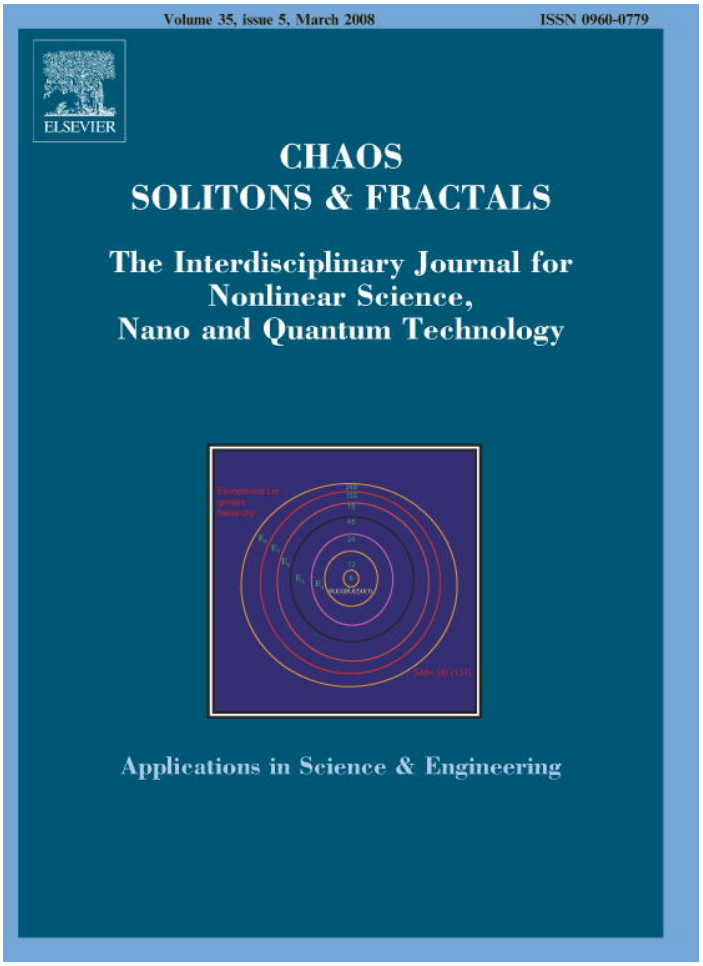

Available online at www.sciencedirect.com
ScienceDirect
Chaos, Solitons and Fractals 35 (2008) 871–877
CHAOS SOLITONS & FRACTALS
www.elsevier.com/locate/chaos

Encryption and decryption of information in chaotic communication systems governed by delay-differential equations

M.D. Prokhorov *, V.I. Ponomarenko

Saratov Branch of the Institute of Radio Engineering and Electronics of Russian Academy of Sciences, Zelyonaya Street, 38, Saratov 410019, Russia

Accepted 26 May 2006

Abstract

We consider different ways for encryption and decryption of information in communication systems using chaotic signal of a time-delay system as a carrier. A method is proposed for extracting a hidden message in the case when the parameters of the chaotic transmitter are a priori unknown. For different configurations of the transmitter the procedure of information signal extraction from the transmitted signal is demonstrated using numerical data produced by nonlinear mixing of the chaotic signal of the Mackey–Glass system and frequency-modulated harmonic signal.

1. Introduction

The discovery of the phenomenon of synchronization in chaotic systems [1] has given rise to active development of secure communication methods using chaotic signal as a carrier [2–5]. Chaotic communication systems are particularly attractive due to the broadband power spectrum of chaotic signals, high rates of information transmission, and efficiency at sufficiently low signal-to-noise ratio. Besides, many chaotic communication schemes are simply realized and demonstrate a rich variety of different oscillating regimes. However, many chaotic communication schemes are not as secure as expected and can be successfully unmasked [6–10]. To improve the security of data transmission it has been proposed to employ time-delay systems demonstrating chaotic dynamics of a very high dimension [11–17]. However, even in communication schemes using masking chaotic signals of time-delay systems the hidden message can be extracted in certain cases by an eavesdropper [18–20].

In this paper we consider various ways of information encoding in communication schemes based on time-delay systems and propose a technique for extracting a hidden message in the case when the transmitter parameters are unknown.

* Corresponding author. Tel.: +7 8452 511 180; fax: +7 8452 261 156.
E-mail address: sbire@sgu.ru (M.D. Prokhorov).

0960-0779/$ - see front matter
doi:10.1016/j.chaos.2006.05.081

2. Communication schemes with nonlinear mixing of information signal and time-delay system signal

A block diagram of a transmitter, representing the ring system composed of delay, nonlinear, and inertial elements, is shown in Fig. 1. For the case when the filter is a low-frequency first-order filter, this transmitter is described in the absence of information signal by the delay-differential equation

$$\varepsilon_0 \dot{x}(t) = -x(t) + f[x(t-\tau_0)], \tag{1}$$

where $x(t)$ is the system state at time t, function f defines nonlocal correlations in time, τ_0 is the delay time, and parameter ε_0 characterizes the inertial properties of the system. The information signal $m(t)$ can be injected into the ring system (1) at different points denoted in Fig. 1 by the numerals I–III. Depending on the point at which the message signal is injected into the feedback circuit of the transmitter, the system's dynamics is governed by one of the following equations:

$$\varepsilon_0 \dot{x}(t) = -x(t) + f[x(t-\tau_0) + m(t-\tau_0)], \tag{2}$$

$$\varepsilon_0 \dot{x}(t) = -x(t) + f[x(t-\tau_0) + m(t)], \tag{3}$$

$$\varepsilon_0 \dot{x}(t) = -x(t) + f[x(t-\tau_0)] + m(t). \tag{4}$$

Eq. (2) corresponds to the case when the signal $m(t)$ is injected into the transmitter at the point I. The cases of information signal injection at the points II and III are described by Eqs. (3) and (4), respectively. With this nonlinear mixing the information signal is directly involved in the formation of a complicated dynamics of the chaotic system. The signal $s(t)$ transmitted into the communication channel can be also taken from different points of the ring system indicated in Fig. 1 by the numerals 1–3. Thus, there are nine different ways for realizing the transmitter depicted in Fig. 1.

Similar approach for the information encryption in delayed nonlinear feedback systems has been considered in [14]. The possibility of the message signal recovery at the receiver was discussed in [14] for different ways of the information signal injection into the time-delay system and different output points of the transmitter. The configuration and the parameters of the transmitter were assumed to be known to the authorized receiver. Nevertheless, in a number of cases the message recovery required processing of the signal at the receiver output, including determination of the reciprocal function of the nonlinear element. Since the transfer function of a nonlinear element is not necessarily one-to-one, this transformation may be incorrect. In such cases, we suggest using an approximate approach for recovering the information signal. This approach allows one to avoid inverse transformation. Moreover, using our method the information signal can be extracted from the transmitted signal $s(t)$ even in the case when the transmitter parameters are a priori unknown.

Let us consider different configurations of the transmitter shown in Fig. 1 and determine the corresponding signals at the output of the receiver being an identical copy of the transmitter. Fig. 2 illustrates the communication scheme based on the transmitter configuration denoted as III/1. In this case, with the help of a summator the information signal $m(t)$ is added at the point III to the chaotic signal of the transmitter whose dynamics is described by Eq. (4), and the signal $s(t) = x(t)$ is transmitted into the communication channel from the point 1. The receiver is composed of the same elements as the transmitter, except that the summator is replaced by a subtracter breaking the feedback circuit. The receiver equation is

$$\varepsilon_0 \dot{y}(t) = -y(t) + f[x(t-\tau_0)]. \tag{5}$$

At the output of the subtracter we have the signal $z(t) = x(t) - y(t)$.

The values of the signal $z(t)$ at the receiver output are presented in Table 1 for various configurations of the communication scheme. In the simplest cases I/1, II/2, and III/3, where the information signal is injected into the feedback circuit of the transmitter and simultaneously transmitted into the communication channel, we immediately have the

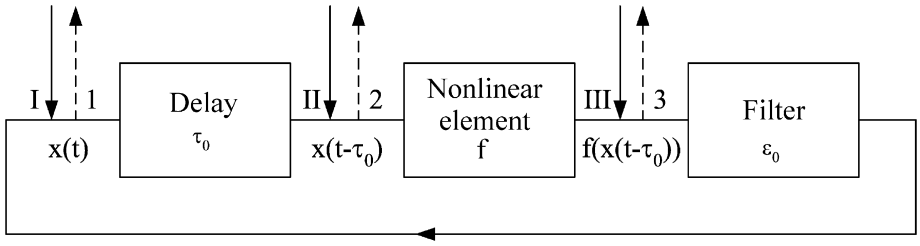

Fig. 1. Block diagram of a delayed nonlinear feedback system generating a chaotic signal. The numerals I–III indicate points where an information signal can be injected into the system. The numerals 1–3 indicate the output points of the transmitter.

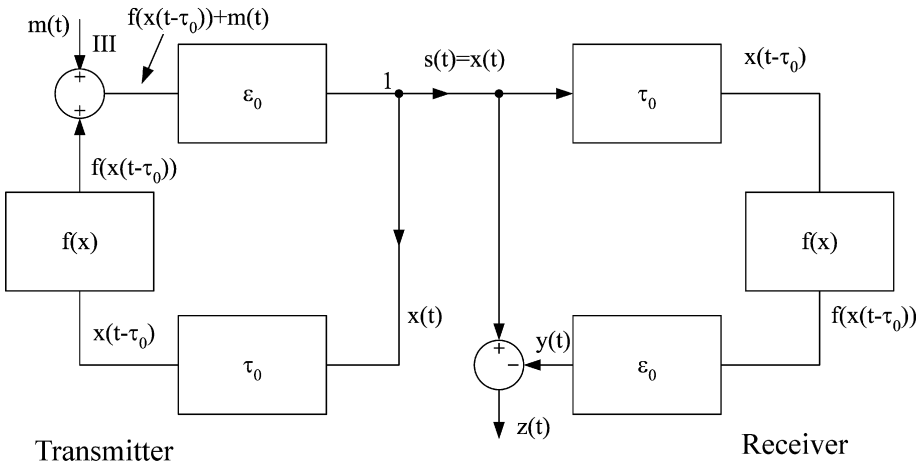

Fig. 2. Block diagram of the chaotic communication scheme for the case III/1.

Table 1
The difference signal $z(t)$ at the output of the receiver for different points of information signal injection into the feedback circuit of the transmitter and different points of the signal output

Input point	Output point		
	1	2	3
I	$m(t)$	$m(t-\tau_0)$	$f[x(t-\tau_0)+m(t-\tau_0)]-f[x(t-\tau_0)]$
II	$\varepsilon_0[\dot{y}(t)-\dot{x}(t)]+f[x(t-\tau_0)+m(t)]-f[x(t-\tau_0)]$	$m(t)$	$f[x(t-\tau_0)+m(t)]-f[x(t-\tau_0)]$
III	$x(t)-y(t)$	$x(t-\tau_0)-y(t-\tau_0)$	$m(t)$

extracted message signal $z(t)=m(t)$ at the output of the receiver. In these cases the quality of extraction of the message $m(t)$ does not depend on its amplitude and frequency characteristics. By this is meant that for the considered configurations the communication schemes allow one to transmit complicated information signals without distortion. For the case I/2 the information signal is also recovered accurately, but with the delay τ_0.

For the other five configurations of the communication scheme the procedure of the message signal extraction is more complicated since the processing of the signal $z(t)$ at the receiver output is required. For example, for recovering the information signal in the case III/1 depicted in Fig. 2, let us subtract Eq. (5) describing the dynamics of the receiver from Eq. (4) for the transmitter. The expression for $m(t)$ takes the form

$$m(t)=\varepsilon_0[\dot{x}(t)-\dot{y}(t)]-[x(t)-y(t)]. \tag{6}$$

Taking into account that $z(t)=x(t)-y(t)$, the information signal can be obtained from the signal at the receiver output as follows:

$$m(t)=\varepsilon_0\dot{z}(t)-z(t). \tag{7}$$

In a similar way one can recover the signal $m(t)$ for the case III/2:

$$m(t)=\varepsilon_0\dot{z}(t-\tau_0)-z(t-\tau_0). \tag{8}$$

In the communication system II/3 the difference signal at the output of the receiver is

$$z(t)=f[x(t-\tau_0)+m(t)]-f[x(t-\tau_0)]. \tag{9}$$

Assuming that the information signal $m(t)$ is small in comparison with $x(t)$, let us expand the first term in Eq. (9) in a Taylor series and restrict our consideration to the two first terms of the expansion:

$$f[x(t-\tau_0)+m(t)]\approx f[x(t-\tau_0)]+\frac{\mathrm{d}f[x(t-\tau_0)]}{\mathrm{d}x}m(t). \tag{10}$$

This assumption is justified because the level of information signal in the communication schemes with nonlinear mixing must be sufficiently low, otherwise the chaotic signal may not provide enough masking [4]. From Eqs. (9) and (10) we obtain

$$m(t) \approx \frac{z(t)}{\mathrm{d}f[x(t-\tau_0)]/\mathrm{d}x}. \tag{11}$$

Eq. (11) can be used also for approximate recovery of the message signal in the case I/3. However, the recovered message signal is delayed by τ_0 in this case.

For the case II/1 the message signal $m(t)$ can be approximately determined as follows:

$$m(t) \approx \frac{z(t)+\varepsilon_0\dot{z}(t)}{\mathrm{d}f[x(t-\tau_0)]/\mathrm{d}x}. \tag{12}$$

3. Recovery of information signal nonlinearly mixed with chaotic signal of the time-delay system

The security of chaotic communication systems is based on the assumption that the parameters of the chaotic transmitter are known only to the authorized receiver having an identical copy of the transmitter. However, a hidden message can be extracted by a third party having only the time series of the transmitted signal $s(t)$. To do this, one has to recover the parameters of the time-delay system (1) generating a masking chaotic signal. In this case the nonlinear function f and the parameters τ_0 and ε_0 are a priori unknown.

To reconstruct the parameters of the transmitter governed in the absence of message by delay-differential Eq. (1), we use the method proposed recently in [21]. This method is based on the statistical analysis of time intervals between extrema in the time series of time-delay systems and the projection of infinite-dimensional phase space of these systems to suitably chosen low-dimensional subspaces. The method allows one to reconstruct the model equation of a ring time-delay system from chaotic time series of various dynamical variables [$x(t)$, $x(t-\tau_0)$, or $f[x(t-\tau_0)]$ (see Fig. 1)] measured at different points of the system. The method is still efficient in the presence of message in the transmitted signal if the message signal has small amplitude. In this case the information signal can be considered as noise deteriorating the accuracy of the transmitter parameters estimation. We have found out that our technique of time-delay system recovery provides sufficiently accurate estimation of the system parameters for noise levels up to 10%. To ensure the security of message transmission, the level of information signal in the considered communication systems is usually much lower.

Successful recovery of hidden message without knowing the transmitter parameters was demonstrated in [19] for the simplest case I/1. In the present paper we illustrate the efficiency of our method for extracting a hidden message in the more complicated cases III/1 and II/3.

Let us consider a transmitting time-delay system described by the Mackey–Glass equation

$$\dot{x}(t) = -bx(t) + \frac{ax(t-\tau_0)}{1+x^c(t-\tau_0)}, \tag{13}$$

which can be converted to Eq. (1) with $\varepsilon_0 = 1/b$ and the function

$$f[x(t-\tau_0)] = \frac{ax(t-\tau_0)}{b[1+x^c(t-\tau_0)]}. \tag{14}$$

The parameters of the system (13) are chosen to be $a = 0.2$, $b = 0.1$, $c = 10$, and $\tau_0 = 300$ to produce a dynamics on a high-dimensional chaotic attractor. As an information signal nonlinearly mixed with the chaotic signal of the system (13), we use the frequency-modulated harmonic signal

$$m(t) = A\sin[2\pi f_c t - B\cos(2\pi f_m t)], \tag{15}$$

where A defines the message amplitude, f_c is the central frequency of the power spectrum of the signal, B is the frequency modulation index, and f_m is the modulation frequency.

Fig. 3 shows parts of the time series and the power spectra of the frequency-modulated signal $m(t)$ and the transmitted signal $s(t)$ for the communication scheme III/1. With a fourth-order Runge–Kutta method for delay-differential equations we record 50,000 points of $s(t)$ with the sampling interval $h = 1$. As it can be seen from Fig. 3, the amplitude of the information signal comprises about 1% of the amplitude of the chaotic carrier and the presence of message is not noticeable in the power spectrum of the transmitted signal $s(t)$.

To recover the delay time τ_0 of the transmitter we determine the extrema in the time series of $s(t)$ applying a local parabolic approximation, define for different values of time τ the number N of pairs of extrema separated in time by τ, and construct the $N(\tau)$ plot (Fig. 4(a)). The step of τ variation is set by 1. The time series exhibits about 3000 extrema

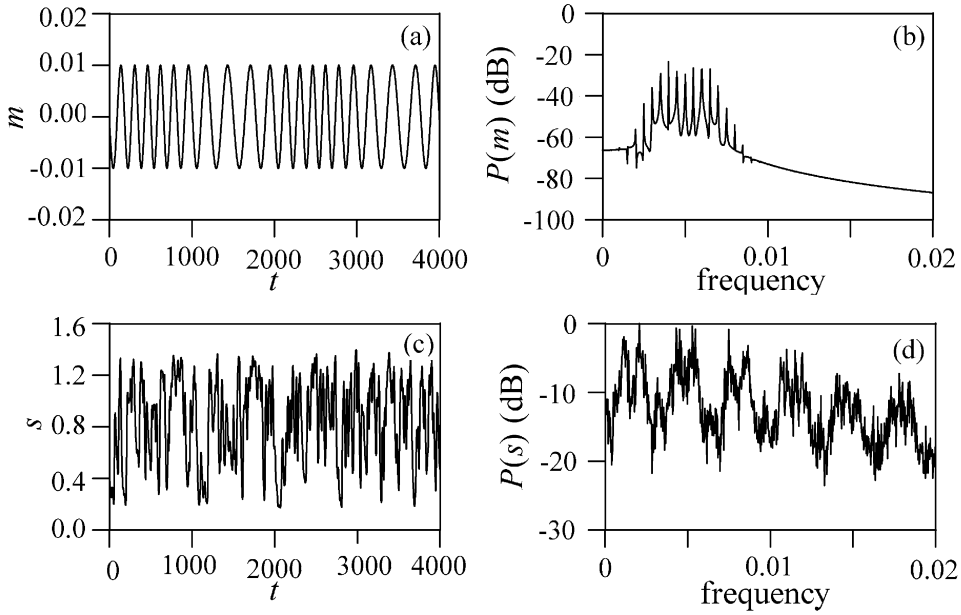

Fig. 3. (a) The frequency-modulated signal for $A = 0.01$, $B = 3$, $f_c = 5 \times 10^{-3}$, $f_m = 5 \times 10^{-4}$. (b) The power spectrum of the frequency-modulated signal $m(t)$. (c) The transmitted signal. (d) The power spectrum of the transmitted signal $s(t)$.

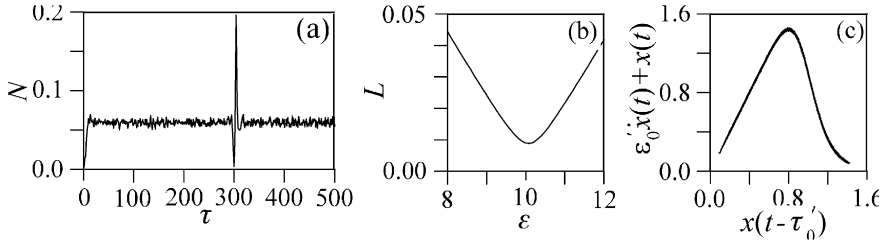

Fig. 4. Reconstruction of the transmitter parameters for the case III/1. (a) The $N(\tau)$ plot. $N_{\min}(\tau) = N(300)$. (b) The $L(\varepsilon)$ plot. $L_{\min}(\varepsilon) = L(10.1)$. (c) The recovered nonlinear function at $\tau_0' = 300$ and $\varepsilon_0' = 10.1$.

and $N(\tau)$ is normalized to their total number. It was shown in [21] that there are practically no extrema separated in time by the delay time in time series of a time-delay system. In Fig. 4(a) the absolute minimum of $N(\tau)$ is observed at $\tau_0' = 300$.

To recover the parameter ε_0 we calculate for different ε values the length L of a line connecting all points ordered with respect to abscissa in the plane $[x(t-\tau_0'), \varepsilon\dot{x}(t) + x(t)]$ and construct the $L(\varepsilon)$ plot (Fig. 4(b)) [21]. $L(\varepsilon)$ is normalized to the number of points in the plane. The $L(\varepsilon)$ plot, constructed with the step of ε variation equal to 0.1, demonstrates the minimum at $\varepsilon_0' = 10.1$ ($\varepsilon_0 = 1/b = 10$). The set of points constructed for the defined τ_0' and ε_0' in the plane $[x(t-\tau_0'), \varepsilon_0'\dot{x}(t) + x(t)]$ reproduces with a good accuracy the nonlinear function (14) of the Mackey–Glass equation (Fig. 4(c)). For the approximation of the recovered function we use a polynomial of degree 12.

After the transmitter parameters are determined, one can construct the receiver. The more accurate is the estimation of the system parameters, the higher is the quality of synchronous chaotic response of the receiver and, as a consequence, the higher is the quality of the message extraction. Part of the time series of the extracted frequency-modulated harmonic signal $m'(t)$ calculated using Eq. (7) is presented in Fig. 5(a). The power spectrum of this signal is shown in Fig. 5(b).

As another example, let us consider the recovery of the frequency-modulated signal (15) nonlinearly mixed with the chaotic signal of the Mackey–Glass system in the communication scheme II/3. The parameters of the information signal and the Mackey–Glass system are chosen the same as in the considered above case III/1. The temporal realization of the transmitted signal $s(t) = f[x(t-\tau_0) + m(t)]$ is qualitatively similar to the one shown in Fig. 3(c).

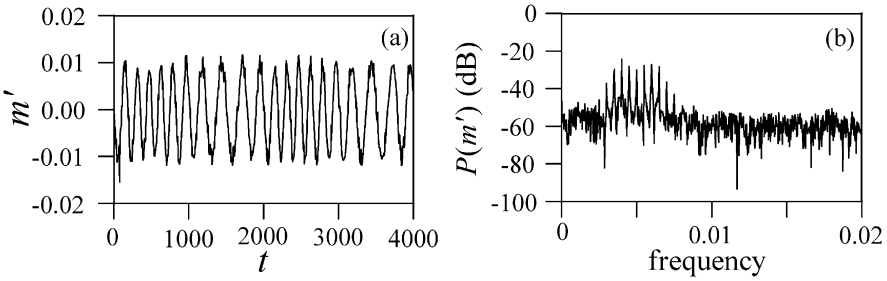

Fig. 5. (a) The extracted frequency-modulated harmonic signal for the communication scheme III/1. (b) The power spectrum of the extracted message signal.

For various τ values we count the number N of situations when $\dot{s}(t)$ and $\dot{s}(t-\tau)$ are simultaneously equal to zero and construct the $N(\tau)$ plot (Fig. 6(a)). The location of minimum of $N(\tau)$ allows us to define the delay time accurately, $\tau_0' = 300$.

To estimate the parameter ε_0 from time series of the dynamical variable measured between the nonlinear element and the filter (see Fig. 1), we exploit the method proposed in [21]. We filter the time series of $s(t)$ under variation of the filter cut-off frequency $\nu = 1/\varepsilon$ and plot $s(t)$ versus $u(t-\tau_0')$, where $u(t-\tau_0')$ is the signal at the filter output shifted by the time τ_0'. Then, we calculate the length L of a line connecting all points in the plane $[u(t-\tau_0'), s(t)]$ ordered with respect to $u(t-\tau_0')$ and construct the $L(\varepsilon)$ plot (Fig. 6(b)). For the step of ε variation equal to 0.1, the minimum of $L(\varepsilon)$ is observed at $\varepsilon_0' = 10.0$. For the filter cut-off frequency $\nu_0 = 1/\varepsilon_0$, in the absence of message $u(t-\tau_0) = x(t-\tau_0)$ and the set of points in the plane $\{x(t-\tau_0), f[x(t-\tau_0)]\}$ reproduces the function f. The nonlinear function recovered from $s(t)$ using the estimated τ_0' and ε_0' is shown in Fig. 6(c). We approximated the recovered function with a polynomial of degree 15.

Part of the time series of the extracted information signal calculated using formula (11) and the power spectrum of this extracted signal are presented in Fig. 7. From formula (11) it follows that the message signal may be recovered with a large error at the points where the derivative in the denominator is close to zero. This error can be reduced using frequency filtering of the recovered message signal.

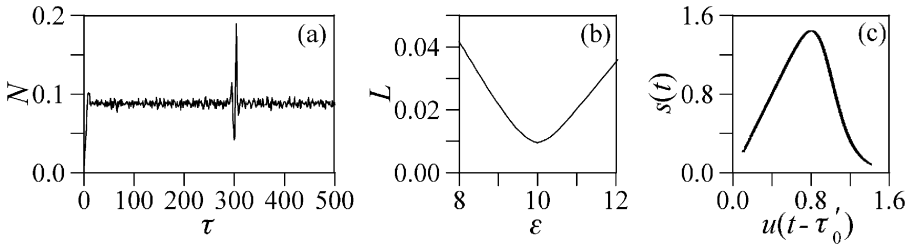

Fig. 6. Reconstruction of the transmitter parameters for the case II/3. (a) The $N(\tau)$ plot. $N(\tau)$ is normalized to the total number of extrema in the time series. $N_{\min}(\tau) = N(300)$. (b) The $L(\varepsilon)$ plot. $L(\varepsilon)$ is normalized to the number of points. $L_{\min}(\varepsilon) = L(10.0)$. (c) The recovered nonlinear function at $\tau_0' = 300$ and $\varepsilon_0' = 10.0$.

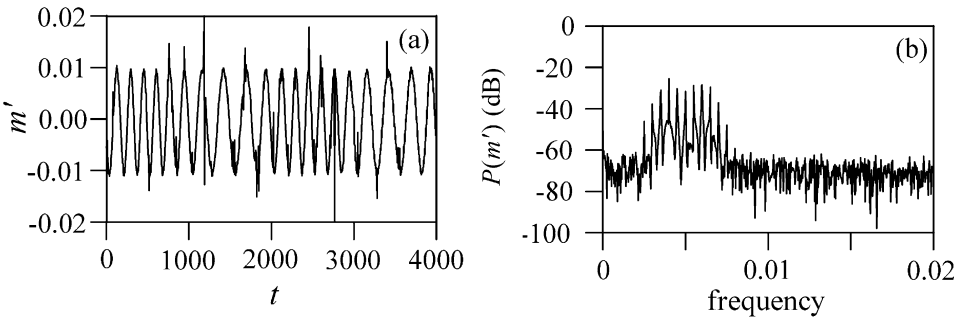

Fig. 7. (a) The extracted frequency-modulated harmonic signal for the communication scheme II/3. (b) The power spectrum of the extracted message signal.

4. Conclusion

We have considered different communication schemes with nonlinear mixing of information signal and chaotic signal of time-delay system. We have shown that in these communication systems the hidden message can be successfully extracted from the transmitted signal even in the case when the transmitter parameters are a priori unknown. The procedure of message extraction is based on the method of time-delay systems reconstruction. For different configurations of the transmitter and different measured dynamical variables this method allows one recover the model delay-differential equation of the transmitter from chaotic time series even in the presence of message signal of small amplitude. Thus, even chaotic communication systems with complicated configuration, where the information signal is injected into the feedback circuit of the transmitter with delay-induced dynamics at one point and transmitted into the communication channel from another point, can be successfully unmasked. The extraction of hidden message from the transmitted signal is demonstrated for different configurations of the transmitter for the case of mixing of chaotic signal of the Mackey–Glass system and frequency-modulated harmonic signal. A possible way to improve the level of security of the considered chaotic communication systems is to use modulation of their parameters or to employ high-dimensional time-delay systems.

Acknowledgements

The authors thank B.P. Bezruchko for stimulating discussions. This work is supported by the Russian Foundation for Basic Research, Grant No. 06-02-16619. M.D.P. was supported by INTAS, Grant No. 03-55-920.

References

[1] Pecora LM, Carroll TL. Synchronization in chaotic systems. Phys Rev Lett 1990;64:821–4.
[2] Kocarev L, Halle KS, Eckert K, Chua LO, Parlitz U. Experimental demonstration of secure communications via chaotic synchronization. Int J Bifurcat Chaos 1992;2:709–13.
[3] Cuomo KM, Oppenheim AV. Circuit implementation of synchronized chaos with applications to communications. Phys Rev Lett 1993;71:65–8.
[4] Dmitriev AS, Panas AI, Starkov SO. Experiments on speech and music signals transmission using chaos. Int J Bifurcat Chaos 1995;5:1249–54.
[5] Pecora LM, Carroll TL, Johnson GA, Mar DJ, Heagy JF. Fundamentals of synchronization in chaotic systems, concepts, and applications. Chaos 1997;7:520–43.
[6] Pérez G, Cerdeira HA. Extracting messages masked by chaos. Phys Rev Lett 1995;74:1970–3.
[7] Short KM. Signal extraction from chaotic communications. Int J Bifurcat Chaos 1997;7:1579–97.
[8] Zhou C-S, Chen T-L. Extracting information masked by chaos and contaminated with noise: some considerations on the security of communication approaches using chaos. Phys Lett A 1997;234:429–35.
[9] Yang T, Yang L-B, Yang C-M. Breaking chaotic secure communication using a spectrogram. Phys Lett A 1998;247:105–11.
[10] Álvarez G, Montoya F, Pastor G, Romera M. Breaking a secure communication scheme based on the phase synchronization of chaotic systems. Chaos 2004;14:274–8.
[11] Pyragas K. Transmission of signals via synchronization of chaotic time-delay systems. Int J Bifurcat Chaos 1998;8:1839–42.
[12] Mensour B, Longtin A. Synchronization of delay-differential equations with application to private communication. Phys Lett A 1998;244:59–70.
[13] Goedgebuer J-P, Larger L, Porte H. Optical cryptosystem based on synchronization of hyperchaos generated by a delayed feedback tunable laser diode. Phys Rev E 1998;80:2249–52.
[14] Udaltsov VS, Goedgebuer J-P, Larger L, Rhodes WT. Communicating with optical hyperchaos: information encryption and decryption in delayed nonlinear feedback systems. Phys Rev Lett 2001;86:1892–5.
[15] Li C, Liao X, Wong K. Chaotic lag synchronization of coupled time-delayed systems and its applications in secure communication. Physica D 2004;194:187–202.
[16] Kye W-H, Choi M, Kim C-M, Park Y-J. Encryption with synchronized time-delayed systems. Phys Rev E 2005;71:045202.
[17] Bai E-W, Lonngren KE, Uçar A. Secure communication via multiple parameter modulation in a delayed chaotic system. Chaos, Solitons & Fractals 2005;23:1071–6.
[18] Zhou C, Lai C-H. Extracting messages masked by chaotic signals of time-delay systems. Phys Rev E 1999;60:320–3.
[19] Ponomarenko VI, Prokhorov MD. Extracting information masked by the chaotic signal of a time-delay system. Phys Rev E 2002;66:026215.
[20] Udaltsov VS, Goedgebuer J-P, Larger L, Cuenot J-B, Levy P, Rhodes WT. Cracking chaos-based encryption systems ruled by nonlinear time delay differential equations. Phys Lett A 2003;308:54–60.
[21] Prokhorov MD, Ponomarenko VI, Karavaev AS, Bezruchko BP. Reconstruction of time-delayed feedback systems from time series. Physica D 2005;203:209–23.