# Secure Communication via Chaotic Parameter Modulation

Tao Yang and Leon O. Chua

***Abstract*—In this letter, we extend chaotic switching to general chaotic parameter modulation. By using adaptive controller, synchronization between transmitter and receiver is maintained and message signal is recovered. Computer simulation results are given.**

## I. Introduction

Chaotic switching [1], [2] is the simplest form of chaotic parameter modulation. In this method, the message signal $s(t)$ is assumed to be binary, and is used to modulate one or more parameters of a chaotic switching transmitter by representing binary "one" for one set of parameters and binary "zero" for a different set. At the receiver, $s(t)$ is decoded by using the synchronization error to decide whether the received signal corresponds to one set of parameters, or the other.

Although chaotic switching is more robust against noise than chaotic masking, it suffers from a lower information transmission rate than those methods which transmit analog signals directly. This is because the receiver has to wait until synchronization and desynchronization have been achieved before the next bit is transmitted. On the other hand, Tao Yang [3] found that an intruder could use short-time zero-crossing rate (STZCR) to recover $s(t)$ from the transmitted chaotic signal. So, it has a low degree of security.

In this letter, we propose a more general chaotic parameter modulation scheme with applications to secure communication. In our method $s(t)$ may be analog or digital.

## II. Transmission of Signal by Chaotic Parameter Modulation

In this letter, all results are based on Chua's circuit [4], [5], which exhibits a family of chaotic attractors and can be easily implemented in hardware. As shown in Fig. 1(a), Chua's circuit consists of a linear inductor $L$, a linear resistor $R$, two linear capacitors $C_1$ and $C_2$ and a nonlinear resistor—the Chua's diode $N_R$. The state equations for Chua's circuit are given by

$$\begin{cases} \frac{dv_1}{dt} = \frac{1}{C_1}[G(v_2 - v_1) - f(v_1)] \\ \frac{dv_2}{dt} = \frac{1}{C_2}[G(v_1 - v_2) + i_3] \\ \frac{di_3}{dt} = \frac{1}{L}[-v_2 - R_0 i_3] \end{cases} \tag{1}$$

where $v_1$, $v_2$, and $i_3$ are the voltage across $C_1$, the voltage across $C_2$ and the current through $L$, respectively. We set $G = \frac{1}{R}$. The term $R_0 i_3$ is added to account for the small resistance of the inductor in the physical circuit. The piece-wise linear $v$-$i$ characteristic $f(v_1)$ of the Chua's diode, is given by

$$f(v_1) = G_b v_1 + \frac{1}{2}(G_a - G_b)(|v_1 + E| - |v_1 - E|) \tag{2}$$

where $E$ is the breakpoint voltage of the Chua's diode as shown in Fig. 1(b).

To transmit $s(t)$ via our chaotic parameter modulation scheme, the receiver must chosen as follows:

$$\begin{cases} \frac{d\tilde{v}_1}{dt} = \frac{1}{C_1}[\tilde{G}(\tilde{v}_2 - \tilde{v}_1) - f(\tilde{v}_1) + K_1(v_1 - \tilde{v}_1)] \\ \frac{d\tilde{v}_2}{dt} = \frac{1}{C_2}[\tilde{G}(\tilde{v}_1 - \tilde{v}_2) + \tilde{i}_3 + K_1(v_1 - \tilde{v}_1)] \\ \frac{d\tilde{i}_3}{dt} = \frac{1}{L}[-\tilde{v}_2 - \tilde{R}_0\tilde{i}_3 + K_1(v_1 - \tilde{v}_1)] \end{cases} . \tag{3}$$

We first use a "modulation rule" to modulate $s(t)$ in a parameter of the transmitter in (1). Then an adaptive controller is used at the receiver to maintain synchronization by continuously tracking the changes in the modulated parameter. So, $s(t)$ can be recovered by this adaptive controller. The parameter for the unmodulated Chua's circuit were chosen as follows: $C_1 = 5.56$ nF, $C_2 = 50$ nF, $G = 0.700\,28$ mS, $L = 7.14$ mH, $R_0 = 0\ \Omega$, $G_a = -0.8$ mS, $G_b = -0.5$ mS, $E = 1$ V, $K_1 = 0.01$. In this case, the Chua's circuit exhibits a double-scroll Chua's attractor as shown in Fig. 2. In this letter, we discuss the cases when only one parameter of the transmitter is modulated while the others remain constant. At the receiver, the corresponding parameter is changed by an adaptive controller while the others are fixed at the same values as in the transmitter.

### A. *G-Modulation*

In this case, the modulation rule is given by

$$G(t) = Gs(t), \tilde{G}(t) = G\tilde{s}(t) \tag{4}$$

where $\tilde{s}(t)$ is the recovered message signal.

The adaptive controller is given by

$$\begin{aligned} \dot{\tilde{s}}(t) &= k_1 \operatorname{sgn}\left(\frac{\partial \dot{\tilde{v}}_1}{\partial \tilde{s}(t)}\right)(v_1 - \tilde{v}_1) \\ &= k_1 \operatorname{sgn}\left(\frac{1}{C_1} G(\tilde{v}_2 - \tilde{v}_1)\right)(v_1 - \tilde{v}_1). \end{aligned} \tag{5}$$

Simulation result is shown in Fig. 3 with $k_1 = 10^6$. The signal $s(t)$(dashed line) is defined as follows:

$$s(t) = \begin{cases} 1.05, & 0 \le t < 20 \text{ ms} \\ 1.15, & 20 \text{ ms} \le t < 40 \text{ ms} \\ 1.1 - 0.05\sin\left(\frac{15\pi}{2}t\right), & 40 \text{ ms} \le t < 100 \text{ ms} \end{cases} . \tag{6}$$

Observe that $\tilde{s}(t)$(solid line) tracks $s(t)$ continuously except for an interval from 40 ms to 66 ms when $\tilde{s}(t)$ is almost constant while $s(t)$ changes. This is because for the parameter range corresponding to the waveform of $s(t)$ in this interval, synchronization is maintained even though $\tilde{s}(t) \neq s(t)$.

### B. $C_1$*-Modulation*

In this case, the modulation rule is given by

$$\frac{1}{C_1(t)} = \frac{s(t)}{C_1}, \frac{1}{\tilde{C}_1(t)} = \frac{\tilde{s}(t)}{C_1}. \tag{7}$$

The adaptive controller is given by

$$\begin{aligned} \dot{\tilde{s}}(t) &= k_1 \operatorname{sgn}\left(\frac{\partial \dot{\tilde{v}}_1}{\partial \tilde{s}(t)}\right)(v_1 - \tilde{v}_1) \\ &= k_1 \operatorname{sgn}\left(\frac{1}{C_1}[G(\tilde{v}_2 - \tilde{v}_1) - f(\tilde{v}_1) + K_1(v_1 - \tilde{v}_1)]\right) \\ &\quad \times (v_1 - \tilde{v}_1). \end{aligned} \tag{8}$$

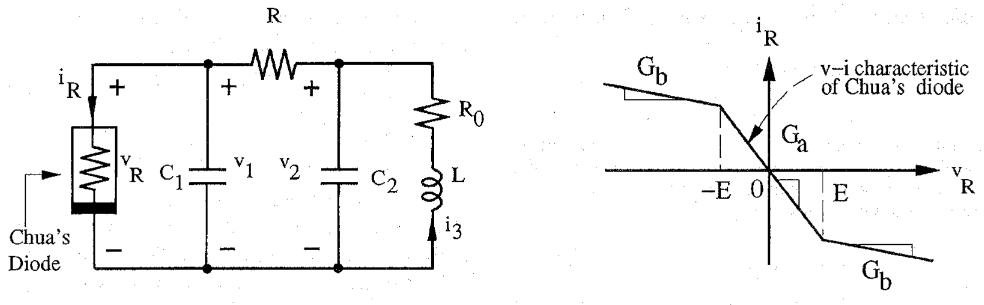
Simulation result is shown in Fig. 4 with $k_1 = 2 \times 10^6$. The signal $s(t)$ (dashed line) is defined by (6). Observe that $\tilde{s}(t)$ (solid line) tracks $s(t)$ continuously with a relatively big error.

Manuscript received January 23, 1996. This paper was recommended by Associate Editor B. Sheu.

T. Yang is with the Electronics Research Laboratory and the Department of Electrical Engineering and Computer Sciences, University of California, Berkeley, CA 94720 USA on leave from the Department of Automatic Control Engineering, Shanghai University of Technology, Shanghai 200072, P. R. China.

L. O. Chua is with the Department of Electrical Engineering and Computer Sciences, University of California, Berkeley, CA 94720 USA.

Publisher Item Identifier S 1057-7122(96)06839-0.



(a) (b)

Fig. 1. (a) Chua's circuit. (b) Nonlinear $v$-$i$ characteristic of Chua's diode.

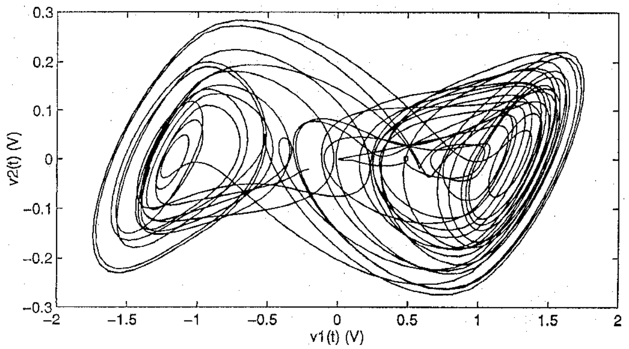


Fig. 2. Chaotic attractor of Chua's circuit used in simulations.

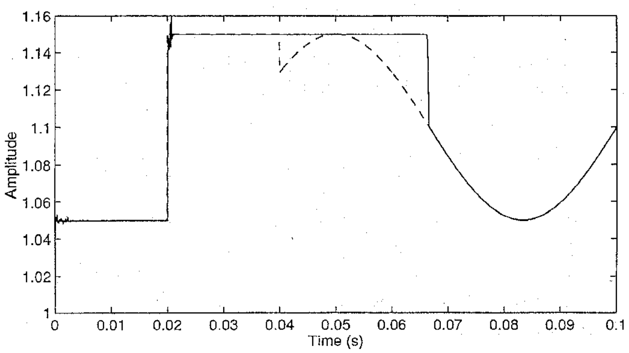


Fig. 3. Transmitted signal $s(t)$ (dashed line) and recovered signal $\tilde{s}(t)$ (solid line) obtained by modulating the parameter $G$.

### C. $C_2$-Modulation

In this case, the modulation rule is given by

$$\frac{1}{C_2(t)} = \frac{s(t)}{C_2}, \frac{1}{\tilde{C}_2(t)} = \frac{\tilde{s}(t)}{C_2}. \tag{9}$$

The adaptive controller is given by

$$\begin{aligned}\dot{\tilde{s}}(t) &= k_1 \operatorname{sgn}\left(\frac{\partial \dot{\tilde{v}}_2}{\partial \tilde{s}(t)}\right)(v_1 - \tilde{v}_1)\\ &= k_1 \operatorname{sgn}\left(\frac{1}{C_2}[G(\tilde{v}_1 - \tilde{v}_2) + \tilde{i}_3 + K_1(v_1 - \tilde{v}_1)]\right)(v_1 - \tilde{v}_1).\end{aligned} \tag{10}$$

Simulation result is shown in Fig. 5 with $k_1 = 10^6$. The signal $s(t)$ (dashed line) is defined by (6). Observe that $\tilde{s}(t)$ (solid line) tracks $s(t)$ continuously with a small error.

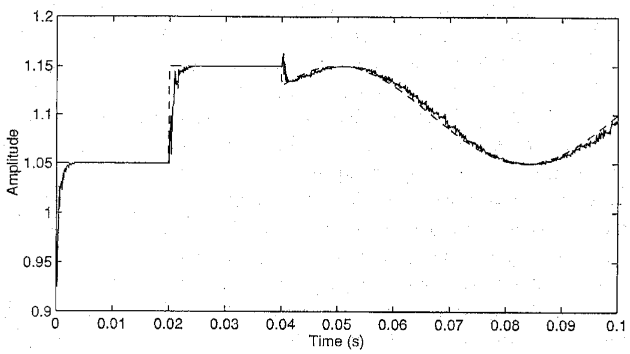


Fig. 4. Transmitted signal $s(t)$ (dashed line) and recovered signal $\tilde{s}(t)$ (solid line) obtained by modulating the parameter $C_1$.

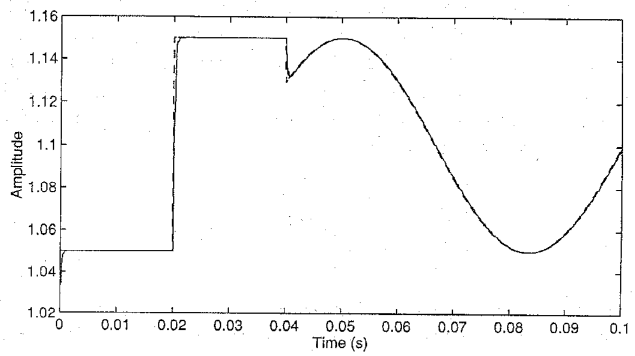


Fig. 5. Transmitted signal $s(t)$ (dashed line) and recovered signal $\tilde{s}(t)$ (solid line) obtained by modulating the parameter $C_2$.

### D. $L$-Modulation

In this case, the modulation rule is given by

$$\frac{1}{L(t)} = \frac{s(t)}{L}, \frac{1}{\tilde{L}(t)} = \frac{\tilde{s}(t)}{L}. \tag{11}$$

The adaptive controller is given by

$$\begin{aligned}\dot{\tilde{s}}(t) &= k_1 \operatorname{sgn}\left(\frac{\partial \dot{\tilde{i}}_3}{\partial \tilde{s}(t)}\right)(v_1(t) - \tilde{v}_1)\\ &= k_1 \operatorname{sgn}\left(\frac{1}{L}[-\tilde{v}_2 - R_0\tilde{i}_3 + K_1(v_1 - \tilde{v}_1)]\right)(v_1 - \tilde{v}_1).\end{aligned} \tag{12}$$

Simulation result is shown in Fig. 6 with $k_1 = 10^6$. The signal $s(t)$(dashed line) is defined by (6). Observe that $\tilde{s}(t)$(solid line) tracks $s(t)$ continuously with very small error and big overshoot.

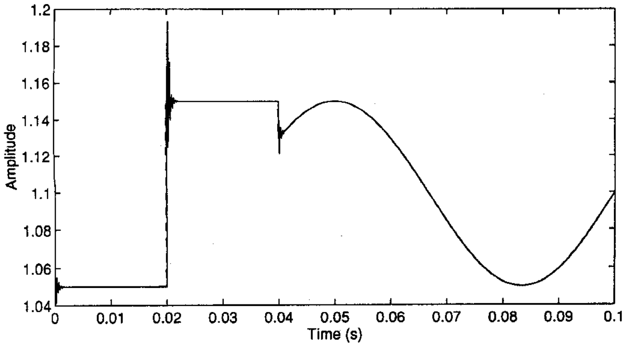


Fig. 6. Transmitted signal $s(t)$ (dashed line) and recovered signal $\tilde{s}(t)$ (solid line) obtained by modulating the parameter $L$.

### E. $R_0$-Modulation

In this case, the modulation rule is given by

$$R_0(t) = R_0 + s(t), \tilde{R}_0(t) = R_0 + \tilde{s}(t). \tag{13}$$

The adaptive controller is given by

$$\begin{aligned}\dot{\tilde{s}}(t) &= k_1 \operatorname{sgn}\left(\frac{\partial \dot{\tilde{i}}_3}{\partial \tilde{s}(t)}\right)(v_1(t) - \tilde{v}_1)\\ &= k_1 \operatorname{sgn}\left(-\frac{\tilde{i}_3}{L}\right)(v_1 - \tilde{v}_1).\end{aligned} \tag{14}$$

Simulation result is shown in Fig. 7 with $k_1 = 10^8$. The signal $s(t)$(dashed line) is defined by (6). Observe that $\tilde{s}(t)$(solid line) tracks $s(t)$ continuously with a small error.

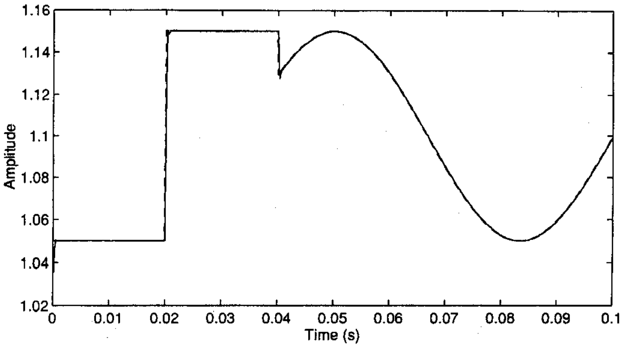


Fig. 7. Transmitted signal $s(t)$ (dashed line) and recovered signal $\tilde{s}(t)$ (solid line) obtained by modulating the parameter $R_0$.

## III. Conclusion

Different schemes of chaotic parameter modulation are presented. Their performances are shown by computer simulation results.

## References

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

[2] H. Dedieu, M. P. Kennedy, and M. Hasler, "Chaotic shift keying: Modulation and demodulation of a chaotic carrier using self-synchronization Chua's circuits," *IEEE Trans. Circuits Syst. II*, vol. 40, pp. 634–642, Oct. 1993.

[3] T. Yang, "Recovery of digital signals from chaotic switching," *Int. J. Circuit Theory Applicat.*, vol. 23, no. 6, pp. 611–615, Nov.–Dec. 1995.

[4] L. O. Chua, "Chua's circuit—An overview ten years later," *J. Circuits, Syst., Comput.*, vol. 4, no. 2, pp. 117–159, June 1994.

[5] J. M. Cruz and L. O. Chua, "An IC chip of Chua's circuit," *IEEE Trans. Circuits Syst. II*, vol. 40, pp. 614–625, Oct. 1993.