New Communication Systems via Chaotic Synchronizations and Modulations

Makoto ITOH[†] *and* Hiroyuki MURAKAMI[†], *Members*

SUMMARY   In this paper, we demonstrate how Yamakawa's chaotic chips and Chua's circuits can be used to implement a secure communication system. Furthermore, their performance for the secure communication is discussed.
key words: *chaos synchronization, communication systems, Yamakawa's chaotic chip, Chua's circuit*

1. Introduction

Recently, there has been much interest in utilizing chaotic circuits to implement a secure communication system [1]–[8]. Most of them are realized by the continuous-time dynamical system, and are using Chua's circuit as its basic circuit elements.

In this paper, we propose a new scheme to utilize Yamakawa's chaotic chip in constructing a secure communication system. This system is realized by the discrete-time dynamical system. We shall first introduce the Yamakawa's chaotic chip and its dynamics. Then, we construct the communication system by using this chip. The basic idea of our communication system is based on the new chaotic modulation and demodulation technique proposed in Ref. [9]. This system has the following nice properties:
(a) Only a few circuit elements, it is built up of.
(b) High security.

Next, we show the communication system via Chua's circuits, in which the same chaotic modulation and demodulation technique is employed. Finally, we discuss the performance of the Yamakawa's chaotic chips and the Chua's circuits for the secure communication systems.

2. Yamakawa's Chaotic Chips

Yamakawa's chaotic chip is a remarkably flexible and robust element, which realizes discrete-time dynamical systems [10]. It has three elements, that is, a nonlinear delay element, a linear delay element, and a summing element (see Figs. 1 and 2). By connecting these elements with each other, we can get a number of discrete-time dynamical systems. The following equations describe some of its basic dynamics:

(a) 1-dimensional system

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

(b) 2-dimensional system

$$x_{n+1} = f(x_n) - \alpha y_n, \qquad y_{n+1} = x_n - \beta y_n, \qquad (2)$$

where $f(\cdot)$ is a nonlinear function represented by a 3-segment piecewise linear function (see Fig. 3) and α, β are parameters. The systems (1) and (2) exhibit a number of bifurcations and chaotic phenomena by changing the control parameters α, β and the characteristic of the nonlinear function f.

3. Communication Systems via Yamakawa's Chaotic Chips

The basic concept of our secure communication system can be written as follows [11]: two processes are used to construct the system. One is the chaotic coding, and the other is the chaotic modulation.

The transmitting system is given by

$$x_{n+1} = f(x_n) + \varepsilon s_n,$$
$$y_{n+1} = g(y_n) - \alpha z_n + \delta x_n, \quad z_{n+1} = y_n - \beta z_n, \qquad (3)$$

where α, β are some constants, ε, δ are sufficiently small, and $f(\cdot)$, $g(\cdot)$ are 3-segment piecewise linear functions. We suppose that (3) has chaotic behaviors for $\varepsilon = \delta = 0$. The informational signal and the transmitted signal are given by s_n and y_n, respectively. The chaotic codings and the chaotic modulations are performed by the first equation and the remaining equations in (3), respectively. Therefore, the chaotically modulated signal y_n is transmitted to the channel. Considering the systems (1) and (2), the transmitting system (3) is easily built by using the Yamakawa's chaotic chips and the summing elements.

The receiver constructs the following system by using the transmitted signal y_n:

$$z'_{n+1} = y_n - \beta z'_n,$$
$$t_n = \frac{y_{n+1} - g(y_n) + \alpha z'_n}{\delta}, \quad r_n = \frac{t_{n+1} - f(t_n)}{\varepsilon}, \qquad (4)$$

where r_n is the recovered signal.

Next, we show how the informational signal can be recovered (demodulation process). Establishing the
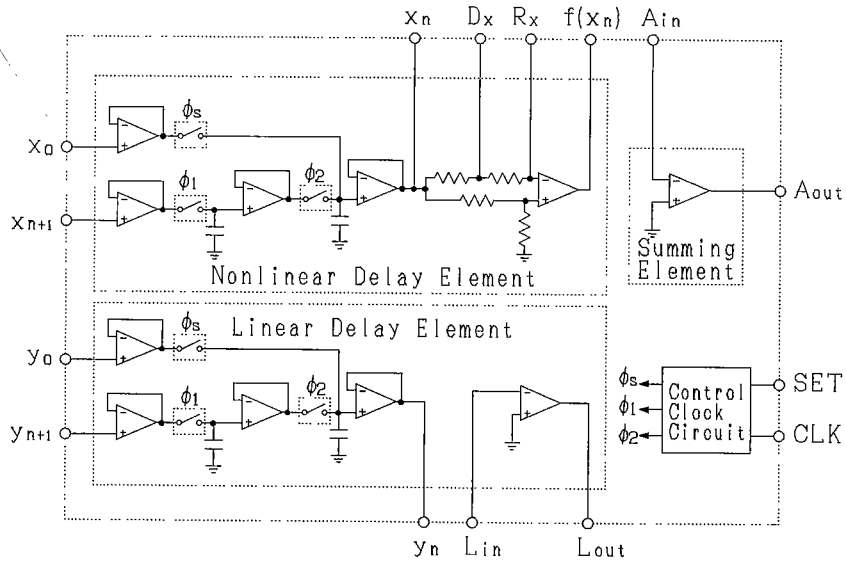
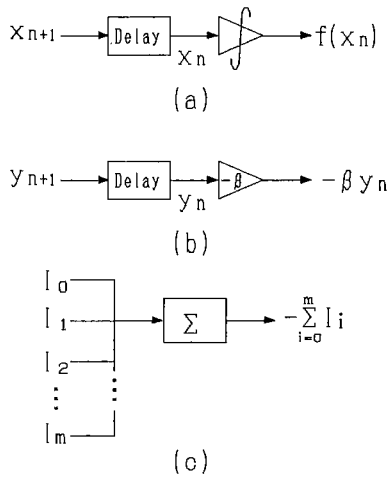**Fig. 1** Circuit for Yamakawa's chaotic chip. (Based on Ref. [10].)

Fig. 2 Block diagrams of (a) a nonlinear delay element, (b) a linear delay element, (c) a summing element. (Based on Ref. [10].)
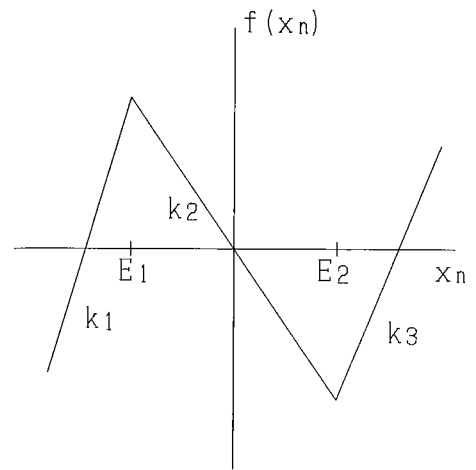

Fig. 3 Nonlinear function $f(x_n)$.

difference $p_n = z_n - z'_n$ and subtracting (4) from (3), we get the variational equations:

$$p_{n+1} = -\beta p_n. \qquad (5)$$

If $\mid \beta \mid < 1$, then $\mid p_n \mid = \mid z_n - z'_n \mid \to 0$ as $n \to \infty$, that is, z_n and z'_n will synchronize. Therefore, $\mid t_n - x_n \mid = \mid \alpha(z_n - z'_n)/\delta \mid \to 0$. It implies that $r_n = \{t_{n+1} - f(t_n)\}/\varepsilon \to s_n = \{x_{n+1} - f(x_n)\}/\varepsilon$ as $n \to \infty$ (that is, the informational signal is recovered).

The receiving system is also built by using the Yamakawa's chaotic chips for their flexibility. The experimental circuit of our communication system is shown in Fig. 4. It is possible to construct the similar secure communication systems by reversing the chaotic coding and the chaotic modulation processes. Furthermore, we can repeat the chaotic modulation and the chaotic cod-

ing again and again (for the transmitting signal y_n; see Ref. [12]). These repeated processes can make the transmitting signal more and more secure. This is due to the following reason:

(a) The transmitted signal becomes more and more complex.

(b) The system has the high sensitivity to parameter changes.

These properties are the remarkable merit of our new communication systems. The parameters we use in the laboratory experiments are:

$$\alpha = 0.11, \quad \beta = 0.196, \quad \delta = 0.1, \quad \varepsilon = 0.1,$$
$$k_1 = 3.6, \quad k_2 = -1.3, \quad k_3 = 2.1,$$
$$E_1 = -1.5V, \quad E_2 = 2.4V, \quad \text{for} \quad f(\cdot),$$
$$k'_1 = 4.0, \quad k'_2 = -1.5, \quad k'_3 = 2.5,$$
$$E'_1 = -1.3V, \quad E'_2 = 0.8V, \quad \text{for} \quad g(\cdot). \qquad (6)$$
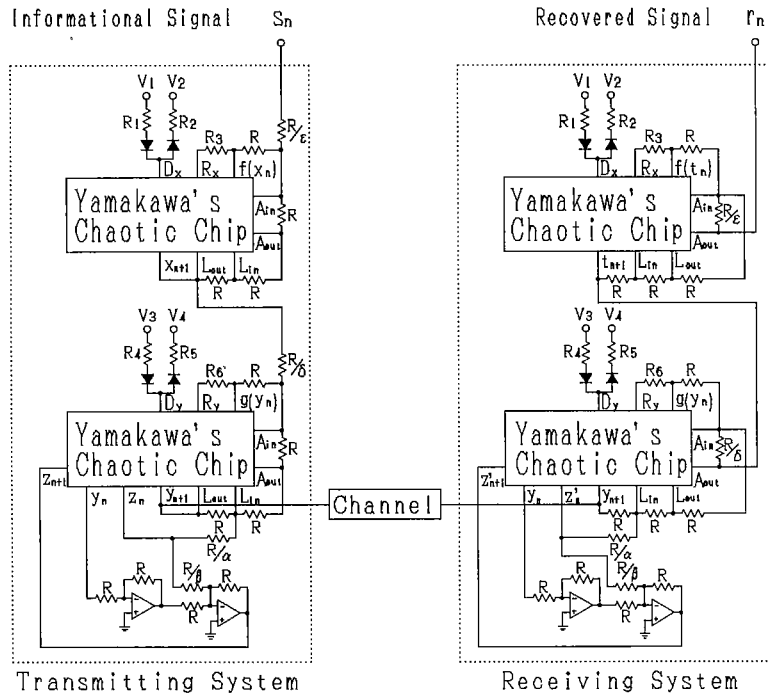
Fig. 4 Communication system via Yamakawa's chaotic chips.

Fig. 5 Chua's circuit.

Fig. 6 v-i characteristic of the nonlinear resistor N_R.
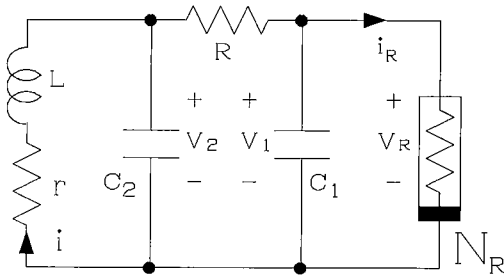
4. Chua's Circuit

Chua's circuit is the simple and robust circuit, which exhibits the complex dynamics of bifurcation and chaos. The circuit consists of a linear inductor L, two linear resistors R and r, two linear capacitors C_1 and C_2, and a nonlinear resistor N_R (see Fig. 5 and Ref. [13]). The state equations are given by

$$C_1 \frac{dv_1}{dt} = \frac{v_2 - v_1}{R} - h(v_1),$$

$$C_2 \frac{dv_2}{dt} = \frac{v_1 - v_2}{R} + i,$$

$$L \frac{di}{dt} = -v_2 - ri, \tag{7}$$

where $h(\cdot)$ is a piecewise linear function defined by

$$h(v_R)$$
$$= G_b v_R + \frac{1}{2}(G_a - G_b)(|\ v_R + B_p\ | - |\ v_R - B_p\ |), \tag{8}$$

and shown in Fig. 6. The circuit parameters we use are $C_1 = 10.3\,\mathrm{nF}$, $C_2 = 97.4\,\mathrm{nF}$, $L = 20.7\,\mathrm{mH}$, $R = 1.41\,\mathrm{k\Omega}$, $B_p = 1.85\,\mathrm{V}$, $G_a = -0.87\,\mathrm{mS}$, $G_b = -0.52\,\mathrm{mS}$, and $r = 64.2\,\Omega$.

5. Communication Systems via Chua's Circuits

The basic construction of our communication system is shown in Fig. 7. The outline of this system was given in Refs. [7] and [8], however, in order to compare the performance of Chua's circuits with Yamakawa's chaotic chips, we refer their results briefly. The circuit equations for the transmitting system are given by
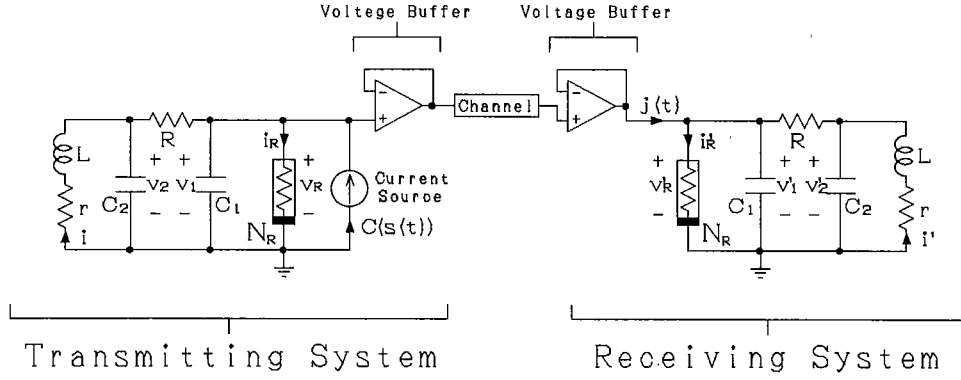
Fig. 7 Communication system via Chua's circuits.

$$C_1 \frac{dv_1}{dt} = \frac{v_2 - v_1}{R} - h(v_1) + C(s(t)),$$

$$C_2 \frac{dv_2}{dt} = \frac{v_1 - v_2}{R} + i,$$

$$L \frac{di}{dt} = -v_2 - ri, \qquad (9)$$

where C is a coding function with an inverse. We use the current source $s(t)$ as an informational signal, and $v_1(t)$ as a transmitted signal. That is, the equation (9) performs a chaotic modulation of the signal $s(t)$, and so the chaotically modulated signal $v_1(t)$ is transmitted to the channel.

The circuit equations for the receiving system are given by

$$C_1 \frac{dv_1'}{dt} = \frac{v_2' - v_1'}{R} - h(v_1'),$$

$$C_2 \frac{dv_2'}{dt} = \frac{v_1' - v_2'}{R} + i',$$

$$L \frac{di'}{dt} = -v_2' - ri', \qquad (10)$$

where $v_1 = v_1'$.

Next, we show how the informational signal can be recovered (that is, the demodulation process). From the first equation in (9), we have

$$s(t) = C^{-1}(C_1 \frac{dv_1}{dt} - \frac{v_2 - v_1}{R} + h(v_1)), \qquad (11)$$

The current $j(t)$ in Fig. 7 is given by

$$j(t) = C_1 \frac{dv_1'}{dt} - \frac{v_2' - v_1'}{R} + h(v_1'). \qquad (12)$$

Establishing the difference $p(t) = v_2(t) - v_2'(t)$ and $q(t) = i(t) - i'(t)$, and subtracting (10) from (9) we get

$$C_2 \frac{dp}{dt} = -\frac{p}{R} + q,$$

$$L \frac{dq}{dt} = -p - rq. \qquad (13)$$

Since the origin is globally asymptotically stable, $| p | = | v_2 - v_2' | \to 0$ and $| q | = | i - i' | \to 0$ as $t \to \infty$, that is,
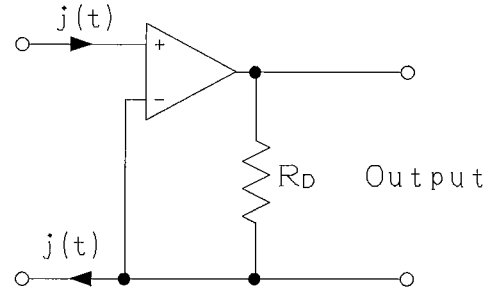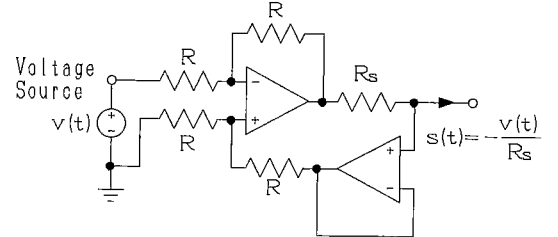

Fig. 8 Current detector.

Fig. 9 Current source.

the (v_2, i)-subsystem and the (v_2', i')-subsystem will synchronize. Therefore, $C^{-1}(j(t)) \to s(t)$ as $t \to \infty$. This implies that the informational signal $s(t)$ is recovered by $C^{-1}(j(t))$. For details, see Refs. [7],[8] and [14]. In our experiment, the coding function is chosen so that $C(u) = u$, and therefore we used the simple current detector shown in Fig. 8. The proper use of the complex coding function C makes the transmitting signals more and more secure [7]. The current source is realized by the circuit in Fig. 9.

6. Impedance Converters

In our communication systems, the chaotic synchronization is used to recover the signal. If the parameters of the receiving system are slightly different from those of the transmitting system, then the recovered signal $j(t)$ is corrupted by the chaotic noises. Accordingly, parameter matching are indispensable to recover the informational
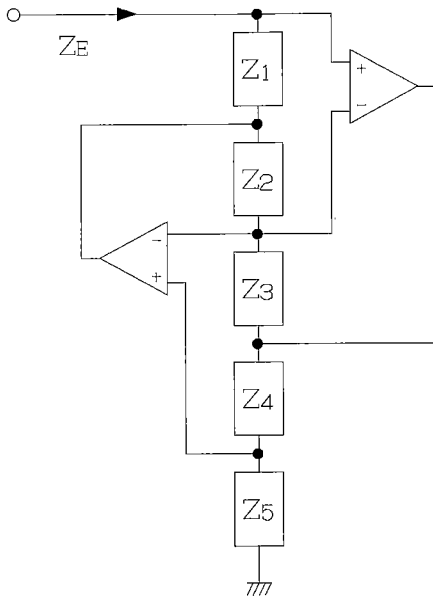
Fig. 10 Impedance converter.

signal with high fidelity. For this purpose, impedance converters are very useful.

The impedance of the circuit in Fig. 10 is given by

$$Z_E = \frac{Z_1 Z_3 Z_5}{Z_2 Z_4}. \tag{14}$$

Therefore, by setting $Z_1 = R_1$, $Z_2 = R_2$, $Z_3 = R_3$, $Z_4 = (j\omega C_4)^{-1}$, and $Z_5 = R_5$, we get the ideal inductor with the impedance:

$$Z_E = \frac{j\omega C_4 R_1 R_3 R_5}{R_2}. \tag{15}$$

Similarly, by setting $Z_1 = R_1$, $Z_2 = R_2$, $Z_3 = R_3$, $Z_4 = R_4$, and $Z_5 = (j\omega C_5)^{-1}$, we get the ideal capacitor with the impedance:

$$Z_E = \frac{1}{j\omega C_5} \cdot \frac{R_1 R_3}{R_2 R_4}. \tag{16}$$

By adjusting the value of R_i, we can easily match the parameters of the capacitors and inductors used in the communication systems.

7. Performance of Yamakawa's Chaotic Chips and Chua's Circuits

We built the two types of communication systems, that is, the communication system via Chua's circuits and the one via Yamakawa's chaotic chips. Both systems are tested by using human voices and music signals. Then, the following experimental results are obtained[†]:

A. Common features of two systems (see Refs. [7]–[9],[11] and [12])
(a) Two systems exhibit the good performance for the secure communication. That is, the transmitting signals

can mask the informational signals, and have the spread spectra.

(b) The security property comes from the high sensitivity of synchronization versus parameter changes. To eliminate the masking signal, very accurate knowledge of the parameter of the system is required to synchronize the chaotic signal. That is, the parameters of the systems serve as the "encryption key".

(c) The informational signals are recovered with high quality, however the retrieved signals are corrupted by the channel noise.

B. Features of the systems via Yamakawa's chaotic chips (see Refs. [11] and [12])
(a) The chaotic chip is expensive at this point of time (about \$50/chip), but the construction of the system is very easy. (We have only to connect the chips with wires.)

(b) We must eliminate the noise accompanied with the sampling, since the communication system is realized by the discrete-time dynamical system. Furthermore, the channel bandwidth must be great.

(c) The repeated chaotic modulations or chaotic codings make the system more and more secure. We can easily implement these processes by using a few chaotic chips.

C. Features of the systems via Chua's circuits (see Refs. [7]–[9])
(a) Low cost (all the systems are built at an expense \$20).

(b) The channel bandwidth is not so great.

(c) The coding function is easily implemented. However, the implementation of the repeated chaotic modulations requires a number of ICs.

8. Concluding Remarks

We proposed the new schemes to utilize Yamakawa's chaotic chips and Chua's circuits in constructing the secure communication systems. It is based on the new chaotic modulation-demodulation techniques. Both systems show the good performance for the secure communication, and have some merits and demerits. The details of this research and its related topics will be given elsewhere. Lastly, we refer the work of Ushio [15], which may bring a new scheme in this field.

[†] The recording tape is available. For more information, please contact: itoh@ec.nagasaki-u.ac.jp.

References

[1] Oppenheim, A.L., Wornell, G.W., Isabelle, S.H. and Cuomo, K.M., "Signal processing in the context of chaotic signals," *Proc. 1992 IEEE ICASSP, IV*, pp.117–120, 1992.

[2] Kocarev, Lj., Halle, K.S., Eckert, K., Parlitz, U. and Chua, L.O., "Experimental demonstration of secure communications via chaos synchronization," *Int. J. Bifurcation and Chaos*, vol.2, no.3, pp.709–713, 1992.

[3] Parlitz, U., Chua, L.O., Kocarev, Lj., Halle, K.S. and Shang, A., "Transmission of digital signals by chaotic synchronization," *Int. J. Bifurcation and Chaos*, vol.2, no.4, pp.973–977, 1992.

[4] Kennedy, M.P. and Dedieu, H., "Experimental demonstration of binary chaos-shift-keying using self-synchronizing Chua's circuits," *Workshop on Nonlinear Dynamics of Electronic Systems*, Dresden, 1993.

[5] Dedieu, H., Kennedy, M.P. and Hasler, M., "Chaos shift keying: Modulation of a chaotic carrier using self-synchronizing Chua's circuits," *IEEE Trans. Circuits and Systems (part II)*, vol.40, no.10, pp.634–642, 1993.

[6] Hasler, M., Dedieu, H. and Kennedy, M.P., "Synchronization of chaotic signals," *Workshop on Nonlinear Dynamics of Electronic Systems*, Dresden, 1993.

[7] Halle, K.S., Wu, C.W., Itoh, M. and Chua, L.O., "Spread spectrum communication through modulation of chaos," *Int. J. Bifurcation and Chaos*, vol.3, no.2, pp.469–477, 1993.

[8] Itoh, M., Murakami, H., Halle, K.S. and Chua, L.O., "Transmission of signals by chaos synchronization," *IEICE Technical Report*, CAS93-39, NLP93-27, 1993.

[9] Itoh, M., Murakami, H. and Chua, L.O., "Communication systems via chaotic modulations," *IEEE Trans. Fundamentals*, vol.E77-A, no.6, pp.1000–1006, Jun. 1994.

[10] Yamakawa, T., Miki, T. and Uchino, E., "A chaotic chip for analyzing nonlinear discrete dynamical systems," *Proc. of the 2nd International Conference on Fuzzy Logic & Neural Networks*, pp.563–566, 1992.

[11] Itoh, M. and Murakami, H., "Chaos synchronization in discrete-time dynamical systems and secure communication," *Proc. of the 11th European Conference on Circuit Theory and Design*, Davos, pp.611–614, 1993.

[12] Itoh, M., Murakami, H. and Momiki, S., "Application of Yamakawa's chaotic chips to secure communications," *Record of 1993 Joint Conference of Electrical and Electronics Engineering in Kyushu*, p.58, 1993.

[13] Kennedy, M.P., "Robust op amp realization of Chua's circuit," *Frequent*, vol.46, no.3–4, pp.66–80, 1992.

[14] Chua, L.O., Eckert, K., Kocarev, Lj. and Itoh, M., "Experimental chaos synchronization in Chua's circuit," *Int. J. Bifurcation and Chaos*, vol.2, no.3, pp.705–708, 1992.

[15] Ushio, T., "Chaotic synchronization in one-dimensional chaotic neural networks with unidirectional connections," *IEICE Technical Report*, NLP93-50, 1993.
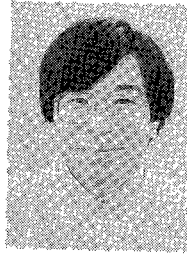
Makoto Itoh received the B.E., M.E., and Dr.E. degree in Computer Science and Communication Engineering from Kyushu University in 1977, 1979, and 1983, respectively. He was a Research Associate of Kyushu University from 1982 to 1984. In 1984, he joined Nagasaki University, where he is presently an Associate Professor of Electrical Engineering and Computer Science. His research interests are in nonlinear networks and dynamical systems.

Hiroyuki Murakami was born in Nagasaki, Japan on Mar. 14, 1971. He received the B.E. in Electrical Engineering and Computer Science from Nagasaki University in 1993. He is now studying towards the M.E. degree in Nagasaki University. His research interests is in nonlinear dynamical systems.