数理解析研究所講究録
1011 巻 1997 年 89-106

Chaotic Binary Sequences with Their Applications to Communications

Tohru KOHDA and Akio TSUNEDA
Department of Computer Science and Communication Engineering,
Kyushu University

Abstract: In spread spectrum systems, a lot of pseudo-random numbers with good properties are required as spreading sequences, most of which are generated by linear feedback shift register (LFSR). In this paper, we propose chaotic binary sequences which are based on chaos generated by one-dimensional nonlinear ergodic maps, and evaluate their performances in spread spectrum systems. Furthermore, we propose an image communication system based on SS techniques which utilize characteristics of chaotic binary sequences.

1 Introduction

Spread spectrum techniques are due primarily to properties of spreading sequences (or pseudonoise (PN) sequences)[1]. Various classes of PN sequences have been proposed most of which are generated by LFSR (linear feedback shift registers) such as the families of the Gold sequences and of the Kasami sequences with low even-correlation values [1]. On the other hand, we proposed simple methods to obtain binary sequences from chaotic trajectories generated by nonlinear ergodic maps whose even and odd correlation functions can be theoretically given. The empirical distributions of correlation values of chaotic bit sequences are shown to tend to the Gaussian distribution.

In this paper, we investigate the performance of chaotic binary sequences as spreading sequences empirically and theoretically. Furthermore, we propose an image communication system based on SS techniques which utilize characteristics of chaotic binary sequences.

2 CDMA System Based on Direct Sequence Spread Spectrum

In direct sequence spread spectrum (DS/SS) systems, data symbols are directly multiplied by a pseudonoise (PN) code or a spreading code, which is independent of the data. Such systems are due primarily to properties of spreading sequences(or PN sequences) [1]. For the most fundamental technique, both data symbols and code symbols are bipolar. Figure 1 shows a model of a CDMA system based on such DS/SS techniques. For simplicity, we consider baseband communications. In such a system, spread spectrum signals of J users, $s^{(j)}(t)$, $j = 1, 2, \cdots, J$, are transmitted through a common channel simultaneously.

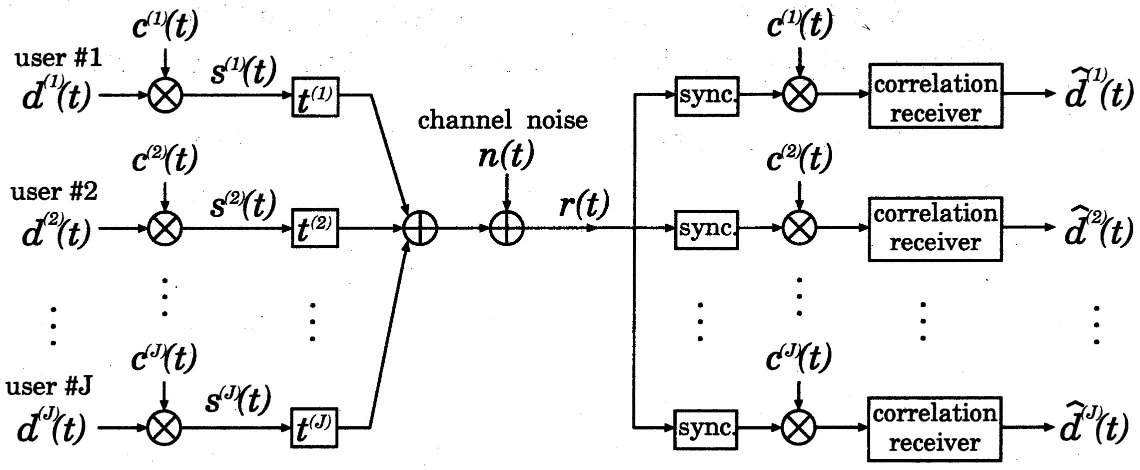


Figure 1: A model of a baseband CDMA system

The data signal $d^{(j)}(t)$ of the j-th user and the assigned PN code signal $c^{(j)}(t)$ can be written as

$$d^{(j)}(t) = \sum_{p=-\infty}^{\infty} d_p^{(j)} u_T(t-pT), \; d_p^{(j)} \in \{1,-1\} \tag{1}$$

$$c^{(j)}(t) = \sum_{q=-\infty}^{\infty} c_q^{(j)} u_{T_c}(t-qT_c), \; c_q^{(j)} \in \{1,-1\} \tag{2}$$

where $u_T(t)$ is defined by

$$u_T(t) = \begin{cases} 1 & \text{for } 0 \le t \le T \\ 0 & \text{otherwise.} \end{cases} \tag{3}$$

We assume that the j-th user's PN code sequence $\{c_p^{(j)}\}_{p=0}^{N-1}$ has period $N = T/T_c$ so that there is a PN sequence $c_0^{(j)}, c_1^{(j)}, \cdots, c_{N-1}^{(j)}$ per data symbol. For simplicity, assume that $T_c = 1$ through this paper. For a DS/SS system, the PN code bit $c_q^{(j)}$ is referred to as a *chip*. Thus the baseband spread spectrum signal $s^{(j)}(t)$ is given by

$$s^{(j)}(t) = c^{(j)}(t) d^{(j)}(t). \tag{4}$$

For asynchronous systems, the received signal $r(t)$ can be represented as

$$r(t) = \sum_{j=1}^{J} c^{(j)}(t - t^{(j)}) d^{(j)}(t - t^{(j)}) + n(t) \tag{5}$$

where $t^{(j)}$ is the time delay in the j-th channel and $n(t)$ is a common channel noise process. If the received signal $r(t)$ is the input to the correlation receiver matched to $s^{(i)}(t)$, the output during the p-th time-interval is

$$Z_p^{(i)} = \int_{pT}^{(p+1)T} r(t) c^{(i)}(t) dt. \tag{6}$$

Assume that the system is quasi-synchronous (all of $t^{(j)}$ are constrained to be integral multiples of T_c) and $n(t) = 0$ and define $\ell_{ij} = t^{(i)} - t^{(j)}$. Then we can write

$$Z_p^{(i)} = N + I_{J,p}^{(i)} \tag{7}$$

$$I_{J,p}^{(i)} = \sum_{\substack{j=1 \\ j\neq i}}^{J} \left\{ \frac{d_p^{(j)} + d_{p+1}^{(j)}}{2} R^E(\ell_{ij}; \{c^{(i)}\}, \{c^{(j)}\}) + \frac{d_p^{(j)} - d_{p+1}^{(j)}}{2} R^O(\ell_{ij}; \{c^{(i)}\}, \{c^{(j)}\}) \right\} \tag{8}$$

where $I_{J,p}^{(i)}$ denotes co-channel interference from other $J-1$ channels and $R^E(\ell; \{c^{(i)}\}, \{c^{(j)}\})$ and $R^O(\ell; \{c^{(i)}\}, \{c^{(j)}\})$ denote the even and the odd cross-correlation functions, respectively $(0 \leq \ell \leq N-1)$. They are defined by [1]

$$R^E(\ell; \{c^{(i)}\}, \{c^{(j)}\}) = R^A(\ell; \{c^{(i)}\}, \{c^{(j)}\}) + R^A(N-\ell; \{c^{(j)}\}, \{c^{(i)}\}) \tag{9}$$

$$R^O(\ell; \{c^{(i)}\}, \{c^{(j)}\}) = R^A(\ell; \{c^{(i)}\}, \{c^{(j)}\}) - R^A(N-\ell; \{c^{(j)}\}, \{c^{(i)}\}) \tag{10}$$

where $R^A(\ell; \{c^{(i)}\}, \{c^{(j)}\})$ is called an aperiodic cross-correlation function or a partial correlation function, defined by [1]

$$R^A(\ell; \{c^{(i)}\}, \{c^{(j)}\}) = \sum_{n=0}^{N-1-\ell} c_n^{(i)} c_{n+\ell}^{(j)}. \tag{11}$$

In order to reduce co-channel interference, absolute values of such even and odd cross-correlation functions, which depend on the family of PN sequences, are desired to be small.

3 Chaotic Bit Sequences

3.1 Generation

To give methods for generating chaotic bit sequences, we discuss the solutions of the difference equation [2],[3]

$$\omega_{n+1} = \tau(\omega_n), \; \omega_n \in I = [d, e], \; n = 0, 1, 2, \cdots \tag{12}$$

where τ is a piecewise continuous function which maps some interval I into itself. It is well known that the solutions of eq.(12) may be *chaotic*. For example, the Chebyshev map of degree k with $I = [-1, 1]$ defined by [4]

$$\tau(\omega) = \cos(k \cos^{-1} \omega), \; k = 2, 3, 4, \cdots \tag{13}$$

have chaotic trajectories. In our previous study [5], we proposed two simple methods to obtain binary sequences from chaotic real-valued sequences $\{\tau^n(\omega)\}_{n=0}^{\infty}$, both of which can give efficient methods to generate simultaneously different sequences of i.i.d. binary random variables for some ergodic maps. The first is used by the second method.

Method-1: Using the threshold function defined by

$$\Theta_t(\omega) = \begin{cases} 0 & \text{for } \omega < t \\ 1 & \text{for } \omega \geq t, \end{cases} \tag{14}$$

we can obtain a binary sequence $\{\Theta_t(\omega_n)\}_{n=0}^{\infty}$, which is referred to as *a chaotic threshold sequence* (called *a Chebyshev threshold sequence* when $\tau(\cdot)$ is a Chebyshev polynomial).

The second method was based on a binary expansion of the absolute value of ω when $|\omega| \leq 1$ as follows.

Method-2: We write the value of ω ($|\omega| \leq 1$) in a binary representation:

$$|\omega| = 0.A_1(\omega)A_2(\omega)\cdots A_i(\omega)\cdots, \quad A_i(\omega) \in \{0,1\}, \quad |\omega| \leq 1. \tag{15}$$

The i-th bit $A_i(\omega)$ can be expressed as

$$A_i(\omega) = \sum_{r=1}^{2^i-1} (-1)^{r-1} \left\{1 - \Theta_{-\frac{r}{2^i}}(\omega) + \Theta_{\frac{r}{2^i}}(\omega)\right\}. \tag{16}$$

Thus we can obtain a binary sequence $\{A_i(\omega_n)\}_{n=0}^{\infty}$ which we call *a chaotic bit sequence* (or *a Chebyshev bit sequence* when $\tau(\cdot)$ is a Chebyshev polynomial).

3.2 Correlation Properties

For any L_1 function $F(\cdot)$, consider the sum defined by

$$F_N(\omega) = \frac{1}{N} \sum_{n=0}^{N-1} F(\tau^n(\omega)). \tag{17}$$

According to the Birchoff individual ergodic theorem [3], we have

$$\lim_{N \to \infty} F_N(\omega) = \langle F \rangle \quad \text{a.e.} \tag{18}$$

under the assumption that $\tau(\cdot)$ is mixing on I with respect to an absolutely continuous invariant (or briefly ACI) measure, denoted by $f^*(\omega)d\omega$, where $\langle F \rangle$ is the ensemble-average of F over I, defined by

$$\langle F \rangle = \int_I F(\omega) f^*(\omega) d\omega. \tag{19}$$

It is known that the ensemble average technique is useful in theoretically evaluating statistics of chaotic sequences, such as means and correlation functions. Applying this technique to several ergodic maps, we can get the fact that the chaotic binary sequences have good statistical properties [5].

Now we consider two $\{0,1\}$-valued sequences $\{g(\tau^n(\omega))\}_{n=0}^{\infty}$ and $\{h(\tau^n(\omega))\}_{n=0}^{\infty}$. Define

$$R_N(\omega,\ell;g,h)=\frac{1}{N}\sum_{n=0}^{N-1}(2g(\tau^n(\omega))-1)(2h(\tau^{n+\ell}(\omega))-1) \tag{20}$$

which is the cross-correlation function between these two sequences from a seed ω, where ℓ is the time delay.

Let X be a set of seeds and let M be its cardinality. We introduce the average values of $R_N(\omega,\ell;g,h)$ over M seeds given by

$$\widehat{R}_{N,M}(\ell;g,h)=\frac{1}{M}\sum_{\omega_{0m}\in X}R_N(\omega_{0m},\ell;g,h). \tag{21}$$

Then this function $\widehat{R}_{N,M}(\ell;g,h)$, called an *empirical* one, approaches to $\langle R(\ell;g,h)\rangle$ when N and M are sufficiently large because $\langle R(\ell;g,h)\rangle$ is regarded as the average over all possible seeds.

Next, let $R_N^A(\omega,\ell;g,h)$ be an aperiodic correlation function between two binary sequences $\{g(\tau^n(\omega))\}_{n=0}^{N-1}$ and $\{h(\tau^n(\omega))\}_{n=0}^{N-1}$ defined as [1]

$$R_N^A(\omega,\ell;g,h)=\frac{1}{N}\sum_{n=0}^{N-1-\ell}(2g(\tau^n(\omega))-1)(2h(\tau^{n+\ell}(\omega))-1) \tag{22}$$

which gives the even and odd correlation function to be considered in evaluating the performance of SS systems. Its empirical correlation function is given by

$$\widehat{R}_{N,M}^A(\ell;g,h)=\left(1-\frac{\ell}{N}\right)\widehat{R}_{N-\ell,M}(\ell;g,h). \tag{23}$$

The empirical function $\widehat{R}_{N-\ell,M}(\ell;g,h)$ also approaches to $\langle R(\ell;g,h)\rangle$ when N and M are sufficiently large. Thus the ensemble average $\langle R_N^A(\ell;g,h)\rangle$ can be written as

$$\langle R_N^A(\ell;g,h)\rangle=\left(1-\frac{\ell}{N}\right)\langle R(\ell;g,h)\rangle. \tag{24}$$

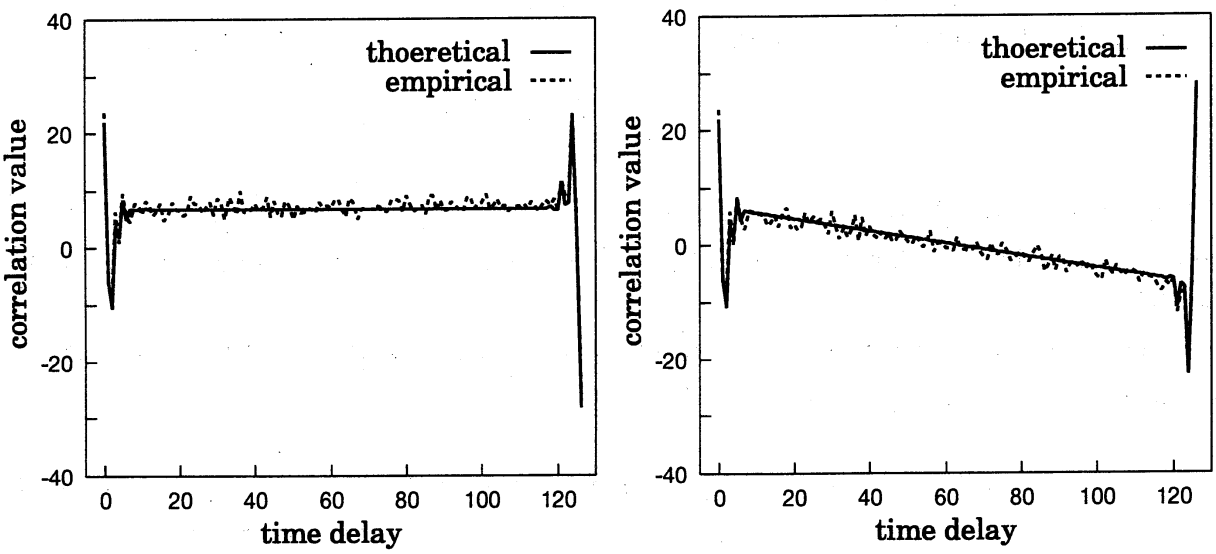
Therefore, the theoretical even correlation function $\langle R_N^E(\ell;g,h)\rangle$ and odd correlation function $\langle R_N^O(\ell;g,h)\rangle$ are respectively given by

$$\langle R_N^E(\ell;g,h)\rangle = \langle R_N^A(\ell;g,h)\rangle+\langle R_N^A(N-\ell;h,g)\rangle, \tag{25}$$
$$\langle R_N^O(\ell;g,h)\rangle = \langle R_N^A(\ell;g,h)\rangle-\langle R_N^A(N-\ell;h,g)\rangle. \tag{26}$$

3.3 Numerical Examples

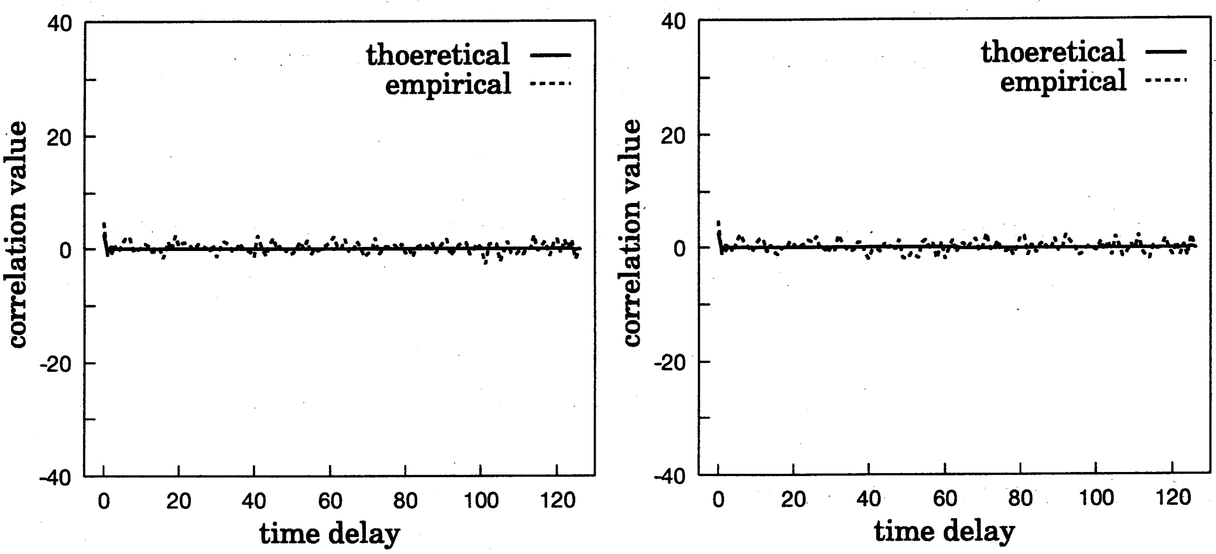
Some numerical examples of even and odd correlation functions of Chebyshev bit sequences are shown. Figures 2 and 3 show the theoretical even (respectively odd) correlation functions $\langle R_N^E(\ell;A_i,A_j)\rangle$ (respectively $\langle R_N^O(\ell;A_i,A_j)\rangle$), indicated by solid lines, and the empirical ones $\widehat{R}_{N,M}^E(\ell;A_i,A_j)$ (respectively $\widehat{R}_{N,M}^O(\ell;A_i,A_j)$), indicated by dotted lines, where

$N = 127$ and $M = 100$. In each figure, the degree of Chebyshev maps and the bit numbers are indicated. The theoretical values are in good agreement with the empirical ones. Besides, we can find that their cross-correlation values become low when the degree k and the bit numbers are large. Note that their auto-correlation values except $\ell = 0$ are similar to their cross-correlation values.



(a) even (b) odd

Figure 2: (a) $\langle R_N^E(\ell; A_2, A_3)\rangle$ and $\widehat{R}_{N,M}^E(\ell; A_2, A_3)$, (b) $\langle R_N^O(\ell; A_2, A_3)\rangle$ and $\widehat{R}_{N,M}^O(\ell; A_2, A_3)$, where $N = 127$, $M = 100$, and $k = 2$.



(a) even (b) odd

Figure 3: (a) $\langle R_N^E(\ell; A_8, A_9)\rangle$ and $\widehat{R}_{N,M}^E(\ell; A_8, A_9)$, (b) $\langle R_N^O(\ell; A_8, A_9)\rangle$ and $\widehat{R}_{N,M}^O(\ell; A_8, A_9)$, where $N = 127$, $M = 100$, and $k = 16$.

4 Distributions of Statistics of Chaotic Sequences

It should be noted that $R_N^E(\omega, \ell; A_i, A_j)$ and $R_N^O(\omega, \ell;\ A_i, A_j)$ have large scattered values because they are random variables. Thus we must investigate distributions of such random variables for a certain set of seeds $\{\omega_{0m}\}_{m=1}^M$ because bit error probabilities in asynchronous CDMA systems depend on distributions of correlation values, called *empirical distributions*. Figure 4 shows such empirical distributions of $\{R_N^E(\omega_{0m}, \ell; A_i, A_j)\}_{m=1}^M$ and the ones of $\{R_N^O(\omega_{0m}, \ell; A_i, A_j)\}_{m=1}^M$, where $M = 8001$. We can observe that these distributions tend to Gaussian distributions [6] defined by

$$\phi(\omega) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left[-\frac{(\omega-\nu)^2}{2\sigma^2}\right], \quad (-\infty < \omega < \infty) \tag{27}$$

where ν is mean and σ^2 is variance. Of course, the theoretical estimates of mean, denoted respectively by ν_τ^E and ν_τ^O, are respectively given by

$$\nu_\tau^E = \langle R_N^E(\ell; A_i, A_j)\rangle, \tag{28}$$

$$\nu_\tau^O = \langle R_N^O(\ell; A_i, A_j)\rangle \tag{29}$$

and those of variance, respectively denoted by $(\sigma_\tau^E)^2$ and $(\sigma_\tau^O)^2$, are also given by

$$(\sigma_\tau^E)^2 = \langle (R_N^E(\omega, \ell; A_i, A_j))^2\rangle - \langle R_N^E(\omega, \ell; A_i, A_j)\rangle^2 \tag{30}$$

$$(\sigma_\tau^O)^2 = \langle (R_N^O(\omega, \ell; A_i, A_j))^2\rangle - \langle R_N^O(\omega, \ell; A_i, A_j)\rangle^2. \tag{31}$$

We refer to the Gaussian distribution with mean ν_τ^E (respectively ν_τ^O) and variance $(\sigma_\tau^E)^2$ (respectively $(\sigma_\tau^E)^2$) as the *estimated distribution* of $\{R_N^E(\omega_{0m}, \ell;\ A_i, A_j)\}_{m=1}^M$ (respectively $\{R_N^O(\omega_{0m}, \ell; A_i, A_j)\}_{m=1}^M$). Figure 4 leads us to find that the theoretical estimates of mean and variance are given by

$$\nu_\tau^E \simeq 0 \tag{32}$$

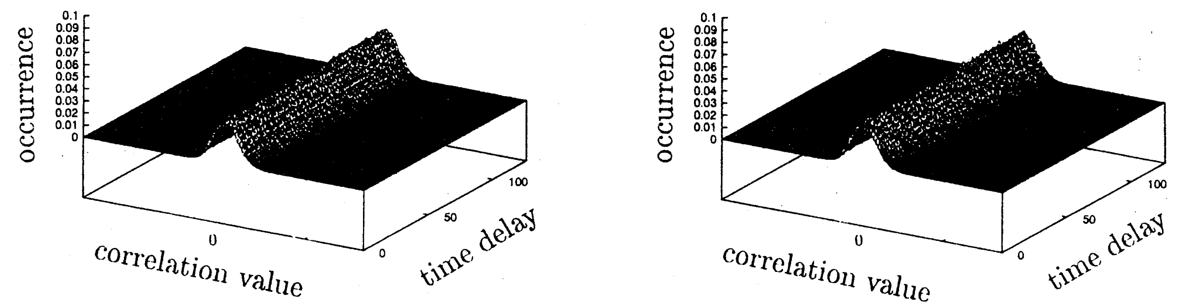
$$\nu_\tau^O \simeq 0 \tag{33}$$

$$(\sigma_\tau^E)^2 \simeq \frac{1}{N} \tag{34}$$

$$(\sigma_\tau^O)^2 \simeq \frac{1}{N} \tag{35}$$

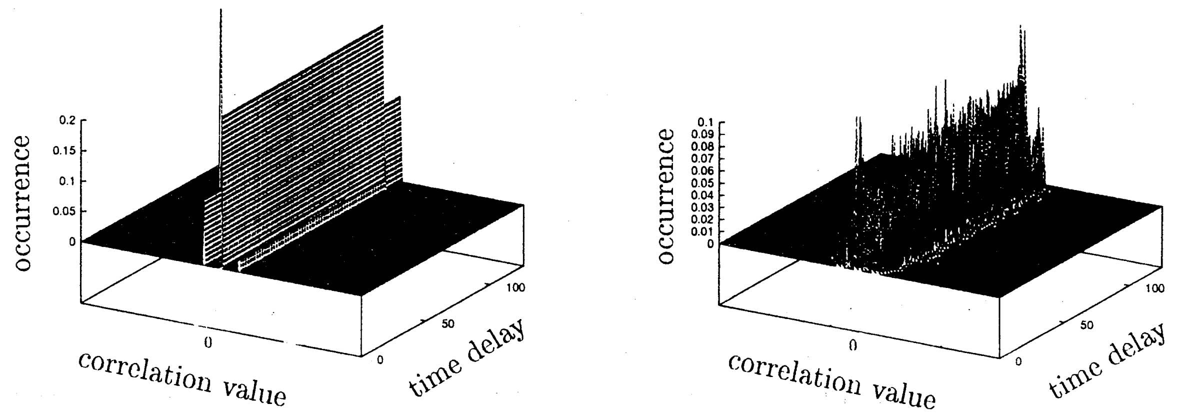
each of which is independent of the bit numbers i, j and the delay ℓ when the degree of the Chebyshev map and the bit numbers are large. It is easily checked that the estimated distribution are in good agreement with the empirical ones.

For comparison, the distributions of correlation values of Gold sequences are shown in Figure 5.



(a) even (b) odd

Figure 4: Distributions of correlation values of Chebyshev bit sequences, where $N = 127$, $M = 8001$, $(i, j) = (8, 9)$, and $k = 16$.



(a) even (b) odd

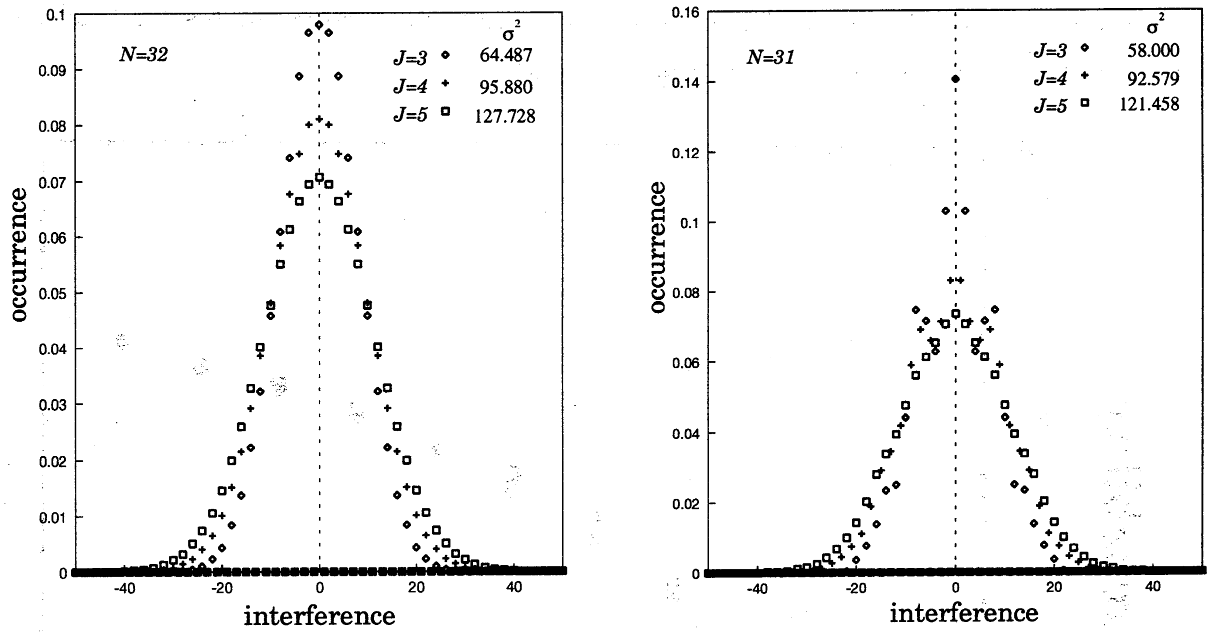
Figure 5: Distributions of correlation values of 8001 pairs of Gold sequences, where $N = 127$.

5 Evaluation of Bit Error Probabilities

As is well known, bit error probabilities in asynchronous CDMA systems depend on distributions of even and odd correlation values between each pair of spreading sequences.

Now assume that J users communicate through a CDMA system independently and quasi-synchronously. Thus the distribution of the co-channel interference to the i-th user from other $J - 1$ channels are estimated by the Gaussian distribution with mean 0 and variance $(J - 1)N$ because of the additive property of the Gaussian distribution. Figure 6(a) shows numerical examples of such distributions of the co-channel interference in asynchronous CDMA systems using Chebyshev bit sequences. For reference, Figure 6(b) shows the ones of the systems using Gold sequences. We can find that the distributions for

Chebyshev bit sequences tend to the Gaussian distribution irrespective of the number of channels. On the other hand, the ones for Gold sequences are not the Gaussian distribution when the number of channels, J, is small. However, it is shown that the distributions for Gold sequences tend to the Gaussian distribution as the number of channels increases.



(a) Chebyshev bit sequences (b) Gold sequences

Figure 6: Distributions of co-channel interference from $J-1$ channels in an asynchronous CDMA system, where $N = 32$.

The bit errors occur when the co-channel interference is greater than N if the i-th information bit during the p-th time-interval is $d_p^{(i)} = -1$ (or is smaller than $-N$ if the i-th information bit is $d_p^{(i)} = 1$). Hence, if $\Pr\{d_p^{(j)} = 1\} = \Pr\{d_p^{(j)} = -1\} = \frac{1}{2}$ for all j and $n(t) = 0$, the bit error probability can be estimated by

$$P_e = \Pr\{I_{J,p}^{(i)} > N | d_p^{(i)} = -1\} \tag{36}$$

$$= \int_N^{\infty} \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left[-\frac{\omega^2}{2\sigma^2}\right] d\omega \tag{37}$$

$$= Q\left(\frac{N}{\sigma}\right) \tag{38}$$

where

$$\sigma^2 = (J-1)N \tag{39}$$

$$Q(x) = \int_x^{\infty} \frac{1}{\sqrt{2\pi}} \exp\left[-\frac{\omega^2}{2}\right] d\omega. \tag{40}$$

The above quantity P_e indicates that N and σ^2 correspond respectively to $\sqrt{E_b}$ and $N_J/2$ in the well-known bit error probability of a coherent BPSK system [10],[11], where E_b and $N_J/2$ denote the bit energy and the noise power spectral density, respectively.

Finally, we show the bit error probabilities in asynchronous CDMA systems by computer simulation in Figure 7. We can find that theoretical estimates are in good agreement with the results by simulation for Chebyshev bit sequences. It is interesting that the results for Gold sequences are also in good agreement with the theoretical estimates for Chebyshev bit sequences when the number of channels is large.

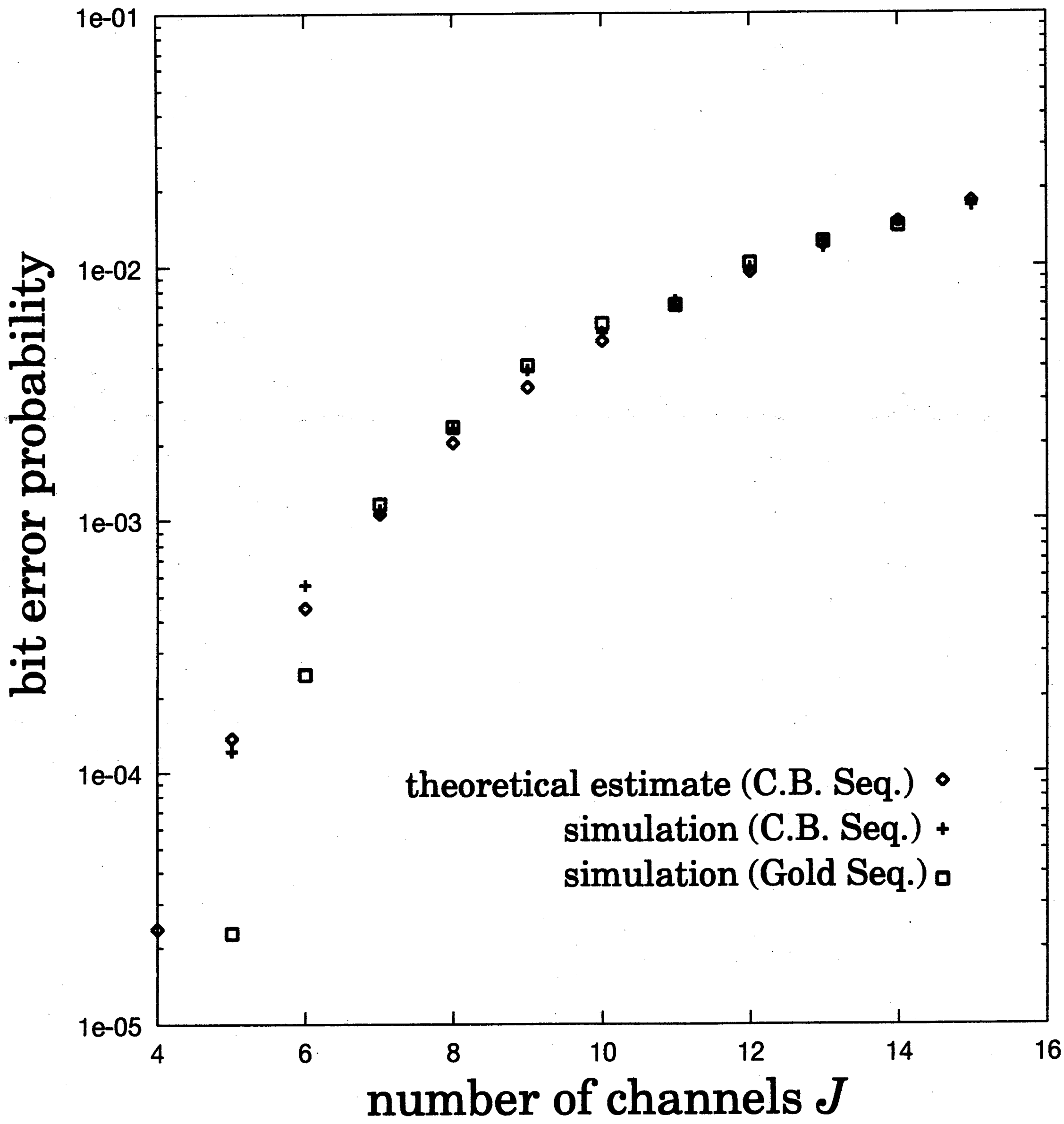


Figure 7: Bit error probabilities in an asynchronous CDMA system, where $N = 63$.

6 Applications to Image Communications

In image transmission systems using spread spectrum (SS) techniques[10],[11], the main problem is how to transmit the image with enormous data efficiently[7]−[9]. In an image coding, the discrete cosine transform (DCT) is extensively used. Note that images have different significant DCT coefficients.(The most significant coefficient is known to be the D.C. term.)

In general, a wide bandwidth is required for the transmission of images. In a CDMA system, spreading sequences of the same period are usually assigned to the channels[1]−[11], and hence each of the erroneously transmitted bits occurs nearly equiprobably. Obviously, a much wider bandwidth is required for the transmission of images using such CDMA systems. To reduce such a bandwidth, we consider a CDMA system in which spreading sequences of longer period are assigned to more significant bits than to less ones[13]. Such a system, which is asynchronous, permits us to reduce the error probabilities of more significant bits. This technique is analogous to the Shannon-Fano encoding. The quality of reconstructed images is shown to be drastically improved within such a limited bandwidth even if the system is asynchronous.

6.1 Image Communications Based on Asynchronous DS/CDMA Systems [13],[14]

A basic image communication system using spread spectrum technique is illustrated in Figure 8. First, images are partitioned into small blocks (8×8 pixels), and the discrete cosine transform (DCT) of two-dimensional (2-D) signal $p(i, j)$ in each block is computed. Next the 2-D DCT coefficients $q(u, v)$ are quantized and appropriate numbers of bits are assigned to them. Note that encoding and decoding are implemented block by block. The DCT coefficients are numbered as shown in Figure 9. We assign more bits to low frequency coefficients than to high ones. The bit allocation map we use is shown in Figure 10. We transmit only the first 15 DCT coefficients, namely 54bits/block, 0.84bit/pixel. Furthermore, the n-th significant bit of the m-th coefficient q_m is denoted by $q_{m\text{-}n}$, for example, $q_{0\text{-}1}$ is the most significant bit (MSB) of the DCT coefficient q_0 and $q_{0\text{-}8}$ is the least significant bit (LSB). In this paper, a gray-scale image (8bits per pixel, 720×576 pixels, 6480blocks) called “Barbara” is used, as shown in Figure 11.

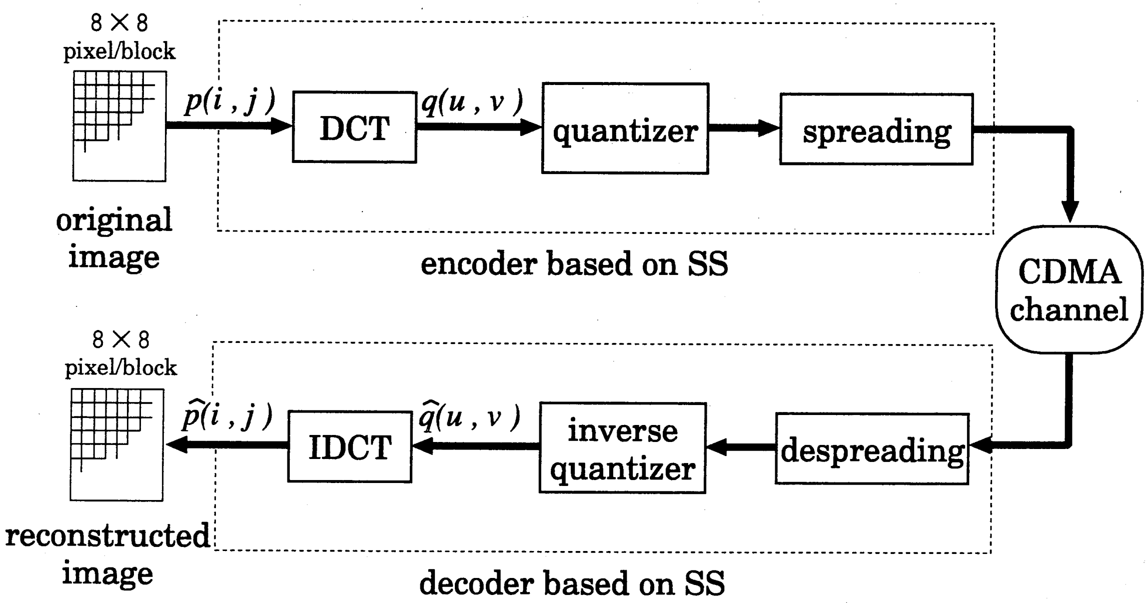


Figure 8: Image communication system using SS techniques.

0 → v, ↓ u

q0	q1	q5	q6	q14	q15	q27	q28
q2	q4	q7	q13	q16	q26	q29	q42
q3	q8	q12	q17	q25	q30	q41	q43
q9	q11	q18	q24	q31	q40	q44	q53
q10	q19	q23	q32	q39	q45	q52	q54
q20	q22	q33	q38	q46	q51	q55	q60
q21	q34	q37	q47	q50	q56	q59	q61
q35	q36	q48	q49	q57	q58	q62	q63

Figure 9: Coefficient numbers.

0 → v, ↓ u

8	6	4	3	2	0	0	0
6	4	3	2	0	0	0	0
4	3	2	0	0	0	0	0
3	2	0	0	0	0	0	0
2	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

Figure 10: Bit allocation map.

Figure 11: The original image "Barbara".

For an image, we assign each bit $q_{m\text{-}n}$ to CDMA channels (6 channels in this paper) appropriately. Now we define

$$t_{m\text{-}n} = \text{the period of the spreading sequence to be assigned to } q_{m\text{-}n}. \tag{41}$$

Assume that the total number of chips in each channel defined by

$$T_i = \sum_{q_{m-n} \in \text{ the } i\text{-th channel}} t_{m\text{-}n}, \quad i = 1, 2, \cdots, 6.$$

is equal to others, that is,

$$T_i = T, \quad \text{for all } i.$$

We call T the "block-period".

Various kinds of models can be considered according to assignments of each bit $q_{m\text{-}n}$ to 6 channels. First, we proposed the simplest model as shown in Figure 12, called "Model-1", where spreading sequences of fixed-period are used.

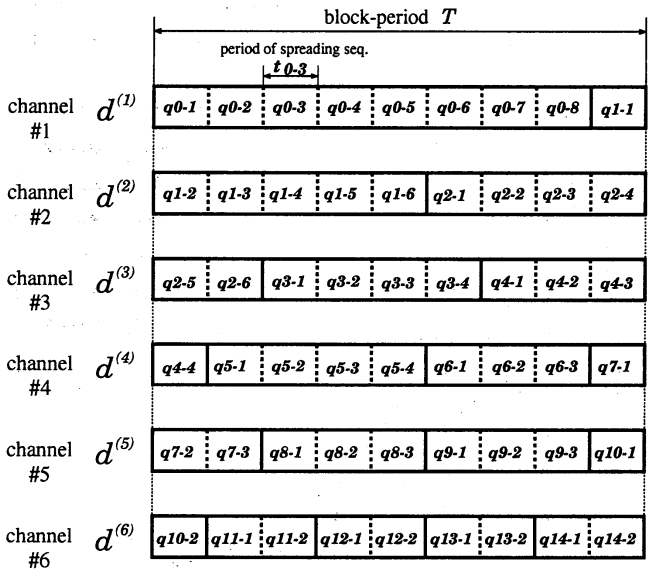


Figure 12: Model-1 with spreading sequences of fixed-period.

Now define the mean absolute error (MAE) by

$$\text{MAE} = \frac{1}{6480 \times 8 \times 8} \sum_{k=1}^{6480} \sum_{i=0}^{7} \sum_{j=0}^{7} |p_k(i,j) - \widehat{p}_k(i,j)| \tag{42}$$

where $p_k(i,j)$ and $\widehat{p}_k(i,j)$ denote intensity values of the (i,j) element of the k-th block in the original image and in the reconstructed image, respectively. In order to investigate the significance of each bit $q_{m\text{-}n}$, we compute the values of MAE when each bit $q_{m\text{-}n}$ is transmitted erroneously[12], as shown in Figure 13. Furthermore, the insignificance of $q_{m\text{-}n}$ is calculated from (MAE$-$lower bound of MAE)$^{-1}$ which means the number of the erroneously transmitted bit q_{m-n} to cause a constant MAE, as shown in Figure 14.

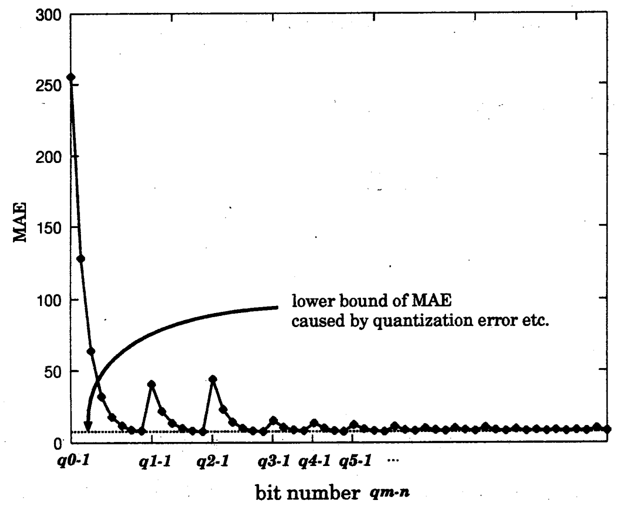


Figure 13: MAE when each bit q_{m-n} is transmitted erroneously.

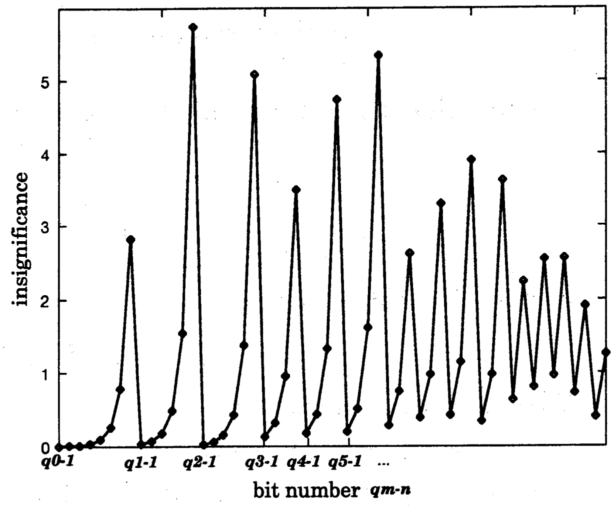


Figure 14: Insignificance of the bit q_{m-n}, namely, the number of erroneously transmitted bits q_{m-n} to cause a constant MAE.

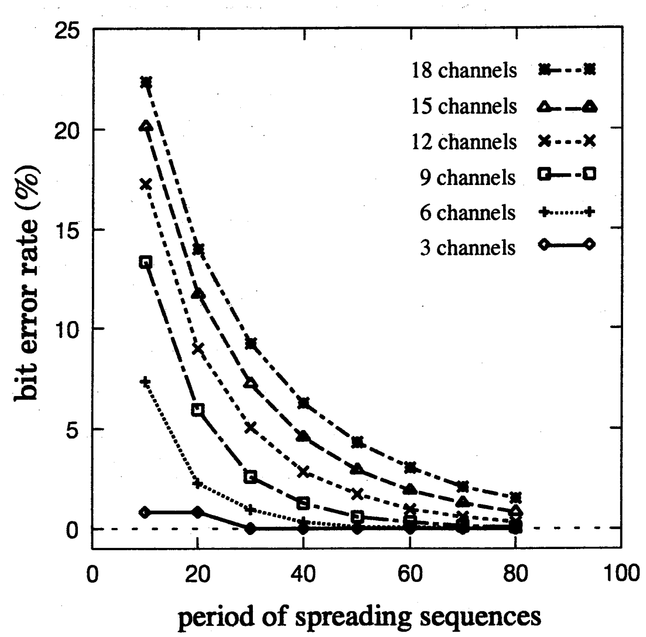


Figure 15: Bit error rates in asynchronous CDMA systems using Chebyshev bit sequences.

Model-1 is not efficient because each bit q_{m-n} is equiprobably transmitted in error. As is well known, for a constant number of channels, spreading sequences of longer periods can reduce bit error rates than ones of shorter periods. This motivates us to assign spreading sequences of an appropriate period to the bit q_{m-n} according to its significance. To do this, we should investigate the bit error rates for various periods of spreading sequences and for various numbers of channels. In this paper, as spreading sequences of variable-period, we use

"Chebyshev bit sequences[5]" which are generated by the Chebyshev map. Such sequences are quite different from LFSR sequences such as M sequences, Kasami sequences, and Gold sequences[1]. We have already calculated the bit error rates for the Chebyshev bit sequences as shown in Figure 15.

Using the results of Figures 14 and 15, we can construct "Model-2" where spreading sequences of variable-period are used as shown in Figure 16. Figure 17 shows the desired periods $t_{m\text{-}n}$ for each bit $q_{m\text{-}n}$, indicated by the solid line, when the minimum $t_{m\text{-}n}$ is equal to 15. If the periods $t_{m\text{-}n}$ given by the solid line in Figure 17 are used, then T_i $(i = 1, 2, \cdots, 6)$ are not equal to each other. Thus the periods $t_{m\text{-}n}$ in Model-2, indicated by the dotted line in Figure 17, are used to satisfy $T_i = 240$ for all i.

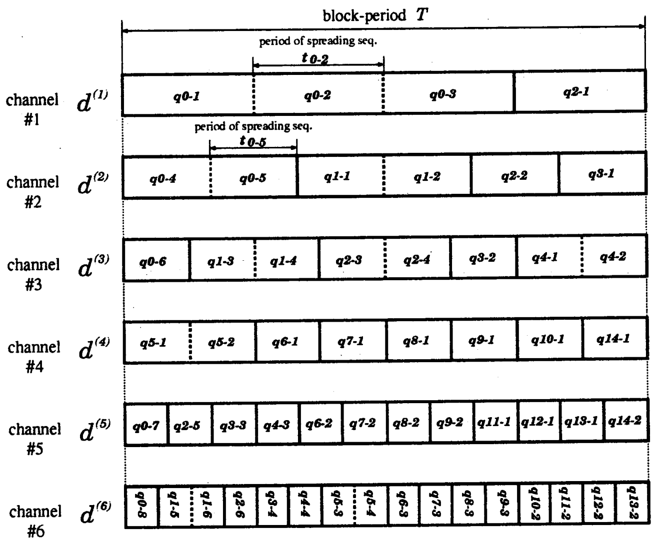


Figure 16: Model-2 with spreading sequences of variable-period.

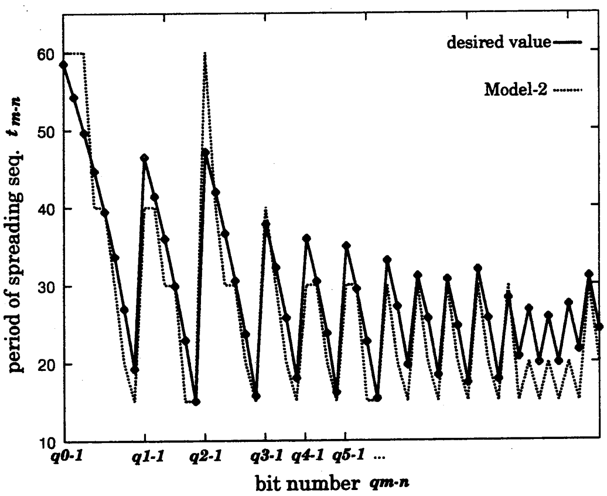


Figure 17: Fig.10: Periods $t_{m\text{-}n}$ for each bit $q_{m\text{-}n}$.

6.2 Computer Simulation

As a criterion to evaluate the quality of reconstructed images, we use the mean square error (MSE) defined by

$$\text{MSE} = \frac{1}{N \times 8 \times 8} \sum_{k=1}^{N} \sum_{i=0}^{7} \sum_{j=0}^{7} \left(p_k(i,j) - \widehat{p}_k(i,j)\right)^2 . \tag{43}$$

In Model-2, we use the periods obtained by multiplying $t_{m\text{-}n}$ indicated by the dotted line in Figure 17 by a constant value according to given block-periods. Figures 18 and 19 show bit error rates versus block-periods and MSEs versus block-periods, respectively. We can find that the bit error rates in the two models are similar to each other. On the other hand, the MSE performance of Model-2 has shown to be much better than that of Model-1. This implies that the quality of reconstructed images in Model-2 is drastically improved as shown in Figures 20 and 21.

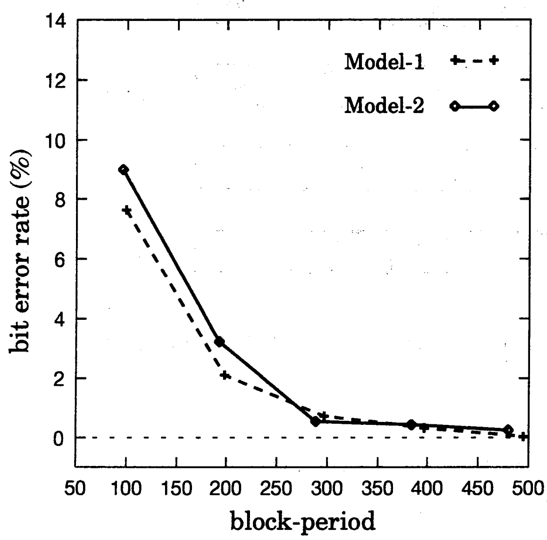


Figure 18: Bit error rates versus block-periods.

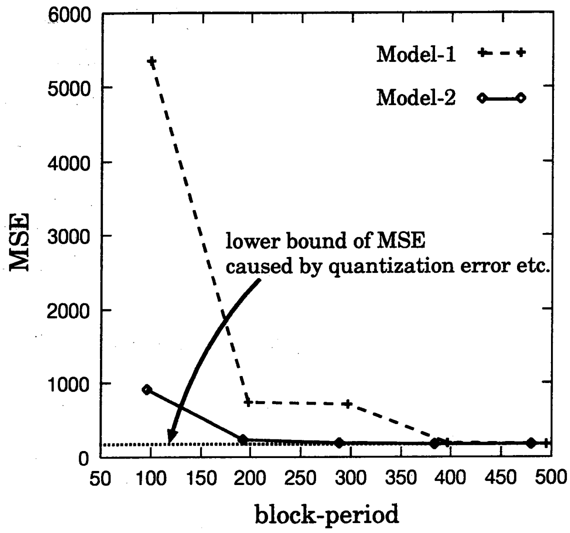


Figure 19: MSEs versus block-periods.

Figure 20: The reconstructed image in Model-1 for block-period 99.

Figure 21: The reconstructed image in Model-2 for block-period 96.

7 Concluding Remarks

Bit error probabilities in asynchronous CDMA systems using chaotic binary sequences have been discussed. It is observed that the central limit theorem holds for correlation values of chaotic bit sequences. This enable us to theoretically estimate such bit error probabilities. Since the central limit theorem doesn't hold for LFSR sequences such as Gold sequences, as shown in Fig.5, it is difficult to theoretically estimate the bit error probabilities in the system using LFSR sequences. However, it is noteworthy that the bit error probabilities for chaotic bit sequences are capable of estimating the ones for Gold sequences when the number of channels is large.

Furtheremore, image communication systems using CDMA channels with spreading sequences of variable-period are proposed. We have given an efficient method for assigning periods of spreading sequences based on the insignificance of each bit of DCT coefficients. The CDMA systems using spreading sequences of variable-period have the following advantages: 1) The quality of reconstructed images are drastically improved within a limited bandwidth; and hence 2) The bandwidth is not so much for the transmission of images. Note that such techniques can be also applied to color image communications.

References

[1] D. V. Sarwate and M. B. Pursley, "Crosscorrelation properties of pseudorandom and related sequences," Proc. IEEE, Vol.68, no.3, pp.593-619, 1980.

[2] Jackson, E. Atlee, *Perspective nonlinear dynamics*, Cambridge Univ. Press, 1989.

[3] A. Lasota and M. C. Mackey, *Chaos, Fractals, and Noise*, Springer-Verlag, 1994.

[4] R. L. Adler and T. J. Rivlin, "Ergodic and mixing properties of Chebyshev polynomials," Proc. Amer.Math.Soc., vol.15, pp. 794-796,1964.

[5] T.Kohda and A.Tsuneda, "Pseudonoise Sequence by Chaotic Nonlinear Maps and Their Correlation Properties," IEICE Trans. on Communications, vol.E76-B, no.8, 855-862, 1993.

[6] William Feller, *An Introduction to Probability Theory and Its Applications*, vol.2, John Wiley & Sons, 1966.

[7] N. MacDonald, "Transmission of compressed video over radio link," Visual Communication and Image Processing '92, No.1818-149, 1992.

[8] W. F. Schreiber, "Spread-Spectrum Television Broadcasting," SMPTE Journal, pp.538-549, August, 1992.

[9] N. Doi, T. Yano, N. Kobayashi, H. Kishida, and M. Ohnishi, "Development of Wireless TV-phones using Spread-Spectrum Communication," Proc. The 16th Symposium on Information Theory and Its Applications (SITA '93), pp.121-124, 1993.

[10] M. K. Simon, J. K. Omura, R. A. Scholtz, and B.K.Levitt, *Spread Spectrum Communications Handbook*, McGraw-Hill, 1994.

[11] R. L. Peterson, R. E. Ziemer, and D. E. Borth, *Introduction to Spread Spectrum Communications*, Prentice-Hall, 1995.

[12] Y. Koyama and S. Yoshida, "Still Image Transmission using ARQ over Fading Channel ", Proc. the 17th Symposium on Information Theory and Its Applications, pp.257-260, 1994.

[13] T. Kohda, A. Tsuneda, A. Osiumi and K. Ishii, "A study on pseudonoise-coded image communications" Proc. of SPIE's Visual Communications and Image Processing '94, pp.874–884, 1994.

[14] T. Kohda, K. Ishii, and A. Tsuneda, "Image Transmission Systems through CDMA Channels Using Spreading Sequences of Variable-Period", Proc. of IEEE Fourth International Symposium on Spread Spectrum Techniques & Applications, pp.781–784, 1996.