Digital signal transmission with cascaded heterogeneous chaotic systems

K. Murali*
Department of Physics, Anna University, Chennai - 600 025, India
(Received 8 April 2000; revised manuscript received 21 August 2000; published 27 December 2000)

A new chaos based secure communication scheme is proposed to transmit digital signals by combining the concepts of chaotic-switching and chaotic-modulation approaches. In this scheme two heterogeneous chaotic circuits are used both at the transmitter and receiver modules. First a binary message signal is scrambled by two chaotic attractors produced by a set of chaotic systems (No. 1) of the drive module. The so produced small amplitude scrambled chaotic signal is further directly injected or modulated by different chaotic system (No. 2) within the drive module. Then the chaotic signal generated by this second chaotic system No. 2 is transmitted to the response module through the channel. An appropriate feedback loop is constructed in the response module to achieve synchronization among the variables of the drive and response modules and the binary information signal is recovered by using the synchronization error followed by low-pass filtering and thresholding. Simulation results are reported in which the quality of the recovered signal is higher and the encoding of the information signal is potentially secure. The effect of perturbing factors like channel noise and nonidentity of parameters are also considered.

DOI: 10.1103/PhysRevE.63.016217 PACS number(s): 05.45.Gg, 05.45.Vx, 05.45.Pq

I. INTRODUCTION

Recently, many studies have shown the possibility of synchronizing chaotic systems and its potential usefulness in secure communications [1–27]. The most frequently studied chaos synchronization schemes can in general be classified as (i) *conventional synchronization* (CS) [13,15–17] and (ii) *generalized synchronization* (GS) [15,17,22]. Recently in Refs. [19,22,23] the concept of synchronization and communication through compound chaotic signal generated using *encryption key functions* have been reported. In these approaches both CS and GS are used where all the *drive system* variables are combined suitably to produce a compound chaotic drive signal to drive the *response system*. Based on the above synchronization schemes, in typical communication systems the information to be transmitted is carried from the trasmitter to the receiver by a chaotic signal through an analog channel. The decoding of the information signal in the receiver can be carried out by means of either (synchronization) coherent or (without synchronization) noncoherent demodulation schemes [21]. Following these approaches, the reported secure communication methods may be classified as: *chaotic masking* [2,4,7–9,16], *chaotic modulation* [6,9,14,18,19,22], *chaotic switching* [3–5,10,16], and *chaotic parameter modulation* [3,4,9,10]. In the first case, the message is just added to the chaotic carrier signal. In the second case the message is not just added to the carrier but the carrier is modulated by the information signal. In both cases, the intensity of the message must be small enough to avoid detection in the time or frequency domains. In the third case, chaos switching is based on the requirement of two distinct chaotic attractors for bits ''1'' and ''0.'' The receiver has two replicas of the transmitting systems, each one designed for detecting either a bit 1 or 0. In this scheme, the bit rate is smaller because the period of modulation cannot be smaller than the time to entrain each of the states. Finally, for the fourth case, for chaotic parameter modulation, the secure communication scheme that detects the self-synchronization error of the receiver caused by intentional parameter perturbations in the transmitter. Further this approach has been extended by using suitable adaptive controllers [24,25]. In the case of chaotic-switching method of a chaos based secure communication, it has been shown that it has a low level of security because one can extract the encoded digital information signal from the transmitted chaotic signal by using different unmasking techniques [26,27]. However, to overcome the problem of unmasking the informating message from the chaotic carrier generated from the *chaos-shift-keying* or *chaotic-switching* scheme based transmitter system, in this paper, a new approach has been adapted in which the *chaotic-switching* and the *chaotic-modulation* techniques are combined suitably by exploiting the potentials of heterogeneous chaotic systems [28]. Using this approach the encoding of digital information signal can be made potentially secure.

II. PROPOSED SECURE COMMUNICATION SCHEME

In the present scheme the CS approach is used and a set of cascaded heterogeneous (comprising of nonautonomous and autonomous) chaotic systems are considered both in transmitter module and receiver module. The block diagram of the present communication scheme is depicted in Fig. 1. It includes a transmitter module, a receiver module, and a communication channel between them. In the transmitter module, depending upon the digital message signal level, a scrambled chaotic signal is produced from the first chaotic system No. 1. Then a small amplitude version of this scrambled chaotic signal generated from this first system is cascadingly encoded by the second chaotic system No. 2. Thus a kind of nonlinear information mixing is achieved within the transmitter chaotic module by utilizing two entirely different types of chaotic systems. The advantage here is that the

*Email address: kmurali@ns.annauniv.edu

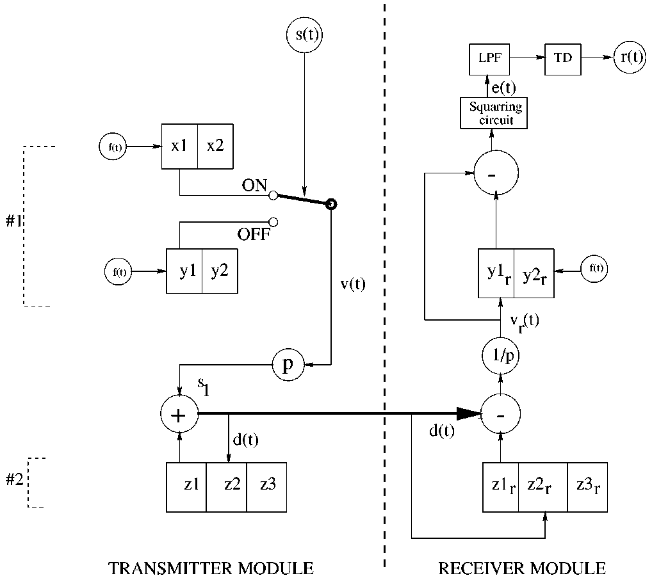

FIG. 1. Schematic diagram showing the digital signal transmission scheme using cascaded heterogeneous chaotic systems. Here $s(t)$ is the digital information signal, $d(t)$ is the transmitted chaotic signal, $v_r(t)=(d(t)-z_{1r})/p$ is the regenerated chaotic signal, and $r(t)$ is the recovered information signal. $f_1(t)$, $f_2(t)$, and $f_3(t)$ are the local periodic drives used for the nonautonomous chaotic systems. LPF is the *low-pass filter* and TD is the *threshold detector*. Here $x1=x_1$, $y1=y_1$, $x2=x_2$, $y2=y_2$, $z1=z_1$, $z2=z_2$, $z3=z_3$, $y1_r=y_{1r}$, $y2_r=y_{2r}$, $z1_r=z_{1r}$, $z2_r=z_{2r}$, and $z3_r=z_{3r}$.

small amplitude chaotic signal of system No. 1 is now masked by the chaotic signal of system No. 2 and transmitted through the channel to the receiver module. So the actual transmitted chaotic signal now masks only the chaotic signal generated by system No. 1. Due to the usage of cascaded heterogeneous chaotic systems at the transmitter module, the scrambled chaotic signal $v(t)$ is potentially as well as securely masked by the chaotic signal generated by the system No. 2.

The presently suggested method of signal transmission using chaos synchronization can be described as follows. Let us consider the following form of the transmitter-module equations:

Transmitter module: *System No. 1:*

$$\dot{x}_1=f_1(x_1,x_2), \tag{1}$$

$$\dot{x}_2=f_2(x_1,x_2)+f_1(t), \tag{2}$$

$$\dot{y}_1=f_1(y_1,y_2), \tag{3}$$

$$\dot{y}_2=f_2(y_1,y_2)+f_2(t), \tag{4}$$

System No. 2:

$$\dot{z}_1=g_1(z_1,z_2,z_3), \tag{5}$$

$$\dot{z}_2=g_2(d(t),z_2,z_3), \tag{6}$$

$$\dot{z}_3=g_3(d(t),z_2,z_3), \tag{7}$$

where *system No. 1* consists two independant chaotic systems (*nonautonomous systems*) and *system No. 2* is another heterogeneous chaotic system (*autonomous system*). In Eqs. (1)–(7), $f_1(t)$ and $f_2(t)$ are the external periodic driving signals, $v(t)=x_1$ or y_1 when $s(t)=0$ (ON) or 1 (OFF), respectively, $s_1(t)=pv(t)$ and $d(t)=z_1+s_1(t)$. Here $s(t)$ is the actual digital information signal, $s_1(t)$ is the small amplitude scrambled chaotic signal generated by *system No. 1*, which is further modulated within *system No. 2*. Also, p is the control (intensity) parameter for $v(t)$ and $d(t)$ is the actual transmitted chaotic signal to the receiver module from transmitter module. *System No. 2* represents the two subsystems configuration of an *autonomous chaotic system* [14,18,29]. We have in fact explicitly shown numerically the applicability of this kind of setup in the following discussions. By establishing the concept of chaos synchronization through *drive-response* formalism, then by considering the *receiver-module* equations as

Receiver module: *System No. 1:*

$$\dot{y}_{1r}=f_1(y_{1r},y_{2r})+\epsilon_r[v_r(t)-y_{1r}], \tag{8}$$

$$\dot{y}_{2r}=f_2(y_{1r},y_{2r})+f_3(t), \tag{9}$$

System No. 2:

$$\dot{z}_{1r}=g_1(z_{1r},z_{2r},z_{3r}), \tag{10}$$

$$\dot{z}_{2r}=g_2(d(t),z_{2r},z_{3r}), \tag{11}$$

$$\dot{z}_{3r}=g_3(d(t),z_{2r},z_{3r}), \tag{12}$$

where Eqs. (10)–(12) are copies of Eqs. (5)–(7), which are driven by the transmitted chaotic signal $d(t)$. Also Eqs. (8) and (9) are the replica of Eqs. (3) and (4), which are then driven by $v_r(t)=(d(t)-z_{1r})/p$ through one-way coupling [11,30]. Here ϵ_r is the one-way coupling parameter. If the maximal Lyapunov exponents (conditional Lyapunov exponents) of Eqs. (10)–(12) and (8) and (9) are negative under the influence of the chaotic signal $d(t)$ and $v_r(t)$, respectively, then $|z_{1r}-z_1|\to 0$, $|z_{2r}-z_2|\to 0$, $|z_{3r}-z_3|\to 0$, $|y_{1r}-y_1|\to 0$, and $|y_{2r}-y_2|\to 0$, for $t\to\infty$. Although the conditional Lyapunov exponents generally guarantee synchronization in the case of identical, noiseless systems, they do not guarantee robust synchronization [31,32].

In this scheme, the synchronization error between Eqs. (8) and (9) and (1)–(4) is denoted as $e(t)=[y_{1r}-v_r(t)]^2$. The message signal $r(t)$ can be further recovered from $e(t)$ by using low-pass filtering and by applying suitable thresholding [3,4].

III. NUMERICAL EXPERIMENTS

To illustrate the performance of the above scheme, as a test case, we have used the well-known Chua's circuit [29] for the *autonomous chaotic system* and the Murali-

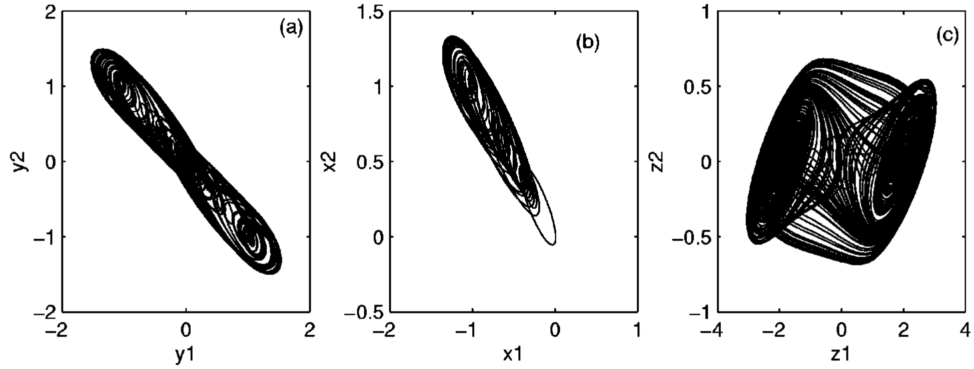

FIG. 2. Basic attractors of the chaotic systems: (a) Chaotic attractor in (y_1-y_2) plane of the MLC circuit [Eqs. (15) and (16)] for encoding 0 ($F_2=0.17$). (b) Chaotic attractor in (x_1-x_2) plane of the MLC circuit [Eqs. (13)–(14)] for encoding 1 ($F_1=0.11$). (c) Chaotic attractor in (z_1-z_2) plane of *system No. 2* Chua's circuit [Eqs. (17)–(19)] for $\alpha=10.0$ and $\beta=14.87$. All other paramters are fixed as in the text. Here $x1=x_1$, $x2=x_2$, $y1=y_1$, $y2=y_2$, $z1=z_1$, and $z2=z_2$.

Lakshmanan-Chua (MLC) circuit [33] for the *nonautonomous chaotic system* both at the transmitter and receiver modules. However, one can as well use different lower- or higher-order chaotic or hyperchaotic models also as system No. 1. For the present case, the system operation is described by the following set of equations:

Transmitter module: *System No. 1:*

$$\dot{x}_1=x_2-g_2(x_1), \tag{13}$$

$$\dot{x}_2=-\sigma x_2-x_1+F_1\sin(\omega t), \tag{14}$$

$$\dot{y}_1=y_2-g_2(y_1), \tag{15}$$

$$\dot{y}_2=-\sigma y_2-y_1+F_2\sin(\omega t), \tag{16}$$

System No. 2:

$$\dot{z}_1=\alpha(z_2-z_1-g_1(z_1)), \tag{17}$$

$$\dot{z}_2=d(t)-z_2+z_3, \tag{18}$$

$$\dot{z}_3=-\beta z_2, \tag{19}$$

where $g_1(z)=b_1 z+0.5(a_1-b_1)(|z+1|-|z-1|)$, $g_2(x)=b_2 x+0.5(a_2-b_2)(|x+1|-|x-1|)$, and $a_1=-1.27$, $b_1=-0.68$, $a_2=-1.02$, $b_2=-0.55$, $\sigma=1.015$, $\omega=0.75$, $\alpha=10.0$, and $\beta=14.87$. From Eqs. (13) and (14) and (15) and (16) (system No. 1) one can generate two different chaotic attractors to encode 1 and 0, respectively. The paramter for encoding 1 is $F_1=0.11$. The parameter for encoding 0 is $F_2=0.17$. These two sets of paramters generate two different chaotic attractors as shown in Figs. 2(a) and 2(b). For the system No. 2, a double-scroll-type chaotic attractor as depicted in Fig. 2(c) is used as basic mode for further investigations. In Eqs. (17)–(19), $d(t)=z_1+s_1(t)$, $s_1(t)=pv(t)$, $v(t)=x_1$, or y_1 when $s(t)=1$ or 0, respectively, and $p=0.1$. Then the receiver-module equations are represented as

Receiver module: *System No. 1:*

$$\dot{y}_{1r}=y_{2r}-g_2(y_{1r})+\epsilon_r(v_r(t)-y_{1r}), \tag{20}$$

$$\dot{y}_{2r}=-\sigma y_{2r}-y_{1r}+F_3\sin(\omega t). \tag{21}$$

System No. 2:

$$\dot{z}_{1r}=\alpha(z_{2r}-z_{1r}-g_1(z_{1r})), \tag{22}$$

$$\dot{z}_{2r}=d(t)-z_{2r}+z_{3r}, \tag{23}$$

$$\dot{z}_{3r}=-\beta z_{2r}. \tag{24}$$

Under the influence of $d(t)$ and for suitable value of the coupling parameter $\epsilon_r=1.3$, the receiver system's variables synchronize with the transmitter system's variables. In particular the *system No. 1* of the receiver module [Eqs. (20) and (21)] will be synchronized with the trasmitter [Eqs. (15) and (16)] at bit 0. For simulation, we have assumed all the local periodic drive signal [$F_1\sin(\omega t)$, $F_2\sin(\omega t)$, $F_3\sin(\omega t)$] are all in phase. However, suitable synchronization schemes for nonautonomous cases can be implemented when the periodic drives are considered as out-of-phase condition [12,20]. The significance of the present type of encoding is that the scrambled chaotic signal $s_1(t)$ is not only added just to a chaotic carrier but it also simultaneously drives the transmitter dynamical system No. 2. Such an encoding procedure ensures potential security and also avoids the typical distortion errors that occur in almost all previous communication schemes based on chaos synchronization [6,19,22].

By employing this scheme, the digital signal is recovered at the response system [Eqs. (20)–(24)] with $v_r(t)=[d(t)-z_{1r}]/p$. Figure 3 shows the numerical simulation results. Figure 3(a) shows the binary message signal $s(t)$. Figure 3(b) shows the scrambled chaotic signal $v(t)$ generated by the chaotic system No. 1 [Eqs. (13)–(16)]. If $s(t)=1$ (ON) then $v(t)=x_1$. If $s(t)=0$ (OFF) then $v(t)=y_1$. Figure 3(c) shows the actual transmitted chaotic signal $d(t)=z_1+s_1(t)$.

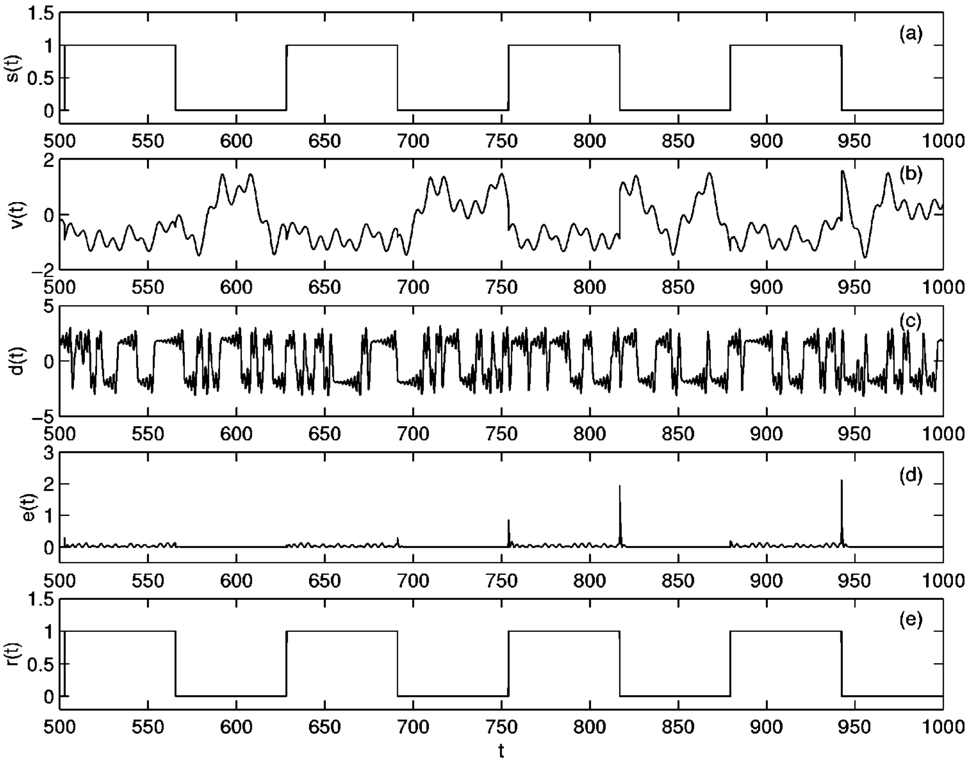

FIG. 3. (a) Digital information signal $s(t)$, (b) scrambled chaotic signal $v(t)$, (c) transmitted chaotic signal $d(t)=z_1+s_1(t)$, (d) synchronization error $e(t)$ of MLC circuit [Eqs. (20) and (21)] corresponding to 0 ($F_3=0.17$), (e) recovered information signal $r(t)$ from $e(t)$ after low-pass filtering and thresholding with $\epsilon_r=1.3$, $p=0.1$. All other parameters are fixed as in the text.

Figure 3(d) shows the synchronization error of the MLC circuit at the receiver [Eqs. (20) and (21), $\epsilon_r=1.3$, $F_3=0.17$] corresponding the $s(t)=0$. We can easily use low-pass filtering and thresholding to decode or recover the binary message signal $r(t)=s(t)$ from the error signal (d) as depicted in Fig. 3(e). Figure 4 depicts the power spectrum of the low-amplitude chaotic signal $s_1(t)$ and the actual transmitted signal $d(t)$ through the channel from the transmitter module. From the power spectrum, it is evident that from the chaotic signal $d(t)$ it is difficult to decipher the information signal $s(t)$ because the transmitted chaotic signal $d(t)$ is actually masking another chaotic signal $s_1(t)$, thus enchancing the potential security of the information signal transmission.

In order to study the robustness of the present synchronization scheme in recovering the information signal, we have considered the influence of channel noise $\eta(t)$ to the transmitted chaotic signal. Now the transmitted signal through a noisy channel corrupted with additive white Gausian noise (AWGN) is represented as $d(t)+\eta(t)$, where $\eta(t)$ is the AWGN of zero mean with correlation function $\langle \eta(t),\eta(t')\rangle=2D\,\delta(t-t')$ [23]. Here D is the noise intensity level. Figure 5 depicts the influence of channel noise and

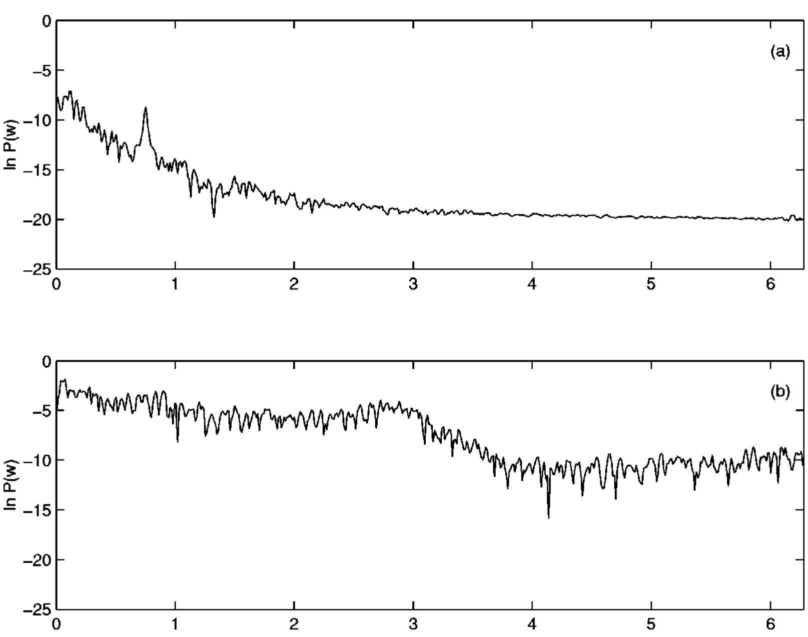

FIG. 4. Power spectrum of the low-amplitude chaotic signal $s_1(t)$ (a), transmitted chaotic signal $d(t)$ through the channel (b).

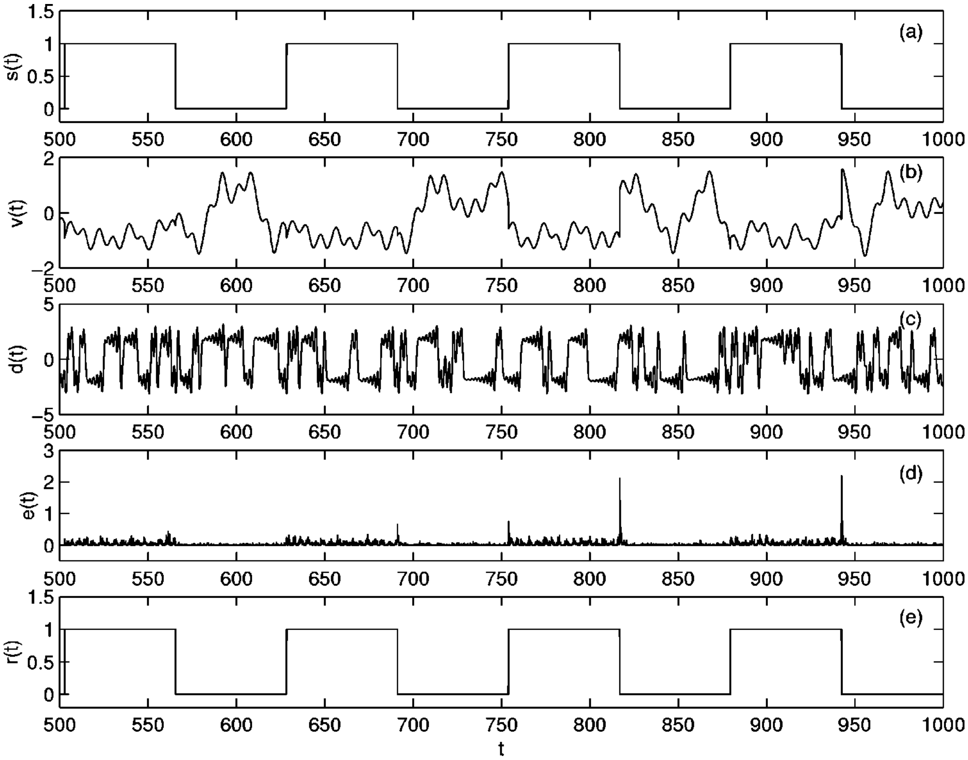

FIG. 5. (a) Digital information signal $s(t)$, (b) scrambled chaotic signal $v(t)$, (c) transmitted chaotic signal through a noisy channel corrupted with AWGN with noise intensity level $D=0.01$ and $d(t)=z_1+s_1(t)+\eta(t)$, (d) synchronization error $e(t)$ of MLC circuit [Eqs. (20) and (21)] corresponding to 0 ($F_3=0.17$), (e) recovered information signal $r(t)$ from $e(t)$ after suitable low-pass filtering and thresholding with $\epsilon_r=1.3$, $p=0.1$. All other parameters are fixed as in the text.

the recovered information signal $r(t)$ for the noise intensity level $D=0.01$. To estimate the system performance under additive channel noise, simulations are done to examine the signal-to-noise ratio (SNR) on the probability of bit error or bit error rate (BER) [21] as shown in Fig. 6. As expected, the error rate decreases with increase in the value of SNR (dB). On other hand, it is equivalent to saying that a decrease in noise results in a decrease in error rate. The general error rate is low and thus, the system is feasible.

Also a typical perturbing factor that decrease the communication quality is the nonidentical parameters of the transmitter and receiver modules. Therefore, one has to consider the case of a slightly different receiver-module system than that of the transmitter-module system, by introducing small parameter mismatch (nonidentity of parameters). Figure 7 shows the relationship between BER versus the percentage of parameter mismatch in α, β, σ, and ϵ_r of the receiver module equations. One finds that a slight mismatch ($<0.6\%$) in the above parameters introduces small distortions (like in Fig. 5) in the error signal $e(t)$, which can further be removed by suitable filtering and thresholding to produce the recovered digital information signal. However large

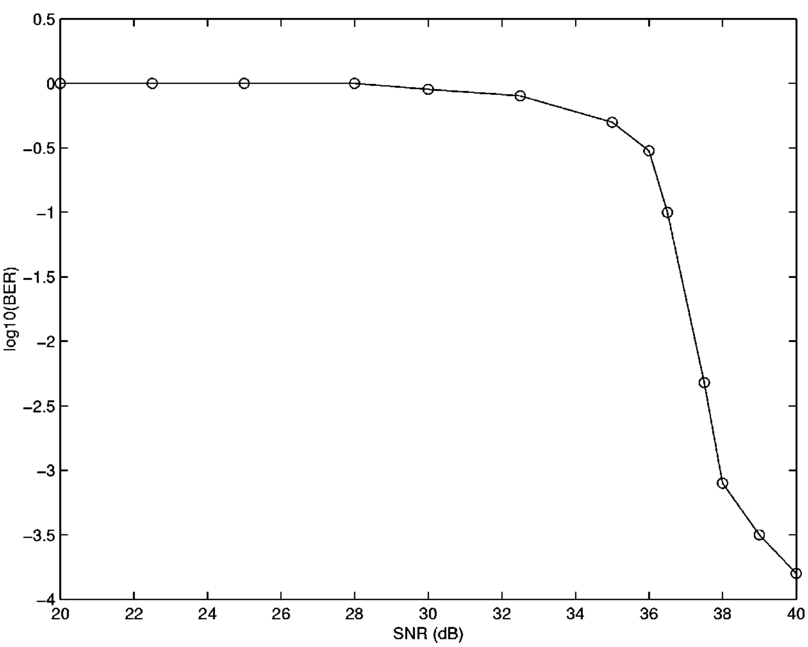

FIG. 6. BER under additive white Gaussian noise in the channel. Here log 10 (BER)$=\log_{10}$ (BER).

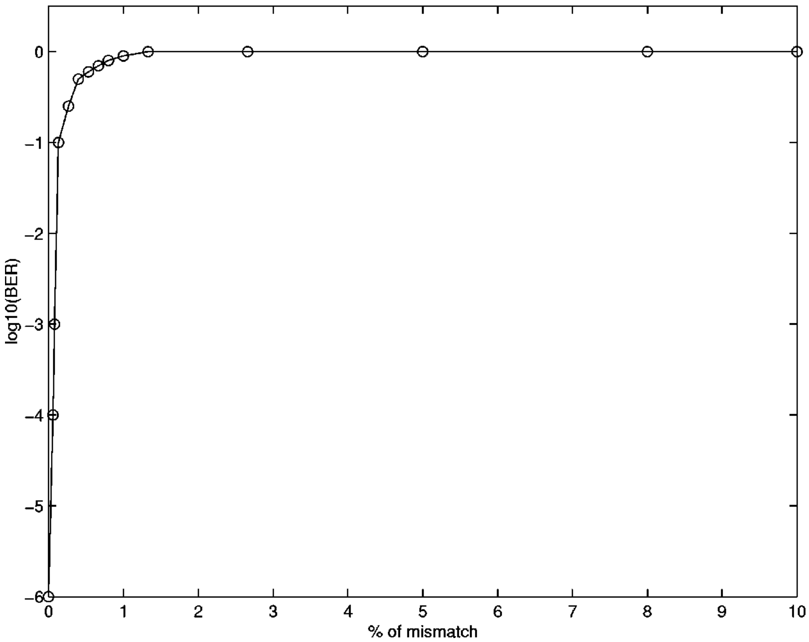

FIG. 7. Relationship between BER and percentage of receiver parameter mismatch. Here log 10 (BER) = $\log_{10}$ (BER).

deviation of even one receiver parameter with respect to the corresponding transmitter parameter leads to complete desynchronization signal at the receiver output.

IV. CONCLUSION

We have presented a procedure of achieving a potentially secure digital signal transmission using cascaded heterogeneous chaotic systems. By considering two different chaotic systems both in the transmitter and receiver modules, according to the digital message, suitable scarmbled chaotic signal is produced by the set of first chaotic systems. A small amplitude scrambled chaotic signal from this first system is further cascadingly encoded by the second chaotic system within the drive module. The chaotic signal generated from the second system of the drive module is then transmitted to the response module through an analog channel. By constructing an appropriate feedback loop in the response module, synchronization among the variables of the drive and response modules is achieved. Further, the binary message is decoded by using the synchronization error followed by low-pass filtering and suitable thresholding. Due to the present scheme of encoding the message signals with cascaded heterogeneous chaotic systems through a kind of nonlinear information mixing, security of the transmitted signal is potentially enhanced. The effect of perturbing factors on the transmission quality is investigated. It is shown that up to a certain level of channel noise intensity and parameter mismatch, the signal recovery is possible after performing suitable filtering and thresholding operations.

ACKNOWLEDGMENT

This work was carried out by using the computational facilities of The Institute of Mathematical Sciences, Chennai, India.

[1] L.M. Pecora and T.L. Carroll, Phys. Rev. Lett. **64**, 821 (1990).

[2] Lj. Kocarev, K. Halle, K. Eckert, L.O. Chua, and U. Parlitz, Int. J. Bifurcation Chaos Appl. Sci. Eng. **2**, 709 (1992).

[3] U. Parlitz, L.O. Chua, Lj. Kocarev, K.S. Halle, and A. Shang, Int. J. Bifurcation Chaos Appl. Sci. Eng. **2**, 973 (1992).

[4] K.M. Cuomo and A.V. Oppenheim, Phys. Rev. Lett. **71**, 65 (1993).

[5] H. Dedieu, M.P. Kennedy, and M. Hasler, IEEE Trans. Circuits Syst. **40**, 634 (1993).

[6] K.S. Halle, C.W. Wul, M. Itoh, and L.O. Chua, Int. J. Bifurcation Chaos Appl. Sci. Eng. **3**, 469 (1993).

[7] K. Murali and M. Lakshmanan, Phys. Rev. E **48**, R1624 (1993).

[8] C.W. Wu and L.O. Chua, Int. J. Bifurcation Chaos Appl. Sci. Eng. **3**, 1619 (1993).

[9] M.J. Ogorzalek, IEEE Trans. Circuits Syst. **40**, 639 (1993).

[10] U. Parlitz and S. Ergezinger, Phys. Lett. A **188**, 146 (1994).

[11] K. Murali and M. Lakshmanan, Phys. Rev. E **49**, 4882 (1994).

[12] T.L. Carroll and L.M. Pecora, IEEE Trans. Circuits Syst. **40**, 646 (1995).

[13] T.L. Carroll, IEEE Trans. Circuits Syst. **42**, 105 (1995).

[14] A.S. Dmitriev, A.I. Panas, and S.O. Starkov, Int. J. Bifurcation Chaos Appl. Sci. Eng. **5**, 1249 (1995).

[15] N.F. Rulkov, M.M. Sushchik, L.S. Tsimring, and H.D.I. Abarbanel, Phys. Rev. E **51**, 980 (1995).

[16] M. Lakshmanan and K. Murali, *Chaos in Nonlinear Oscillators: Controlling and Synchronization* (World Scientific, Singapore, 1996).

[17] Lj. Kocarev and U. Parlitz, Phys. Rev. Lett. **76**, 1816 (1996).

[18] A.S. Dmitriev, A.I. Panas, S.O. Starkov, and L.V. Kuzmin, Int. J. Bifurcation Chaos Appl. Sci. Eng. **7**, 2511 (1997).
[19] K. Murali and M. Lakshmanan, Int. J. Bifurcation Chaos Appl. Sci. Eng. **7**, 415 (1997); Phys. Rev. E **56**, 251 (1997).
[20] L.M. Pecora, T.L. Carroll, G.A. Johnson, D.J. Mar, and J.F. Heagy, Chaos **7**, 520 (1997).
[21] G. Kolumban, M.P. Kennedy, and L.O. Chua, IEEE Trans. Circuits Syst., I: Fundam. Theory Appl. **45**, 1129 (1998).
[22] K. Murali and M. Lakshmanan, Phys. Lett. A **241**, 303 (1998).
[23] M.N. Lorenzo, V. Perez-Munuzuri, K. Murali, and V. Perez-Villar, IEEE Trans. Circuits Syst. I, Fundam, Theory Appl. (submitted).
[24] T. Yang and L.O. Chua, IEEE Trans. Circuits Syst., I: Fundam. Theory Appl. **43**, 817 (1996).
[25] H. Dedieu and M.J. Ogorzalek, IEEE Trans. Circuits Syst., I: Fundam. Theory Appl. **44**, 948 (1997).
[26] K.M. Short, Int. J. Bifurcation Chaos Appl. Sci. Eng. **4**, 959 (1994); **6**, 367 (1996); G. Perez and H.A. Cerdeira, Phys. Rev. Lett. **74**, 1970 (1995).
[27] T. Yang, L.B. Yang, and C.M. Yang, IEEE Trans. Circuits Syst., I: Fundam. Theory Appl. **45**, 1062 (1998); Physica D **124**, 248 (1998).
[28] K. Murali, Phys. Lett. A **272**, 184 (2000); Int. J. Bifurcation Chaos, Appl. Sci. Eng. (to be published).
[29] R.N. Madan, *Chua's Circuit: A Paradigm for Chaos* (World Scientific, Singapore, 1993).
[30] K. Pyragas, Phys. Lett. A **170**, 421 (1992).
[31] P. Ashwin, J. Buescu, and I. Stewart, Phys. Lett. A **193**, 126 (1994); Nonlinearity **9**, 703 (1994)
[32] S.C. Venkataramani, B. Hunt, and E. Ott., Phys. Rev. E **54**, 1346 (1996).
[33] K. Murali, M. Lakshmanan, and L.O. Chua, IEEE Trans. Circuits Syst., I: Fundam. Theory Appl. **41**, 462 (1994); Int. J. Bifurcation Chaos Appl. Sci. Eng. **4** 1511 (1994); **5**, 563 (1995); M. Lakshmanan and K. Murali, Philos. Trans. R. Soc. London, Ser. A **353**, 33 (1995).