A METHOD OF GENERATING CHAOTIC SPREAD-SPECTRUM SEQUENCES BASED ON MULTILEVEL QUANTIFICATION

An Chengquan , Zhou Tingxian

Harbin Institute of Technology, China, Harbin, 150001

ABSTRACT

According to the advantages of chaotic analog sequences and chaotic binary sequences, this paper presents a method of generating chaotic binary spread-spectrum sequences by multilevel quantifying. This paper proves that the even correlation and odd correlation between such sequences of length N are Gauss distributed, with mean 0 and variance N. The performance of CDMA communication system is closely related to the mean-square cross-correlation value between sequences, so this paper also presents the distribution of the mean-square cross-correlation value between the sequences. The sequences have good correlation properties and a large amount of such sequences can be generated. The results of simulation verify the correctness of the theoretical analysis.

1. INTRODUCTION

In recent years, there has been growing interest in the chaotic behavior in non-linear dynamic system. Researchers are looking for its possible application in communication, some have used the synchronization properties of chaotic systems in secure communication, others have presented the application of chaos in spread-spectrum communication [1], [2], [4], [6], [7].

There are two kinds of chaotic sequences used in direct-sequence spread-spectrum communication: real sequences and binary sequences [4]. Because real sequences are not compatible to most existing communication systems, most recent researches focus on binary chaotic sequences. To generate a 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 a binary chaotic spread-spectrum sequence [1], [4], [6]. The sequences have good correlation properties and their quantity is large which make them suitable for CDMA system. But in most research chaotic systems are realized at finite precision, thus the sequences generated by chaotic map must be finitely periodic, and therefore the quantity of spread-spectrum sequences will decrease [8].

States of the chaotic real sequences generated by computer iteration amount to the dozenths power of 2, but traditional methods generating chaotic binary sequences by binary quantifying chaotic real sequences lose 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 correlation of this kind of sequence is the same as that of sequence in [1], [4], [6]. According to the conclusion in [3], 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 researches give simulation of mean-square cross-correlation of chaotic sequences [3], but no theoretical analysis is given. This paper presents a detailed theoretical analysis of the distribution of mean-square cross-correlation between chaotic spread-spectrum sequences.

This paper is organized as follows. In Section 2 we present the method in details. In section 3, we analyze the performance of the chaotic spread-spectrum sequences, and present the distribution of the correlation and the mean-square correlation between the sequences. In section 4, Simulation results are given and a comparison is made among different sequences. In section 5, some conclusions are drawn finally.

2. PRINCIPLE OF THE METHOD

Principle of the method is as follow:

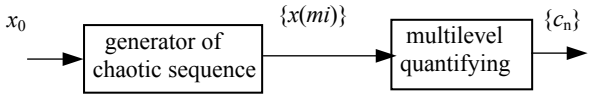

Figure.1 Principle of generating chaotic sequence by multilevel quantifying

With the initial value x_0, the generator of chaotic sequences generates chaotic real sequence $\{x(mi): i=1, 2,\cdots\}$ by iterating Logistic map at interval m, where $x \in (0, 1)$. The chaotic map can also be Chebyshev map where $\{x(mi)\}$ should be converted 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 result is

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

where $b_l(i) \in \{0, 1\}$, $l \in \{0, 1, \cdots r-1\}$ 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$\cdots$) 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 with –1 in $\{b_n\}_{n=0}^{N-1}$, that is

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

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

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

3. PERFORMANCE ANALYSIS

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

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

and odd correlation function

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

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

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

where $\{u_n\}$、$\{v_n\} \in \{-1, 1\}$ are binary sequences of length N. Taking the peak of even correlation as criteria, some researchers have 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, few researches has been accomplished. 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 (5) is a 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, which indicating that real value $x(mi)$ has r bits certain information, after $m(m \geq r)$ times Logistic maps, $x(m(i+1))$ will lose all certain information, so $x_T(m(i+1))$ and $x_T(mi)$ are independent.

Quantifying $x(mi)$ evenly in 2^r levels is equivalent to iterating Saw-Tooth Map r times 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 which is $b_l(i) = 0.5(\mathrm{sgn}(x'_l(i)) + 1)$ in (2). Saw Tooth Map, as shown in (9), is chaotic map whose Lyapunov exponent is ln2.

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

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 is 0.5. So whatever c_n is, the probability of c_{n+1} = -1 or c_{n+1} =1 is 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-pace shift matrix is $\boldsymbol{P}^k = \boldsymbol{P}(k \neq 0)$. According to 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 (5) with large length N, the even cross-correlation, odd cross-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 (6), (7), it can be seen that the even correlation and odd correlation have the same distribution. So only researching even correlation is sufficient. The even correlation is as follows:

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

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, (10) is Gauss distributed with mean 0 and variance N. As $\{u_n\}_{n=0}^{N-1} = \{v_n\}_{n=0}^{N-1}$, (10) is auto-correlation and $\tau \neq 0$, the analysis of auto-correlation 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 users, the input signal-to-noise ratio of the ith user is [3]

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

It shows that SNR of an asynchronous DS/CDMA system is closely related to the mean-square cross-correlation value between sequences.

Theorem 2: $\{u_n\}_{n=0}^{N-1}$, $\{v_n\}_{n=0}^{N-1}$ are binary chaotic sequences generated by (5) with large length N, the mean-square cross-correlation between $\{u_n\}_{n=0}^{N-1}$ and $\{v_n\}_{n=0}^{N-1}$ is $\chi^2(N)$ distributed.

Proof: Considering that the even cross-correlation and odd cross-correlation have the same distribution, here we only analyze the mean-square even cross-correlation. From theorem 1,

it can be seen that $R_{uv}(\tau)$ and $R_{uv}(\eta)$ ($\tau \neq \eta$)are Gauss distributed with mean 0 and variance N, and there is

$$\begin{aligned} & E[R_{uv}(\tau) \cdot R_{uv}(\eta)] \\ &= E[(\sum_{n=0}^{N-1} u_n v_{n+\tau}) \cdot \sum_{n=0}^{N-1} (u_n v_{n+\eta})] \\ &= \sum_{n=0}^{N-1} \sum_{m=0}^{N-1} E(u_n v_{n+\tau} u_m v_{m+\eta}) \\ &= \sum_{n=0}^{N-1} \sum_{m=0}^{N-1} E(u_n u_m) E(v_{n+\tau} v_{m+\eta}) = 0 \\ &= E[R_{uv}(\tau)] \cdot E[R_{uv}(\eta)] \end{aligned} \tag{12}$$

So $R_{uv}(\tau)$ and $R_{uv}(\eta)$ ($\tau \neq \eta$) are unrelatable, and hence they are independent. From above conclusion, $R_{uv}(\tau)/\sqrt{N}$ and $R_{uv}(\eta)/\sqrt{N}$ ($\tau \neq \eta$) are independent each other and Gauss distributed with mean 0 and variance 1, so $\frac{1}{N}\sum_{\tau=0}^{N-1} R_{uv}^2(\tau)$ is $\chi^2(N)$ distributed with mean N and variance $2N$ and its probability density is as follows

$$p(x) = \begin{cases} \dfrac{1}{2^{\frac{N}{2}}\Gamma(\frac{N}{2})} x^{\frac{N}{2}-1} e^{-\frac{x}{2}} & x > 0 \\ 0 & x \leq 0 \end{cases} \tag{13}$$

where $\Gamma(s) = \int_0^{\infty} x^{s-1} e^{-x} dx, s > 0$.

From above theorem, it can be clearly seen what concluded in [1], [4], [6] through simulation meets well with theoretical analysis in this paper. In fact, the method generating chaotic sequence in [1], [4], [6] is a special instance of the method presented in this paper when $r = m = 1$. Because r, m is variable, the number of sequences generated by the proposed method in this paper is larger than that of the method in [1], [4], [6].

4. SIMULATION RESULT

The following figures are simulation results.

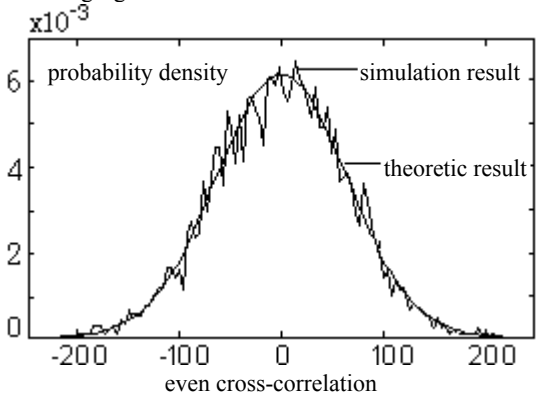

Figure.**2** Distribution of even cross-correlation

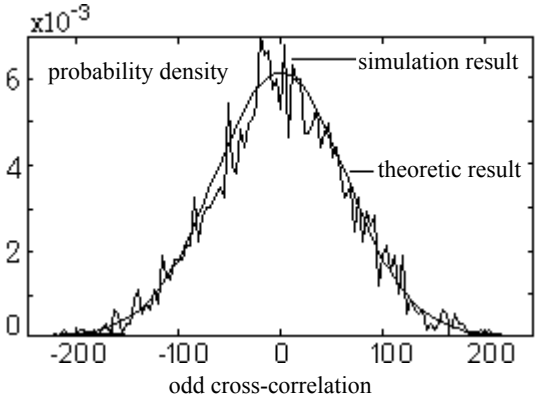

Figure.3 Distribution of odd cross-correlation

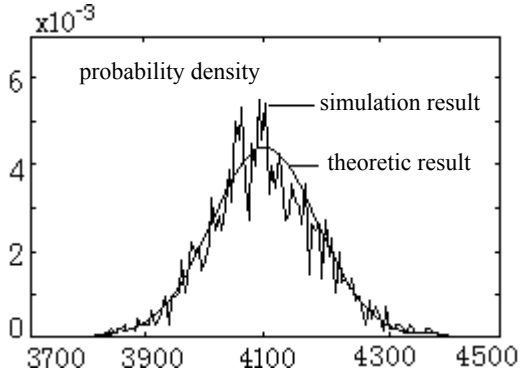

Figure.4 Distribution of mean-square even cross-correlation

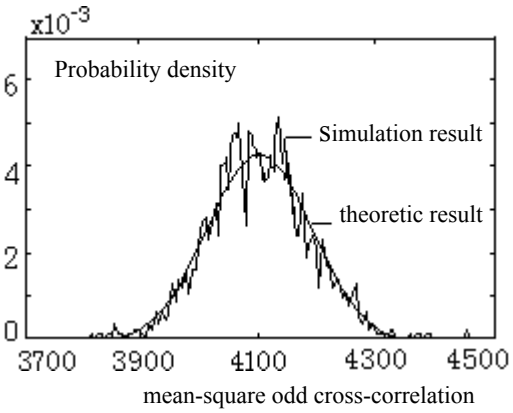

Figure.5 Distribution of mean-square odd cross-correlation

Figure.2 and Figure.3 are simulation results of even cross-correlation and odd cross-correlation of sequences generated by the proposed method, where $N = 4096$, $r = m = 50$, the chaotic map is logistic map and the initial values are 0.001 and 0.0011.

Figure.4 and Figure.5 are simulation results of mean-square even cross-correlation and mean-square odd cross-correlation between chaotic sequences. They are the statistic results after calculating 1000 mean-square cross-correlation results randomly.

Table.1 give the performance comparison of the sequences generated by multilevel quantifying and other spread-sequences. The 'MCL sequence' is the sequence generated by multilevel qualifying and the chaotic map is Logistic map. The 'MCC sequence' is the sequence generated by multilevel qualifying and the chaotic map is Chebyshev map, the 'C sequence ' is the chaotic sequence presented in [4], [6]. From table.1, it can be seen that the performance of chaotic sequences generated by multilevel quantifying almost is the same as that of other spread spectrum sequences.

Table 1 Performance comparison of the sequences

sequence	$\max\lvert R_{uv}(\tau)\rvert$	$\frac{1}{N}\sum_{\tau=0}^{N-1}R_{uv}^2(\tau)$	$\max\lvert \theta_{uv}(\tau)\rvert$	$\frac{1}{N}\sum_{\tau=0}^{N-1}\theta_{uv}^2(\tau)$
MCL sequence				
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
MCC sequence				
R=m=40	223	4097	216	4076
R=m=20	231	4080	231	3898
r=m=10	220	4011	228	4143
r=m=4	217	3986	225	4043
C sequences	218	3979	224	4003
m sequence	255	4078	225	4151
Bent sequence	65	4026	215	3956

5. CONCLUSION

This paper presents a method of generating chaotic sequences in details and proves that the even correlation and odd correlation between such sequences of length N are all Gauss distributed, with mean 0 and variance N, the mean-square cross-correlation are $\chi^2(N)$ distributed.

The method can increase the quantity of the chaotic sequences and make the spread spectrum communication more secure. The correlation of such sequences is almost the same as traditional spread-spectrum sequences, so the sequences can be used in CDMA system.

6. REFERENCES

[1] An Chengquan, Zhou Tingxian. Generating Spread Spectrum Sequences by a Class of Chaotic Maps. Proceeding of Annual International Telemetering Conference USA 2001. Vol XXXVII, p762-776, LAS VEGAS 2001

[2] Ghobad Heidari-Bateni, Clare D. McGillem. A Chaotic Direct-Sequence Spread-Spectrum Communication System IEEE Trans.on Communications, 1994, 42:1524-1527

[3] 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

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

[5] Manuel Delgado-Restituto, Angel Rodriguez-Vazquez. Mixed-Signal Map-Configurable Integrated Chaos Generator for Chaotic Communications IEEE Transactions on Circuits and System I: Fundamental Theory and Applications, VOL.48,NO12, Dec12, 2001 p1462-1474.

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

[7] Zhiwen Zhu, Henry Leung. Adaptive Blind Equalization for Chaotic Communication Systems Using Extended-Kalman Filter. IEEE Transactions on Circuits and System-I:Fundamental Theory and Applications Vol.48, No.8 979-989.

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