ISSN 1063-7850, Technical Physics Letters, 2011, Vol. 37, No. 7, pp. 657–660. © Pleiades Publishing, Ltd., 2011.
Original Russian Text © A.S. Karavaev, V.I. Ponomarenko, E.P. Seleznev, E.E. Glukhovskaya, M.D. Prokhorov, 2011, published in Pis'ma v Zhurnal Tekhnicheskoĭ Fiziki, 2011, Vol. 37, No. 14, pp. 24–31.

Digital System of Hidden Data Transmission with Delayed Feedback

A. S. Karavaev, V. I. Ponomarenko, E. P. Seleznev, 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 March 4, 2011

Abstract—A system of hidden data transmission with nonlinear admixture of informative signal to a chaotic carrier signal of oscillator with delayed feedback has been experimentally implemented for the first time. The prototype system employs a programmable microcontroller with analog signal input and digital transmission line.

DOI: 10.1134/S1063785011070248

In recent years, the development of information-communication systems employing the phenomenon of synchronization of chaotic self-sustained oscillations has received much attention [1–11]. A widely used principle of hidden data transmission with a chaotic carrier consists in the nonlinear admixture of informative signal to the chaotic carrier [12, 13]. One of the main disadvantages of these systems is their low interference immunity [3, 9], which is related to the fact that, in order to ensure the security of transmitted data, the level of admixed signal must be significantly lower than that of the carrier. Under these conditions, the presence of interference in the communication channel leads to a significant distortion of the informative signal separated at the output.

In this Letter, we propose a scheme of data transmission based on the principle of nonlinear admixture, in which the informative signal is added to a chaotic signal that is formed as a result of digital calculations on a microcontroller. The receiver, whose parameters are identical with those of the transmitter, receives a digital signal from which the informative component is also separated using digital calculations. This data transmission system allows the informative signal to be masked by a chaotic signal of high dimensionality and possesses sufficiently high interference immunity that is inherent in digital data transmission systems.

In order to increase the level of security in communication systems employing chaotic signals, it was repeatedly suggested to use hidden data transmission using systems with delayed feedback (time-delay systems), which demonstrate chaotic dynamics of very high dimensionality [14–17]. For this reason, we also selected a scheme of hidden data transmission with nonlinear admixture of informative signal to a chaotic carrier signal of oscillator with delayed feedback, a block scheme of which is presented in Fig. 1. A transmitter represents a ring circuit comprising a delay line, a nonlinear element, and a linear low-pass filter. The informative (useful) signal $m(t)$ is admixed by an adder to a chaotic signal $f(x(t-\tau))$ at the output of the nonlinear element and the total signal $s(t) = f(x(t-\tau)) + m(t)$ is transmitted into the communication channel and simultaneously fed into the feedback circuit of the transmitting system, where the oscillations are described by a first-order differential equation with time delay:

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

where $x(t)$ is the system state at time t, f is a nonlinear function, τ is the delay time, and ε is a parameter that characterizes the inertia of the system. In this mode of admixture, the informative signal is directly involved in the formation of a complicated dynamics of the chaos generator.

A receiver contains the same elements as the transmitter, except for the adder that is replaced by a subtractor introduced into the feedback chain. The equation of receiver dynamics is as follows:

$$\varepsilon\dot{y}(t) = -y(t) + f(x(t-\tau)) + m(t). \qquad (2)$$

The subtractor output yields the recovered useful signal as $m'(t) = f(x(t-\tau)) + m(t) - f(y(t-\tau))$. If the analogous elements of the receiver and transmitter are identical, the two systems will be synchronized after a certain transient process. Indeed, the difference $\Delta(t) = x(t) - y(t)$ between oscillations of systems (1) and microcontroller (2) decreases with the time for any $\varepsilon > 0$, since $\dot{\Delta}(t) = -\frac{\Delta(t)}{\varepsilon}$. As a result of this synchronization, we have $x(t) = y(t)$ and, hence, $f(x(t-\tau)) = f(y(t-\tau))$ and $m'(t) = m(t)$. The quality of recovery of the $m(t)$ signal is independent of its amplitude and fre-

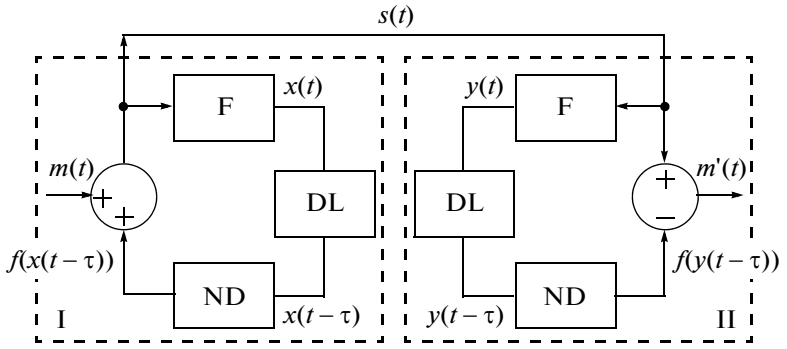

Fig. 1. Block scheme of the system of hidden data transmission with nonlinerar admixture of the informative signal to the chaotic carrier: (I) transmitter; (II) receiver; (DL) delay lines; (ND) nonlinear elements; (F) filters.

quency characteristics, which implies the possibility of transmitting complicated informative signals.

A nonlinear element selected for the implementation provided a quadratic transformation, for which the transmitter equation was as follows:

$$\varepsilon\dot{x}(t) = -x(t) + \lambda - (x(t-\tau))^2 + m(t). \qquad (3)$$

Here, λ is the nonlinearity parameter that was set at 1.9, which corresponded to a chaotic behavior of the system.

The transmitter was implemented on a programmable microcontroller. Since this device had no built-in facilities supporting the floating point operations, the system response speed was increased by using digital calculations. For this purpose the variables and parameters of Eq. (3) were scaled as follows. For small ε, the permissible limits of variation of the parameter λ for which system (3) has a periodic or chaotic attractor are from 0 to 2. When λ varies within these limits, the dynamic variable $x(t)$ can take values from −2 to +2. Let us pass to integer arithmetic and transform Eq. (3) so that the dynamic variable would occur in a 16-bit memory cell, whereby its integer values vary between -2^{15} and 2^{15}. This can be by substituting variables as $X(t) = 2^{14}x(t)$ and $M(t) = 2^{14}m(t)$. Then, Eq. (3) takes the following form

$$\frac{\varepsilon\dot{X}(t)}{2^{14}} = -\frac{X(t)}{2^{14}} + \lambda - \left(\frac{X(t-\tau)}{2^{14}}\right)^2 + \frac{M(t)}{2^{14}}. \qquad (4)$$

Multiplying both sides of Eq. (4) by 2^{14} and introducing parameter $\Lambda = 2^{14}\lambda$, we arrive at the following equation:

$$\varepsilon\dot{X}(t) = -X(t) + \Lambda - \frac{(X(t-\tau))^2}{2^{14}} + M(t). \qquad (5)$$

This differential equation can be reduced to a difference relation, which is more convenient for implementation on a microcontroller:

$$X_{n+1} = \left(1 - \frac{\Delta t}{\varepsilon}\right)X_n + \frac{\Delta t}{\varepsilon}(F(X_{n-k}) + M_n), \qquad (6)$$

where n is the discrete time, Δt is the time step, k is the delay time (in units of discretization steps), and

$$F(X_{n-k}) = \Lambda - \frac{X_{n-k}^2}{2^{14}}.$$

Figure 2 shows a block scheme of the transmitter based on a programmable microcontroller. At the first microcontroller program operation step, the circular buffer array (containing the values from X_{n-k} to X_n) is initiated by a certain constant value as the initial condition. Then, the nonlinear function $F(X_{n-k})$ is calculated and summed with the informative signal M_n, after which the sum S_n is transmitted into the communication channel that is organized as a serial digital interface. The subsequent value of the discrete dynamic variable X_{n+1} is calculated in accordance with relation (6) and fed into the circular buffer. For k cycles, the initiation process is accomplished and the buffer is filled by realistic values.

The linear transformation of the signal in our scheme was performed using a digital low-pass first-order Butterworth filter with an infinite or finite pulse characteristic, which usually allows the security of the communication system to be increased. The greater the number of coefficients in the equation that describes the filter, the greater the number of previous values of the variable involved in calculations of the next value and, hence, the higher the security level of transmitted data. The nonlinear transformation can also be of various types. For example, it is possible to use a Bernoulli map, a tent map, or other maps with chaotic dynamics.

The transmitter was implemented on a programmable microcontroller of the Atmel megaAVR family. The informative test signal was harmonic with a frequency of 10 Hz. Figure 3a shows a fragment of the corresponding time series. The analog informative signal $m(t)$ is fed to the input of an analog-to-digital converter, and the digitized output signal M_n is admixed to the chaotic transmitter system dynamics. The calculations are performed in terms of integer arithmetic, with the chaotic signal amplitude varying within 16 bit

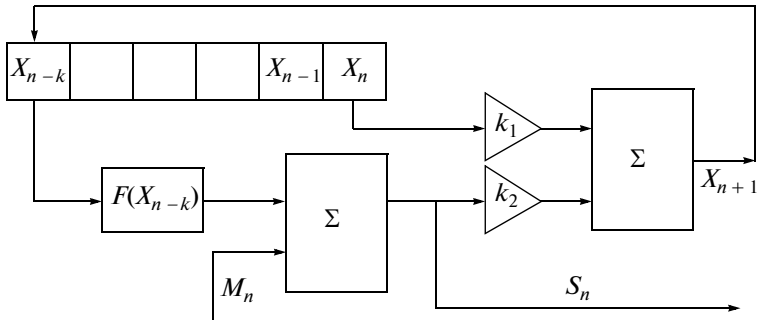

Fig. 2. Block scheme of the transmitter implemented on a microcontroller: (Σ) adder; (k_1, k_2) constant multipliers $\left(k_1 = 1 - \frac{\Delta t}{\varepsilon}, k_2 = \frac{\Delta t}{\varepsilon}\right)$.

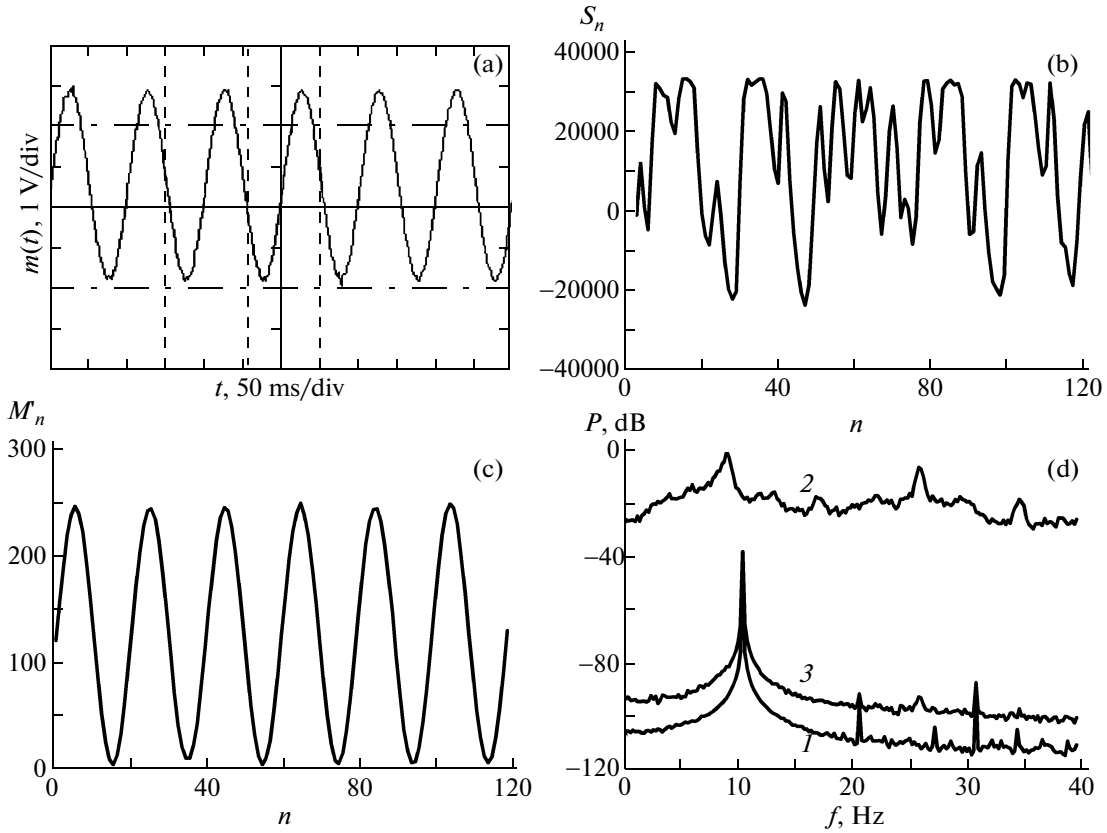

Fig. 3. Operation of the proposed system of hidden data transmission: (a) fragment of time series of informative (harmonic) signal $m(t)$; (b) fragment of time series of chaotic signal S_n; (c) fragment of time series of useful signal M'_n separated in the receiver; (d) power spectra of signals M_n (*1*), S_n (*2*), and M'_n (*3*).

and the informative signal within 8 bit. Figure 3b shows a fragment of the time series of a chaotic signal $S_n = F(X_{n-k}) + M_n$ generated by the oscillator and delayed by the microcontroller for $\Delta t/\varepsilon = 0.5$ and $k = 10$. This signal had a discretization frequency of 200 Hz ($\Delta t = 5$ ms) and was transmitted via RS-232 interface and a digital communication channel at a rate of 57.6 kbit/s.

The receiver was a personal computer, which performed separation of the informative signal. The output signal is $M'_n = F(X_{n-k}) + M_n - F(Y_{n-k})$. If the receiver parameters are identical with those of the transmitter and noise is absent, we obtain $F(Y_{n-k}) = F(X_{n-k})$ and $M'_n = M_n$. Figure 3c shows a fragment of the time series of the useful signal separated in the

receiver. Figure 3d shows the power spectra of the chaotic signal S_n, harmonic informative signal M_n, and the useful signal M'_n separated in the receiver. As can be seen, the quality of recovery of the hidden informative signal is rather high.

Thus, we have demonstrated possibilities of the proposed system of hidden data transmission with nonlinear admixture of informative signal to a chaotic carrier signal of oscillator with delayed feedback. It is shown that the proposed scheme can be implemented on a single integrated circuit.

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. K. M. Cuomo and A. V. Oppenheim, Phys. Rev. Lett. **71**, 65 (1993).
2. L. M. Pecora, T. L. Carroll, G. A. Johnson, et al., Chaos **7**, 520 (1997).
3. A. S. Dmitriev and A. I. Panas, *Dynamic Chaos: New Information Carirers for Communication Systems* (Izdat. Fiz.-Mat. Literatury, Moscow, 2002) [in Russian].
4. V. I. Ponomarenko and M. D. Prokhorov, Phys. Rev. E **66**, 026 215 (2002).
5. J. Y. Chen, K. W. Wong, L. M. Cheng, and J. W. Shuai, Chaos **13**, 508 (2003).
6. W.-H. Kye, M. Choi, C.-M. Kim, and Y.-J. Park., Phys. Rev. E **71**, 045 202 (2005).
7. S. Behnia, A. Akhshani, S. Ahadpour, et al., Phys. Lett. A **366**, 391 (2007).
8. Y. H. Sun, J. Cao, and G. Feng, Phys. Lett. A **372**, 5442 (2008).
9. A. A. Koronovskii, O. I. Moskalenko, and A. E. Hramov, Usp. Fiz. Nauk **179**, 1281 (2009) [Phys. Usp. **52**, 1213 (2009)].
10. A. A. Koronovskii, O. I. Moskalenko, and A. E. Hramov, Zh. Tekh. Fiz. **80** (4), 1 (2010) [Tech. Phys. Lett. **55**, 435 (2010)].
11. Er. V. Kal'yanov and B. E. Kyargiskii, Pis'ma Zh. Tekh. Fiz. **36** (23), 1 (2010) [Tech. Phys. Lett. **36**, 1069 (2010)].
12. A. P. Volkovskii and N. F. Rul'kov, Pis'ma Zh. Tekh. Fiz. **19** (3), 71 (1993). [Sov. Tech. Phys. Lett. **19**, No. 3 (1993)].
13. A. S. Dmitriev, A. I. Panas, and S. O. Starkov, Int. J. Bifurc. Chaos **5**, 1249 (1995).
14. B. Mensour and A. Longtin, Phys. Lett. A **244**, 59 (1998).
15. K. Pyragas, Int. J. Bifurc. Chaos **8**, 1839 (1998).
16. V. I. Ponomarenko and M. D. Prokhorov, Radiotekh. Elektron. (Moscow) **49**, 1098 (2004).
17. E. V. Kal'yanov, Pis'ma Zh. Tekh. Fiz. **35** (6), 56 (2009) [Tech. Phys. Lett. **35**, 275 (2009)].

Translated by P. Pozdeev