Chaotic Masking Scheme with a Linear Inverse System

Ali Oksasoglu and Tayfun Akgul
Department of Electrical and Electronics Engineering, Çukurova University, 01330 Adana, Turkey
(Received 7 July 1995)

In this Letter, we propose a simple chaotic signal masking scheme employing Chua's circuit without the requirement of chaos synchronization. Although, in general, our procedure involves the inverse system approach, the resulting inverse system in our case is a linear one. Therefore, the difficulty of inverse realization of the transmitter's nonlinear parts also at the receiving end, which is encountered in the general scheme of the inverse system approach, is eliminated.

PACS numbers: 05.45.+b

Chaotic signal masking is one of the new and exciting application areas of chaos for communication purposes. The idea is to mask the information-bearing signal, i.e., the message, with a chaotic signal by direct addition, and later recover this message at the receiving end of the communication channel. It was reported in [1] that certain chaotic systems possess a self-synchronization property. Since then, different approaches based on this self-synchronization property have been proposed (e.g., [2–5]). In such a procedure, the chaotically masked signal is used at the receiving end to drive and synchronize the receiver subsystem for the purpose of message recovery. It is obvious that the success of such a procedure depends not only on the synchronization alone, but also on the robustness of the synchronization to the perturbations of the synchronizing drive signal [5].

In the context of chaotic and thus secure communication systems, one other approach is what is called the *inverse system approach* [6,7]. In this approach, first the message drives a chaotic system to create a chaotic output. Then this chaotic output is used to drive an inverse system for the recovery of the message. In the general scheme of this procedure, one faces the difficulty of inversely duplicating the transmitter nonlinearities at the receiving end.

However, as we will see later, our proposed simple scheme overcomes these difficulties. A block diagram for the overall proposed system is given in Fig. 1. The basic idea, as in the case of classical chaotic signal masking techniques, is to add the message $m(t)$ to a chaotic signal produced by an autonomous system. Later, this signal is used to drive a linear receiver subsystem, which is the inverse system of our case. First of all, this procedure does not require synchronization. Second, the fact that our choice of inverse system is totally linear eliminates the need to realize the inverse nonlinearities of the receiving end. Thus, with no parameter mismatch, exact recovery is possible involving only some simple signal processing techniques, such as summation, integration, and differentiation.

We will demonstrate our approach by using the well-known Chua circuit (e.g., [8–10]) shown in Fig. 2 as the transmitter subsystem. The choice of Chua's circuit for this purpose is due to the fact that it is quite simple, has been widely studied, and is easily realizable [11,12]. The governing equations for this circuit can be given by

$$\begin{aligned} \frac{dv_2}{dt} &= \frac{G}{C_2}(v_1 - v_2) - \frac{1}{C_2}h(v_2), \\ \frac{dv_1}{dt} &= -\frac{G}{C_1}(v_1 - v_2) + \frac{1}{C_1}i_L, \\ \frac{di_L}{dt} &= -\frac{1}{L}v_1, \end{aligned} \tag{1}$$

where $h(\cdots) = G_1(\cdots) + 0.5(G_0 - G_1)[|(\cdots) + B_p| - |(\cdots) - B_p|]$ is a three-segment piecewise linear function for Chua's diode with G_0 and G_1 as the slopes, and B_p the break point for those segments, respectively. For simplicity, without loss of generality, we will put the systems of (1) into a nondimensional form, and perform our analysis on this transformed system. For that purpose let us use $v_2 = V_0 x$, $v_1 = V_0 y$, $i_L = I_0 z$, and $t \rightarrow \omega_0 t$ where V_0, I_0, and ω_0 are, respectively, the arbitrary voltage, current, and frequency scaling factors, x, y, and

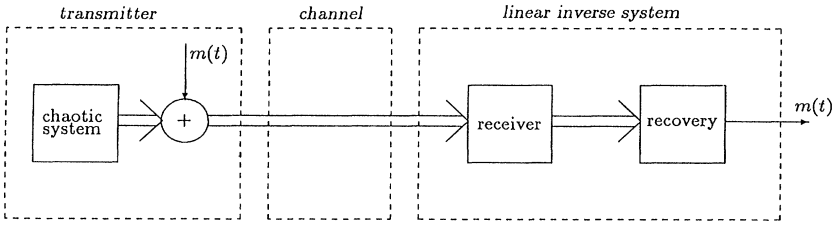

FIG. 1. Overall system.

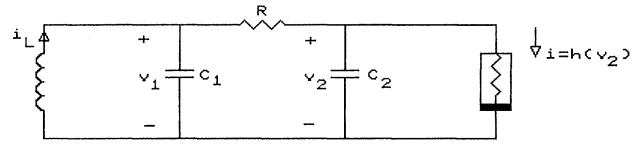

FIG. 2. Chua's circuit as transmitter.

z are the new dimensionless state variables, and t is now the dimensionless time variable. In this case, we have

$$\dot{x} = \alpha[y - r(x)],$$
$$\dot{y} = \gamma(\dot{x} - y + \eta z), \tag{2}$$
$$\dot{z} = -\beta y,$$

where $\alpha = G/C_2\omega_0$, $\gamma = G/C_1\omega_0$, $\eta = I_0/V_0G$, $\beta = V_0/I_0\omega_0 L$, and $r(x) = m_1 x + 0.5(m_0 - m_1)(|x + \varepsilon| - |x - \varepsilon|)$ with $m_0 = G_0/G + 1$, $m_1 = G_1/G + 1$, and $\varepsilon = B_p/V_0$. Now, let us consider the following receiver subsystem:

$$\dot{y}_r = \gamma[s(t) - y_r + \eta z_r],$$
$$\dot{z}_r = -\beta y_r, \tag{3}$$

where $s(t) = x(t) - m(t)$ is the receiver driving signal. Note that the subsystem of (3) is a second-order linear system, which is stable for $\eta, B > 0$. If we now define $u = y - y_r$, $\omega = z - z_r$, and use $\dot{\omega} = -\beta u$, we obtain the following recovering equation:

$$m(t) = \frac{\dot{u}}{\gamma} + u + \eta\beta \int u. \tag{4}$$

We see from (3) and (4) that this overall procedure requires a two-channel transmission, i.e., the transmission of both x and y. The block diagram implementations for the receiver and the recovering subsystems are given in Figs. 3 and 4, respectively. Actual analog circuit realizations for these subsystems can easily be accomplished by using operational amplifiers.

As a numerical example, consider the case where $m(t) = \cos t$ and

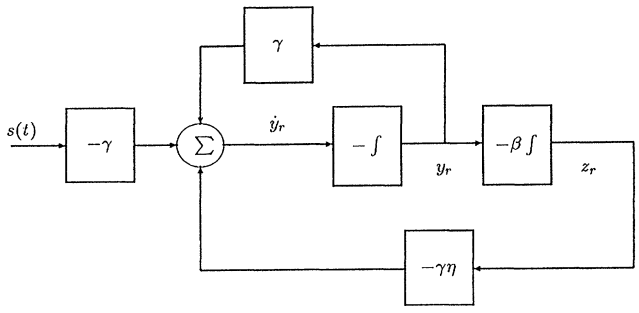

FIG. 3. Receiver subsystem.

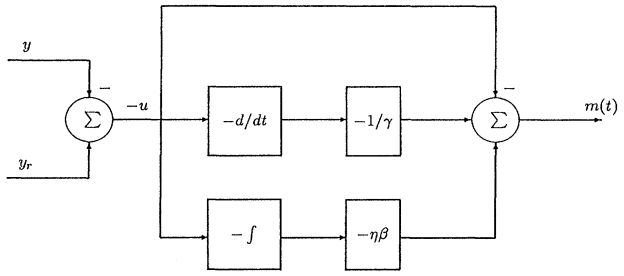

FIG. 4. Recovering subsystem.

$$(\alpha, \beta, \gamma, \eta, \varepsilon, m_0, m_1) = (9.8, 14.2, 1, 1, 1, -\tfrac{1}{7}, \tfrac{2}{7}). \tag{5}$$

For the parameter values chosen in (5), the system of (2) behaves chaotically. A chaotic trajectory in the x-y plane, the time behavior of the state variable x, the message $m(t)$, and the recovery of $m(t)$ through (4) are given in Fig. 5. The time axis in this figure starts from 150 since the time interval 0–150 is used to eliminate the transients. As expected, Figs. 5(c) and 5(d) are identical, which means that the message $m(t)$ can be recovered faithfully.

Here we should point out that the choice of the receiver subsystem is not unique. However, different receiver subsystems will yield different recovering equations. Hence, the type of transmission required (i.e., one-, two-, or three-channel transmission) will be determined by the choice of the receiver and its resulting recovering subsystem.

In conclusion, we have discussed the usage and the implementation of a simple chaotic masking scheme with a *linear* inverse system approach. We have shown that,

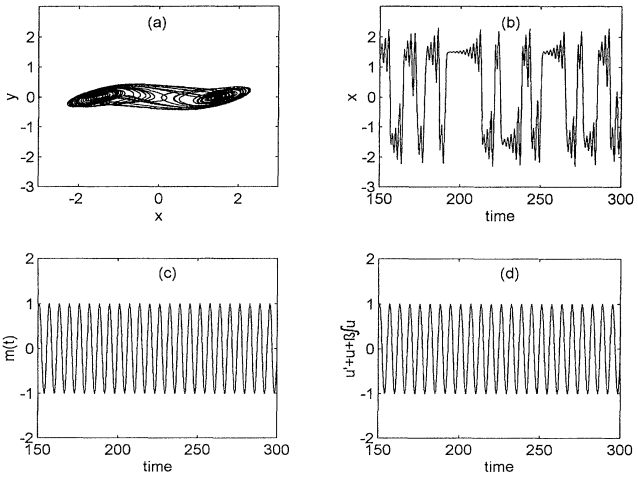

FIG. 5. (a) A chaotic attractor from the transmitter subsystem of (2). (b) Time behavior of x. (c) The message $m(t)$. (d) Signal recovered at the receiving end.

under the assumption of no parameter mismatch, the exact recovery of the message is possible. Compared to other systems or approaches, our proposed system has the following advantages over them: First, it does not require chaos synchronization. Second, its inverse system is completely linear, which makes it easily realizable. Third, the physical realization of the overall system is quite easy due to the fact that it employs the well-studied and easily realizable Chua's circuit, and its receiver and the recovering subsystems are linear.

[1] L. M. Pecora and T. L. Carroll, Phys. Rev. Lett. **64**, 821 (1990).
[2] T. L. Carroll and L. M. Pecora, IEEE Trans. Circuits Syst. **38**, 453 (1991).
[3] K. M. Cuomo, Int. J. Bif. Chaos **3**, 1327 (1993).
[4] K. M. Cuomo, A. V. Oppenheim, and S. H. Strogatz, IEEE Trans. Circuits Syst. **40**, 626 (1993).
[5] K. M. Cuomo and A. V. Oppenheim, Int. J. Bif. Chaos **3**, 1629 (1993).
[6] M. Hasler, in *Proceedings of the IEEE international Symposium on Circuits and Systems, London, 1994* (IEEE, New York, 1994), Chap. 6.2, p. 314.
[7] U. Feldmann, M. Hasler, and W. Schwarz, in *Proceedings of the International Symposium on Circuits and Systems, Seattle, Washington, 1995* (IEEE, New York, 1995), Vol. 1, p. 3.
[8] T. Matsumoto, IEEE Trans. Circuits Syst. **31**, 1055 (1984).
[9] G.-Q. Zhong and F. Ayrom, Int. J. Circuit Theory Appl. **13**, 93 (1985).
[10] L. O. Chua, M. Komuro, and T. Matsumoto, IEEE Trans. Circuits Syst. **33**, 1073 (1986).
[11] J. M. Cruz and L. O. Chua, IEEE Trans. Circuits Syst. **39**, 985 (1992).
[12] M. P. Kennedy, Frequenz **46**, 66 (1992).