ICSP'04 Proceedings

Frequency-hopping Sequences Based on Chaotic Map

MI Liang ZHU Zhongliang
(Southwest Electronic & Tele-communication Technology Institute, Chengdu China 610041)
Email: ml5757@sina.com

Abstract: Based on chaotic map, a new method for generating chaotic frequency-hopping (FH) sequences is proposed. The real-valued trajectory of chaotic system is first encoded to binary sequences by means of a quantization function, and then we can obtain chaotic FH sequences by reshaping bits of these binary sequences. Theory analysis and performance experiment results show that this sequence is Bernoulli sequence and its Hamming correlation is shown to be Poisson distributed. It is comparable to other FH sequences on the properties of uniform distribution, Hamming correlation and linear complexity when they have the same number of frequency slots and the same period, but its map iterative number has reduced largely. Consequently, more FH sequences can be generated by this method and they are suitable for FH code-division multiple-access systems.

Key words: Chaos Frequency-hopping Sequences Hamming Correlation Function Linear Complexity

1. Introduction

The research on the applications of chaos theory to communications has made great progress in the last decade[1-4]. In particular chaotic frequency-hopping (FH) sequences, which generated by a non-linear dynamical system in chaotic state, have received much attention in the past years[5-9]. Classical FH sequences are based either on m sequences or else on Reed-Solomon (RS) codes. These sequences having short linear complexity are potentially weak when the threat of intelligent jamming exists. In addition, the amount of these sequences is limited in the multiple access application. Consequently it is desirable to employ new sets of chaos-based FH sequences, which can overcome above drawbacks, in the FH communications.

The generation of FH sequences has been addressed in several papers. In [5] the FH generator based on the Logistic map is presented. The asymptotic statistical properties of these sequences are analyzed using the ergodic theory of chaos. It is found that the Hamming correlation function is approximately Poisson distributed. However, the Hamming correlation property of these chaotic FH sequences is not good enough. In [6][7] an improved construction of completely random hopping sequences by chaotic map is presented. The Hamming correlation is reduced significantly and is shown to be Poisson distributed. Nevertheless, the iterative number of chaotic map is increased. In [8], a generator architecture adopting nonlinear auto-regressive (AR) filter structure is proposed and a generator prototype is realized in field programmable gate arrays (FPGAs).

In this paper, we present a new approach to generating chaotic FH sequences by chaotic map. These FH sequences are comparable to other chaotic FH sequences on the properties of uniform distribution, Hamming correlation and linear complexity when they have the same number of frequency slots and the same period, but its map iterative number has reduced largely.

The rest of the paper is organized as follows. Section 2 presents a new approach to design FH sequences based on chaotic map in detail. Experimental results and performance tests are described in section 3. Finally, in section 4 the conclusion is given.

2. Chaotic FH Sequences Design

The Logistic map is defined by

$$x_{n+1} = 1 - 2x_n^2, \quad x_n \in [-1,1] \tag{1}$$

whose invariant probability density $\rho(x)$ is known to be

$$\rho(x) = \begin{cases} \dfrac{1}{\pi\sqrt{1-x^2}}, & x \in (-1,1) \\ 0, & Otherwise \end{cases} \tag{2}$$

Since chaotic systems have a very sensitive dependence on their initial conditions and parameters, the amount of such sequences is almost unlimited.

Let $X = \{X_0, X_1, \cdots, X_{N-1}\}$ denote a frequency hopping sequence of length N, $X_n \in \{f_0, f_1, \cdots, f_{q-1}\}$, where f_i is one of the q frequency slots. A frequency hopping sequence is desired to be uniformly distributed on q frequency slots. This is achieved by choosing a partition of $[-1,1]$ such that the probability of every point into x_n into a disjoint partition is equal. Suppose the dividing points are $d_0, d_1, d_2, \cdots, d_q$, where $d_0 = -1$, $d_q = 1$. We can define the dividing points as

$$d_k = -\cos(k\pi / q), \quad k = 0,1,2,\cdots,q \tag{3}$$

In [5], the chaotic FH sequences is generated by

$$X_n = Q(x_n) \tag{4}$$

where the quantization function is defined as

$$Q(x) = k, \ d_k \le x < d_{k+1}$$

In [6][7], an improved construction of chaotic FH sequences is proposed to reduce Hamming correlation by using a decimation of $\log_2 q$. That means when

$\delta = \log_2 q$, the chaotic FH sequences $\{X_n\}$ defined as

$$\{X_n = Q(x_{\delta n})\} \tag{5}$$

is Bernoulli sequence, i.e. a sequence of independent, identically (and uniformly) distributed random variables. However, its map iterative number is increased by $(\log_2 q - 1)$ compared with the method in [5]. In order to get rid of this flaw, we proposed a new approach to generating chaotic FH sequences by chaotic map. The real-valued trajectory of chaotic system is first encoded to binary sequences by means of a quantization function, and then we can obtain chaotic FH sequences by reshaping bits of these binary sequences.

In order to generate chaotic FH sequences of period N for q frequency slots, firstly real-valued sequences x_n of period N are generated by chaotic map, such as the Logistic map, and then are encoded by quantization function as [5]. The quantization of x_n is given by

$$X_n = Q(x_n) = b_1(x_n)b_2(x_n)\cdots b_{\log_2 q}(x_n), \quad b_i(x_n) \in \{0,1\} \tag{6}$$

then, we can obtain a matrix like

$$\begin{bmatrix} b_1(x_0) & b_2(x_0) & \cdots & b_{\log_2 q}(x_0) \\ b_1(x_1) & b_2(x_1) & \cdots & b_{\log_2 q}(x_1) \\ \vdots & \vdots & \vdots & \vdots \\ b_1(x_{N-1}) & b_2(x_{N-1}) & \cdots & b_{\log_2 q}(x_{N-1}) \end{bmatrix}. \tag{7}$$

Every $\log_2 q$ elements of the matrix are grouped by the column order. Get all the element of the matrix so we can obtain the chaotic FH sequences $\{F_n\}$. In this paper we define this transform as $F_n = H[X_n]$. Obviously, the map iterative number of this method is still N while the method in [6][7] needs $N \log_2 q$ in the same conditions, so that we can generate more FH sequences by our method.

This method can easily be extended to the one-dimensional (1-D) chaotic map that can be described by

$$x_{n+1} = f(x_n), \tag{8}$$

where $x_n \in I, n = 0,1,2,\cdots$, and $f: I \to I$ is a nonlinear map. The chaotic FH sequence generated by this method is Bernoulli sequence. The proof is straightforward and will be omitted in this paper.

3. Performance Tests

In this section, we compare the performance of the chaotic FH sequences generated by the proposed method with those generated by the method in [6][7].

A. *Chi-Squared Tests*

The chi-squared test compares the FH sequences to the desired uniform distribution. Let N_i denote the number of occurrence times of the i th frequency within a length-N FH sequence for q frequency slots. The chi-squared value is defined by

$$\chi^2_{q-1} = \sum_{i=1}^{q} \frac{(N_i - N/q)^2}{N/q}. \tag{9}$$

Lower chi-squared values indicate more uniform distribution.

Fig. 1 shows the chi-squared test results of two kinds of chaotic FH sequences of period 1024 for 64 frequency slots. Every method generates 100 chaotic FH sequences. As can be seen from Fig. 1, on average these two kinds of chaotic FH sequences almost have the same uniform distribution.

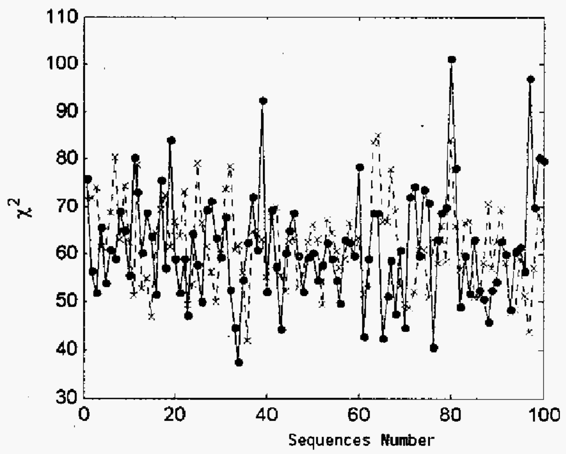


Fig. 1. Comparison of the chi-squared values for test of 1-D uniform distribution for chaotic FH sequences generated by proposed method (solid curve with ".") and the method in [6][7] (dashed curve with "x").

B. *Hamming Correlation Properties*

The periodic Hamming cross-correlation between two sequences X and Y of period N is defined by [5] as

$$H_{XY}(\tau) = \sum_{i=0}^{N-1} h(X_i, Y_{i+\tau}), \quad 0 \le \tau \le N-1 \tag{10}$$

where

$$h(x,y) = \begin{cases} 0, & x \ne y \\ 1, & x = y \end{cases},$$

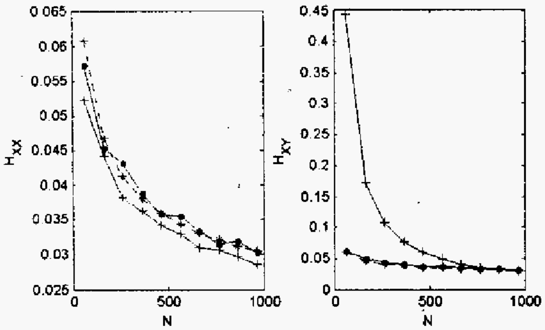
and the sum is carried out modulo N. The Hamming auto-correlation is defined as $H_{XX}(\tau)$. When $N >> q$, the Hamming correlation of chaotic FH sequences is asymptotically Gaussian with mean N/q and variance $N(1-1/q)/q$ [6].

In order to evaluate the peak of the Hamming auto-correlation sidelobes and the peak of the Hamming cross-correlation, we define two measures as follows

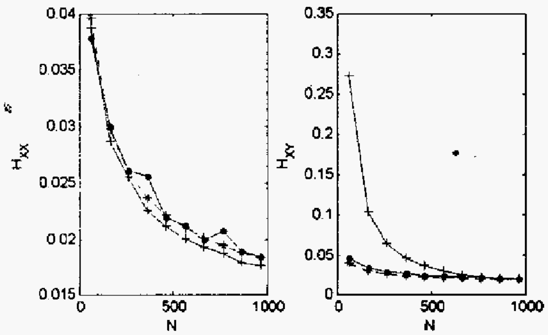
$$H_{XX} = \max_{1\le\tau<N}\{H_{XX}(\tau)\}/N \tag{11}$$

$$H_{XY} = \max_{0\le\tau<N}\{H_{XY}(\tau)\}/N \tag{12}$$

These two measures have been used as the basis for comparing the Hamming correlation properties of chaotic FH sequences. These two measures almost have the same theoretic value $\left(1+\sqrt{2q\ln(N)/N}\right)/q$ [9].



(a) q=64



(b) q=128

Fig. 2. Comparison of Hamming correlation properties for chaotic FH sequences generated by the proposed method (solid curve with "."), the method in [6][7] (solid curve with "+"), and theoretic value (dashed curve with "*").

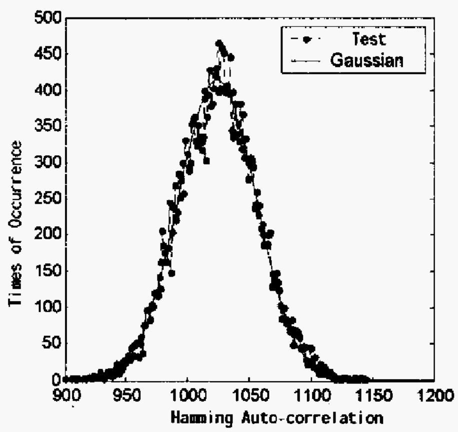


Fig. 3. The Hamming auto-correlation distribution of a chaotic FH sequence (N=32768, q=32) generated by the proposed method.

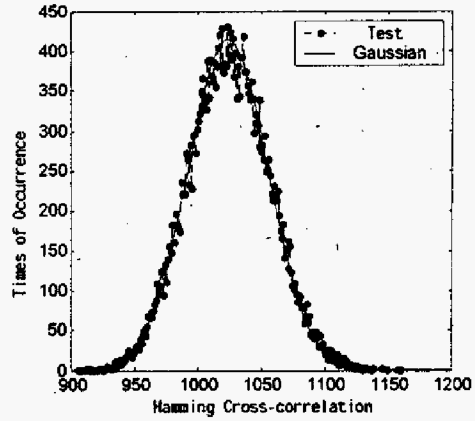


Fig. 4. The Hamming cross-correlation distribution of two chaotic FH sequences (N=32768, q=32) generated by the proposed method.

Fig. 2 shows comparison of Hamming correlation properties for chaotic FH sequences generated by proposed method, the method in [6][7], and theoretic value. As can be seen from Fig. 2, on average these two kinds of chaotic FH sequences almost have the same Hamming correlation properties and close to their theoretic value. Fig. 3 shows the auto-correlation distribution of the FH sequence generated by the proposed method. The cross-correlation distribution between two FH sequences is also illustrated in Fig. 4.

C. *Linear Complexity*

The linear complexity of a sequence is the least number of stages required to generate the sequence using a linear feedback shift register (LFSR). The linear complexity of a sequence has an important role in the anti-jamming communications. The greater the linear complexity of a sequence is, the more difficult the jammer can reconstruct this sequence. Because of theirs low linear complexity, Linear code sequences are therefore unacceptable for anti-jamming FH systems. Since chaotic sequences are inherently nonlinear and random, theirs linear complexity is roughly half of the sequence length. This near optimum linear complexity is a major advantage of the chaotic FH sequence in comparison with the classic linear FH sequence.

The linear complexity of the logistic map binary sequences generated by different methods computed by the Massey algorithm is shown in Table 1. As can be seen from Tabel 1, all results are very close to half of the sequence length.

4. Conclusion

In this paper, we proposed a new method for generating chaotic FH sequences based on chaotic map. In our method, the real-valued trajectory of chaotic system is first encoded to binary sequences by means of a quantization function, and then we can obtain chaotic FH sequences by reshaping bits of these binary sequences. Theory analysis and performance experiment results show that this sequence is Bernoulli sequence and its Hamming correlation is shown to be Poisson distributed. These FH sequences are comparable to other FH sequences on the properties of uniform distribution, Hamming correlation and linear complexity when they have the same number of frequency slots and the same period, but the map iterative number has reduced largely. Consequently, more FH sequences can be generated by this method and they are suitable for FH code-division multiple-access systems.

References

[1] Mbabane H. D. I. and Linsay P. S., *Secure Communications and Unstable periodic orbits of strange attractors.* IEEE Trans. Circuits and Syst., vol.40, no.10, pp. 643-645, Oct.1993.

[2] Frey D. R., *Chaotic digital encoding: An approach to secure communication.* IEEE Trans. Circuits and Syst., vol.40, no.10, pp.660-666, Oct.1993.

[3] Heidari-Bateni G. and McGillem C. D., *A chaotic direct-sequence spread-spectrum communication system.* IEEE Trans. Commun., vol.42, no.2/3/4, pp.1524-1527, 1994.

[4] Mazzini G., Setti G. and Rovatti R., *Chaotic complex spreading sequences for asynchronous DS-CDMA-Part I: System modeling and results.* IEEE Trans. Circuits and Syst., vol.44, no.10, pp.937-947, 1997.

[5] Ling Cong, Sun Songgeng, *Frequency-hopping sequences by the Logistic map* (in Chinese). Chin. J. Electron., vol.25, no.10, pp.79-81, 1997.

[6] Ling Cong, Sun Songgeng, *Chaotic frequency hopping sequences.* IEEE Tans. Commun., vol.46, no.11, pp.1433-1437, Nov.1998.

[7] Ling Cong, Sun Songgeng, *Frequency-hopping sequences by Chaotic maps for FH/CDMA communications* (in Chinese). Chin. J. Electron., vol.27, no.1, pp.67-69,1999.

[8] Ling Cóng, Wu Xiaofu, *Design and realization of an FPGA-based generator for chaotic frequency hopping sequences.* IEEE Trans. Circuits and Syst., vol.48, no.5, pp.521-532, 2001.

[9] Luo Wen, Gan Liangcai, *A kind of method of generating chaotic FH sequences through combined map* (in Chinese). Chin. J. Radio Science, vol.16 no.3, pp.375-378, 2001.

Table I: Linear Complexity of Chaotic Sequences

	N=200	*N=400*	*N=600*	*N=800*	*N=1000*
q=64, Method in [6][7]	100	200	301	400	500
q=64, Proposed Method	100	200	300	402	500
q=128, Method in [6][7]	100	200	300	401	498
q=128, Proposed Method	99	198	300	402	498