Electrical Engineering in Japan, Vol. 163, No. 3, 2008
Translated from Denki Gakkai Ronbunshi, Vol. 125-C, No. 4, April 2005, pp. 582–590

Chaotic Synchronization-Based Communications Using Constant Envelope Pulse

KAZUHIKO NAKAMURA,[1] TERUYUKI MIYAJIMA,[2] and KAZUO YAMANAKA[2]
[1]University of Yamanashi, Japan
[2]Ibaraki University, Japan

SUMMARY

We propose use of a constant-envelope pulse for the purpose of improving noise-rejection property in chaotic synchronization-based communication systems. In a conventional system where discrete-time chaotic signals are transmitted through the pulse amplitude modulation, the correlator output variance increases as the spreading factor decreases, while the synchronization error increases as the spreading factor increases. Therefore, it is difficult to control the bit error rate only by adjusting the spreading factor. In the proposed system, use of pulse width modulation keeps the envelope of transmitted signals constant, which leads to the correlator output with zero variance. The synchronization error is kept small because the spreading factor can be set to be one without increasing the correlator output variance. We have a result of computer simulation showing that the proposed system achieves a bit error performance better than the conventional system. In addition, a new blind adaptive algorithm is proposed which suppresses intersymbol interference. Electr Eng Jpn, 163(3): 47–56, 2008; Published online in Wiley InterScience (www.interscience.wiley.com). DOI 10.1002/eej.20318

Key words: chaotic synchronization; chaotic communication; pulse width modulation (PWM); security; blind adaptive equalizer.

1. Introduction

Chaos is a deterministic signal with random behavior, and the application of chaos to communications has been studied extensively in recent years [1–9]. Chaotic communications are attractive because transmitters and receivers can be configured using relatively simple devices. In addition, interference-resistant communications can be implemented by using broadband chaotic signals, and the randomness of chaotic signals contributes to communications security.

Many chaotic communications systems use chaotic synchronization. The phenomenon of chaotic synchronization means that multiple chaotic systems with different initial values show similar behavior in the course of time [1]. Communications based on chaotic synchronization is a method of modulating and demodulating information by synchronizing chaotic systems on the transmitter and receiver sides. Secure communications can be established because data demodulation requires that the chaotic system of the transmitter side be known exactly at the receiver side.

Available methods of chaotic communications can be grouped into chaotic masking [2, 3], chaotic modulation [4, 5], and chaos shift keying (CSK) [6–9]. In terms of digital information transfer, chaotic masking and chaotic modulation deal basically with analog information, and are disadvantageous due to their very low efficiency with respect to signal power. On the other hand, in CSK, chaotic systems are switched according to digital information, and optimal communications by white-noise channels can be expected due to demodulation using correlation detection.

Thus, CSK is a very interesting method of chaotic communications, but there are the following two problems with conventional CSK [8, 9]. First, in the transfer of discrete-time chaotic signals using pulse amplitude modulation (PAM), the signal components at the correlation detector are varied with every bit, leading to a noise-like effect. Second, when channel noise and interference exist, perfect chaotic synchronization cannot be achieved, which considerably degrades performance. To deal with the latter problem of CSK, a new method called differential CSK (DCSK) that does not use chaotic synchronization was recently proposed. This method shows good noise tolerance and interference immunity [10]. As regards the former problem, there is a method that involves obtaining a constant envelope signal by frequency modulation of a continuous-time chaotic signal. This method proves effective in solving the problem of correlator output fluctuations [11]. However, DCSK is a reference transmission system in which the chaotic signal used for data modulation is transmitted subsequent to the data-modulated chaotic signal. Therefore, demodulation at the receiver end is possible even without knowing the chaos, and communications is not secure.

In this study, aiming at better noise-tolerance of communications based on chaotic synchronization, we propose a chaotic synchronization-based communications system using constant envelope pulses. The constant envelope transformation of a discrete-time chaotic signal using pulse width modulation (PWM) prevents the performance drop caused by correlator output fluctuations in PAM-based communications. In addition, one sample of the chaotic signal is used for every bit of information data, resulting in low error of chaotic synchronization, and hence better performance.

In addition, in this paper we consider the problems of performance deterioration because of intersymbol interference. When intersymbol interference exists, perfect chaotic synchronization is not achieved, and performance drops considerably. This also holds true for the proposed communications method. Several techniques have been proposed to reduce the effect of channel distortion by means of adaptive equalizers [12, 13]. Considering the security and efficiency of chaotic communications, a blind adaptive equalizer that does not require a training signal seems preferable. Here we propose a new blind adaptive algorithm using the constant envelope characteristic of the PWM pulses, and demonstrate its effectiveness as a measure against intersymbol interference in chaotic communications.

2. Chaotic Synchronization-Based Communications Using PAM

2.1 Configuration of communications system

In this study, we consider communications using discrete-time chaos, which offers good reproducibility. In PAM-based chaotic communications, binary information data $b(i) \in \{-1, +1\}$, $i = 0, 1, 2, \ldots$ are transmitted using L samples per bit. The configuration of chaotic synchronization-based communication using PAM is shown in Fig. 1.

At the transmitter, chaos is generated by using the following discrete-time one-dimensional chaotic system:

$$x(k+1) = ax(k) + f(y(k)) \tag{1}$$

$$y(k) = b\left(\left[\frac{k}{L}\right]\right)x(k) \tag{2}$$

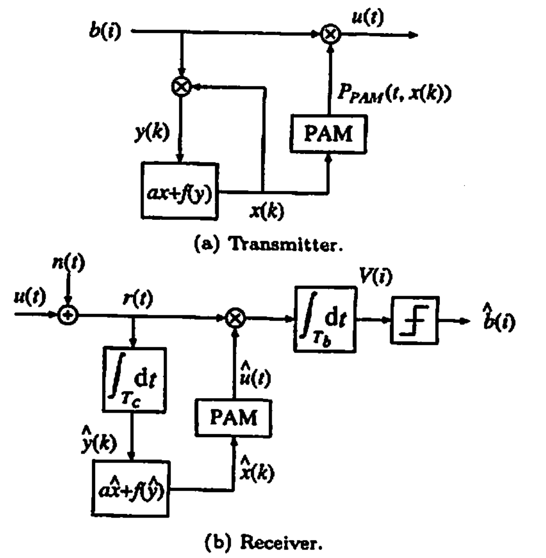

Fig. 1. Chaotic synchronization-based communication using PAM.

Here a is a constant with an absolute value below 1, $f(\cdot)$ denotes $R^1 \to R^1$ mapping, and $[\cdot]$ denotes a Gaussian signal. In addition, $[k/L]$ stands for the greatest integer smaller than k/L. A PAM pulse is generated by a Gaussian signal $x(k)$:

$$P_{PAM}(t, x(k)) = \begin{cases} x(k) & \cdots \quad 0 \le t - kT_c < T_c \\ 0 & \cdots \quad \text{otherwise} \end{cases} \tag{3}$$

Here $t \geq 0$ is the time, and T_c is the PAM pulse duration per sample of the chaotic signal. The transmitted signal is obtained by multiplying the PAM pulse train by the information data $b(i)$:

$$u(t) = \sum_{k=0}^{\infty} b\left(\left[\frac{k}{L}\right]\right) P_{PAM}(t - kT_c, x(k)) \tag{4}$$

In this paper, we call L the spreading factor, as in spread spectrum (SS) communications. In the communications channel, zero-mean white Gaussian noise $n(t)$ with a two-sided power spectrum density of $N_0/2$ is added, so that the received signal is

$$r(t) = u(t) + n(t) \tag{5}$$

At the receiver, a discrete-time signal is obtained by integration of the received signal:

$$\hat{y}(k) = \frac{1}{T_c}\int_{kT_c}^{(k+1)T_c} r(t)\mathrm{d}t \tag{6}$$

This $\hat{y}(k)$ is used in the input to the chaotic system. The receiver has the same chaotic system as the transmitter, and the chaos estimate is generated as follows:

$$\hat{x}(k+1) = a\hat{x}(k) + f(\hat{y}(k)) \quad (7)$$

Consider the behavior of $x(k)$ in Eq. (1) and of $\hat{x}(k)$ above. The synchronization error $e(k)$ is expressed as follows:

$$\begin{aligned} e(k) &= \hat{x}(k) - x(k) \\ &= ae(k-1) \\ &\quad + \{f(\hat{y}(k-1)) - f(y(k-1))\} \end{aligned} \quad (8)$$

In the absence of noise, the integrator output is

$$\hat{y}(k) = b\left(\left[\frac{k}{L}\right]\right)x(k) \quad (9)$$

that is, it is equal to $y(k)$. Therefore, the second term on the right-hand side of Eq. (8) is zero, and the synchronization error is

$$\lim_{k\to\infty} e(k) = 0 \quad (10)$$

Hence, synchronization is established. When there is noise, the second term on the right-hand side of Eq. (8) is not zero, and perfect synchronization cannot be achieved.

Correlation detection is performed in order to obtain a data estimate. For this purpose, a replica of the PAM pulse train is generated from the chaos estimate $\hat{x}(k)$:

$$\hat{u}(t) = \sum_{k=0}^{\infty} P_{PAM}\left(t - kT_c, \hat{x}(k)\right) \quad (11)$$

Using a replica of this $u(t)$, the correlator output $V(i)$ is as follows:

$$V(i) = \frac{1}{T_b}\int_{iT_b}^{(i+1)T_b} r(t)\hat{u}(t)\mathrm{d}t \quad (12)$$

Here $T_b = LT_c$ is the duration of 1 bit. The data estimate is obtained in the following way:

$$\hat{b}(i) = \mathrm{sgn}\left(V(i)\right) \quad (13)$$

In perfect chaotic synchronization, that is, if $\hat{x}(k) = x(k)$, Eq. (12) can be rewritten as

$$\begin{aligned} V(i) &= \frac{b(i)}{T_b}\sum_{k=iL}^{(i+1)L-1} T_c \cdot P_{PAM}(t-kT_c, x(k))^2 \\ &\quad + \frac{1}{T_b}\int_{iT_b}^{(i+1)T_b} n(t)\hat{u}(t)\mathrm{d}t \\ &= \frac{b(i)}{L}\sum_{k=iL}^{(i+1)L-1} x^2(k) \\ &\quad + \frac{1}{T_b}\int_{iT_b}^{(i+1)T_b} n(t)\hat{u}(t)\mathrm{d}t \end{aligned} \quad (14)$$

The first term in the above equation stands for the signal component. However, this signal fluctuates with every bit, and performance is degraded by this noise-like action.

2.2 Problems of PAM-based method

Here we estimate the performance of conventional PAM-based chaotic communications while varying L at a fixed bit duration T_b.

First, consider the performance when perfect chaotic synchronization is achieved. Figure 2 shows the bit error rate as a function of E_b/N_0 (E_b: signal energy per bit). Here $f(x) = 2|x \bmod 1| - 1$ was used as the chaotic map, and $a = 0$ was selected as the optimum value on the basis of preliminary experiments. As is evident from Fig. 2, the bit error rate is poor with small L despite the perfect synchronization. Here the variance of the signal component in the correlator output V_i is

$$\begin{aligned} \sigma_{\mathrm{sig}}^2 &= Var\left[\frac{1}{L}\sum_{k=iL}^{(i+1)L-1} x^2(k)\right] \\ &= \frac{1}{L}Var\left[x^2(k)\right] \end{aligned} \quad (15)$$

The above equation suggests that the bit error rate worsens with small L because the spread of the signal component grows.

Now consider the performance when chaotic synchronization is used. Figure 3 shows the bit error rate characteristic, with the chaotic map being the same as in Fig. 2. As is evident from Fig. 3, the results are very poor at $L = 1, 2, 8$. This is because of the large variance of the correlator output, as explained above. On the other hand, when $L = 64$ or higher, the bit rate error worsens as L increases. The variance of the noise component per sample of the input $\hat{y}(k)$ into the chaotic system increases directly with L as follows:

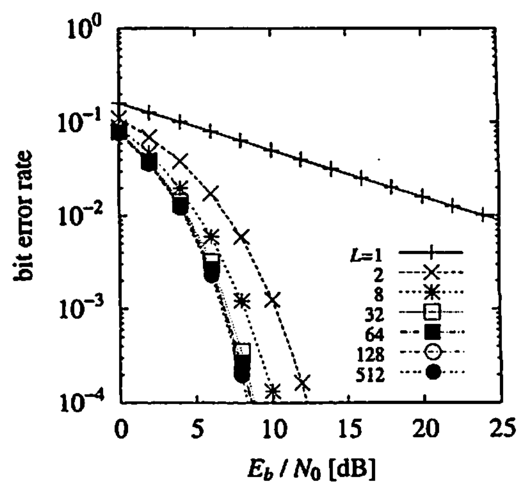

Fig. 2. Bit error rate of conventional system (perfect synchronization).

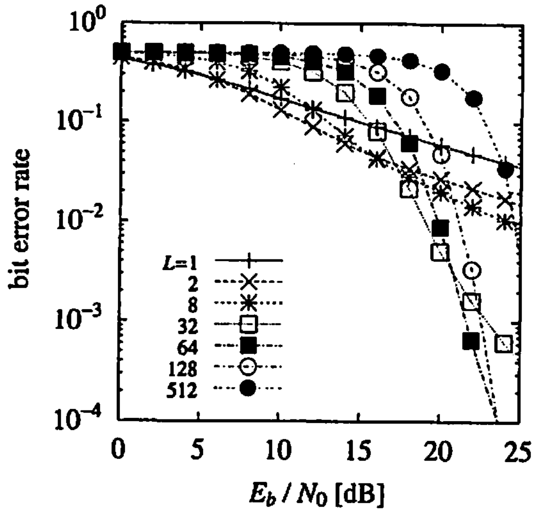

Fig. 3. Bit error rate of conventional system (chaotic synchronization).

$$\sigma^2_{\text{noise}} = Var\left[\frac{1}{T_c}\int_{kT_c}^{(k+1)T_c} n(t)\mathrm{d}t\right] = \frac{LN_0}{2T_b} \tag{16}$$

Therefore, one may attribute the deterioration of the bit error rate to the fact that the chaotic synchronization error increases with L. Hence, a square synchronization error

$$\overline{e^2} = \frac{1}{N}\sum_{k=0}^{N} e^2(k) \tag{17}$$

is shown in Fig. 4 at $E_b/N_0 = 10, 20, 30$ dB. As indicated by the diagram, the synchronization error increases with L. Now consider the nonsynchronized case when $x(k)$ and

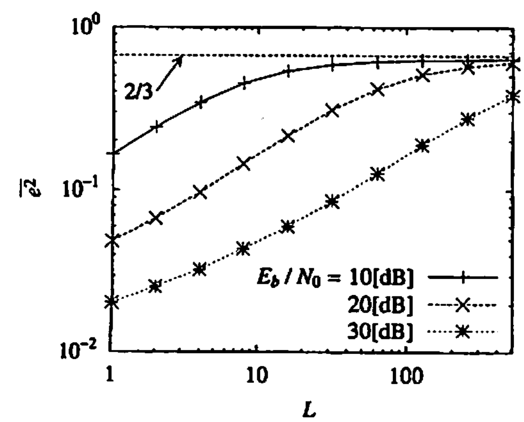

Fig. 4. Chaotic synchronization error.

$\hat{x}(k)$ are independent uniform random numbers. Here the square error variance is

$$E\left[(\hat{x}(k) - x(k))^2\right] = \frac{2}{3} \tag{18}$$

As is evident from Fig. 4, the square synchronization error is about 2/3 for L over 100 when $E_b/N_0 = 20$ dB. Thus, one may assume that little if any synchronization takes place.

The above indicates that the bit error rate improves with larger L in the sense that the variance of signal component in the correlator output decreases. As is evident from Fig. 3, the best bit error rate performance is obtained at $L =$ 64, being below 10^{-3} at 22 dB or greater.

3. Chaotic Communications Using PWM

Applying the constant envelope transformation to the transmitted signal assures zero variance of the correlator output, thus solving the problem of PAM-based communications [11]. While a continuous-time chaotic signal was frequency-modulated in Ref. 11, this study proposes a method of transmitting a discrete-time chaotic signal using a constant-envelope pulse. On the other hand, the spreading factor L should be decreased in order to suppress the chaotic synchronization error. However, with small L, communication becomes vulnerable to interference even in case of perfect synchronization. Interference immunity is a feature of broadband chaotic communications, but when chaotic synchronization is used, there is a trade-off between interference immunity and synchronization error. In this study, we place the emphasis on suppression of synchronization error, thus proposing $L = 1$. As regards the degradation of interference immunity, measures against intersymbol interference will be discussed in Section 4.

3.1 PWM pulse

Here we consider a method of generating binary pulses $P(t, x(k))$ {−1, +1} from a chaotic signal $x(k)$ with a continuous value of (−1, +1). The binary pulses used for chaotic communications must meet the following conditions in order to assure good noise resistance and security.

C1) The original continuous chaotic signal can be extracted at the receiver.

C2) Demodulation is possible by correlation detection.

C3) The pulse form is continuous for chaotic signal $x(k)$.

C4) The data cannot be estimated easily from the received pulse.

The proposed constant-envelope pulse is shown in Fig. 5. When $x(k) \geq 0$, the proposed pulse is

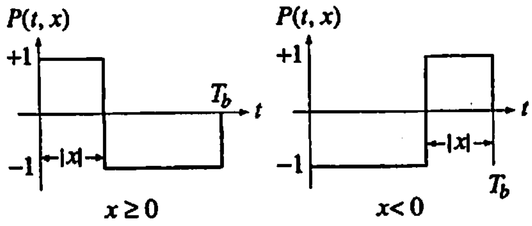

Fig. 5. Constant-envelope pulse.

$$P(t, x(k)) = \begin{cases} +1 \cdots 0 \le t - kT_b < |x(k)|T_b, \\ -1 \cdots |x(k)|T_b \le t - kT_b < T_b, \\ 0 \cdots \text{otherwise} \end{cases} \quad (19)$$

When $x(k) < 0$, it is

$$P(t, x(k)) = \begin{cases} -1 \\ \cdots 0 \le t - kT_b < (1 - |(x(k)|)T_b, \\ +1 \\ \cdots (1 - |x(k)|)T_b \le t - kT_b < T_b, \\ 0 \cdots \text{otherwise} \end{cases} \quad (20)$$

This pulse is composed of two rectangular pulses +1, −1, and the pulse width is varied according to $|x(k)|$, while the time direction is inverted depending on the sign of $x(k)$. With this pulse, not only the pulse width but also the time direction is inverted by using the randomness of chaos. Hence, all of conditions C1 to C4 are satisfied.

3.2 Configuration of communications system

In PWM-based chaotic communications, binary information data $b(i) \in \{-1, +1\}, i = 0, 1, 2, \ldots$ are transmitted using one chaotic sample. A block diagram of the proposed system is shown in Fig. 6.

At the transmitter, chaos is generated by the following discrete-time one-dimensional chaotic system:

$$x(k+1) = ax(k) + f(y(k)) \quad (21)$$

$$y(k) = b(k)(2|x(k)| - 1) \quad (22)$$

The difference of $y(k)$ in Eq. (22) from the PAM-based system (2) will be explained later.

A PWM pulse train is generated by the chaotic signal $x(k)$, and the transmitted signal is produced by multiplying it by the information data $b(k)$:

$$u(t) = \sum_{k=0}^{\infty} b(k) P_{\mathrm{PWM}}(t - kT_b, x(k)) \quad (23)$$

Here $P_{\mathrm{PWM}}(t, x(k))$ is the PWM pulse (19), (20) proposed in Section 3.1. Since the pulse width variation of $P_{\mathrm{PWM}}(t, x(k))$ is finite at $(0, T_b)$, a correction is applied so that 1 is obtained at $x(k) > 1$, and −1 is obtained at $x(k) < -1$.

At the receiver, the input to the discrete-time chaotic system is obtained by integration of the received signal $r(t) = u(t) + n(t)$:

$$\hat{y}(k) = \frac{1}{T_b} \int_{kT_b}^{(k+1)T_b} r(t) \mathrm{d}t \quad (24)$$

In the absence of noise, the above integrator output becomes

$$\hat{y}(k) = b(k)(2|x(k)| - 1) \quad (25)$$

which is equivalent to Eq. (22). That is, $y(k)$ was selected as in Eq. (22) to obtain equal inputs to the chaotic system at the transmitter and receiver.

The chaotic systems at the transmitter and receiver are identical, and the chaos estimate is produced as follows:

$$\hat{x}(k+1) = a\hat{x}(k) + f(\hat{y}(k)) \quad (26)$$

In the absence of noise, the synchronization error is

$$e(k) = \hat{x}(k) - x(k) = ae(k-1) \quad (27)$$

and synchronization takes place as in the case of PAM.

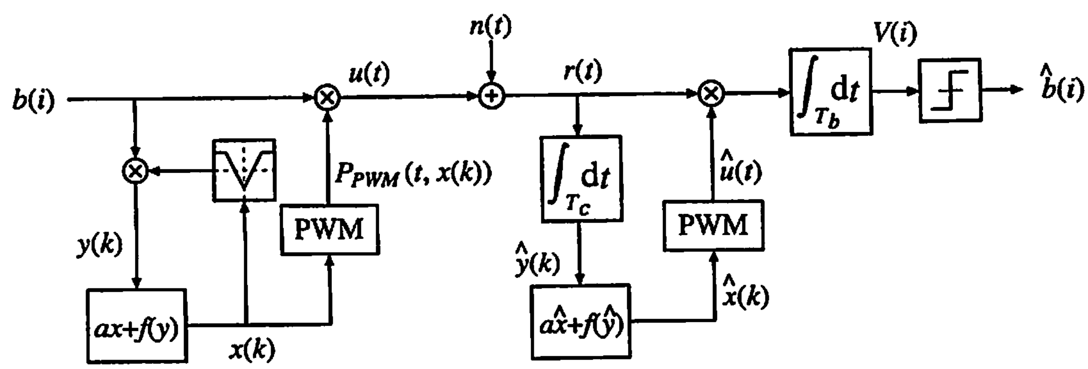

Fig. 6. Communication system based on chaotic synchronization using PWM.

Then, a replica of the PWM pulse train is generated using the chaos estimate $\hat{x}(k)$:

$$\hat{u}(t) = \sum_{k=0}^{\infty} P_{\mathrm{PWM}}(t - kT_b, \hat{x}(k)) \tag{28}$$

The correlator output $V(i)$ for the information data $b(k)$ is

$$V(i) = \frac{1}{T_b} \int_{iT_b}^{(i+1)T_b} r(t)\hat{u}(t)\mathrm{d}t \tag{29}$$

The information data estimate is obtained as $\hat{b}(i) = \mathrm{sgn}(V(i))$. When the chaotic synchronization is perfect, that is, when $\hat{x}(k) = x(k)$, Eq. (29) can be rewritten as follows:

$$\begin{aligned} V(i) &= \frac{b(i)}{T_b}\{T_b \cdot \underbrace{P_{PWM}(t - kT_b, x(k))^2}_{=1}\} \\ &\quad + \frac{1}{T_b} \int_{iT_b}^{(i+1)T_b} n(t)\hat{u}(t)\mathrm{d}t \\ &= b(i) + \frac{1}{T_b} \int_{iT_b}^{(i+1)T_b} n(t)\hat{u}(t)\mathrm{d}t \end{aligned} \tag{30}$$

The first term above expresses the signal component. Unlike PAM-based systems, there is no scatter for every bit.

3.3 Bit error rate characteristic

The bit error rate performance of the proposed system is shown in Fig. 7.

The chaotic synchronization parameter is set to a = 0, 0.05, 0.1, 0.2, 0.3, 0.4, 0.5. In the proposed system, the nonlinear mapping shown in Eq. (25) is used, and hence

$$x(k+1) = ax(k) + f(b(k)(2|x(k)| - 1)) \tag{31}$$

Here $f(x) = x$ is assumed, so that the second term on the right-hand side of Eq. (31) is the same as in PAM. In addition, for $a = 0$, the chaotic signal $x(k)$ on the transmitter side is the same for PAM and PWM. For comparison, we also show the bit error rate for PAM-based chaotic communications ($L = 64$), and for OOK (On-Off Keying) envelope detection. As is evident from Fig. 7, the bit error rate is best at $a = 0$. In the proposed system, a bit error rate below 10^{-3} is reached at E_b/N_0 above 14 dB, which suggests an improvement of about 8 dB compared to PAM. This difference is explained by the fact that the variance of the signal component in the correlator output becomes zero due to the use of a constant-envelope pulse, and the synchronization error is reduced by setting the spreading factor to $L = 1$. Compared to perfect synchronization, E_b/N_0 becomes about 7 dB worse in order to reach a bit error rate below 10^{-3}. In the proposed system, the correlator output is identical to that of BPSK if the chaotic synchronization is perfect, regardless of the noise. Therefore, the reason for the poor bit error rate is synchronization error.

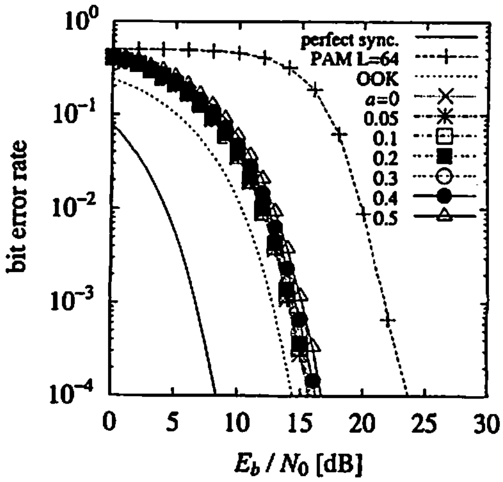

Fig. 7. Bit error rate of proposed system.

3.4 Security considerations

Various decoding methods have been developed for chaotic masking [18, 19], but there are few if any studies for CSK. In CSK, decoding is possible if statistical values such as the mean and variance of the transmitted signal and the return maps and attractors differ depending on the information data [20].

In conventional PAM-based chaotic communications without noise, the transmitted signal is an irregular signal at first sight. However, two kinds of return maps with different phase corresponding to the information data {+1, −1} can be obtained by sampling of the transmitted signal at appropriate time intervals. Thus, in conventional chaotic communications, the information data may be estimated even in the absence of knowledge of the chaotic synchronization system by observing the time series at 1-bit duration and checking the return maps. However, the spreading factor L must be set to 2 or higher (the higher the better) in order to obtain different return maps.

In the proposed method, the number of chaotic signal samples allocated to 1 bit is $L = 1$. Hence, it is difficult to extract a sufficient number of samples from the transmitted signal in order to estimate statistically significant per-bit values. Thus, it is extremely difficult to obtain two different return maps corresponding to the information data. Similarly, $L = 1$ proves effective with respect to decoding methods using statistical values of the chaotic signal. In addition, if chaotic maps of even functions are employed, the distribution of the chaotic signal is symmetric, and the statistical values of the transmitted signal can be fixed regardless of the information data. Therefore, the proposed method can be called confidential in the sense that conventional decoding techniques would not work.

The chaotic signal is a random broadband signal, which offers the possibility of secure communications. However, chaotic communications is not necessarily better in every aspect than conventional cryptographic technologies. Still, chaotic signals are very attractive in that they can be generated by using very simple hardware, and their real advantages can be demonstrated when used in combination with state-of-the-art technologies.

4. Suppression of Intersymbol Interference by Using Blind Adaptive Equalizer

Above we examined communication channels free of interference. In this section, we consider an AR communications channel as a channel with intersymbol interference. The proposed communications based on chaotic synchronization is rather vulnerable to interference, even in case of perfect chaotic synchronization, because $L = 1$. In addition, chaotic communications becomes very difficult in the presence of interference. Therefore, we consider the suppression of intersymbol interference by applying an adaptive equalizer prior to chaotic synchronization.

In adaptive algorithms that require training signals, the transfer efficiency drops because of the sending of training signals. In addition, chaotic communications assumes that the chaotic signal used at the transmitter side is not known at the receiver side. Therefore, blind adaptive algorithms that do not require training signals are preferable for chaotic communications.

CMA [14] is known as a typical blind adaptive algorithm that can be applied to constant-envelope signals. The problem with this algorithm is that convergence of the weight coefficients to the optimal solution is not guaranteed [15]. Applying CMA to constrained equalizers [16] was proposed as a solution to the problem. However, this solution does not work well when the direct wave gain of the AR communications channel is small. In addition, using differential CMA instead of CMA was also examined [17], but in this case, optimality is guaranteed only for a first-order AR channel. In this study, we propose a new algorithm that guarantees optimality regardless of the direct wave magnitude in an Nth-order AR channel.

4.1 Communications channel model and equalizer

When noise can be ignored, the received signal sampled at time intervals of T_s can be expressed as follows:

$$r_k = Gu_k + \sum_{i=1}^{N} a_i r_{k-i} \tag{32}$$

Here $G \in R$ is the direct wave gain and $a_i \in R$ is the AR channel parameter. In addition, r_k, u_k are, respectively, the k-th received signal and the transmitted signal sampled at T_s. In this study, we consider an FIR equalizer constrained at a first tap weight of 1 [13, 17]. The output y_k of this nonlinear constrained equalizer is

$$\begin{aligned} y_k &= r_k + \sum_{i=1}^{N} w_i r_{k-i} \\ &= Gu_k + I_k \end{aligned} \tag{33}$$

Here

$$I_k = \sum_{i=1}^{N} (w_i + a_i) r_{k-i} \tag{34}$$

is the intersymbol interference, and $\omega_i \in R$ is the equalizer's tap weight. The first tap input r_k includes intersymbol interference with the received signal u_k, but the intersymbol interference included in the first tap input is eliminated by adjustment of the second and subsequent tap weights.

4.2 Blind adaptive equalization algorithm

The following evaluation function is proposed in this study:

$$J = \frac{1}{4} E\left[\left(y_k^2 - E\left[y_k^2\right]\right)^2\right] \tag{35}$$

Since the transmitted signal is a constant-envelope signal in PWM-based communications, Eq. (35) is obviously zero. If channel noise can be ignored, weight convergence to the optimal solution is assured by minimization of evaluation function (35) by the gradient method (see Appendix 1). Performance evaluation in the presence of noise is considered in the following section.

A stochastic gradient algorithm is obtained by partial differentiation of Eq. (35) with respect to ω_i, and replacing the expectation with the instantaneous value:

$$\begin{aligned} w_i(k+1) &= w_i(k) \\ &\quad - \mu \left(y_k^3 r_{k-i} - \overline{y_k^2} y_k r_{k-i} \right) \end{aligned} \tag{36}$$

Here μ is the step size and $\overline{y_k^2}$ is the mean square of the output; at a stationary point, $\overline{y_k^2} = G^2$. Finally, the equalizer's output $\overline{y_k}$ is corrected as follows to obtain the original discrete-time chaotic signal:

$$y_k' = \frac{y_k}{\sqrt{\overline{y_k^2}}} \tag{37}$$

4.3 Computer simulation

In order to verify the effectiveness of the adaptive equalizer using the proposed algorithm, a computer simulation was performed for a second-order AR channel at $G = 1, a_1 = 0.3, a_2 = 0.2$. The interference-to-signal power ratio (ISR) is shown in Fig. 8. Here $E_b/N_0 = 30$ dB is assumed.

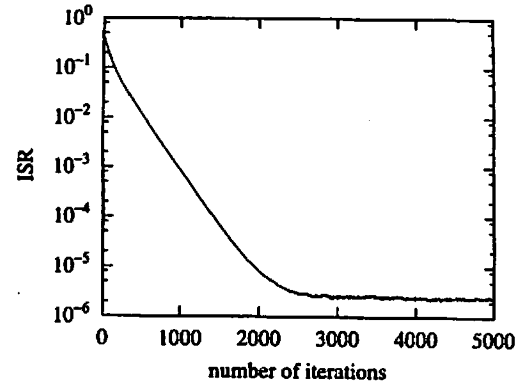

Fig. 8. ISR characteristic.

The ISR was calculated by the equation

$$\mathrm{ISR} = \frac{\sum_{i=0}^{10} g_i^2 - \max_i g_i^2}{\max_i g_i^2} \tag{38}$$

and the ensemble average for 1000 samples was found. Here $g_i = \sum_{l=0}^{N} \omega_l h_{i-l}$ is the system impulse response including the communication channel and equalizer, and $\{h_l\}$ is the impulse response of the communication channel. As is evident from the diagram, the proposed algorithm efficiently suppresses interference. In addition, the bit error rate is given in Fig. 9. As indicated by the diagram, the bit error rate performance is considerably worse than in the case of a white-noise channel without interference (Fig. 7). However, when the equalizer is applied, a bit error rate below 10^{-3} is obtained at E_b/N_0 of about 15 dB, which indicates satisfactory effectiveness.

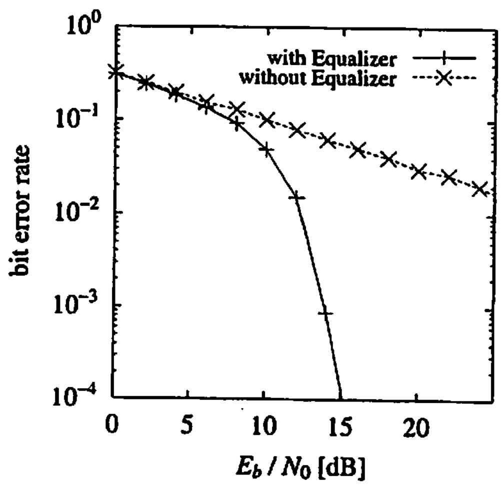

Fig. 9. Bit error rate characteristic.

5. Conclusions

In this paper, we have proposed PWM-based constant-envelope transformation of a transmitted signal in order to improve the performance of communications based on chaotic synchronization. In the proposed method, the variance of the correlator output is kept small, as is the synchronization error, thus yielding a good bit error rate compared to conventional PAM-based communications. In addition, we proposed a blind adaptive equalization algorithm to reduce intersymbol interference, and demonstrated its effectiveness for communication based on chaotic synchronization.

Security analysis and further improvement of the bit error rate are topics for future research. In addition, we plan to investigate the influence of chaos maps and synchronization errors, and to compare the proposed method to DCSK and other communication techniques not using chaotic synchronization.

REFERENCES

1. Pecora LM, Carroll TL. Synchronization in chaotic systems. Phys Rev Lett 1990;64:821–824.
2. Oppenheim AV, Wornell GW, Isabelle SH, Cuomo KM. Signal processing in the context of chaotic signals. Proc 1992 IEEE ICASSP 1992;4:117–120.
3. Cuomo KM, Oppenheim AV, Strogatz SH. Synchronization of Lorenz-based chaotic circuits with applications to communications. IEEE Trans Circuits Syst.-II 1993;40:626–633.
4. Itou M, Murakami H. Chaos synchronization and secure communications in discrete dynamical systems. Tech Rep IEICE 1992;NLP92-50:25–31.
5. Wu CW, Chua LO. A simple way to synchronize chaotic systems with applications to secure communication systems. Int J Bifurcation and Chaos 1993;3:1619–1627.
6. Parlitz U, Chua LO, Kocarev L, Halle KS, Shang A. Transmission of digital signals by chaotic synchronization. Int J Bifurcation and Chaos 1992;2:973–977.
7. Dedieu H, Kennedy MP, Hasler M. Chaos shift keying: modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuits. IEEE Trans Circuits & Syst.-II 1993;40:634–642.
8. Ushio T, Innami T, Kodama S. Chaos shift keying based on in-phase and anti-phase chaotic synchronization. IEICE Trans Fundamentals 1996;E79-A:1689–1693.
9. Nakamura K, Miyajima T, Yamanaka K. A digital multiplex communication system using chaos. IEICE Trans Fundamentals 1999;J82-A:1483–1485. *(in* Japanese)

10. Kolumbán G, Kennedy MP. The role of synchronization in digital communications using chaos—Part III: performance bounds for correlation receivers. IEEE Trans Circuits & Syst.-I 2000;47:1673–1683.
11. Kolumbán G, Kis G, Jákó Z, Kennedy MP. FM-DCSK: A robust modulation scheme for chaotic communications. IEICE Trans Fundamentals 1998; E81-A:1798–1802.
12. Cuomo KM, Oppenheim AV, Barron RJ. Channel equalization for self-synchronizing chaotic systems. Proc 1996 IEEE ICASSP 1996;3:1605–1608.
13. Nakamura K, Miyajima T, Suzuki N, Yamanaka K. Communication systems using chaotic synchronization in multipath channels. Proc 1999 NOLTA 1999;1:223–226.
14. Treichler JR, Agee BG. A new approach to multipath correction of constant modulus signals. IEEE Trans Acoust, Speech, Signal Proc 1983;31:459–472.
15. Ding Z, Kennedy RA, Anderson BDO, Johnson CR. Ill convergence of godard blind equalizers in data communication systems. IEEE Trans Circuits Syst-I 1991;39:1313–1327.
16. Kamel RE, Barness Y. Anchored blind equalization using the constant modulus algorithm. IEEE Trans Circuits Syst-I 1997;44:397–403.
17. Miyajima T. Differential constant modulus algorithm for anchored blind equalization of AR channels. IEICE Trans Fundamentals 2002;E85-A:2939–2942.
18. Short KM. Steps toward unmasking secure communications. Int J Bifurcation and Chaos 1994;4:959–977.
19. Short KM. Unmasking a modulated chaotic communications scheme. Int J Bifurcation and Chaos 1996;6:367–375.
20. Rubezic V, Ostojic R. Breaking chaotic switching using generalised synchronization. Proc 2000 IEEE NORSIG.

APPENDIX

1. Stationary Point of Equalization Algorithm

Evaluation function (35) can be rewritten as

$$J = \frac{1}{4}E\left[\left(y_k^2 - E[y_k^2]\right)^2\right] = \frac{1}{4}\left(E\left[y_k^4\right] - E\left[y_k^2\right]^2\right) \qquad \text{(A.1)}$$

Considering the randomness of chaos, let us assume $E[u_k] = E[u_k^3]$. In addition, $u_k^2 = 1$, because of the use of constant-envelope PWM pulses. Partial differentiation of Eq. (A.1) with respect to ω_i gives

$$\begin{aligned}\frac{\partial J}{\partial w_i} &= E\left[y_k^3 r_{k-i}\right] - E\left[y_k^2\right]E\left[y_k r_{k-i}\right] \\ &= E\left[(Gu_k + I_k)^3 r_{k-i}\right] \\ &\quad - E\left[(Gu_k + I_k)^2\right]E\left[(Gu_k + I_k) r_{k-i}\right] \\ &= \left(2G^2 - E[I_k^2]\right)E[I_k r_{k-i}] \\ &\quad + E[I_k^3 r_{k-i}] \end{aligned} \qquad \text{(A.2)}$$

Here $E[I_k r_{k-i}] = E[I_k^3 r_{k-i}]$ if $I_k = 0$; therefore, $\partial J/\partial\omega_i = 0, \forall i$, indicating a stationary point.

In addition, by multiplying both sides of Eq. (A.2) by $(\omega_i + a_i)$, and summing from $i = 1$ to N, we obtain

$$\begin{aligned}&\sum_{i=1}^{N}(w_i + a_i)\frac{\partial J}{\partial w_i} \\ &= E\left[y_k^3 \sum_{i=1}^{N}(w_i + a_i)\, r_{k-i}\right] \\ &\quad - E\left[y_k^2\right]E\left[y_k \sum_{i=1}^{N}(w_i + a_i)\, r_{k-i}\right] \\ &= E\left[y_k^3 I_k\right] - E\left[y_k^2\right]E\left[y_k I_k\right] \\ &= 2G^2 E\left[I_k^2\right] + E\left[\left(I_k^2 - E\left[I_k^2\right]\right)^2\right] \geq 0 \end{aligned} \qquad \text{(A.3)}$$

For a stationary point $\partial J/\partial\omega_i = 0, \forall i$, the above becomes zero. On the other hand, $I_k = 0$ is required for the above to become zero. Therefore, $y_k = Gu_k, I_k$ at a stationary point; and J takes its minimum value of 0.

Denoting the correlation matrix of equalizer's tap input by $\mathbf{R} = [E[r_{k-i} r_{k-j}]]$, $\overline{\mathbf{w}} = [\omega_1 + a_1 \cdots \omega_N + a_N]^T$, the following can be derived:

$$\text{if } \overline{\mathbf{w}} = [w_1 + a_1 \cdots w_N + a_N]^T$$
$$E[I_k^2] = \overline{\mathbf{w}}^T \mathbf{R} \overline{\mathbf{w}} \qquad \text{(A.4)}$$

Since $\mathbf{R}$ is positive definite, $\overline{\mathbf{w}} = 0$ is required for $E[I_k^2] = 0$. Therefore, $\omega_i = -a_i, \forall i$ at a stationary point. In addition, at such a point,

$$\frac{\partial^2 J}{\partial w_i \partial w_j} = 2G^2 E[r_{k-i} r_{k-j}],\ I_k = 0 \qquad \text{(A.5)}$$

Since the Hesse matrix $\mathbf{H} = 2G^2\mathbf{R}$ is positive definite, this stationary point is stable.

As follows from the above, I_k can be eliminated by minimizing J.

AUTHORS (from left to right)

  

Kazuhiko Nakamura (nonmember) graduated from Ibaraki University (systems engineering) in 1996, completed the doctoral program in 2004, and joined the faculty of the University of Yamanashi as a research associate. His research interests are communications engineering, signal processing, and chaotic communications. He holds a D.Eng. degree, and is a member of IEICE.

Teruyuki Miyajima (nonmember) graduated from Saitama University (electrical engineering) in 1989, completed the doctoral program in 1994, and joined the faculty of Ibaraki University as a research associate, becoming a lecturer in 1998 and a research associate professor in 2004. His research interests are communications technologies and signal processing. He holds a D.Eng. degree, and is a member of IEICE and IEEE.

Kazuo Yamanaka (member) graduated from Waseda University (electrical engineering) in 1974, completed the doctoral program in 1979, and joined the faculty of Ibaraki University as a research associate, becoming an associate professor in 1988 and a professor in 1993. His research interests are estimation and control of uncertain systems. He holds a D.Eng. degree, and is a member of SICE, ISCIE, and other societies.