Design of FH Sequences Based on Chaotic Map

Mi Liang Tang Gang
Southwest Institute of Electronic & Telecommunication Technology, Chengdu China 610041
Email: ml5757@sina.com

***Abstract*—Based on one-dimensional chaotic map, a novel method for generating chaotic frequency-hopping (FH) sequences was proposed. In order to maintain the useful chaos properties of the nonlinear dynamical system as much as possible, the chaotic real-valued sequences of nonlinear maps were directly encoded to bit sequences rather than by a threshold function, then chaotic FH sequences by reshaping bits of these bit sequences were obtained. The performance analysis and experiment results show that the sequence has the same balance properties, FH number and sequence length as other FH sequences, but much less requirements of iterative operation and much more anti-jamming and anti-intercept capacities. It can be concluded that the FH sequences generated by the novel method are suitable for FH code-division multiple-access systems.**

I. INTRODUCTION

Simple deterministic systems can exhibit very complex and random behavior called chaos. 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 nonlinear dynamical system in chaotic state, have received much attention in the past years [5-10]. 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 order to get rid of this flaw, reference [8] presents a new method to generate 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 chaotic FH sequences by reshaping bits of these binary sequences were obtained. However, two level or multilevel quantization function was used to obtain the binary sequences from chaotic real-valued sequences in above all methods. This operation may destroy some useful chaos property of the real-valued sequences. In [9], 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 generate FH sequences by one-dimensional (1-D) chaotic map. During the construction of FH sequences, quantization function was not used to maintain the chaotic properties of the nonlinear dynamical system as much as possible. The FH sequence has the same balance properties, FH number and sequence length as other FH sequences, but much less requirements of iterative operation and much more anti-jamming and anti-intercept capacities.

The rest of the paper is organized as follows. Section 2 presents a new approach to design FH sequences based on 1-D chaotic map in detail. Experimental results and performance tests are described in section 3. Finally, in section 4 the conclusion is given.

II. CHAOTIC FH SEQUENCES DESIGN

The 1-D chaotic map that can be described by

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

where $x_n \in I, n = 0,1,2,\Lambda$, and $f : I \to I$ is a nonlinear map. As is well known, Logistic map is the most common 1-D chaotic map, which is defined by

$$x_{n+1} = 4x_n(1-x_n), \quad x_n \in [0,1] \tag{2}$$

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

$$\rho(x) = \begin{cases} \dfrac{1}{\pi\sqrt{x(1-x)}}, & x \in (0,1) \\ 0, & Otherwise \end{cases} \tag{3}$$

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

Let $X = \{X_0, X_1, \Lambda , X_{N-1}\}$ denote a frequency hopping sequence of length N , $X_n \in \{f_0, f_1, \Lambda , f_{q-1}\}$, where f_i is one of the q frequency slots. A frequency hopping sequence is desired to be uniformly distributed on q frequency slots.

We write the Logistic map value of x_n in a floating-point number with m bits:

0-7803-9128-4/05/$20.00 © 2005 IEEE.

$$x_n = 0.b_1(x_n)b_1(x_n)\Lambda\ b_i(x_n)\Lambda\ b_m(x_n),$$
$$b_i(x_n) \in \{0,1\}. \quad (4)$$

The i-th bit $b_i(x_n)$ can be expressed as

$$b_i(x_n) = \sigma_{1/2}\left(2^{i-1}x_n - \lfloor 2^{i-1}x_n \rfloor\right) \quad (5)$$

where $\lfloor x \rfloor$ denotes the maximum integer not exceeding x, and a threshold function $\sigma_c(x)$ is defined as

$$\sigma_c(x) = \begin{cases} 0, & x \le c \\ 1, & x > c \end{cases}. \quad (6)$$

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 Logistic map, and then extract $\log_2 q$ bits from m bits of x_n is given by

$$X_n = D(x_n) = b_{j+1}(x_n)b_{j+2}(x_n)\Lambda\ b_{j+\log_2 q}(x_n),$$
$$b_i(x_n) \in \{0,1\} \quad (7)$$

where j denotes a positive integer. Then, we can obtain a matrix like

$$\begin{bmatrix} b_{j+1}(x_0) & b_{j+2}(x_0) & \Lambda & b_{j+\log_2 q}(x_0) \\ b_{j+1}(x_1) & b_{j+2}(x_1) & \Lambda & b_{j+\log_2 q}(x_1) \\ \mathrm{M} & \mathrm{M} & \mathrm{O} & \mathrm{M} \\ b_{j+1}(x_{N-1}) & b_{j+2}(x_{N-1}) & \Lambda & b_{j+\log_2 q}(x_{N-1}) \end{bmatrix}. \quad (8)$$

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. In addition, a nonlinear transform is performed during the construction of the FH sequences, so these sequences have much more anti-jamming and anti-intercept capacities than the conventional FH sequences.

This method can easily be extended to the 1-D chaotic map. The chaotic FH sequence generated by this method is Bernoulli sequence. The proof is straightforward and was omitted in this paper.

III. 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]. We set $j = 6$ and $m = 51$ in the below tests.

A. *Chi-Squared Tests*

First, We perform the standard chi-squared test to compare 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

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

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.

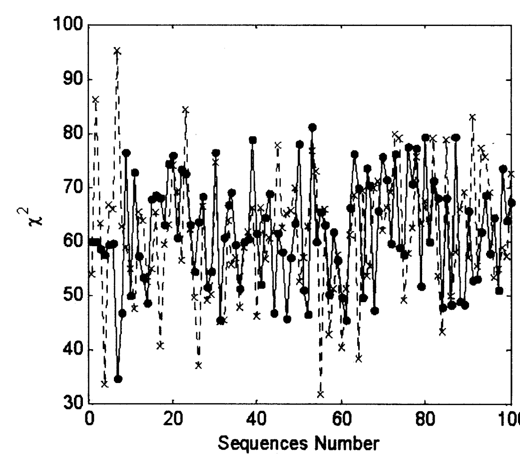


Fig. 1. Comparison of the chi-squared values for test of 1-D uniform distribution for chaotic FH sequences generated by proposed method (solid curve with ".") and the method in [6][7] (dashed curve with "x").

B. *Hamming Correlation Properties*

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

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

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

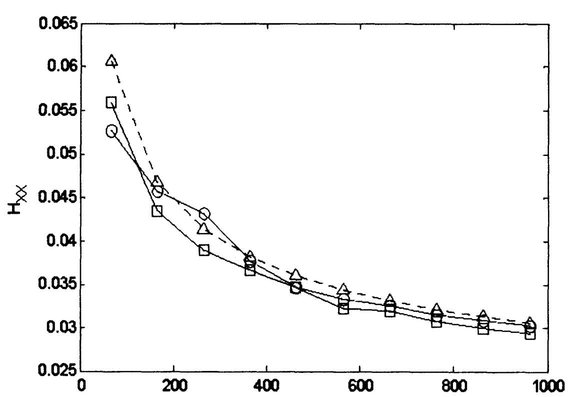
$$H_{XX} = \max_{1\le\tau<N}\{H_{XX}(\tau)\}/N \ , \tag{11}$$

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

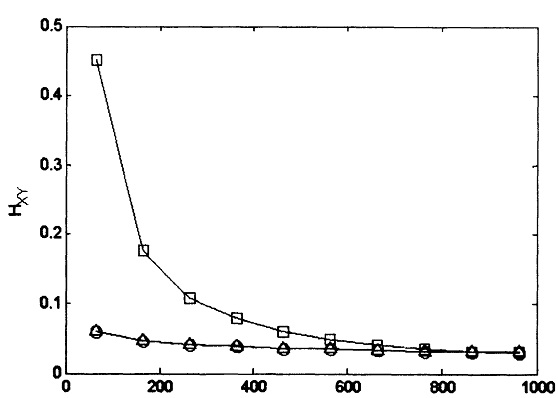
These two measures have been used as the basis for comparing the Hamming correlation properties of chaotic FH sequences. These two measures almost have the same theoretic value $\left(1+\sqrt{2q\ln(N)/N}\right)/q$ [10].

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 auto-correlation properties and close to their theoretic value, but the chaotic FH sequences generated by the proposed method have better Hamming cross-correlation properties than the FH sequences generated by the method in [6][7].

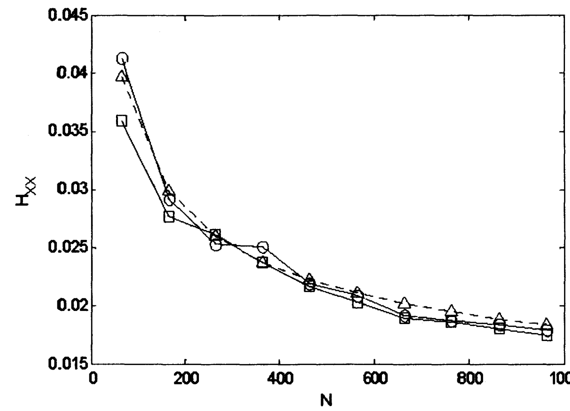
Fig. 3 shows the auto-correlation distribution of the FH sequence generated by the proposed method. The cross-correlation distribution between two FH sequences is also illustrated in Fig. 4. We can see that the Hamming correlation of chaotic FH sequences is asymptotically Gaussian.



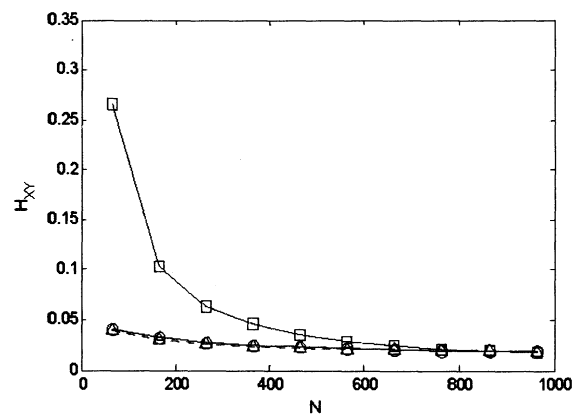
(a) Hxx (q=64)



(b) Hxy (q=64)



(c) Hxx (q=128)



(d) Hxy (q=128)

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

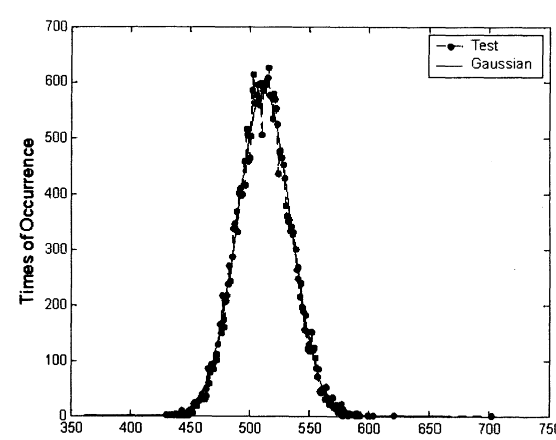


Fig. 3. The Hamming auto-correlation distribution of a chaotic FH sequence of period 32768 for q=64 generated by the proposed method.

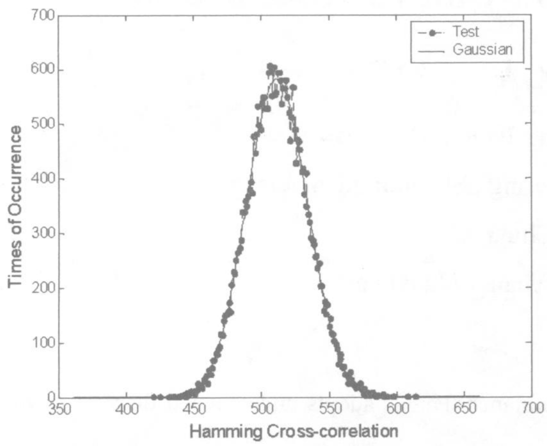


Fig. 4. The Hamming cross-correlation distribution of two chaotic FH sequences of period 32768 for q=64 generated by the proposed method.

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.

IV. CONCLUSION

In this paper, we proposed a new method for generating chaotic FH sequences based on 1-D chaotic map. In order to maintain the useful chaos properties of the nonlinear dynamical system as much as possible, the chaotic real-valued sequences of nonlinear maps were directly encoded to bit sequences rather than by a threshold function, then chaotic FH sequences by reshaping bits of these bit sequences were obtained. The performance analysis and experiment results show that the sequence has the same balance properties, FH number and sequence length as other FH sequences, but much less requirements of iterative operation and much more anti-jamming and anti-intercept capacities. It can be concluded that the FH sequences generated by the novel method are suitable for FH code-division multiple-access systems.

REFERENCES

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

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

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

[4] G. Mazzini, G. Setti, and R. Rovatti, "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] Mi Liang, Zhu Zhongliang, "Chaotic frequency-hopping sequences based on Logistic map (in Chinese)," *Chin. J. Radio Science*, vol.19 no.3, pp.333-337, 2004.

[9] Ling Cong, 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.

[10] 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 1: Linear Complexity of Chaotic Sequences

	N=200	*N=400*	*N=600*	*N=800*	*N=1000*
q=64, Method in [6][7]	100	200	299	399	500
q=64, Proposed Method	101	200	301	400	502
q=128, Method in [6][7]	101	199	300	402	499
q=128, Proposed Method	101	200	300	399	500