1994 Symposium on Nonlinear Theory and its Applications

Proceedings

Green Pia Ibusuki, KAGOSHIMA, JAPAN
October 6 - 8, 1994

Sponsored by:
Research Society of Nonlinear Theory and its Applications, IEICE

In cooperation with:
Japanese Neural Network Society
Technical Group of Nonlinear Problems, IEICE
Technical Group of Circuits and Systems, IEICE

1994 Symposium on Nonlinear Theory and its Applications October 6-8, 1994

Secure Communications Via Chaotic Synchronization in Chua's Circuit: Numerical Analysis of the Errors of the Recovered Signal

René Lozi† and Ahmed Aziz-Alaoui‡

† Laboratoire de mathématiques, U.R.A. 168,
Université de Nice-Sophia Antipolis,
Parc Valrose, 06108 NICE Cedex 2, France
e.mail: lozi@math.unice.fr
fax: 33. 93.51.79.74 & 33. 93.52.90.39

‡ Département de mathématiques,
Faculté des Sciences, Université du Havre,
25 Av. Philippe Lebon, B.P. 540
76058 LE HAVRE Cedex, France
fax: 33. 35.19.57.15

Abstract: The signal recovered from the first reported experimental secure communication system via chaotic synchronization contains some inevitable noise which degrades the fidelity of the original message. By *cascading* the output of the receiver in the original system into an *identical* copy of this receiver, it had be shown by computer experiments that this noise can be significantly reduced. We discuss the heuristic laws governing the errors of the recoverred signal which are observed in a new series of very careful computer experiments.

1. Introduction

The first laboratory demonstration of a secure communication system which uses a *chaotic* signal for *masking* purposes [1, 2], and which exploits the chaotic *synchronization* techniques of Pecora and Caroll [3, 4] to recover the signal was reported recently [5]. While the " transmitter " in this system is a direct implementation of the method proposed in [2], the " receiver " differs from their computer simulation approach in that it actually contains *two* subsystems of the " chaotic " transmitter (Chua's circuit in this case). In both implementations -- electronic circuit realization or computer simulation -- there is an inevitable error introduced by the signal s(t).
In [6] it is shown by computer experiments that by connecting two *identical* receivers in cascade, a significant amount of the noise can be reduced, thereby allowing the recovery of a much higher quality signal.
While other noise reduction methods could conceivably be introduced, the technique reported there has the advantage that it is easy to implement in practice. Two copies of the receiver are made and connected as shown in Fig. 1. Although no two electronic circuits can be made perfectly identical in practice, this ideal situation can now be approached with the help of the integrated circuit technology demonstrated recently in [7]. By fabricating several identical Chua's circuits on *the same* silicon chip, the resulting circuits are almost " clones " of each other. This technique has the additional security advantage in that even if someone else has discovered the parameters (α, β) used in the system, integrating it into *another* silicon chip invariably introduces discrepancies due to the different processing parameters from different silicon " foundries ".

2. Noise Reduction Via Cascading

2.1 Single Chaotic Synchronization

The basic building block is a Chua's circuit, the dynamics of which is given by the Chua's equation

$$\begin{cases} \dot{x} = \alpha\,(y - x - f(x)) \ , \\ \dot{y} = x - y + z \ , \\ \dot{z} = -\beta y \ , \end{cases} \qquad (1)$$

where

$$f(x) = b\,x + \frac{1}{2}(a - b)\,[\,|x + 1| - |x - 1|\,] \qquad (2)$$

Here, x(t) is used as a noise-like "masking" signal. Let s(t) be an information-bearing signal. The transmitted signal is r(t) = x(t) + s(t), where the power level of s(t) is assumed to be significantly lower than that of x(t), in order to have the signal effectively hidden.
The receiver consists of two subsystems. The first one is driven by the transmitted signal r(t):

$$\begin{cases} \dot{y}_1 = r(t) - y_1 + z_1 \ , \\ \dot{z}_1 = -\beta y_1 \ , \end{cases} \qquad (3)$$

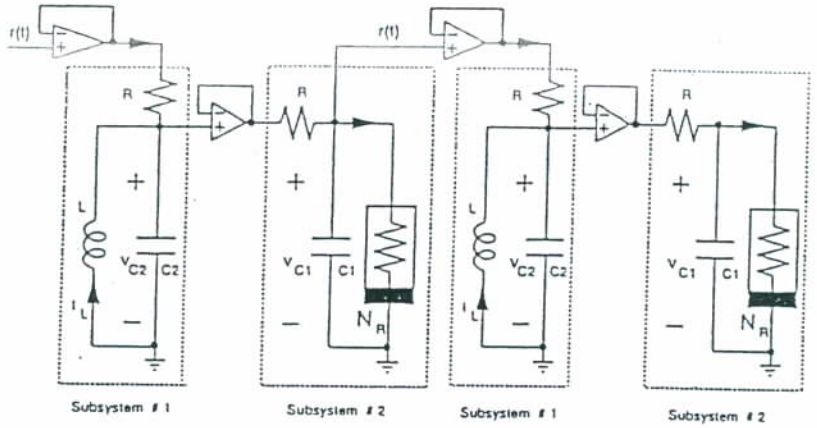

Fig. 1. Electronic circuit implementation of the two-stage " receiver " consisting of two identical copies of the circuit given in Fig. 2 (b) of [5].

The second subsystem is driven by the signal $y_1(t)$ and s(t) is recovered as

$$\dot{x}_2 = \alpha\,(y_1(t) - x_2 - f(x_2)) \qquad (4)$$

$$s_2(t) = r(t) - x_2(t) \approx s(t) \qquad (5)$$

Actually the dynamics of the experimental set up (see Fig. 1) is described by

$$\begin{cases} \dot{x}_2 = \alpha\,(y_1(t) - x_2 - f(x_2)) \ , \\ \dot{z}_2 = -\beta\, y_1(t) \ . \end{cases} \qquad (6)$$

However, as long as we do not need $z_2(t)$ to recover $s_2(t)$, we will continue to use Eq. (5) instead of Eq. (6) in the following improved system.

2.2 Cascade Chaotic Synchronization

In order to improve the previous method to recover a signal nearer to s(t) than $s_2(t)$, we couple two receivers in cascade in the following way. The second receiver consists also of two subsystems.
The first one is driven by the signal $x_2(t)$ which is assumed to be more synchronized to x(t) than the transmitted signal r(t):

$$\begin{cases} \dot{y}_3 = x_2(t) - y_3 + z_3 \ , \\ \dot{z}_3 = -\beta\, y_3 \ , \end{cases} \qquad (7)$$

The second subsystem of the second receiver is then driven by the signal $y_3(t)$ from Eq. (7) and s(t) is recovered as

$$\dot{x}_4 = \alpha\,(y_3(t) - x_4 - f(x_4)) \qquad (8)$$

$$s_4(t) = r(t) - x_4(t) \approx s(t) \qquad (9)$$

3. Numerical Experiments

Let us define *the errors*

$$\| e_s(k,\omega) \|_2 = \| s_2(t) - s(t) \|_2 =$$

$$= \| x_2(t) - x(t) \|_2 \qquad (10)$$

$$\| e_c(k,\omega) \|_2 = \| s_4(t) - s(t) \|_2 =$$

$$= \| x_4(t) - x(t) \|_2 \qquad (11)$$

where $\| f(t) \|_2 \triangleq \lim_{T \to \infty} \frac{1}{T} \left[\int_0^T f^2(t)\, dt \right]^{1/}$ denotes the *quadratic norm* of f(t).

Four parameters (a,b,α,β) completely characterized Chua's equation, which is known to exhibit an immensely rich variety of behaviors [8]. We have performed our numerical results with the parameter values $a = -1/7$, $b = 2/7$, $\alpha = 9.7633$, $\beta = 15.5709$) for which the signal $x(t)$ is chaotic [6].

3.1 Single Tone Signal

In this subsection we assume that the input (information-bearing) signal $s(t)$ is a single tone (sine wave) of amplitude k belonging to the range $0 < k < 1.5$:

$$s(t) = k \sin(\omega t) \qquad (12)$$

Our numerical computations are done using the most common fourth-order Runge-Kutta algorithm [9]. All computations are performed with 17 decimal-digit numbers. In order to obtain reliable numerical results, the step size of the Runge-Kutta algorithm is chosen to be equal to 10^{-5}. Three sets of different initial values are chosen for the transmitter and both the receivers.
The errors are averaged on a very long period of time (the first 3×10^7 steps are ignored (transient regime), the averaging uses the steps $3 \times 10^7 + 1$ to 19×10^7).
For the values $1 \le \omega \le 15$, both

$$\| e_s(k,\omega,t) / s(t) \|_2 = E_s(k,\omega) \qquad (13)$$

and

$$\| e_c(k,\omega,t) / s(t) \|_2 = E_c(k,\omega) \qquad (14)$$

are independent of k, increasing with ω from 1 to 6, decreasing after.
For the value $15 \le \omega \le 409{,}600$ a power regression analysis leads us to both the heuristic laws 1 and 2 which are obtained with a correlation coefficient better than 0.999,999 (0.999,999,996 if we use only the data corresponding to $400 \le \omega \le 102{,}400$).

Heuristic law 1.

$$E_s(k,\omega) = 81.46 \times k / \omega^2 \qquad (15)$$

Heuristic law 2.

$$E_c(k,\omega) = 1329.17 \times k / \omega^3 \qquad (16)$$

3.2 Multi-tone Signal

We have performed the same numerical experiments with various multi-tone signal instead of the single tone signal.

$$s(t) = k \sin(\omega t) + k \sin(n\omega t) + k \sin(m\omega t) \qquad (17)$$

The different values chosen for n and m are ($n = 2$, $m = 4, 8, 16, 32$; $n = 4$, $m = 8, 16, 32$)
In a first approximation whatever are the values of n and m we find that:

$$\| e_s(k,\omega,n\omega,m\omega) \|_2 = 0.60 \times E_s(k,\omega) \qquad (18)$$

and

$$\| e_c(k,\omega,n\omega,m\omega) \|_2 = 0.60 \times E_c(k,\omega) \qquad (19)$$

3.3 Discrepancies Between The Parameters

We have also tested the possible discrepancies between the parameter values of the transmitter and both the receivers. For this, α is replaced with $\alpha \times (1 + \delta_\alpha)$ in Eqs. (4), (6) (8), while kept the same in Eq. (1) and β is replaced with $\beta \times (1 + \delta_\beta)$ in Eqs. (3), (6) (7), while kept the same in Eq. (1). A power regression analysis is pointed out from the preliminary observations (where δ_α takes 15 values between 0.0001 to 0.08 and δ_β takes 12 values between 0.001 to 0.08) with correlation coefficients better than 0.99:

Observation 1.

$$\| e_s(k,\omega,t) \|_2 = 75 \times |\delta_\alpha|^{1.10} \qquad (20)$$

Observation 2.

$$\| e_s(k,\omega,t) \|_2 = 322 \times |\delta_\beta|^{1.04} \qquad (21)$$

Observation 3.

$$\| e_c(k,\omega,t) \|_2 = 243 \times |\delta_\alpha|^{1.11} \qquad (22)$$

Observation 4.

$$\| e_c(k,\omega,t) \|_2 = 169 \times |\delta_\beta|^{1.13} \qquad (23)$$

These observations have to be detailed carefully in order to understand better the mathematical theory hidden behind the chaotic synchronization.

References

[1] Vernam, G.S. " Cipher printing telegraph systems for secret wire and telegraphic communications," *J. Amer. Inst. Elec. Eng.*, (55), 109 - 115 , 1926.

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

[3] Pecora, L. M. & Carroll, T. L. " Synchronization in chaotic systems," *Phys. Rev. Lett.*, 64, 821 - 823, 1990.

[4] Carroll, T.L. & Pecora, L.M. " A circuit for studying the synchronization of chaotic systems," *Int. J. of Bifurcation and Chaos* , 2, (2) , 659 - 667, 1992.

[5] Kocarev, Lj, Halle, K.S., Eckert, K. and Chua, L.O. " Experimental demonstration of secure communication via chaotic synchronization, " *Int. J. of Bifurcation and Chaos* , 2, (3) , 709 - 713, 1992.

[6] Lozi, R. & Chua, L.O. "Secure communications via chaotic synchronization II: Noise reduction by cascading two identical receivers, " *Int. J. of Bifurcation and Chaos* , 3, (5) , 1319 - 1325, 1993.

[7] Delgado-Restituto, M. & Rodriguez-Vasquez, A. " A CMOS monolithic Chua's circuit," *J. of Circuits, Systems and Computers*, (3) 2, 259-268, 1993.

[8] Chua, L.O. " Global unfolding of Chua's circuits, " *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, Vol. E 76-A, 5, 704-734, 1993.

[9] Parker, T.S. and Chua, L.O. *Practical Numerical Algorithms for Chaotic Systems* , New-York , Springer Verlag, 1989.