Nonlinear Dyn (2013) 74:1013–1020
DOI 10.1007/s11071-013-1019-0

ORIGINAL PAPER

An experimental digital communication scheme based on chaotic time-delay system

V.I. Ponomarenko · M.D. Prokhorov · A.S. Karavaev · D.D. Kulminskiy

Received: 25 January 2013 / Accepted: 21 July 2013 / Published online: 25 August 2013

Abstract We develop an experimental system for secure communication with nonlinear mixing of information signal and chaotic signal of a time-delay system. The proposed scheme is based on programmable microcontrollers with digital transmission line. The scheme allows one to transmit and receive speech and musical signals in real time without noticeable distortion. A high quality of extraction of hidden information signal is achieved due to the use of digital elements in the scheme, which ensures identity of the parameters and high stability to noise. We study a possibility of hidden message extraction from a chaotic carrier by a third party in the case of mismatch of the receiver and transmitter parameters.

Keywords Secure communication scheme · Chaotic synchronization · Time-delay systems

V.I. Ponomarenko · M.D. Prokhorov (✉) · A.S. Karavaev
Saratov Branch of the Institute of Radio Engineering
and Electronics of Russian Academy of Sciences,
38, Zelyonaya Street, 410019, Saratov, Russia
e-mail: mdprokhorov@yandex.ru

V.I. Ponomarenko · A.S. Karavaev · D.D. Kulminskiy
Department of Nano- and Biomedical Technologies,
Saratov State University, 83, Astrakhanskay Street,
410012, Saratov, Russia

1 Introduction

The discovery of the phenomenon of synchronization in chaotic systems [1] has given rise to active development of secure communication schemes using chaotic signal as a carrier [2–10]. Chaotic communication systems have attracted a lot of attention due to the broadband power spectrum of chaotic signals, high rates of information transmission, and tolerance to sufficiently high levels of noise. 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 [11–14]. To improve the security of data transmission, it has been proposed to employ time-delay systems, demonstrating chaotic dynamics of a very high dimension, in private communication [15–21].

Different approaches for the transmission of information signals using chaotic dynamics have been developed. One of the most widespread among them is nonlinear mixing of information signal and chaotic signal [5]. However, one of the main disadvantages of communication systems with nonlinear mixing is their comparatively low interference immunity [8]. It is explained by the fact that, in order to ensure the security of transmitted data, the level of information signal must be significantly lower than that of the chaotic carrier. Under these conditions, the presence of noise in the communication channel leads to an appreciable distortion of the message signal at the scheme output.

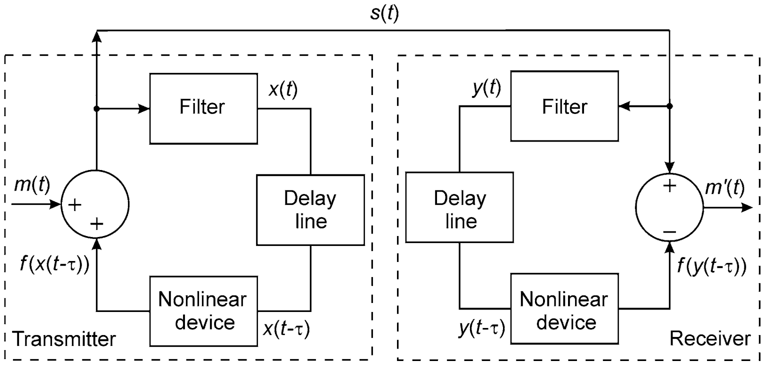

Fig. 1 Block diagram of a communication system with nonlinear mixing

In this paper, we propose a scheme of hidden data transmission with nonlinear mixing, in which an information signal is added to a chaotic signal of oscillator with delayed feedback. The chaotic transmitter is implemented on programmable microcontroller that employs digital calculations. The receiver, whose parameters are identical with those of the transmitter, receives a digital signal from which the information component is extracted using again digital calculations. Such a communication system exploits the masking of the information signal by a chaotic signal of high dimension and possesses sufficiently high stability to noise that is inherent in digital systems of data transmission.

The paper is organized as follows. In Sect. 2, a communication system is described. Section 3 illustrates the results of operation of the proposed communication scheme for the cases of harmonic and musical information signals. In Sect. 4, we consider the extraction of information signal at the mismatch of the receiver and transmitter parameters. In Sect. 5, we summarize our results.

2 Communication scheme

A block diagram of the communication system with nonlinear mixing is shown in Fig. 1. A transmitter represents a ring system composed of a delay line, a nonlinear element, and a linear low-pass filter. The information signal $m(t)$ is added to the chaotic signal $f(x(t-\tau))$ with the help of a summator and the signal $s(t)=f(x(t-\tau))+m(t)$ is transmitted into the communication channel and simultaneously injected into the feedback circuit of the transmitter whose dynamics is described by a first-order delay-differential equation

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

where $x(t)$ is the system state at time t, f is a nonlinear function, τ is the delay time, and ε is the parameter that characterizes the inertial properties of the system. With this nonlinear mixing the information signal is directly involved in the formation of a complicated dynamics of the chaotic system.

A receiver is composed of the same elements as the transmitter, except for the summator that is replaced by a subtractor breaking the feedback circuit. The receiver equation is

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

At the output of the subtractor, we have the extracted information signal $m'(t)=f(x(t-\tau))+m(t)-f(y(t-\tau))$. If the transmitter and the receiver are composed of identical elements, they become completely synchronized after the transient process. The difference between the oscillations of systems (1) and (2), $\Delta(t)=x(t)-y(t)$, decreases in time for any $\varepsilon>0$, since $\dot{\Delta}(t)=-\Delta(t)/\varepsilon$. As the result of synchronization we have $x(t)=y(t)$, and hence, $f(x(t-\tau))=f(y(t-\tau))$ and $m'(t)=m(t)$. It should be noted that the quality of the extraction of message $m(t)$ does not depend on its amplitude and frequency characteristics. By this we mean that the considered communication scheme allows one to transmit complicated information signals without distortion.

The nonlinear element in our scheme provides a quadratic transformation. In this case, the transmitter equation takes the form

$$\varepsilon\dot{x}(t)=-x(t)+\lambda-\big(x(t-\tau)\big)^2+m(t), \tag{3}$$

where λ is the parameter of nonlinearity. The transmitter parameters were chosen to obtain a regime of developed chaotic oscillations.

We used a programmable microcontroller to implement the transmitter. Since this device has no built-in

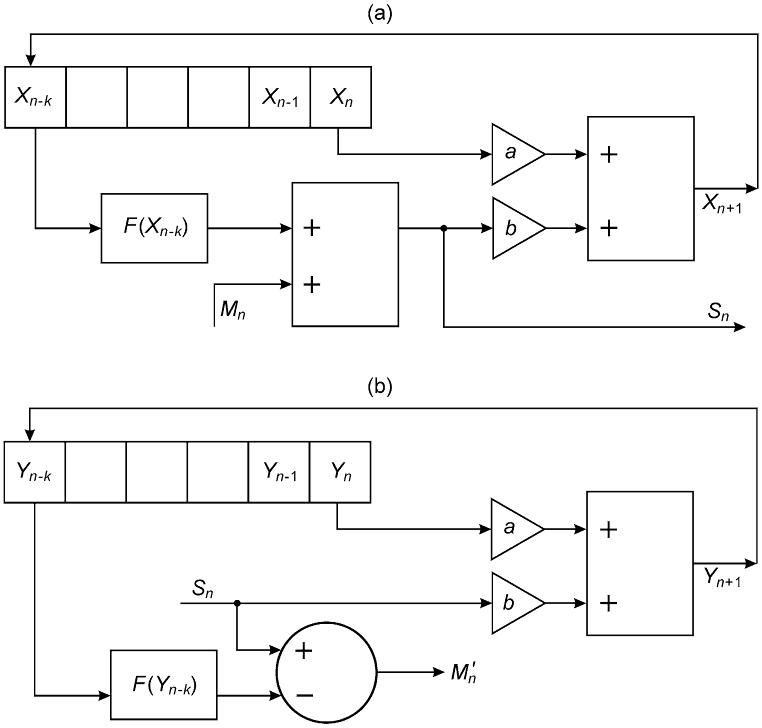

Fig. 2 Block diagrams of transmitter (**a**) and receiver (**b**) implemented on a microcontroller; a and b are constant multipliers, where $a = 1 - \Delta t/\varepsilon$ and $b = \Delta t/\varepsilon$

facilities supporting the floating-point operations, one should use integer calculations in the microcontroller in order to increase the speed of response. For this purpose the variables and parameters of Eq. (3) were scaled as follows. For a small ε, the allowable limits of variation of the parameter λ for which system (3) has a periodic or chaotic attractor are from 0 to 2. Within this range of λ variation, the dynamical variable $x(t)$ can take values from -2 to $+2$. Let us pass to integer arithmetic and transform Eq. (3) in such a way that the dynamical variable is placed in a 16-bit memory location, whereby its integer values vary between -2^{15} and 2^{15}. It can be done 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 the parameter $\Lambda = 2^{14}\lambda$, we obtain 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 equation which is more convenient for program implementation on a microcontroller:

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

where n is the discrete time, Δt is the time step, k is the discrete delay time in units of sampling time Δt, and $F(X_{n-k}) = \Lambda - X_{n-k}^2/2^{14}$.

Figure 2(a) shows a block diagram of the transmitter based on a programmable microcontroller. At the first step of microcontroller program operation, the circular buffer array (containing the values from X_{n-k} to X_n) is initialized by a certain constant value as the initial condition. Then, the nonlinear function $F(X_{n-k})$ is calculated and summed with the information signal M_n. After that, the obtained 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. After k cycles, the process of initialization is accomplished and the buffer is filled by actual values. A block diagram of the receiver implemented on a microcontroller is shown in Fig. 2(b).

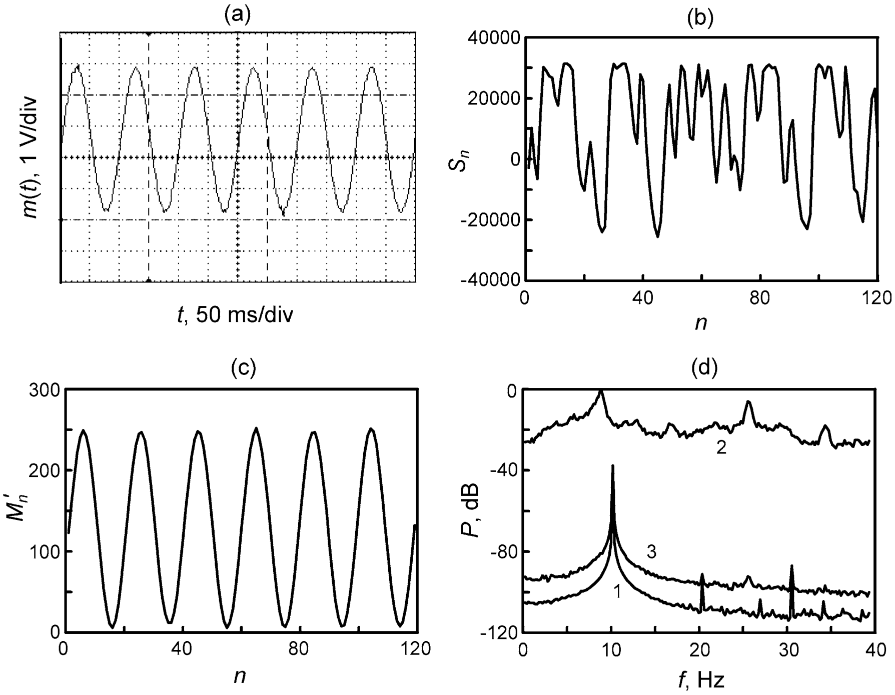

Fig. 3 (**a**) Oscillogram of temporal realization of harmonic information signal $m(t)$. (**b**) Time series of chaotic signal S_n. (**c**) Time series of the extracted information signal M'_n. (**d**) Power spectra of signals $M_n(1)$, $S_n(2)$, and $M'_n(3)$

The linear transformation of the signal in our scheme was performed using a digital low-pass first-order Butterworth filter. It should be noted that employment of high-order filters usually allows one to increase the security of the communication scheme. 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 since one has to know more parameters for hidden message extraction. The nonlinear transformation can also be of various types. For example, one can use a tent map or other maps with chaotic dynamics.

3 Extracting information signal mixed with chaotic signal

3.1 Case of harmonic information signal

In our scheme, the transmitter was implemented on a programmable microcontroller of the Atmel xmega AVR family. As the information signal we choose at first a harmonic signal with a frequency of 10 Hz. Part of the time series of this signal is presented in Fig. 3(a). The analog information signal $m(t)$ is fed to the input of an analog-to-digital converter (ADC) and the signal M_n from its output is mixed with the chaotic signal of the transmitter. The calculations are performed in terms of integer arithmetic, with the chaotic signal amplitude varying within 16 bits and the information signal within 8 bits.

Figure 3(b) shows a part of the time series of a chaotic signal $S_n = F(X_{n-k}) + M_n$ generated by the oscillator with delayed feedback at $\lambda = 1.9$, $\Delta t/\varepsilon = 0.5$, and $k = 10$. This signal had a digitization frequency of 200 Hz ($\Delta t = 5$ ms) and was transmitted over a digital communication channel at a rate of 57.6 kbit/s using UART interface.

The receiver was implemented on the same programmable microcontroller as the transmitter. At the subtractor output of the receiver, we have the extracted information signal $M'_n = F(X_{n-k}) + M_n - F(Y_{n-k})$. 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 3(c) shows a part of the time series of the signal M'_n. Passing the digital signal M'_n through a digital-to-analog converter (DAC), we obtain the analog information signal $m'(t)$ at its output.

Figure 3(d) depicts the power spectra of the chaotic signal S_n, harmonic information signal M_n, and the signal M'_n extracted in the receiver. The amplitude of the information signal comprises about 0.4 % of the amplitude of the chaotic carrier and the presence of message is not noticeable in the power spectrum of the transmitted signal S_n. As it can be seen from Fig. 3, the quality of recovery of the hidden information signal is sufficiently high.

3.2 Case of musical information signal

Let us illustrate now the scheme efficiency for the case of a musical information signal (a song). Part of the time series of this audio signal is presented in Fig. 4(a). For quantization of this signal we used 12 bits of ADC with a digitization frequency of 20 kHz ($\Delta t = 50$ mcs). Figure 4(b) shows a part of the time series of the transmitted chaotic signal S_n generated by the time-delay system at $\lambda = 1.9$, $\Delta t/\varepsilon = 0.5$, and $k = 100$. This 16-bit signal also had a digitization frequency of 20 kHz. If one passes this signal through a DAC and reproduce, he/she will hear only noise without any signs of speech and music.

In the receiver, we extract the information signal M'_n and pass it through a DAC to obtain the analog information signal $m'(t)$ at its output. Part of the time series of $m'(t)$ is also displayed in Fig. 4(a) for the case where the parameters of the receiver and transmitter are identical. As it can be seen from Fig. 4(a), the time series of the original and extracted information signals are very similar. Aurally the original musical signal $m(t)$ and the signal $m'(t)$ at the receiver output are indistinguishable.

Figure 4(c) shows the power spectra of the chaotic signal S_n, musical information signal M_n, and the signal M'_n extracted in the receiver. The power spectra of the signals M_n and M'_n are very close. The amplitude of the musical information signal appreciably varies in time with the loudness of the signal. The maximal amplitude of audio signal is about 6 % of the amplitude of the chaotic signal. Averaged over the entire time series, the message amplitude comprises about 1 % of the amplitude of the chaotic carrier and the presence of audio signal is not noticeable in the power spectrum of the transmitted signal S_n.

Thus, the quality of hidden information extraction at the receiver output is good enough in spite of the presence of noise inherent in a real system. The proposed scheme allows one to transmit and receive speech and musical signals in real time without noticeable distortion.

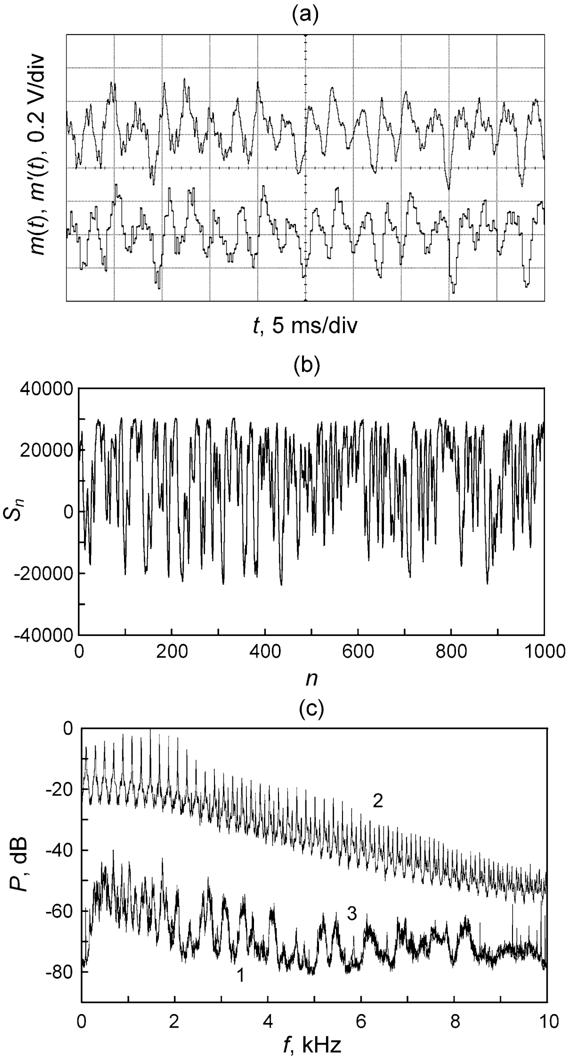

Fig. 4 (**a**) Oscillograms of temporal realizations of musical information signal $m(t)$ at the transmitter input (*on top*) and the extracted information signal $m'(t)$ at the receiver output (*below*). (**b**) Time series of chaotic signal S_n. (**c**) Power spectra of signals $M_n(1)$, $S_n(2)$, and $M'_n(3)$. The spectra of M_n and M'_n are shown by *black* and *grey color*, respectively

4 Extraction of information signal at a mismatch of the receiver and transmitter parameters

In the above-considered examples, the identity of the parameter values in the transmitter and receiver ensures a high quality of hidden message extraction for the authorized listener. The identity of the receiver and transmitter parameters is of crucial importance in communication schemes based on synchronization of chaotic systems. The complete synchronization of the transmitter and receiver takes place only if they are composed of identical elements. In the case of parameter mismatch, we have $x(t) - y(t) \neq 0$, and hence, $m'(t) \neq m(t)$.

With the increase of mismatch of the receiver and transmitter parameters, the quality of chaotic synchronous response of the receiver deteriorates, leading to a worse quality of the information signal extraction [5]. Beginning with a certain value of mismatch, the extraction of hidden message becomes impossible. The advantage of the proposed digital communication scheme is the employment of programmable microcontrollers that allows us to achieve the complete identity of the receiver and transmitter parameters, which is practically unattainable in the case of constructing the receiver and transmitter from analog elements.

For an eavesdropper the signal transmitted over the communication channel is perceived as noise. To extract a hidden message from the chaotic carrier, an unauthorized listener must know the transmitter configuration, i.e., he/she must know that the transmitter is governed by the model time-delay equation (1) and also know the type of nonlinear function f and accurate values of the system parameters. For the reconstruction of model equations of time-delay systems and estimation of their parameters from time series, a number of methods have been proposed [22–28]. In the absence of noise, these methods allow one to recover the unknown parameters of time-delay systems with a good accuracy. However, in the presence of noise, the parameter estimation is less accurate. Moreover, the error of parameter estimation increases with the increase of noise level.

The considered communication scheme employs nonlinear mixing of information signal and chaotic signal of a time-delay system. In this case, the presence of information signal in the chaotic carrier inevitably decreases the accuracy of estimation of the transmitter parameters from time series just as in the case of noise presence. We have examined how accurately the transmitter parameters must be known for extracting a hidden information signal at the receiver output.

Let us choose the same transmitter parameters as in Sect. 3.2 and the same musical information signal. The receiver parameters are chosen the same as for the transmitter except for the discrete delay time k, which is varied in the vicinity of the true value of $k = 100$. Already for a minimal mismatch of k by unity ($k = 99$ or $k = 101$), we hear only noise at the receiver output. Thus, the information signal is completely masked in the case of a 1 % mismatch of the delay time in the transmitter and receiver. Parts of the time series of the original musical signal $m(t)$ and the signal $m'(t)$ extracted in the receiver at $k = 99$ are presented in Fig. 5. The amplitude of the signal $m'(t)$ is significantly greater than the amplitude of $m(t)$. Besides, the signal $m'(t)$ looks like a chaotic carrier.

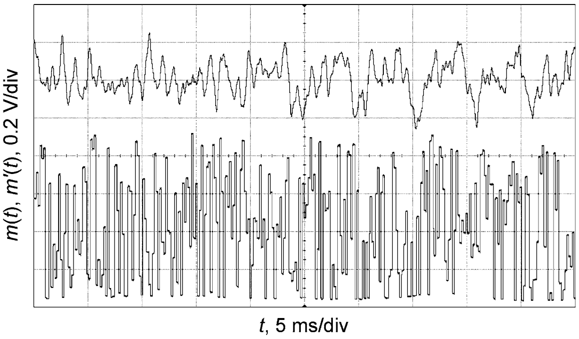

Fig. 5 Oscillograms of temporal realizations of the original information signal $m(t)$ (*on top*) and the information signal $m'(t)$ extracted in the receiver at the mismatch of parameter k ($k = 99$) (*below*)

We study also the influence of the parameter ε mismatch on the quality of the hidden message extraction. The receiver and transmitter parameters are chosen the same except for the parameter ε, which is varied in the vicinity of the true value of $\varepsilon = 100$ mcs. It is found out that neither speech nor music is heard at the receiver output if a mismatch of ε is greater than 1.5 %. In this case, the time series and power spectra of $m'(t)$ and $m(t)$ are appreciably different. In the case of 0.1–1 % mismatch in ε, the information signal is masked partially. We can distinguish single words and a musical background at the receiver output, although the time series and power spectra of $m'(t)$ and $m(t)$ are appreciably different. If a mismatch of ε is 0.05 %, the musical signal is extracted in the receiver with a small noise disturbance, which disappears under the further decrease of mismatch.

Thus, in order to extract a hidden message, an unauthorized listener has to reconstruct the transmitter parameters with a high accuracy that is a very complicated problem for the proposed scheme.

The robustness of our scheme to parameter mismatch is comparable to that of other chaotic communication schemes. For instance, a detailed comparison of 9 popular chaotic communication schemes presented in [8] revealed that a mismatch of the receiver and transmitter parameters should not exceed 1–2 % in each of the schemes to provide the extraction of a hidden message. Similar results are obtained for several communication schemes studied in [5]. To provide a satisfactory quality of message extraction in the optical chaos communication scheme, the authors of [10] had to constrain the parameter mismatches of the receiver and transmitter below 3 %.

5 Conclusion

We have developed the experimental digital communication system with nonlinear mixing of information signal and chaotic signal of time-delay system in which the transmitter and receiver are implemented on simple programmable microcontrollers. This system allows one to transmit and receive speech and musical signals in real time without noticeable distortion. A high quality of hidden message extraction is achieved due to the use of digital elements in the scheme, which ensures identity of the parameters and high stability to noise typical for digital communication systems.

We have studied a possibility of extraction of hidden information signal from a chaotic carrier in the case of mismatch of the parameters of the receiver and transmitter in the proposed scheme. It was found that for the hidden message extraction the parameter mismatch must be less than 1 % which ensures the privacy of the proposed communication scheme.

Acknowledgements This work is supported by the Russian Foundation for Basic Research, Grant No. 13-02-00227 and by the grant of the president of Russian Federation, MK-4435.2012.8.

References

1. Pecora, L.M., Carroll, T.L.: Synchronization in chaotic systems. Phys. Rev. Lett. **64**, 821–824 (1990)
2. Parlitz, U., Chua, L.O., Kocarev, L., Halle, K.S., Shang, A.: Transmission of digital signals by chaotic synchronization. Int. J. Bifurc. Chaos **2**, 973–977 (1992)
3. Cuomo, K.M., Oppenheim, A.V.: Circuit implementation of synchronized chaos with applications to communications. Phys. Rev. Lett. **71**, 65–68 (1993)
4. Pecora, L.M., Carroll, T.L., Johnson, G.A., Mar, D.J., Heagy, J.F.: Fundamentals of synchronization in chaotic systems, concepts, and applications. Chaos **7**, 520–543 (1997)
5. Dmitriev, A.S., Panas, A.I.: Dynamical Chaos: New Information Carriers for Communication Systems. Fizmatlit, Moscow (2002)
6. Chen, J.Y., Wong, K.W., Cheng, L.M., Shuai, J.W.: A secure communication scheme based on the phase synchronization of chaotic systems. Chaos **13**, 508–514 (2003)
7. Tao, Y.: A survey of chaotic secure communication systems. Int. J. Comput. Cogn. **2**, 81–130 (2004)
8. Koronovskii, A.A., Moskalenko, O.I., Hramov, A.E.: On the use of chaotic synchronization for secure communication. Phys. Usp. **52**, 1213–1238 (2009)
9. Wang, M.-J., Wang, X.-Y., Pei, B.-N.: A new digital communication scheme based on chaotic modulation. Nonlinear Dyn. **67**, 1097–1104 (2012)
10. Argyris, A., Syvridis, D., Larger, L., Annovazzi-Lodi, V., Colet, P., Fischer, I., García-Ojalvo, J., Mirasso, C.R., Pesquera, L., Shore, K.A.: Chaos-based communications at high bit rates using commercial fibre-optic links. Nature **437**, 343–346 (2005)
11. Short, K.M.: Signal extraction from chaotic communications. Int. J. Bifurc. Chaos **7**, 1579–1597 (1997)
12. 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 **234**, 429–435 (1997)
13. Yang, T., Yang, L.-B., Yang, C.-M.: Breaking chaotic secure communication using a spectrogram. Phys. Lett. A **247**, 105–111 (1998)
14. Álvarez, G., Montoya, F., Pastor, G., Romera, M.: Breaking a secure communication scheme based on the phase synchronization of chaotic systems. Chaos **14**, 274–278 (2004)
15. Pyragas, K.: Transmission of signals via synchronization of chaotic time-delay systems. Int. J. Bifurc. Chaos **8**, 1839–1842 (1998)
16. Udaltsov, V.S., Goedgebuer, J.-P., Larger, L., Rhodes, W.T.: Communicating with optical hyperchaos: information encryption and decryption in delayed nonlinear feedback systems. Phys. Rev. Lett. **86**, 1892–1895 (2001)
17. Ponomarenko, V.I., Prokhorov, M.D.: Extracting information masked by the chaotic signal of a time-delay system. Phys. Rev. E **66**, 026215 (2002)
18. Kye, W.-H., Choi, M., Kim, C.-M., Park, Y.-J.: Encryption with synchronized time-delayed systems. Phys. Rev. E **71**, 045202 (2005)
19. Prokhorov, M.D., Ponomarenko, V.I.: Encryption and decryption of information in chaotic communication systems governed by delay-differential equations. Chaos Solitons Fractals **35**, 871–877 (2008)
20. Nguimdo, R.M., Colet, P., Larger, L., Pesquera, L.: Digital key for chaos communication performing time delay concealment. Phys. Rev. Lett. **107**, 034103 (2011)
21. Kye, W.-H.: Information transfer via implicit encoding with delay time modulation in a time-delay system. Phys. Lett. A **376**, 2663–2667 (2012)
22. Voss, H., Kurths, J.: Reconstruction of non-linear time delay models from data by the use of optimal transformations. Phys. Lett. A **234**, 336–344 (1997)
23. Tian, Y.-C., Gao, F.: Extraction of delay information from chaotic time series based on information entropy. Physica D **108**, 113–118 (1997)

24. Bünner, M.J., Ciofini, M., Giaquinta, A., Hegger, R., Kantz, H., Meucci, R., Politi, A.: Reconstruction of systems with delayed feedback: (I) Theory. Eur. Phys. J. D **10**, 165–176 (2000)
25. Prokhorov, M.D., Ponomarenko, V.I., Karavaev, A.S., Bezruchko, B.P.: Reconstruction of time-delayed feedback systems from time series. Physica D **203**, 209–223 (2005)
26. Rontani, D., Locquet, A., Sciamanna, M., Citrin, D.S., Ortin, S.: Time-delay identification in a chaotic semiconductor laser with optical feedback: a dynamical point of view. IEEE J. Quantum Electron. **45**, 879–891 (2009)
27. Zunino, L., Soriano, M.C., Fischer, I., Rosso, O.A., Mirasso, C.R.: Permutation-information-theory approach to unveil delay dynamics from time-series analysis. Phys. Rev. E **82**, 046212 (2010)
28. Dai, C., Chen, W., Li, L., Zhu, Y., Yang, Y.: Seeker optimization algorithm for parameter estimation of time-delay chaotic systems. Phys. Rev. E **83**, 036203 (2011)