ISSN 1063-7850, Technical Physics Letters, 2012, Vol. 38, No. 1, pp. 51–54.

Hidden Data Transmission Based on Time-Delayed Feedback System with Switched Delay Time

V. I. Ponomarenko, A. S. Karavaev, E. E. Glukhovskaya, and M. D. Prokhorov*

Institute of Radio Engineering and Electronics (Saratov Branch), Russian Academy of Sciences, Saratov, 410019 Russia
**e-mail: mdprokhorov@yandex.ru*

Received August 3, 2011

Abstract—A scheme of hidden data transmission based on time-delayed feedback system with switched delay time is described. Efficiency of the proposed system and high resistance to interference in the communication channel is demonstrated in numerical experiments on model ring systems with time-delayed feedback.

DOI: 10.1134/S1063785012010129

The discovery of the phenomenon of synchronization of chaotic oscillations between interacting dynamical systems [1] made possible the development of new methods of hidden data transmission based on the use of various types of chaotic synchronization (identical, lag, phase, generalized, etc.) [2–9]. Various schemes of transmitting informative signals using the synchronization of chaotic dynamical systems have been proposed, including chaotic masking [2], switching of chaotic regimes [3], nonlinear mixing of informative and chaotic signals [4], modulation of transmitter parameters in combination with adaptive recept [6], etc. However, it turned out that many communication systems employing chaotic signals can in fact ensure only limited security [10, 11]. In order to increase the level of data protection, it was suggested [12–15] to employ hidden data transmission using systems with time-delayed feedback, which ensure chaotic dynamics of very high dimension.

This Letter describes a scheme of hidden data transmission based on a chaotic oscillator with time-delayed feedback, which employs the principle of delay time switching in the transmitter and the informative signal extraction in the receiver with the aid of two different time-delayed feedback systems.

Figure 1 shows a block diagram of the proposed data transmission system. The transmitter represents a ring system comprising two delay lines characterized

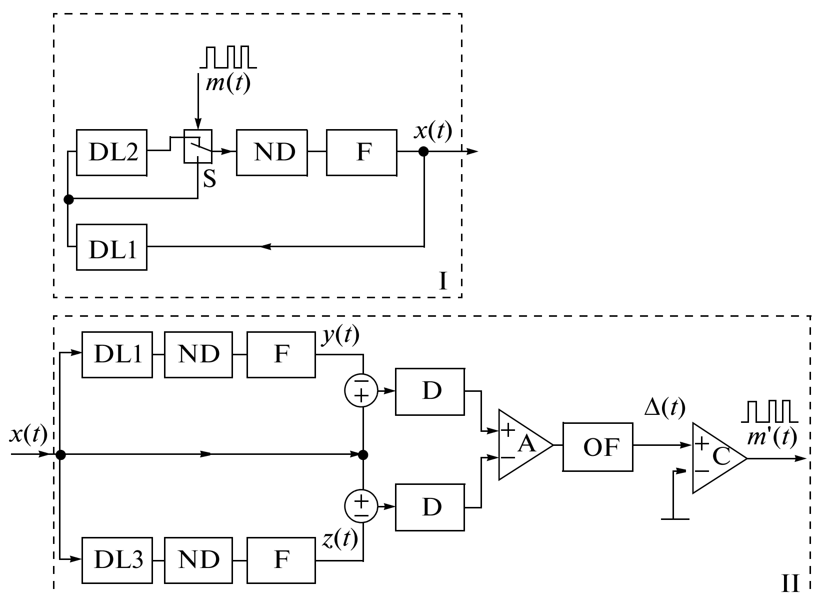

Fig. 1. Block diagram of the hidden data transmission system with switched delay time: (I) transmitter; (II) receiver; (DL1, DL2, DL3) delay lines; (ND) nonlinear elements; (F) filters; (S) switch (commutator); (D) detector; (A) differential amplifier; (OF) output filter; (C) comparator.

by delay times τ_1 and τ_2, a nonlinear element, and linear low-frequency filter, which generates a chaotic signal. The informative signal is a binary code $m(t)$ representing a sequence of binary units and zeros. This informative signal controls a commutator that switches the delay time so that binary zeros are transmitted when $\tau = \tau_1$ and binary units are transmitted when $\tau = \tau_1 + \tau_2$. This transmitter is described by the following first-order delay-differential equation:

$$\varepsilon\dot{x}(t) = -x(t) + f(x(t-(\tau_1 + m(t)\tau_2))), \qquad (1)$$

where $x(t)$ is the system state at time t, f is a nonlinear function, and ε is a parameter that characterizes the inertia of the system. Thus, the informative signal controls the parameters of the transmitter and determines properties of the signal transmitted into the communication channel. Note that, for the sake of secure data transmission, the transmitted signals must possess identical spectral and statistical properties for $\tau = \tau_1$ and $\tau = \tau_1 + \tau_2$.

The receiver consists of two driven time-delay subsystems, one of which contains a delay line with delay time τ_1 and the other—with delay time $\tau_3 = \tau_1 + \tau_2$ (Fig. 1). The parameters of filters and nonlinear elements in the two subsystems are identical to the corresponding values in the transmitter. A subtractor that is situated after the filter breaks the feedback circuit in each driven subsystem. The input signal for each time-delay subsystem in the receiver is the chaotic carrier $x(t)$ of the transmitter. These systems are descried by the following equations:

$$\varepsilon\dot{y}(t) = -y(t) + f(x(t-\tau_1)), \qquad (2)$$

$$\varepsilon\dot{z}(t) = -z(t) + f(x(t-\tau_3)). \qquad (3)$$

The parameters of transmitter and receiver must be chosen so as to ensure that the synchronization with $x(t)$ at every moment of time could take place for only one of the two driven subsystems. When binary zero is transmitted (i.e., delay time in the transmitter is τ_1) the input signal $x(t)$ is synchronized with the output signal $y(t)$ of the first time-delay subsystem in the receiver. In the absence of noise in the communication channel, the synchronization results in $x(t) = y(t)$ and the output signal of subtractor of the first driven subsystem is zero. At the same time, synchronization between $x(t)$ and the output signal $z(t)$ of the second time-delay subsystem in the receiver is absent. Since $x(t) \neq z(t)$, the output signal of subtractor of the second driven subsystem is nonzero. On the contrary, when binary unity is transmitted (i.e., delay time in the transmitter is τ_3), then $x(t) \neq y(t)$ and $x(t) = z(t)$. As a result, the output signal of subtractor of the first driven subsystem is nonzero and of subtractor of the second driven subsystem is zero.

The above principle is employed in most of the well-known communication systems with switching of chaotic regimes [5, 7]. The presence of synchronization between $x(t)$ and the first (or single) driven subsystem in the receiver corresponds to the transmission of binary zero and the absence of this synchronization corresponds to the transmission of binary unity. However, the presence of noise (interference) hinders the establishment of identical synchronization between the transmitter and receiver. As a result, the output signals of subtractors in driven subsystems are always nonzero, which makes recovery of the transmitted binary sequence a difficult task.

In order to increase the stability of our system in the presence of noise, we have introduced some new elements: two amplitude detectors, differential amplifier, output filter , and comparator (Fig. 1). The output signal of each detector represents the modulus of an envelope of the input difference signal. Then, the output signals of detectors are subtracted and smoothed by a low-frequency filter, the output signal of which is $\Delta(t)$. The comparator transforms $\Delta(t)$ into a restored informative signal $m'(t)$, so that the output signal is binary zero for $\Delta(t) \leq 0$ and binary unity otherwise.

After this modification of the data transmission system, its stability with respect to noises present in the communication channel significant increases as compared to the well-known schemes with switching of chaotic regimes. Let us qualitatively consider what happens when an additive noise is introduced into a chaotic signal in the communication channel. Assuming that the informative, chaotic (masking), and noise signals can be considered as independent random processes, we conclude that the dispersion of signals at the output of each detector will increase by a value equal to the dispersion of the additive noise. Therefore, the averaged difference of signals at the output of detectors will have the same sign as that in the absence of noise and, hence, the informative signal will be exactly restored. However, these considerations are only qualitative. In real practice, the chaotic signal and additive noise after passing through elements of the receiver may acquire a correlation (dependent on the system parameters) and, in addition, nonlinearity present in the receiver violates the principle of superposition. However, strict determination of the limits of reliability of the proposed scheme in the presence of noise presents a separate problem that falls beyond the scope of the present study.

Operation of the proposed hidden data transmission scheme can be illustrated by the results of numerical experiments. The transmitter was represented by a time-delayed feedback oscillator with a quadratic nonlinearity of the type $f(x) = \lambda - x^2$, where λ is the nonlinearity parameter, and a low-frequency filter representing a first-order Butterworth filter with cutoff frequency f_c. The parameters of the transmitter were as follows: $\tau_1 = 1000$; $\tau_2 = 10$; $\lambda = 1.8$; $f_c = 0.005$ ($\varepsilon = 200$). With these parameters, the transmitter generates a chaotic signal. In the receiver, the first time-delay subsystem is characterized by $\tau_1 = 1000$, while the second subsystem has delay time $\tau_3 = 1010$ and both have $\lambda = 1.8$ and $f_c = 0.005$. The output filter in the receiver represents a low-frequency eighth-order Butterworth

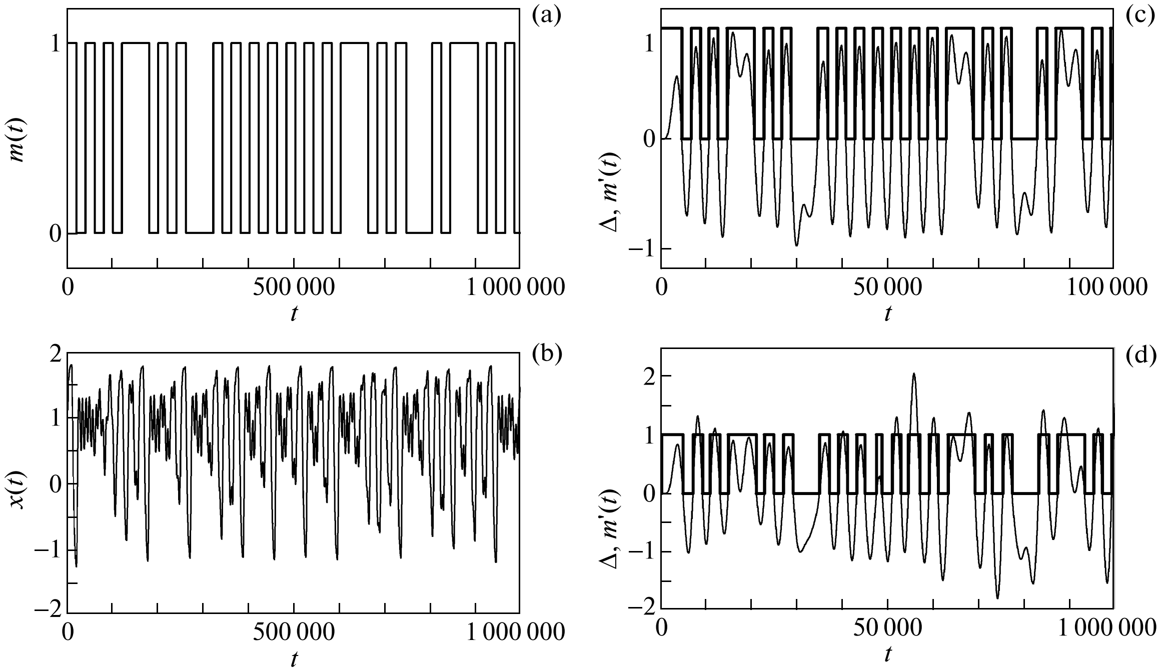

Fig. 2. Operation of the proposed system of hidden data transmission as illustrated by fragments of (a) time series of informative binary signal $m(t)$; (b) time series of the transmitted chaotic signal $x(t)$ in the communication channel; (c) time series of $\Delta(t)$ signal (thin solid curve) and $m'(t)$ signal (thick solid curve) in the absence of noise, and (d) same time series in the presence of 100% noise.

filter with cutoff frequency $f_r = 0.0002$. The informative signal $m(t)$ represented a sequence of binary zeros and units.

Figure 2a shows a time series of the transmitted informative signal, while Fig. 2b presents a fragment of the chaotic signal $x(t)$ that enters the communication channel. Since the values of τ_1 and τ_3 are close to each other, the corresponding fragments of $x(t)$ time series are visually indistinguishable, so that it is extremely difficult to determine which binary symbol (zero versus unity) is transmitted. Figure 2c shows the time series of a signal at the output of the filter in the receiver (thin solid curve) and the informative signal $m'(t)$ as restored at the receiver output (thick solid curve). A comparison of the signals in Figs. 2a and 2c shows that the informative signal is restored exactly, but with some delay. The magnitude of this delay depends on the delay times of system components and the parameters of the output filter in the receiver.

For the numerical investigation of stability of the proposed system with respect to noises in the communication channel, we have added a Gaussian noise with zero mean to the transmitted chaotic signal $x(t)$. Figure 2d shows the results of extraction of a hidden communication in the case where the dispersion of the additive noise was equal to that of the chaotic carrier (i.e., 100% noise level), where the time series of $\Delta(t)$ is shown by a thin solid curve and the $m'(t)$ signal is represented by the thick solid curve. As can be seen, despite the very high noise level, the quality of informative signal restoration is quite good.

It should be noted that the proposed communication scheme is, like all other systems with switching of chaotic regimes, characterized by certain limitation of the data transmission rate. This is related to transient processes that take place after every switching of the chaotic regime. Indeed, after every change in the delay time, of the transmitter a definite time is required for establishing synchronism between the transmitter and one of the two driven time-delay systems in the receiver. The rate of data transmission can be increased by decreasing the characteristic temporal scales of the system. On the other hand, in contrast to other communication schemes with switching chaotic regimes, which employ transmitters based on finite-dimensional systems, the proposed scheme ensures higher security because it is implemented on the time-delay subsystems that possess infinite number of the degrees of freedom.

Another obvious advantage of the proposed scheme of secure data transmission is its high stability of operation in the presence of noises in the communication channel. Numerical simulations have demonstrated that the quality of restoration of the hidden informative signal remains high even if the noise intensity is comparable with the level of a chaotic carrier.

Acknowledgments. This study was supported in part by the Russian Foundation for Basic Research (project no. 10-02-00980) and the Ministry of Science and Education of the Russian Federation within the framework of the Analytical Targeted Program "Development of the Scientific Potential of Higher Education" (project no. 2.1.1/1738).

REFERENCES

1. L. M. Pecora and T. L. Carroll, Phys. Rev. Lett. **64** (8), 821 (1990).
2. L. Kocarev, K. S. Halle, K. Eckert, et al., Int. J. Bifurc. Chaos **2** (3), 709 (1992).
3. U. Parlitz, L. O. Chua, L. Kocarev, et al., Int. J. Bifurc. Chaos **2** (4), 973 (1992).
4. A. R. Volkovskii and N. F. Rul'kov, Pis'ma Zh. Tekh. Fiz. **19** (3), 71 (1993) [Tech. Phys. Lett. **19**, 97 (1993)].
5. A. S. Dmitriev and A. I. Panas, *Dynamic Chaos: New Information* Carriers *for Communication Systems* (Izdat. Fiz.-Mat. Literatury, Moscow, 2002) [in Russian].
6. Y. H. Sun, J. Cao, and G. Feng, Phys. Lett. A **372** (33), 5442 (2008).
7. A. A. Koronovskii, O. I. Moskalenko, and A. E. Hramov, Usp. Fiz. Nauk **179**, 1281 (2009) [Phys. Usp. **52**, 1213 (2009)].
8. A. A. Koronovskii, O. I. Moskalenko, and A. E. Hramov, Zh. Tekh. Fiz. **80** (4), 1 (2010) [Tech. Phys. **55**, 435 (2010)].
9. R. Lavrov, M. Jacquot, and L. Larger, IEEE J. Quant. Electron. **46** (10), 1430 (2010).
10. G. Perez and H. A. Gerdeira, Phys. Rev. Lett. **74** (11), 1970 (1995).
11. K. M. Short, Int. J. Bifurc. Chaos **7** (7), 1579 (1997).
12. B. Mensour and A. Longtin, Phys. Lett. A **244** (1–3), 59 (1998).
13. V. I. Ponomarenko and M. D. Prokhorov, Phys. Rev. E **66** (2), 026215 (2002).
14. E. V. Kal'yanov, Pis'ma Zh. Tekh. Fiz. **35** (6), 56 (2009) [Tech. Phys. Lett. **35**, 275 (2009)].
15. A. S. Karavaev, V. I. Ponomarenko, E. P. Seleznev, E. E. Glukhovskaya, and M. D. Prokhorov, Pis'ma Zh. Tekh. Fiz. **37** (14), 24 (2011) [Tech. Phys. Lett. **37**, 657 (2011)].

Translated by P. Pozdeev