. Set the chaotic sequence as $\{a_1, a_2, \ldots\}$, then we can get an expanded frequency sequence $\{b_1, b_2, \ldots\}$ by using the following method:

$$b_i = \begin{cases} +1, & a_i > c; \\ -1, & a_i > c; \end{cases} \quad i = 1, 2, \ldots \tag{8}$$

where the value of c is the threshold of the method. Now we can generate the expanded frequency sequence by using formula (4) and formula (1) or (2). In this paper, the threshold value of *c* is 0.5 when using formula (1) generating chaotic sequence and the threshold value of *c* is 0 when using formula (2) generating chaotic sequence.

2.1 Randomicity analysis

In order to analysis the performance of the sequence generated by using our method, we compare the randomicity of the extended chaotic sequence and the corresponding logistic chaotic sequence by experiments. The lengths of the sequences are 300 and the experiment results is presented in Fig. 1.

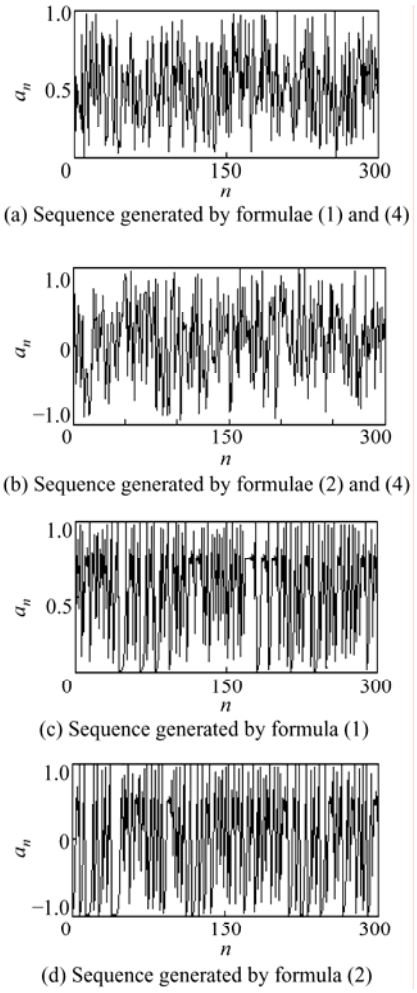


Fig. 1 Randomicity analysis

Figure 1 gives the simulation results of randomicity analysis of the extended chaotic sequence generated by our method and the logistic chaotic sequence generated by formulae (1) and (2), it is shown that the sequence generated by formula (4) and formula (1) or (2) are random in (0,1) and (–1,1). This means the extended chaotic sequences are pseudorandom.

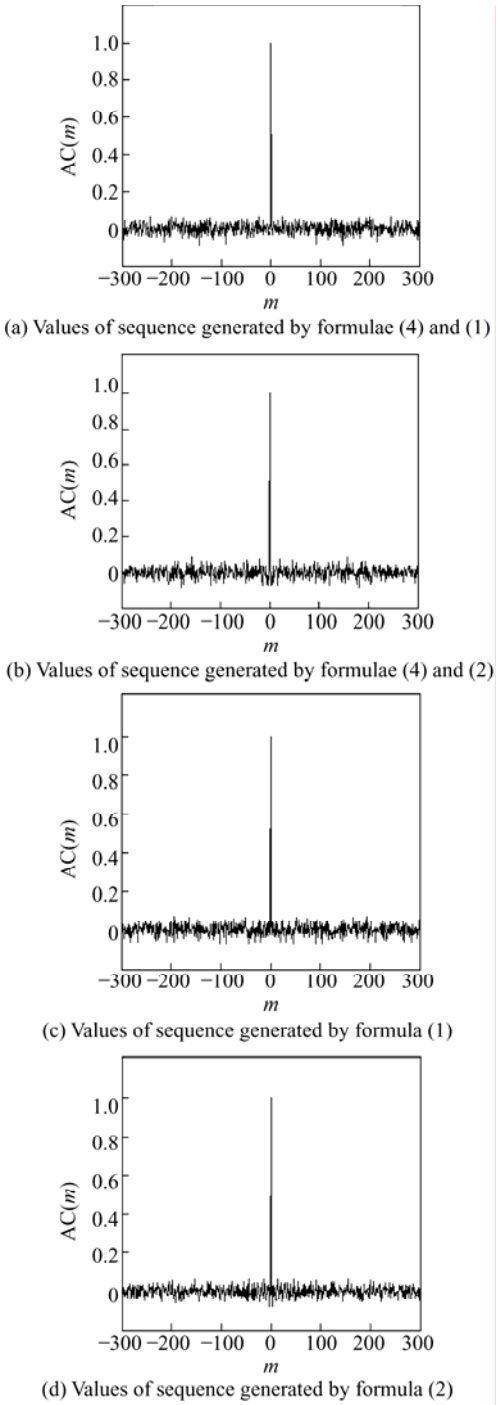
2.2 Correlation performance analysis

Expanded frequency sequence is widely used in expanded frequency communication, and the sequence is binary sequence defined in $\{-1,1\}$. Set the length of the expanded frequency sequence $\{b_1, b_2, \ldots\}$ as *N*, then the autocorrelation coefficient of the expanded frequency sequence is defined as follows[11]:

$$\mathrm{AC}(m) = \frac{1}{N}\bullet\sum_{i=1}^{N-m} b_i \bullet b_{i+m} \tag{9}$$

From the definition of the autocorrelation coefficient we know that the value of the coefficient is related to

the value of the step length m, the less the autocorrelation coefficient change when the value of the step length is changing, the better randomicity the sequences have. Now we compare the autocorrelation coefficient of the extended chaotic sequence and the corresponding logistic chaotic sequence by experiments. The lengths of the sequences are 300 and the experiment results are presented in Fig. 2.



(a) Values of sequence generated by formulae (4) and (1)

(b) Values of sequence generated by formulae (4) and (2)

(c) Values of sequence generated by formula (1)

(d) Values of sequence generated by formula (2)

Fig. 2 Correlation performance analysis

Figure 2 gives the results of the autocorrelation coefficient analysis of extended chaotic sequence generated by our method and logistic chaotic sequence generated by formulae (1) and (2). It is shown that the autocorrelation coefficient of extended chaotic sequences is similar to the corresponding logistic chaotic sequences' autocorrelation coefficient, so the extended chaotic sequence is random.

2.3 Balance performance analysis

Set the length of $\{b_1,b_2,\ldots\}$ as N, P, and Q are the numbers of 1 and -1 in $\{b_1,b_2,\ldots\}$, then we can define balance of the sequence as follows[12]:

$$E(N)=\frac{|P-Q|}{N} \tag{10}$$

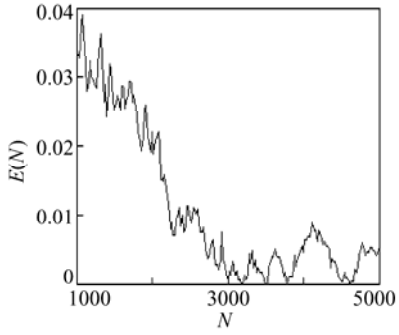
From the definition of the balance we know that the value of the counterbalance is related to the length of the sequence N. In the following experiments, the length of the sequences is changed from 1000 to 5000.

Figure 3 gives the simulation results of the balance analysis about the extended chaotic sequence generated by our method and the logistic chaotic sequence generated by formulae (1) and (2). It is shown that the balance of the extended chaotic sequences is similar to the corresponding logistic chaotic sequences' balance, this means the extended chaotic sequence is random.

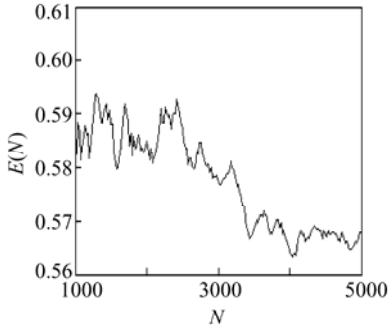
3 Application in Image Encryption

Habutsu et al. presented an image encryption method using logistic chaotic sequence and bit-computation. Now we encrypt image using Habutsu's method and substitute logistic chaotic sequence by the extended chaotic sequence generated. Here the threshold value c is 0.5 and K=3 in formula (4).

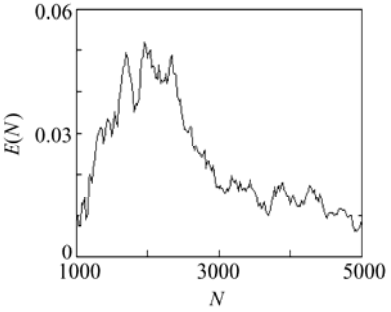
Figures 4 and 5 give the results of encrypted image. It is clear that the performance of the encrypted image using our method is better than that of using logistic chaotic sequences. On the other hand, the extended chaotic generating system's key space is larger than logistic chaotic system because there are K+2 initial parameters for generating an extended chaotic sequence, so the extended method is more secure.



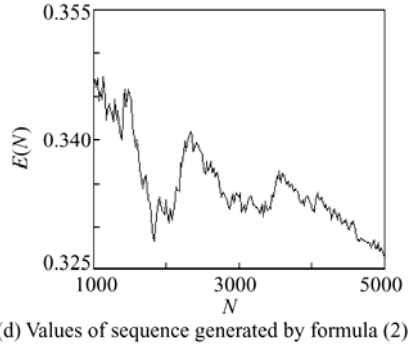
(a) Values of sequence generated by formulae (4) and (1)



(b) Values of sequence generated by formulae (4) and (2)

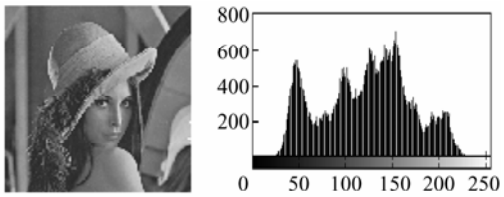


(c) Values of sequence generated by formula (1)

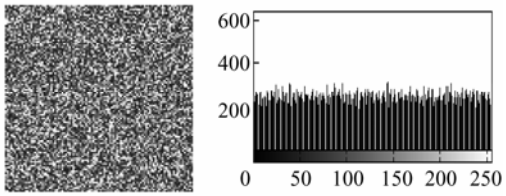


(d) Values of sequence generated by formula (2)

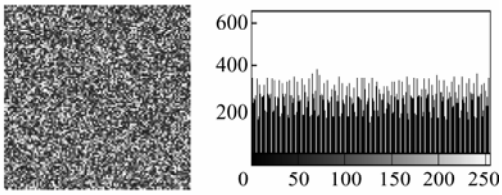
Fig. 3 Balance performance analysis



(a) Original image

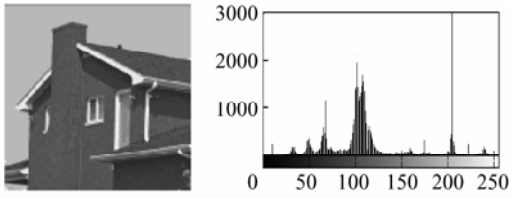


(b) Encrypted image using the extended chaotic sequence

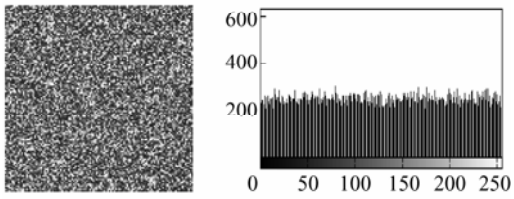


(c) Encrypted image using logistic chaotic sequence

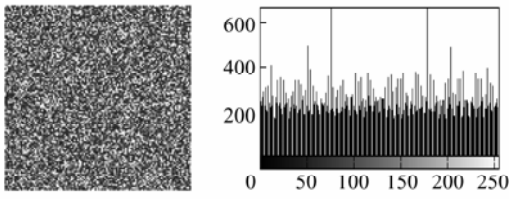
Fig. 4 Encrypted image



(a) Original image



(b) Encrypted image using the extended chaotic sequence



(c) Encrypted image using logistic chaotic sequence

Fig. 5 Encrypted image

4 Conclusions

This paper presented an extended one-dimensional chaotic sequence generating method based on logistic system and Bernstein function. The sequence generated by this method is pseudorandom, and we analyzed random performance, correlation performance, and balance performance of the extended chaotic sequence. And we also presented an application of the extended chaotic sequence in image encryption algorithm. The method we proposed can be extended to high dimension chaotic system.

References

[1] Bianco M E, Mayhew G L. US Patent No. 5, 365-588, 1994.

[2] Yen Jui-Cheng, Guo Jiun-In. A new chaotic key-based design for image encryption and decryption. *IEEE Int.Conf. Circuits and Systems*, 2000, (4): 49-52.

[3] Pareek N K, Patidar V, Sud K K. Discrete chaotic cryptography using external key. *Physics Letters A*., 2003, **309**: 75-82.

[4] Gan Jianchao, Xiao Xianci. Characteristic of addition of chaos. *Acta Physica Sinica*, 2003, **52**(5): 1085-1090. (in Chinese)

[5] Wang Xiaomin, Zhang Jiashu, Zhang Wenfang. One way Hash function construction based on the extended chaotic maps switch. *Acta Physica Sinica*, 2003, **52**(11): 2737-2742. (in Chinese)

[6] Matthews R A J. On the derivation of a chaotic encryption algorithm. *Cryptologia*, 1989, **13**(1): 29-42.

[7] Habutsu T, Nishio Y, Sasase I, et al. A secret cryptosystem by iterating a chaotic map. In: Advances in Cryptology EURCRYPT'91. Berlin: Springer-Verlag, 1991: 127-140.

[8] Zhang Han, Wang Xiufeng. A new image encryption algorithm based on chaos system. In: Proc. IEEE Int. Conf. Robots, Intelligent systems and Signal Processing. Changsha, China, 2003: 778-782.

[9] Les Piegl, Wayne Tiller. The NURBS Book. Springer, 1995: 7-25.

[10] Tohru Kohda, Akio Tsuneda. Statistics of chaotic binary sequences. *IEEE Transactions on Information Technology*, 1997, **43**(1): 104-112.

[11] Liao Nihuan, Gao Jinfeng. The chaotic spreading sequences generated by the extended chaotic map and its performance analysis. *Journal of Electronics & Information Technology*, 2006, **28**(7): 1255-1257. (in Chinese)

[12] Yu Yinhui, Liu Weidong. Analysis of balance of chaotic spreading spectrum sequences based on logistic-map and tent-map. *Journal of Chongqing University of Posts and Telecommunications* (*Natural Science*), 2004, **16**(3): 61-64. (in Chinese)