Performance of Yamakawa's Chaotic Chips and Chua's Circuits for Secure Communications

Makoto Itoh and Hiroyuki Murakami,
Dept. of Electrical Engineering and Computer Science
Nagasaki University
1-14, Bunkyo-machi, Nagasaki-shi, 852
Japan
(+81)958-47-1111 Ext. 2669
itoh@ec.nagasaki-u.ac.jp

Leon O. Chua
Dept. of Electrical Engineering and Computer Sciences
University of California, Berkeley
Berkeley, CA 94720
USA
(+1)510-642-3209
chua@diva.berkeley.edu, chua@fred.berkeley.edu

ABSTRACT

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.

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 [9], [10]. 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.

YAMAKAWA'S CHAOTIC CHIPS

Yamakawa's chaotic chip is a remarkably flexible and robust element, which realizes discrete-time dynamical systems [11]. It has three elements, that is, a nonlinear delay element, a linear delay element, and a summing element (see Figure 1). 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

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

where α, β are parameters, and $f(\bullet)$ is a piecewise linear function defined by

$$f(x)=\begin{cases} k_1(x-E_1)+k_2E_1, & E_1\leq x, \\ k_2x, & E_1\leq x\leq E_2, \\ k_3(x-E_2)+k_2E_2, & x\leq E_2. \end{cases} \qquad (3)$$

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.

COMMUNICATION SYSTEMS VIA YAMAKAWA'S CHAOTIC CHIPS

The basic concept of our secure communication system can be written as follows [12]: two processes are used to construct the system. The one is the chaotic coding and the other is the chaotic modulation.

The transmitting system is given by

$$x_{n+1}=f(x_n)+\epsilon s_n,$$
$$y_{n+1}=g(y_n)-\alpha z_n+\delta x_n,$$
$$z_{n+1}=y_n-\beta z_n, \qquad (4)$$

where α, β are some constants, ϵ, δ are sufficiently small, and $f(\bullet)$, $g(\bullet)$ are 3-segment piecewise linear functions. We suppose that (3) has chaotic behaviors for $\epsilon=\delta=0$. The informational signal and the transmitted signal are given by s_n and y_n, respectively. The chaotically modulated signal y_n is transmitted to the channel. The chaotic codings and the chaotic modulations are performed by the first equation and the remaining equations in (4), respectively. Considering the systems (1) and (2), the transmitting system (4) is easily built by using the Yamakawa's chaotic chips and the summing elements (see Figure 2).

The receiver constructs the following system:

$$\begin{aligned} z'_{n+1} &= y_n - \beta z'_n, \\ t_n &= (y_{n+1} - g(y_n) + \alpha z'_n)/\delta, \\ r_n &= (t_{n+1} - f(t_n))/\epsilon, \end{aligned} \tag{5}$$

where r_n is the recovered signal.

Next, we show how the informational signal can be recovered (demodulation process). Establishing the difference $p_n = z_n - z'_n$, we get the variational equations:

$$p_{n+1} = -\beta p_n. \tag{6}$$

If $|\beta| < 1$, then $|p_n| = |z_n - z'_n| \to 0$ as $n \to \infty$, that is, z_n and z'_n will synchronize. Therefore, we have

$$\begin{aligned} |t_n - x_n| &= |\{y_{n+1} - g(y_n) + \alpha z'_n\}/\delta - \{y_{n+1} - g(y_n) + \alpha z_n\}/\delta| \\ &= |\alpha(z_n - z'_n)/\delta| \to 0. \end{aligned} \tag{7}$$

It implies that $r_n = \{t_{n+1} - f(t_n)\}/\epsilon \to s_n = \{x_{n+1} - f(x_n)\}/\epsilon$ 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 (see Figure 2). It is possible to construct the similar secure communication systems by reversing the chaotic coding and the chaotic modulation. Furthermore, we can repeat the chaotic modulation and the chaotic coding again and again (for the transmitting signal y_n; see [12]). These repeated processes can make the transmitting signal more and more secure. This is due to the following reason:

(a) The transmitted signal become 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:

$$\alpha = 0.11,\ \beta = 0.196,\ \delta = 0.1,\ \epsilon = 0.1,$$

$$\left.\begin{aligned} &k_1 = 3.6,\ k_2 = -1.3,\ k_3 = 2.1, \\ &E_1 = -1.5\text{V},\ E_2 = 2.4\text{V}, \end{aligned}\right\} \quad \text{for } f(\cdot),$$

$$\left.\begin{aligned} &k_1' = 4.0,\ k_2' = -1.5,\ k_3' = 2.5, \\ &E_1' = -1.3\text{V},\ E_2' = 0.8\text{V}, \end{aligned}\right\} \quad \text{for } g(\cdot).$$

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 Figure 3 and [13]). The state equations are given by

$$\begin{aligned} C_1(dv_1/dt) &= (v_2 - v_1)/R - h(v_1), \\ C_2(dv_2/dt) &= (v_1 - v_2)/R + i, \\ L(di/dt) &= -v_2 - ri, \end{aligned} \tag{8}$$

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

$$h(v_R) = G_b v_R + 0.5(G_a - G_b)(|v_R + B_p| - |v_R - B_p|). \tag{9}$$

The circuit parameter we use are:

$$C_1 = 10.3\text{nF},\ C_2 = 97.4\text{nF},\ L = 20.7\text{mH},\ R = 1.41\text{k}\Omega,$$
$$B_p = 1.85\text{V},\ G_a = -0.87\text{mS},\ G_b = -0.52\text{mS},\ r = 64.2\Omega.$$

COMMUNICATION SYSTEMS VIA CHUA'S CIRCUIT

The basic construction of our communication system is shown in Figure 4 (for details, see [7], [8]). The circuit equations for the transmitting system are given by

$$\begin{aligned} C_1(dv_1/dt) &= (v_2 - v_1)/R - h(v_1) + C(s(t)), \\ C_2(dv_2/dt) &= (v_1 - v_2)/R + i, \\ L(di/dt) &= -v_2 - ri, \end{aligned} \tag{10}$$

where C is a coding function with an inverse. We use the current source s(t) as an informational signal, and $v_1(t)$ is a chaotically modulated transmitted signal. The equation (10) performs a chaotic modulation of the signals.

The circuit equations for the receiving system are given by

$$\begin{aligned} C_1(dv_1'/dt) &= (v_2' - v_1')/R, \\ C_2(dv_2'/dt) &= (v_1' - v_2')/R + i', \\ L(di'/dt) &= -v_2' - ri', \end{aligned} \tag{11}$$

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 (10), we have

$$s(t) = C^{-1}\{C_1(dv_1/dt) - (v_2 - v_1)/R + h(v_1)\}, \tag{12}$$

The current j(t) in Figure 4 is given by

$$j(t) = \{C_1(dv_1'/dt) - (v_2' - v_1')/R + h(v_1')\}. \tag{13}$$

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

$$\begin{aligned} C_2(dp/dt) &= -p/R + q, \\ L(dq/dt) &= -p - rq. \end{aligned} \tag{14}$$

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, 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 [7], [8], [14]. (In our experiment, the coding function is chosen so that $C(u) = u$, and therefore we used the simple current detector shown in Figure 5. The proper use of the complex coding function C makes the transmitting signals more and more secure [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 chip. Both systems are tested by using human voices and music signals. Then, the following experimental results are obtained:

A. Common Features [7], [8], [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.

B. Systems via Yamakawa's chaotic chips [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 coding make the system more and more secure. We can easily implement these processes by using a few chips.

C. Systems via Chua's circuits [7], [8]

(a) Low cost (all the systems are built at an expense 20$).

(b) The channel bandwidth is not so great.

(c) In order to implement the repeated chaotic modulations, we need a number of ICs. However, the chaotic coding is easily implemented.

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.

ACKNOWLEDGEMENT

Authors would like to thank Prof. Takashi Yamakawa of Kyushu Institute of Technology and Fuzzy Institute for providing us the chaotic chips. This research was supported in part by the Japanese Ministry of Education.

REFERENCES

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

[2] Lj. Kocarev, K.S. Halle, K. Eckert, U. Parlitz and Chua, L.O.,"Experimental demonstration of secure communications via chaos synchronization," Int. J. Bifurcation and Chaos 2(3), pp.709-713, 1992.

[3] U. Parlitz, L.O. Chua, Lj. Kocarev, K.S. Halle, and A. Shang,"Transmission of digital signals by chaotic synchronization," Int. J. Bifurcation and Chaos, 2(4), pp.973-977, 1992.

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

[5] H. Dedieu, M.P. Kennedy, and M. Hasler,"Chaos shift keying: Modulation of a chaotic carrier using self-synchronizing Chua's circuits, " IEEE Trans Circuits and Systems (part II), 40(10), pp.634-642, 1993.

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

[7] K.S. Halle, C.W. Wu, M. Itoh, and L.O. Chua, "Spread spectrum communication through modulation of chaos," Int. J. Bifurcation and Chaos 3(2), pp.469-477, 1993.

[8] M. Itoh, H. Murakami, K,S. Halle, and L.O. Chua, "Transmission of Signals by Chaos Synchronization," Technical Report of IEICE, CAS93-39, NLP93-27, pp.89-96, 1993.

[9] M. Itoh and H. Murakami,"Chaos synchronization and secure communications in discrete dynamical systems," Technical Report of IEICE, NLP92-50, 25-31, 1992.

[10] M. Itoh and H. Murakami,"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.

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

[12] M. Itoh, H. Murakami, and S. Momiki,"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] M.P. Kennedy,"Robust op amp realization of Chua's circuit," Frequent, 46(3-4), pp.66-80, 1993.

[14] L.O. Chua, K. Eckert, Lj. Kocarev, and M. Itoh, "Experimental chaos synchronization in Chua's circuit," Int. J. Bifurcation and Chaos, 2(3), pp.705-708, 1993.

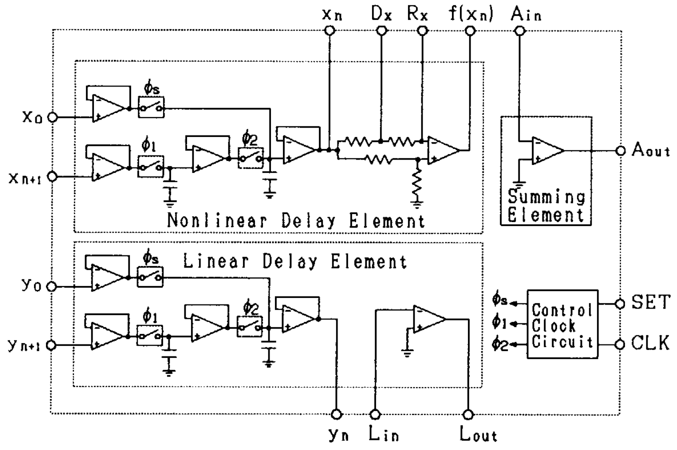

Figure 1 Block diagrams of Yamakawa's chaotic chip. (Based on the Ref [11].)

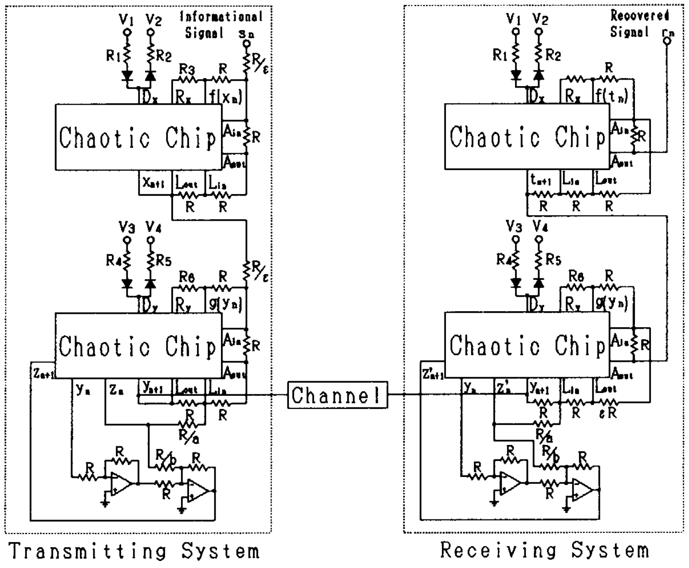

Figure 2 Communication system via Yamakawa's chaotic chip.

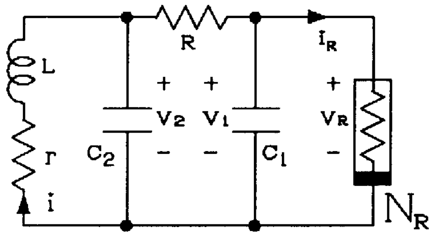

Figure 3 Chua's circuit.

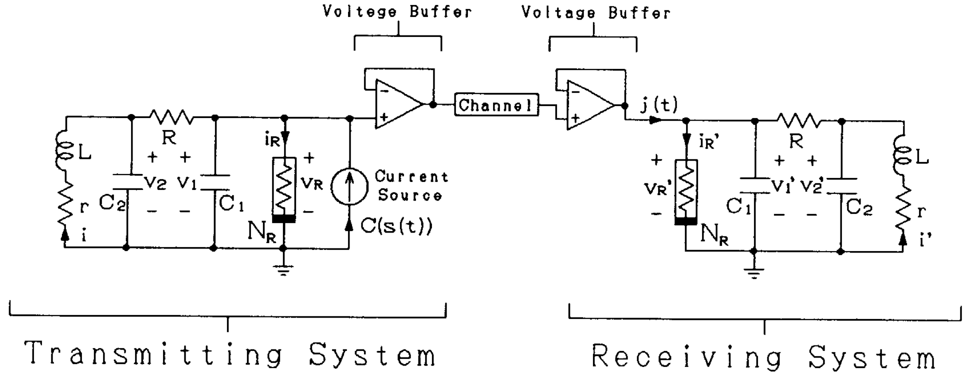

Figure 4 Communication system via Chua's circuit.

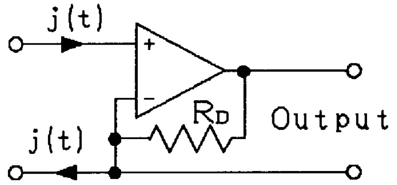

Figure 5 Current detector.