ELSEVIER

18 January 1999

PHYSICS LETTERS A

Physics Letters A 251 (1999) 169–176

A chaotic masking scheme by using synchronized chaotic systems

Ömer Morgül [a,1], Moez Feki [b,2]

[a] *Department of Electrical and Electronics Engineering, Bilkent University, 06533 Bilkent, Ankara, Turkey*

[b] *INRIA LORRAINE Projet CONGE, I.S.G.M.P. BM-bt. A, Université de Metz, Ile du Saulcy 57045, Metz Cedex 01, France*

Received 23 February 1998; revised manuscript received 30 June 1998; accepted for publication 9 November 1998
Communicated by A.P. Fordy

Abstract

We present a new chaotic masking scheme by using synchronized chaotic systems. In this method, synchronization and message transmission phases are separated, and while synchronization is achieved in the synchronization phases, the message is only sent in message transmission phases. We show that if synchronization is achieved exponentially fast, then under certain conditions any message of any length could be transmitted and successfully recovered provided that the synchronization length is sufficiently long. We also show that the proposed scheme is robust with respect to noise and parameter mismatch under some mild conditions. © 1999 Published by Elsevier Science B.V.

PACS: 05.45.+b
Keywords: Chaotic systems; Chaos synchronization; Chaotic masking; Lorenz system

1. Introduction

In recent years the idea of synchronization of chaotic systems has received a great deal of interest among scientists from various fields, see e.g. [1–14]. One of the motivations for synchronization is the possibility of sending messages through chaotic systems for secure communication, see e.g. Refs. [5,7,9]. Such synchronized systems usually consist of two parts: a generator of chaotic signals (drive system), and a receiver (response system). The response system is usually a duplicate of a part (or the whole) of the drive system. A chaotic signal generated by the drive system may be used as an input in the response system to synchronize the common signals of both systems, see e.g. Ref. [2]. After synchronization, one may add the message to the chaotic signal used for synchronization and send this signal to the receiver. This is called chaotic masking, see Ref. [8], and under certain conditions one may recover the message from the signals of the response system, see e.g. Ref. [9].

Recently, a new synchronization scheme based on occasional coupling has been proposed in Ref. [11]. This scheme, as others proposed in the literature, has a potential application for secure communications. In this Letter we propose a chaotic masking scheme based on the occasional synchronization proposed in Ref. [11] and present some simulation results concerning the message transmission.

A related scheme for synchronization of chaotic sys-

[1] E-mail: morgul@ee.bilkent.edu.tr.
[2] E-mail: feki@loria.fr.

PII S0375-9601(98)00868-8

tems was proposed in Ref. [12]. In this scheme, the synchronization signal is used in the response system at discrete times. For a finite time step $\tau > 0$, response system states corresponding to the drive variables used in the synchronization signal are set to the values of corresponding drive variables at instances $t = n\tau$, $n = 1, 2, \ldots$, and it was shown that for τ sufficiently small, synchronization is possible. Hence, the synchronization signal is used only at certain instances in Ref. [12], whereas it is used in an interval in our scheme. We note that the length of this interval is of crucial importance in our analysis, see Section 2. As a result, some of the response system states are instantaneously set to the values of corresponding drive system states in Ref. [12], whereas both system states asymptotically approach to each other in our scheme, see also Ref. [11]. Both schemes use an interval in which the response system is autonomous, and the scheme of Ref. [12] may be related to our scheme in which the switching signal is impulsive, see Remark 2.

This Letter is organized as follows. In Section 2 we introduce our message transmission scheme, show that under some mild conditions successful message recovery is possible and that the scheme is robust with respect to noise and parameter mismatch. In Section 3 we present some simulation results. Finally, we give some concluding remarks.

2. Occasional coupling

Let the chaotic master system be given by the following equation,

$$\dot{u} = f(u, \mu)\,, \tag{1}$$

where $u \in \mathbb{R}^n$ is the state of the master system, $\mu \in \mathbb{R}^p$ is a parameter vector, and $f : \mathbb{R}^n \times \mathbb{R}^p \to \mathbb{R}^n$ is a smooth function. We assume that for certain values of μ, the solutions of (1) exhibit chaotic behaviour. A certain function of u is assumed to be measurable and is sent to the slave system for synchronization. For simplicity, let us assume that this synchronization signal is given as $o = c^{\mathrm{T}}u$ where $c \in \mathbb{R}^n$ is a constant vector, and the superscript T denotes the transpose. The slave system may be chosen as follows,

$$\dot{w} = f(w, \mu) + s(t)K(w)(o - c^{\mathrm{T}}w)\,, \tag{2}$$

where $w \in \mathbb{R}^n$ is the state of the slave system, $s(t) = 0, 1$ denotes the switching signal, and $K : \mathbb{R}^n \to \mathbb{R}^n$ is the feedback gain vector. We assume that K is a smooth function of w. This form indicates that when $s(t) = 0$ (i.e., the switch is off), the slave system is a duplicate of the master system. We assume that when $s(t) = 1$ (i.e., the switch is on), the gain vector $K(w)$ could be chosen so that the synchronization error $e(t) = u(t) - w(t)$ decays exponentially to zero, that is there exist some $M \geqslant 1$, $\alpha > 0$ such that for any $t_0 \geqslant 0$, $e(t_0) \in \mathbb{R}^n$, the following holds,

$$\|e(t)\| \leqslant M\,\mathrm{e}^{-\alpha(t-t_0)}\|e(t_0)\|\,, \quad t \geqslant t_0\,, \tag{3}$$

where $\|\cdot\|$ denotes the standard Euclidean norm in $\mathbb{R}^n$. We note that in some cases (3) may hold only locally, i.e. for $\|e(t_0)\| \leqslant r$ for some $r > 0$, in which case we say that the synchronization holds only locally.

We note that under certain conditions such a gain vector could be found in a systematic way, and that most of the synchronization schemes proposed in the literature satisfy this assumption, see Ref. [14]. The synchronization scheme given by (2) is similar to the observer based synchronization proposed in Refs. [13,14]. In this scheme we assume that the system given by (1) is in the following form,

$$\dot{u} = f(u, \mu) = A(\mu)u + g(u, \mu)\,, \tag{4}$$

where for each $\mu \in \mathbb{R}^p$, $A \in \mathbb{R}^{n\times n}$, is a constant matrix and $g(\cdot) : \mathbb{R}^n \to \mathbb{R}^n$ is a smooth function. By using (2), (4) and assuming that K is a constant vector, we obtain the following error dynamics in the coupling phase (i.e., when $s(t) = 1$),

$$\dot{e} = (A(\mu) - Kc^{\mathrm{T}})e + g(u, \mu) - g(w, \mu)\,, \tag{5}$$

where we used $o = c^{\mathrm{T}}u$. If, for a fixed μ, the pair (A, c) is observable then there exists a constant gain matrix $K \in \mathbb{R}^n$ such that $A_c = A - Kc^{\mathrm{T}}$ is stable, see Refs. [13,14]. Moreover, assume that $g(\cdot)$ is Lipschitz, i.e., the following holds,

$$\|g(u, \mu) - g(w, \mu)\| \leqslant k\|u - w\|\,,$$
$$u, w \in \mathbb{R}^n\,, \quad \mu \in \mathbb{R}^p\,, \tag{6}$$

for some $k > 0$ in a region $\Omega \subset \mathbb{R}^n \times \mathbb{R}^n$ in which the solutions are bounded. If $k > 0$ is sufficiently small, then the synchronization error e decays exponentially

to zero, i.e. (3) holds; if k is not small but A and $g(\cdot)$ are in some special form, then (3) still holds for a particular choice of K, see Refs. [13,14]. In any case, if $\|e(t_0)\|$ is sufficiently small, we may expect (3) to hold. We note that in this paper we assume that the feedback gain K may be a function of w, whereas it is assumed to be constant in Refs. [13,14].

Remark 1. To emphasize the consequences of assumption (3), let us consider the "error system" in terms of the error e. By using (1) and (2), one can obtain the error dynamics, and (3) implies that $e = 0$ is an exponentially stable equilibrium point of the error system. Since the exponentially stable systems are robust with respect to small changes in the system dynamics, see Ref. [15], we expect that the message transmission technique which will be given below is robust with respect to noise and parameter mismatch. This point was proven in Refs. [11,13,14]. We also note that for most of the synchronization techniques proposed in the literature the exponential synchronization property given by (3) is satisfied. By using this fact one can prove the robustness of these techniques with respect to noise and parameter mismatch.

Our chaotic masking scheme by using the occasional coupling proposed in Ref. [11] is based on changing the switching signal $s(t)$ between 0 and 1, periodically. More precisely, let $m(t)$ denote the message to be transmitted, let $T_s > 0$ and $T_m > 0$ denote the intervals for synchronization and message transmission phases, respectively. Then, for $j = 1, 2, \ldots$, our scheme is as follows:

(i) m (jth synchronization phase) For $(j-1)(T_s+T_m) \leqslant t < jT_s + (j-1)T_m$, use the master system given by (1) and the slave system given by (2), with $s(t) = 1$.

(ii) (jth message transmission phase) For $jT_s + (j-1)T_m \leqslant t < j(T_s + T_m)$, use the master system given by (1) and the slave system given by (2), with $s(t) = 0$, and send the masked message $y(t) + m(t)$.

(iii) (message recovery) In the jth message transmission phase, the recovered message $m_r(t)$ can be computed as

$$m_r(t) = o(t) + m(t) - c^{\mathrm{T}} w(t) . \tag{7}$$

Note that with $s(t) = 0$, the response system given (2) becomes an autonomous system in the message transmission phase. Since in the synchronization phase, the error decays to zero exponentially fast (see (3)), at the end of this phase the error becomes extremely small, provided that T_s is sufficiently large. Hence, for the message transmission phase we could exchange the signals of the drive system used for synchronization with the corresponding signals of the response system, which is the rationale behind using $s(t) = 0$ in (2). We have the following result for the message transmission.

Theorem 1. Consider the systems given by (1), (2) and the message transmission scheme given above. Assume that $f(u, \mu)$ is Lipschitz in u, i.e. satisfies an inequality similar to (6) with a Lipschitz bound k_u, and that (3) holds. Let the initial error satisfy $\|e(0)\| \leqslant r$ for some $r > 0$, and let (the precision number) $\epsilon > 0$ be given. Then, for any message of length $T_m > 0$, there exists a synchronization interval $T_s > 0$ such that in the message transmission phase we have

$$\|m_r(t) - m(t)\| \leqslant \epsilon , \tag{8}$$

where $jT_s + (j-1)T_m \leqslant t \leqslant j(T_s + T_m)$, and $j = 1, 2, \ldots$.

Proof. For simplicity, we define the beginning of jth synchronization and message transmission phases T_j^s and T_j^m, respectively, as follows,

$$T_j^s = (j-1)(T_s + T_m) , \quad T_j^m = jT_s + (j-1)T_m , \quad j = 1, 2, \ldots . \tag{9}$$

From (3) it is clear that the following holds in the jth synchronization phase,

$$\|e(t)\| \leqslant M \mathrm{e}^{-\alpha(t - T_j^s)} \|e(T_j^s)\| , \quad T_j^s \leqslant t < T_j^m . \tag{10}$$

From (1) and (2) it follows that the following holds in the jth message transmission phase,

$$e(t) = e(T_j^m) + \int_{T_j^m}^{t} (f(u(\tau), \mu) - f(w(\tau), \mu)) \, \mathrm{d}\tau , \quad T_j^m \leqslant t < T_{j+1}^s . \tag{11}$$

By using Lipschitz inequality, taking norms and using the Bellman–Gronwall lemma, we obtain

$$\|e(t)\| \leqslant e^{k_u(t-T_j^m)}\|e(T_j^m)\|,$$
$$T_j^m \leqslant t < T_{j+1}^s. \tag{12}$$

By using (12) and (10) successively, and noting that the error is continuous, we obtain

$$\begin{aligned}\|e(t)\| &\leqslant e^{k_u T_m}\|e(T_j^m)\|, \quad T_j^m \leqslant t < T_{j+1}^s \\ &\leqslant Me^{(k_u T_m - \alpha T_s)}\|e(T_j^s)\| \\ &\leqslant (Me^{(k_u T_m - \alpha T_s)})^j \|e(0)\|. \end{aligned} \tag{13}$$

Note that we have

$$\|m_r(t) - m(t)\| = \|c^{\mathrm{T}}e(t)\| \leqslant \|c\|\|e(t)\|, \tag{14}$$

see (7). It follows from (13) and (14) that (8) holds if the following is satisfied for all j,

$$\ln M + k_u T_m - \alpha T_s \leqslant \frac{1}{j}\ln\frac{\epsilon}{r\|c\|},$$
$$j = 1, 2, \ldots. \tag{15}$$

If $\ln \epsilon/r\|c\| < 0$, then (15) is satisfied provided that the following holds,

$$\ln M + k_u T_m - \alpha T_s \leqslant \ln\frac{\epsilon}{r\|c\|}. \tag{16}$$

On the other hand, if $\ln \epsilon/r\|c\| \geqslant 0$, then (15) is satisfied provided that the following holds,

$$\ln M + k_u T_m - \alpha T_s \leqslant 0. \tag{17}$$

Once $T_m > 0$ is selected arbitrarily, the required $T_s > 0$ could be found from (16) or (17). □

The result stated in Theorem 1 holds in the ideal case when the signal transmitted (i.e., o) is not corrupted by noise and when the parameter vectors (i.e., μ) are the same in the drive and the response systems. In the sequel we consider the nonideal case and prove that the scheme given above is robust with respect to noise and parameter mismatch under certain conditions. First note that in the nonideal case, the response system given by (2) should be replaced with the following,

$$\dot{w} = f(w, \mu') + s(t)K(w)(o + n - c^{\mathrm{T}}w), \tag{18}$$

where μ' is the parameter vector for the response system, and n is a (random) noise term in the measurements. Then we have the following robustness result.

Theorem 2. Consider the drive and response systems given by (1) and (18), respectively. Assume that the solutions remain in a bounded set. Assume that $f(u, \mu)$ is Lipschitz in both variables. Let the noise n satisfy $\|n(t)\| \leqslant n_m$ for some $n_m > 0$ for $t \geqslant 0$ and let us define $\Delta\mu = \mu - \mu'$. Then in the synchronization phases (i.e., for $s(t) = 1$), the error asymptotically (i.e., as $t \to \infty$) satisfies the following inequality,

$$\|e(t)\| \leqslant C_1 n_m + C_2\|\Delta\mu\|, \tag{19}$$

where $C_1 > 0$ and $C_2 > 0$ are some constants.

Proof. Since the solutions remain in a bounded set, $\|K(w)\|$ remain bounded in this set as well. Hence we have

$$\|K(w)(o_1 - o_2)\| \leqslant k_1\|o_1 - o_2\|,$$

where $k_1 = \max\{\|K(w)\|\}$. Then the proof follows from the exponential stability assumption (3) and the Theorem 2 of Ref. [11]. □

Theorem 2 proves that in the presence of noise and/or parameter mismatch, the synchronization error remains bounded, hence the proposed scheme is robust in the nonideal case. Moreover, the error bound is linear in noise and parameter mismatch bounds; hence as these bounds decrease, the synchronization error bound also decreases. Also note that here we have an asymptotic result, i.e. (19) holds as $t \to \infty$. From practical point of view we may assume that (19) holds if T_s is sufficiently large. We note that the conclusions of Theorem 2 remains true if $c' \neq c$ is used in (18), provided that a term $C_3\|c - c'\|$ is added to (19).

Theorem 3. Consider the drive and response systems given by (1) and (18), respectively, and let $s(t) = 0$ (i.e., in message transmission phase). Assume that $f(u, \mu)$ is Lipschitz in both variables. Assume that T_s is sufficiently large so that (19) is satisfied. Let $\epsilon > 0$ be a given precision level which satisfies

$$\|c\|(C_1 n_m + C_2\|\Delta\mu\|) \leqslant \epsilon. \tag{20}$$

Then there exists a maximum allowable message transmission interval $T > 0$ such that for $T_m \leqslant T$, (8) holds.

Proof. The proof follows from the analysis presented in Ref. [11]. □

We note that some other factors such as finite resolution of simulations or experiments (e.g., A/D converters) may also contribute to the error bound given above, hence may affect T_m.

Remark 2. In Ref. [12], an occasional synchronization scheme based on impulsive coupling was proposed. More precisely, let the given chaotic system $\dot{u} = f(u)$ be decomposed as $\dot{u}_1 = f_1(u_1, u_2)$, $\dot{u}_2 = f_2(u_1, u_2)$. Let $\tau > 0$ be given and use a similar response system, i.e. $\dot{u}_{1r} = f_1(u_{1r}, u_{2r})$, $\dot{u}_{2r} = f_2(u_{1r}, u_{2r})$. Assume that $u_{1r}(0) = u_1(0)$, and $u_{2r}(0) = u_2(0) + \delta$, where δ is sufficiently small. For $t = n\tau, n = 1, 2, \ldots$, set externally $u_{1r}(n\tau) = u_1(n\tau)$, and for $t \neq n\tau$, use the response system given above. It was shown in Ref. [12] that for $\tau > 0$ sufficiently small, synchronization is possible. To see that the coupling is impulsive, we write $\dot{u}_{1r} = f_1(u_{1r}, u_{2r}) + s(t)(u_1 - u_{1r})$ where $s(t) = \sum_{n=0}^{\infty} \delta(t - n\tau)$, and $\delta(\cdot)$ is the Dirac delta function. If we formally integrate this equation in $[n\tau_-, n\tau_+]$, we obtain (formally) $u_{1r}(n\tau_+) = u_1(n\tau)$. We note that in our scheme the switching signal is a square wave which is drastically different from an impulse, and we do not make any assumptions on initial conditions. Consequently, the results presented in Ref. [12] and here cannot be deduced from each other. Moreover, the length of the synchronization interval $T_s > 0$ is of crucial importance for our scheme, and our results do not hold for $T_s = 0$, see (16), (17). Also note that when $s(t) = 1$, i.e. a unit step, our scheme for synchronization is the same as the scheme in Refs. [8,9].

3. Simulation results

For an application of the ideas given above, we consider the well-known Lorenz system for the drive system, see Ref. [2]. Since the state variables of Lorenz equations may vary in a wide dynamical range, for simulation purposes following Ref. [8], we use the following "scaled" Lorenz system,

$$\begin{aligned} \dot{x} &= \sigma(y - x)\,, \\ \dot{y} &= -20xz + rx - y\,, \\ \dot{z} &= 5xy - bz\,. \end{aligned} \tag{21}$$

We choose the parameters σ, r and b so that the Lorenz system (21) is in the chaotic regime. The solution $x(t)$ of (21) will be used to synchronize the solutions of the following response system, see Ref. [8],

$$\begin{aligned} \dot{x}_r &= \sigma(y_r - x_r)\,, \\ \dot{y}_r &= -20x_r z_r + rx_r - y_r + s(t)(-20z_r + r)(x - x_r)\,, \\ \dot{z}_r &= 5x_r y_r - bz_r + 5s(t)y_r(x - x_r)\,. \end{aligned} \tag{22}$$

In our notation we have $u = (x\ y\ z)^{\mathrm{T}}$, $w = (x_r\ y_r\ z_r)^{\mathrm{T}}$, $o = x$, hence we have $c = (1\ 0\ 0)^{\mathrm{T}}$. Note that (22) is of the form (2) with $K(w) = (0 - 20z_r + r\ \ 5y_r)^{\mathrm{T}}$. Moreover, when $s(t) = 1$, (22) becomes

$$\begin{aligned} \dot{x}_r &= \sigma(y_r - x_r)\,, \\ \dot{y}_r &= -20xz_r + rx - y_r\,, \\ \dot{z}_r &= 5xy_r - bz_r\,, \end{aligned} \tag{23}$$

which is the response system used in Refs. [2,8]. By using a suitable Lyapunov function, it could be shown that (21) and (22) synchronize exponentially fast, i.e. (3) holds, see e.g. Refs. [11,13,14].

For longer messages we could choose the synchronization interval T_s sufficiently long so that the error made in the signal recovery is arbitrarily small. Alternatively, we could divide the message into smaller parts, if possible, and send each part in a message transmission phase, followed by a synchronization phase.

Next we present some numerical simulation results which indicate that the suggested method can be used for successful message transmission and recovery. In the first two simulations, we considered the ideal case (i.e., no noise and no parameter mismatch). In the first simulation, as the message to be sent, we used the speech signals corresponding to the sounds of letters "A" and "B". This message is obtained by using the sound tools available in Sun Sparcstations. In this simulation, we use $\sigma = 10$, $r = 20$, $b = 1$, $T_s = 15$ sec. and $T_m = 20$ sec. This message is recovered with good listening quality. The simulation results can be seen in Fig. 1. In the second simulation, the message to be

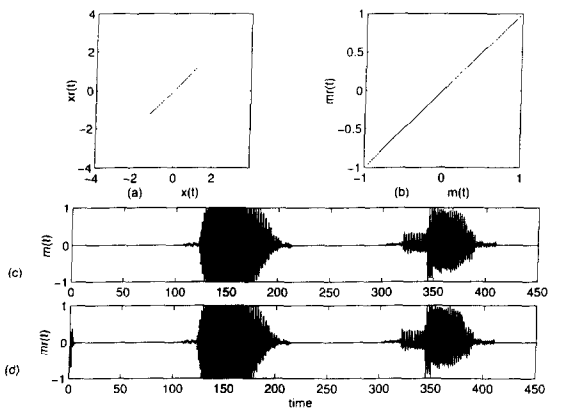

Fig. 1. Transmission of sounds "A" and "B" was received with perfect listening quality. (a) Drive versus response signals; (b) transmitted versus recovered messages (data was plotted after transient time); (c) transmitted message versus time; (d) received message versus time.

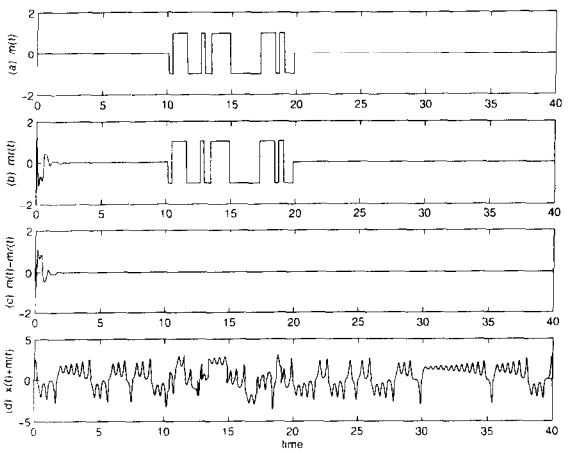

Fig. 2. (a) Transmitted message; (b) recovered message; (c) error in message recovery; (d) signal transmitted to the receiver.

sent is the coded version of the word "chaos". For coding, we used the standard international alphabet code no. 2, see e.g. Ref. [16]. As it is seen in Fig. 2, message recovery is very successful. In this experiment, we choose $\sigma = 16$, $r = 46$, $b = 4$, $T_s = 10$ sec. and $T_m = 10$ sec. In both simulations, message amplitude is not small as compared to that of the drive signal. The message level is not important in this case, with arbitrary message levels one can recover the message successfully. In Fig. 2d, the signal transmitted to the receiver is also plotted. As can be seen, although the message level is comparable to that of the chaotic carrier, it is well masked, and the switching instances are not detectable. Most of the message transmission techniques proposed in the literature require that the message level be sufficiently smaller than the chaotic signal level, and this may be a problem when noise is also present, since then the message level should also be sufficiently bigger than the noise level for successful message recovery. Our aim in these simulations is to show that even if the message level is comparable with the chaotic signals, one can still recover the message successfully in our scheme.

In the remaining simulations we considered the nonideal case. For the noise, we used Gaussian noise with zero mean (and scaled magnitude), generated by computer. In the third simulation, we considered the transmission of the sentence "wish you good luck" in the nonideal case. This sentence is coded by using the same code used above. To show the arbitrariness of the message level, this time we chose the maximum message level as 0.05 and we considered both noise and parameter mismatch. Since in this case we could not send arbitrarily long messages in our scheme, we divided the message into four parts, and sent each word in one message transmission interval, which is then followed by another synchronization interval. We use $\sigma = 10$, $r = 20$, $b = 1$, $T_s = 25$ sec., $T_m = 30$ sec. for the following simulations. For the noise amplitude and the parameter mismatch, we considered two cases. In the first case, noise amplitude is scaled to 10^{-5} and all parameters are changed by 0.02% in the response system (i.e., multiplied by 1.0002). The results are given in Figs. 3a,d. As can be seen, the message is recovered successfully. In the second case, noise amplitude is scaled to 10^{-3} and all parameters are changed by 0.2% in the response system. The results are given in Figs. 3b,e. We also performed various simulations with bigger noise and parameter mismatch values. According to these simulations, as those values become bigger, we could still recover the message with sufficient accuracy by increasing T_s and decreasing T_m. Obviously, the message level should be sufficiently bigger than the noise level.

4. Conclusion

In this paper we considered a chaotic masking scheme by using synchronized chaotic systems. As in

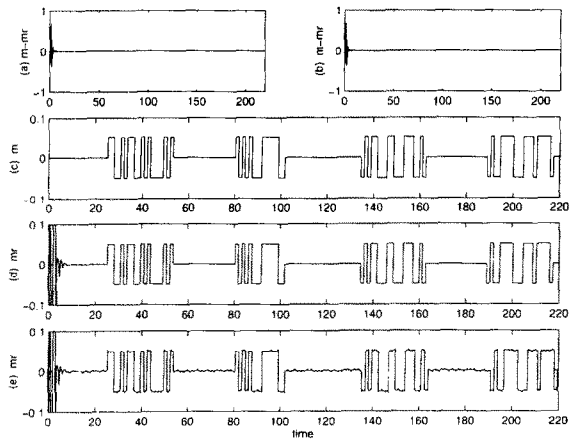

Fig. 3. (a) Error in message recovery for case 1 ($n_m = 10^{-5}$, $p = 0.02\%$ parameter mismatch); (b) error in message recovery for case 2 ($n_m = 10^{-3}$, $p = 0.02\%$); (c) transmitted message; (d) recovered message for case 1; (e) recovered message for case 2.

most synchronization schemes, we assume that a drive system generates chaotic signals and some of these signals are used in the response system for synchronization. In our scheme, communication is divided into synchronization and message transmission intervals, and while the drive and the response systems are only synchronized in the synchronization interval, the message is only sent and recovered in the message transmission interval. In the latter interval, the response system is switched to an autonomous system, and we showed that under certain conditions one can recover the message successfully. We note that the proposed technique is quite general and could be used with any synchronized chaotic system, as long as the stated assumptions hold. We presented some theoretical and simulation results indicating that the proposed technique may be used in some applications.

We did not investigate the security of our scheme. In Ref. [17], the security of communication schemes based on chaotic carriers when the hidden information signal is buried at the order of -30 dB with respect to the chaotic carrier were analyzed and it was concluded that such systems may be useful to increase privacy, but may not provide a high level of security. It was also concluded in Ref. [17] that the hidden signals added to the chaotic carrier at low power make it even easier to recover the hidden signal. We do not claim any level of security for our scheme, and probably the conclusions of Ref. [17] apply to our scheme as well when the message level is low. But we note that our results are independent of the message level, whereas in most of the chaotic masking schemes the message level is required to be sufficiently lower than that of the chaotic carrier. In view of the results of Ref. [17], the flexibility in adjusting the message level might improve the security of our scheme. However, this point requires further research.

We also did not consider the problem of synchronization of the switching signal $s(t)$ between the drive and the response systems. Since $s(t)$ is a periodic signal, oscillators which generate the same $s(t)$ could be built, tuned and used at transmitter and receiver. Such oscillators could be triggered by a signal transmitted through the data channel prior to communication, preferably several periods before the actual transmission. Other schemes may also be possible, but since this is not our main aim, we do not discuss this problem in detail here.

Several improvements on the scheme proposed in this paper are possible. The estimate given by (15) appears to be very conservative. Instead of using the Lipschitz constant k_u in (15), one might use an appropriate Lyapunov exponent associated with the drive system, cf. (10), (12). Then, by choosing the parameters (i.e., σ, b, r) appropriately, one might obtain small positive Lyapunov exponents. This may affect the maximum message transmission interval T_m. We expect that as the positive Lyapunov exponents become smaller, T_m becomes larger. An optimum relation between T_s and T_m may also be obtained. The relations between the Lyapunov exponents, intervals T_s, T_m and the security level of our scheme should also be analyzed. An electronic circuit implementation may also be possible, see Ref. [8]. Work along these lines is in progress and the results will be presented elsewhere.

References

[1] L.M. Pecora, T.L. Carroll, Phys. Rev. Lett. 64 (1990) 821.
[2] L.M. Pecora, T.L. Carroll, Phys. Rev. A 44 (1991) 2374.
[3] L.O. Chua, L. Kocarev, K. Eckert, Int. J. Bifurcation Chaos 2 (1992) 705.
[4] M.J. Ogorzalek, IEEE Trans. Circuits Syst. 40 (1993) 693.
[5] L. Kocarev, K.S. Halle, K. Eckert, L.O. Chua, Int. J. Bifurcation Chaos 2 (1992) 709.
[6] C.W. Wu, L.O. Chua, Int. J. Bifurcation Chaos 3 (1993) 1619.

[7] K.S. Halle, C.W. Wu, M. Itoh, L.O. Chua, Int. J. Bifurcation Chaos 3 (1993) 469.
[8] K.M. Cuomo, A.V. Oppenheim, Phys. Rev. Lett. 71 (1993) 65.
[9] K.M. Cuomo, A.V. Oppenheim, S.H. Strogatz, IEEE Trans. Circuits Syst. 40 (1993) 626.
[10] L. Kocarev, U. Parlitz, Phys. Rev. Lett. 74 (1995) 5028.
[11] Ö. Morgül, M. Feki, Phys. Rev. E 55 (1997) 5004.
[12] R.E. Amritkar, N. Gupte, Phys. Rev. E 47 (1993) 3889.
[13] Ö. Morgül, E. Solak. Phys. Rev. E 54 (1996) 4803.
[14] Ö. Morgül, E. Solak. Int. J. Bifurcation Chaos 7 (1997) 1307.
[15] H.K. Khalil, Nonlinear Systems (Macmillan, New York, 1992) pp. 180–208.
[16] W.D. Gegg, Analog and Digital Communication (Wiley, New York, 1977) p. 526.
[17] K.M. Short, Int. J. Bifurcation Chaos 4 (1994) 959.