CHAOTIC SPREAD-SPECTRUM SEQUENCE GENERATED BY MULTILEVEL QUANTIFYING AND THEIR PROPERTIES

An Chengquan , Zhou Tingxian
Harbin Institute of Technology, P.O.Box 337, Harbin, China 150001

ABSTRACT

According to the advantages of chaotic analog sequences and chaotic binary sequences, this paper proposes a method generating chaotic binary spread-spectrum sequence by multilevel quantifying. This paper proved that even correlation and odd correlation between such sequences of length N are all Gaussian distributed with mean 0 and variance N, the even of mean-square cross-correlation is N, and the variance of mean-square cross-correlation is $2N$. The method can increase the number of chaotic sequences, made the spread-spectrum system more secure. The theoretical analyses and the results of simulation show that the performance of such sequence general is as same as traditional spread-spectrum sequence, its number is very large, and can be used in CDMA in future.

KEY WORDS

Chaos, Spread-spectrum sequences, Correlation.

INTRODUCTION

In recent years, there has been growing interest in the chaotic behavior in non-linear dynamic systems, researchers are looking for its possible application in communication. In some systems, the synchronization properties of chaotic systems have been used in secure communication. Other researchers present the use of chaos for spread-spectrum communication[1][2][4][6][8].

There are two kinds of chaotic sequences used in direct-sequence spread-spectrum communication: real sequence and binary sequence[2]. Because real sequence is not compatible to most existing communication systems, most recent research concentrates on binary chaotic sequence. To generate binary chaotic sequence, firstly starting with an initial condition x_0, repeated applications of the Logistic map or Chebyshev map give rise to the real sequence $\{x_k : k = 0, 1, 2\cdots\}$, then the sequence $\{c_k = \mathrm{sgn}(x_k) : k = 0, 1, 2\cdots\}$ is the binary chaotic spread-spectrum sequence[1][2][4][6]. The sequence has good correlation properties, and their number is large, suitable to be used in CDMA

system. But most research result didn't concern that most chaotic systems are realized in finite precise, thus the sequences generated by chaotic map must be finitely periodic, and therefore the number of spread spectrum sequences generated by chaotic map would decrease[6].

States of the chaotic real sequences generated by computer iteration amount to the dozenths power of 2, but normal method generating chaotic binary sequence by binary quantifying chaotic real sequence lost most information. Different from above method, this paper presents a method generating chaotic binary sequences by multilevel quantifying, this method can increase the number of chaotic spread-spectrum sequences, improve the security of communication system, and the performance of this kind of sequence is same as that of sequence in reference[1][2][4]. According to the conclusion in reference[7], the performance of CDMA communication system is closely related to the mean-square cross-correlation value of the spread-spectrum sequence, the peak cross-correlation merely indicates the worst instance. Now some research give simulation of mean-square cross-correlation of chaotic sequences[7], but this is insufficient, this paper presents the analysis of mean-square cross-correlation between chaotic spread-spectrum sequences.

THE METHOD GENERATING CHAOTICSEQUENCE BY MULTILEVEL QUANTIFYING

Principle of the method is as follow:

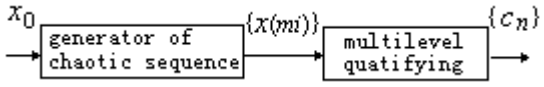

Figure.1 Principle of generating chaotic sequence by multilevel quantifying

With the initial value x_0, the generator of chaotic sequences generate chaotic real sequence $\{x(mi): i=1, 2,\ldots\}$ by iterating Logistic map at interval m, where $x\in(0, 1)$. The chaotic map can also be Chebyshev map, then convert $\{x(mi)\}$ from (-1, 1) to (0, 1) through linear transform.
Transform $x(mi)$ to binary

$$x\ (mi) = 0.b_0(i)b_1(i)b_2(i)\cdots \tag{1}$$

Quantify $x(mi)$ evenly in 2^r level ($m\geq r\geq 1$), the quantifying result is

$$x_T(mi) = b_0(i)b_1(i)\cdots b_{r-1}(i) \tag{2}$$

where $b_l(i)\in\{0,1\}\ \square\ l\in\{0,1,\cdots r-1\}$ and

$$\sum_{l=0}^{r-1} 2^{-(l+1)} b_l(i) < x(mi) < \sum_{l=0}^{r-1} 2^{-(l+1)} b_l(i) + 2^{-r} \tag{3}$$

Link $x_T(mi)$,(i=0,1…)together to the sequence $\{b_n\}_{n=0}^{N-1}$

$$\{b_n : b_n = b_l(i), n = ri + l = 0,1,2\cdots N-1\} \tag{4}$$

Replace 0 to –1 in $\{b_n\}_{n=0}^{N-1}$, that is

$$\{c_n : c_n = \mathrm{sgn}(b_n - 0.5), n = 0,1,2\cdots N-1\} \tag{5}$$

$\{c_n\}_{n=0}^{N-1}$ is the chaotic binary spread-spectrum sequence generate by multilevel quantifying.

Generating sequence $\{x(mi)$: i =0, 1, 2…$\}$ by iteration at interval m can ensure the sensitive dependence of chaotic sequence $\{c_n\}_{n=0}^{N-1}$ on their initial conditions x_0, and $m \geq r$.

PERFORMANCE ANALYSIS OF THE SEQUENCE GENERATED BY MULTILEVEL QUANTIFYING

The performance of the asynchronous DS/CDMA system depends on the even correlation function

$$R_{uv}(\tau) = C_{uv}(\tau) + C_{uv}(\tau - N) \tag{6}$$

and odd correlation function

$$\theta_{uv}(\tau) = C_{uv}(\tau) - C_{uv}(\tau - N) \tag{7}$$

$C_{uv}(\tau)$ is part correlation function, define as

$$C_{uv}(\tau) = \begin{cases} \sum_{n=0}^{N-1-\tau} u_n v_{n+\tau} & 0 \leq \tau \leq N-1 \\ \sum_{n=0}^{N-1-\tau} u_{n-\tau} v_n & 1-N \leq \tau \leq 0 \\ 0 & |\tau| \geq N \end{cases} \tag{8}$$

where $\{u_n\} \square \{v_n\} \square \{-1 \square 1\}$ are binary sequences of length N. Taking the peak of even correlation as criteria, some researcher has generated the optimal sequence families, which reach the Welch lower bound, such as Kasmi sequence (small set), Bent sequence. On odd correlation, which is as important as even correlation, little research had accomplished, and it is hard to generate sequences with good even correlation property and good odd correlation property.

Lemma: The sequence $\{c_n\}_{n=0}^{N-1}$ generated by Equ.5 is variable which is independent and distributed uniformly.

Proof: The Lyapunov exponent of Logistic map and Chebyshev map is In2, if binary value $x_T(mi)$ is r bits and certain, this correspond that real value $x(mi)$ has r bits certain information. After $m(m \geq r)$ time Logistic maps, $x(m(i+1))$ will lost all certain information, so $x_T(m(i+1))$ and $x_T(mi)$ are independent. Quantifying $x(mi)$ evenly in 2^r level is equal to iterating Saw-Tooth Map r time with initial value $x(mi)$ to generate real sequences $(x'_0(i), x'_1(i), \cdots x'_{r-1}(i))$ of length r and quantifying this sequence to binary sequence, that is $b_l(i) = 0.5(\mathrm{sgn}(x'_l(i)) + 1)$ in Equ.2, where $l = 0,1,\cdots r-1$. Saw

Tooth Map is chaotic map whose Lyapunov exponent is ln2.

$$x_{i+1} = g(x_i) = \begin{cases} 2x_i & 0 \le x_i < 0.5 \\ 2x_i - 1 & 0.5 \le x_i < 1 \end{cases} \tag{9}$$

Because the probability density of orbit distribution of Saw Tooth Map is $\rho(x) = 1$, and $x_T(m(i+1))$, $x_T(mi)$ are independent, whether b_n is 1 or 0, the probability of b_{n+1} =0 or b_{n+1}=1 are 0.5. So whatever c_n is, the probability of c_{n+1} = -1 or c_{n+1} =1 are 0.5. Regard $\{c_n\}_{n=0}^{N-1}$ as Markov chain, each element of its one pace shift matrix is 0.5, and its k paces shift matrix is $\boldsymbol{P}^k = \boldsymbol{P}(k \neq 0)$, according the Markov property of sequence, $\{c_n\}_{n=0}^{N-1}$ is independent and distributed uniformly.

Theorem1: $\{u_n\}_{n=0}^{N-1}$, $\{v_n\}_{n=0}^{N-1}$ are binary chaotic sequences generated by Equ.5 with large length N, the even cross-correlation, odd auto-correlation, even auto-correlation sidelobe and odd auto-correlation sidelobe between $\{u_n\}_{n=0}^{N-1}$ and $\{v_n\}_{n=0}^{N-1}$ are Gauss distributed, with mean 0 and variance N.

Proof: $\{c_n\}_{n=0}^{N-1}$ is independent and distributed uniformly, so $\{u_n\}_{n=0}^{N-1}$ and $\{v_n\}_{n=0}^{N-1}$ are independent and distributed uniformly. Because of the sensitive dependence on initial condition, The sequences $\{u_n\}_{n=0}^{N-1}$ and $\{v_n\}_{n=0}^{N-1}$ are independent each other. From Equ.6, Equ.7, it can be seen that the even correlation and odd correlation have same distribution. So only search even correlation is sufficient. The even correlation is as followed:

$$R_{uv}(\tau) = \sum_{n=0}^{N-1} u_n v_{n+\tau} \tag{10}$$

When $\{u_n\}_{n=0}^{N-1} \neq \{v_n\}_{n=0}^{N-1}$, $u_n v_{n+\tau}$ is independent and distributed uniformly to all n, the rule of distribution is $P(-1) = P(1) = 0.5$, with mean 0 and variance 1. On the basis of center limit theorem, when N is large, Equ.10 is Gauss distributed with mean 0 and variance N. As $\{u_n\}_{n=0}^{N-1} = \{v_n\}_{n=0}^{N-1}$, Equ.10 is autocorrelation, if $\tau \neq 0$, the analysis of autocorrelation is as same as that of cross-correlation, so auto-correlation sidelobe is Gauss distributed with mean 0 and variance N.

In a DS/CDMA system (BPSK) of K user, the input signal-to-noise ratio of ith user is[7]

$$SNR_i \approx \left\{ (6N)^{-3} \sum_{\substack{k=1 \\ k \neq i}}^{K} \left[\sum_{\tau=0}^{N-1} R_{ki}^2(\tau) + \sum_{\tau=0}^{N-1} \theta_{ki}^2(\tau) \right] + \frac{N_0}{2E_b} \right\}^{-1/2} \tag{11}$$

It shows that SNR of an asynchronous DS/CDMA system is close related to the mean-square cross-correlation value between sequence. There are analysis of mean-square cross-correlation in the following paragraph.

The even of mean-square cross-correlation between sequence in Equ.5 is

$$E[\frac{1}{N}\sum_{\tau=0}^{N-1} R_{uv}^2(\tau)] = E[R_{uv}^2(\tau)] = D[R_{uv}(\tau)] = N \tag{12}$$

The variance of mean-square cross-correlation between sequence in Equ.5 is

$$D[\frac{1}{N}\sum_{\tau=0}^{N-1} R_{uv}^2(\tau)] = \frac{1}{N} D[R_{uv}^2(\tau)] = \frac{1}{N}\{E[R_{uv}^4(\tau)] - \{E[R_{uv}^2(\tau)]\}^2\}$$

$$= \int_{-\infty}^{\infty} x^4 \cdot \frac{1}{\sqrt{2\pi N}} \exp(-\frac{x^2}{2N}) dx - N = 2N \tag{13}$$

From above analysis, it can be seen that the performance of chaotic sequences generated by multilevel quantifying is as same as that of chaotic sequences presented in reference[1][2][4][6]. In fact, the method generating chaotic sequence in reference[1][2][4][6] is an example of the method presented in this paper when $r = m = 1$. Because r, m is variable, the number of sequences generated by the method in this paper is larger than the number of sequences generated by the method in reference[1][2][4][6].

SIMULATION RESULT

The results of computer simulation coincide with the theoretic analysis. Figure.2 and Figure.3 are simulation results of even cross-correlation and odd cross-correlation of sequences generated by the method in this paper, where $N = 4096$, $r = m = 50$, the chaotic map is logistic map, and the initial value is 0.001 and 0.0011.

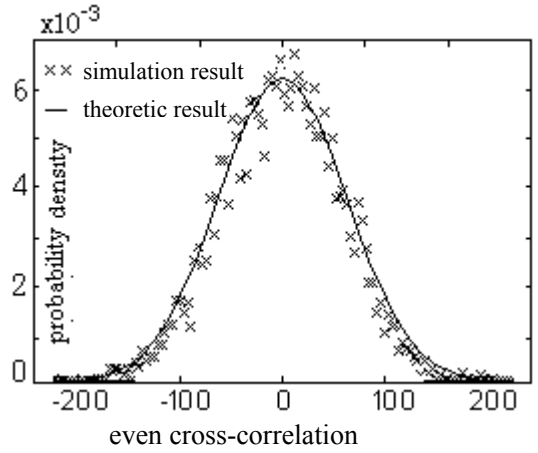

Figure.2 Distribution of even cross correlation

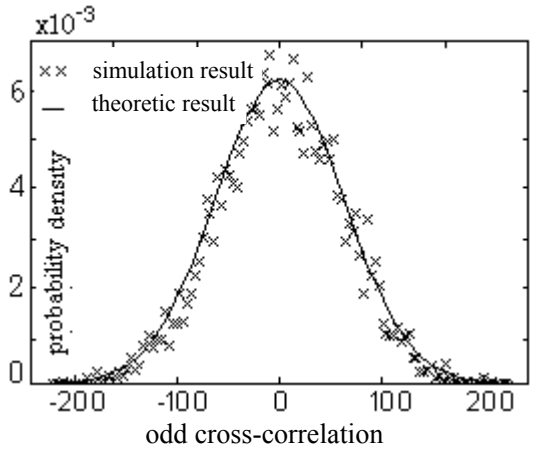

Figure.3 Distribution of odd cross-correlation

Table.1 give the performance comparison of the sequence generated by multilevel quantifying and other spread sequence. ‘sequences in this paper’ is the sequence generated by multilevel qualifying and chaotic map is Logistic map. ‘sequence in reference[1][2]’ is the chaotic sequence presented in reference[1][2]. From the data in table.1, it can be seen performance of chaotic sequences generated by multilevel quantifying general is as same as that of other spread spectrum sequences.

Table 1 Performance comparison of the sequences

sequence	$\max\|R_{uv}(\tau)\|$	$\frac{1}{N}\sum_{\tau=0}^{N-1}R_{uv}^2(\tau)$	$\max\|\theta_{uv}(\tau)\|$	$\frac{1}{N}\sum_{\tau=0}^{N-1}\theta_{uv}^2(\tau)$
sequences in this paper				
r=m=40	228	3942	229	4093
r=m=20	222	3925	217	4110
r=m=10	219	4026	231	3976
r=m=4	239	4103	213	4060
sequences in reference[1][2]	218	3979	224	4003
m sequence	255	4078	225	4151
Bent sequence	65	4026	215	3956

CONCLUSION

This paper presents a method generating chaotic sequences in detail, and prove that the even correlation and odd correlation between such sequences of length N are all Gaussian distributed, with mean 0 and variance N, the even of mean-square cross-correlation is N, and the variance of mean-square cross-correlation is $2N$. The method can increase the number of chaotic sequences, made the spread spectrum more secure. The performance of such sequence general is as same as traditional spread-spectrum sequence, so the sequences can be used in CDMA system in the future.

REFERENCE

1 Wang Hai, Hu Jiandong. Logistic-Map chaotic spread-spectrum sequence ACTA ELECTRONICA SINICA 1997 Vol.25 No.1 19-23.

2 Ling Cong, Sun Songgeng. The Generator of Chaotic Spread-Spectrum Sequence. JOURNAL OF ELECTRONICS. 1998. Vol.20 No.2 235-239

3 Hao Bai-Lin Starting With Parabolas — An Introduction to Chaotic Dynamic. Shanghai Scientific and Technological Education Publishing House, SHANGHAI,1993

4 Cai Guoquan, Song Guowen, Yu Dapeng. On properties of logistic-map chaotic spread spectrum sequences. JOURNAL OF CHINA INSTITUTE OF COMMUNICATIONS 2000 Vol.21.No.1 60-63.

5 Zhou Hong, Ling Xieting. Realizing Finite Precision Chaotic System via Perturbation of m-sequence. ACTA ELECTRONICA SINICA 1997 Vol.25 No.7 95-97.

6 Ling Cong , Sun Songgeng. Correlation Distribution of Spread Sequence by Logistic Maps. ACTA ELECTRONICA SINICA 1999 Vol.27 No.1 140-141.

7 K.H Karkkainen. Meaning of maximum and mean-square cross-correlation as a performance measure for CDMA code families and their influence on system capacity. IEICE Trans commun, 1993, E76-B(8): 848 – 854

8 An Chengquan, Zhou Tingxian. Generating Spread Spectrum Sequences by a Class of Chaotic Maps. Journal of Telemetry, Tracking, and Command 2002 Vol.23 No.2 8-11