ISSN 1063-7850, Technical Physics Letters, 2013, Vol. 39, No. 9, pp. 825–829. © Pleiades Publishing, Ltd., 2013.
Original Russian Text © A.I. Nazimov, A.N. Pavlov, 2013, published in Pis'ma v Zhurnal Tekhnicheskoi Fiziki, 2013, Vol. 39, No. 18, pp. 61–69.

A Method for Protecting Communicated Information Using Neural-Network Detection

A. I. Nazimov and A. N. Pavlov
Saratov State University, Saratov, 410012 Russia
e-mail: pavlov.alexeyn@gmail.com
Received May 14, 2013

Abstract—A method for protecting information transmitted via a communication channel is proposed. According to this method, data messaging is encoded by a change in the shape of pulse sequences and the messages are detected based on the neural-network method of signal identification. The efficiency of the method is analyzed in the case of multichannel transmitting of graphical information.

DOI: 10.1134/S1063785013090228

The problem of protecting information transmitted via a communication channel has a long history and many possible solutions. A comparatively new approach is based on using chaotic self-sustained oscillations as carrying signals [1–5]. In such communication systems, an information message can be detected based, e.g., on the phenomenon of chaotic synchronization [1] or on applying special tools for digital processing of signals [6]. When a large number of messages are transmitted via a single communication channel, these approaches have some restrictions. In this work, we propose a variant for improving the characteristics of this multichanneling; the variant includes encoding information messages by changing the shape of transmitted pulse sequences and the neural-network principle of detection.

For a transmitted pulse, we choose an analog signal of the form

$$G(\mathbf{p}, t) = a_e e^{-(\rho_e(t-q_e))^2}(a_t + b_t th(\rho_t(t-q_t))) \times \sin\left(\frac{2\pi}{T} f_s t + \varphi_s\right), \quad (1)$$

$$\mathbf{p} = \{a_t, b_t, \rho_t, a_e, \rho_e, q_e, f_s, \varphi_s, T\}.$$

The function $G(\mathbf{p}, t)$ is typical for neural action potentials $s_0(i\Delta t)$ (Fig. 1); a series of special approaches have been developed in neurodynamics to recognize them [7–10]. With an appropriate designation of parameter vector $\mathbf{p}$, function (1) permits one to perform a sufficiently exact approximation of the experimental signal $s_0(i\Delta t) \approx G(\mathbf{p}_0, t)$. In the presence of sequences consisting of pulses that are close in shape and belong to different classes, recognizing the pulse shape in the presence of noises can be done, e.g., via analysis of principal components [7]. However, artificial neural networks (NNs) [11] (Fig. 2) are a more efficient tool for recognizing the shape of noisy signals. We use a version in which the NN is constructed in the form of a perceptron,

$$\eta_{jk} = \sum_{i=1}^{M_k} y_{ik-1} w_{ijk} - \theta_{jk}, \quad y_{jk} = Y(\eta_{jk}), \quad j \in [1; N_k], \quad k \in [1; L], \quad (2)$$

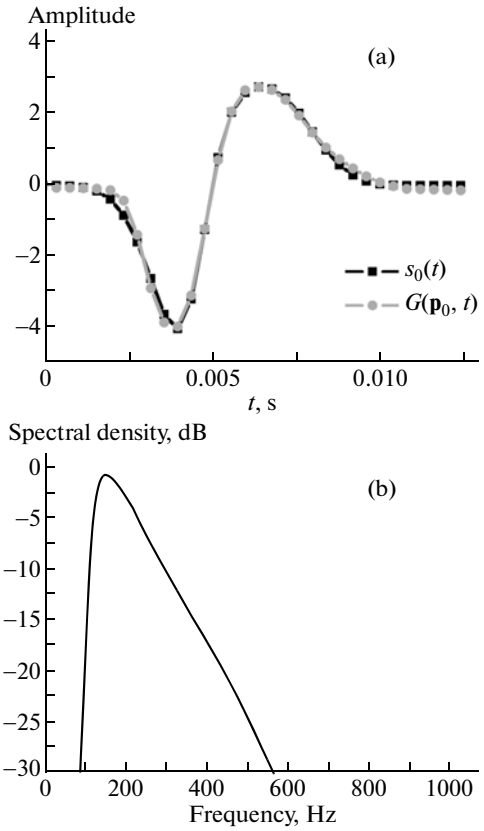

Fig. 1. Pulse signals: (a) pulse $G(\mathbf{p}_0, t)$ and experimentally measured potential of the neuron action $s_0(i\Delta t)$ and (b) spectral characteristic of the pulse $G(\mathbf{p}_0, t)$.

where N_k is the number of neurons in the kth layer, M_k is the number of synapses of a neuron of the kth layer, $Y(x)$ is the activation function, $\{y_{jk}\}$ is the neuron "activity," $\{\theta_{jk}\}$ is the threshold level, and $\{w_{ijk}\}$ is the synaptic coefficient for the i-synapse in the j-neuron at the k-layer. Correspondingly, $x_i = y_{i0}$ is the input vector and y_{jL} is the output vector. The NN is learned based on the error back-propagation principle [11].

In the context of the proposed method of protected data transfer, information messages are encoded in the transmitter as follows. Consider Q_C independent information messages written as matrices $\{I_k^m\}$ in which $m \in [1; Q_C]$ is the index of the message number and $k \in [1; P_I]$ is the number of information values in the m-message.

Step 1. Information signals are normalized with respect to the amplitude to the quantity $D_A > 0$ using expression (3) with obtaining the matrix $\{\nu_k^m\}$

$$\nu_k^m = \frac{D_A}{\max(I_k^{n=m})} I_k^m + D_A. \quad (3)$$

Step 2. Individual fragments of the coded message are constructed in the form of m-matrices $\{B_{ik}^m\}$ in accordance with (4):

$$B_{ik}^m = \alpha_\xi \xi(i\Delta t) + G(\mathbf{p}_m, (i - \nu_k^m)\Delta t), \quad i \in [1; D_S]. \quad (4)$$

An additional source of colored noise $\xi(t) \in [-1.0; 1.0]$ is used with amplitude parameter α_ξ and continuous spectrum in the range of $[0; f_\xi]$ and m pulses of type (1) with parameter vectors $\mathbf{p}_m$ and similar duration T are introduced. Length parameter of the code unit $D_S = 2D_A + [T/\Delta t]$ is established.

Step 3. Using mapping (5) consisting of n iterations ($n \in [1; Q_C P_I]$) by matrices $\{B_k^m\}$ given based on (4), a coded message is constructed in the form of signal $S(t)$:

$$\begin{cases} \xi_{num}^{(n+1)} = \begin{cases} \xi_{num} \in \{1, 2, \ldots, Q_C\}, \\ \tau_{1n} \neq P_I \wedge \tau_{2n} = P_I \wedge \ldots \wedge \tau_{Q_C n} \neq P_I, \\ \xi_{num} \in \{l | l \in \{1, 2, \ldots, q, \ldots, Q_C\} \wedge l \neq q\}, \\ \tau_{qn} = P_I \wedge \tau_{1n} \neq P_I \wedge \tau_{2n} \neq P_I \wedge \ldots \wedge \tau_{Q_C n} \neq P_I, \\ \xi_{num} \in \{l | l \in \{1, 2, \ldots, q, r, \ldots, Q_C\} \wedge l \neq q \wedge l \neq r\}, \\ \tau_{qn} = P_I \wedge \tau_{rn} = P_I \wedge \tau_{1n} \neq P_I \wedge \ldots \wedge \tau_{Q_C n} \neq P_I, \\ \vdots \end{cases} \\ \tau_{kn+1} = \begin{cases} \tau_{kn} + 1, & \xi_{num}^{(n)} = k, \\ \tau_{kn}, & \xi_{num}^{(n)} \neq k, \end{cases} \quad \begin{cases} S(i\Delta t) = B_{q\tau_{mn}}^m, \\ m = \xi_{num}^{(n)}, \\ i = q + (n-1)D_S, \quad q \in [1; D_S]. \end{cases} \end{cases} \quad (5)$$

The iterations are executed using a uniformly distributed random value ξ_{num}; the range of ξ_{num} values is bounded by the set $\{1, 2, \ldots, Q_C\}$ and a τ-matrix with dimensions $Q_C \times Q_C P_I$ is additionally introduced. When implementing mapping (5), the following values are used as initial conditions: $n = 1$, $\xi_{num}^{(n)} \in \{1, 2, \ldots, Q_C\}$, $\tau_{\xi_{num}^{(n)} n} = 1$, $\forall k \neq \xi_{num}^{(n)}$, and $\tau_{kn} = 0$.

Parameters D_A and D_S are constant (a priori given) quantities. Coded signal S for Q_C information messages consists of $Q_C P_I$ sequences of samples with length D_S. Executing $Q_C P_I$ iterations for the transmitter (5) entails a necessity to perform $Q_C P_I$ iterations for the receiver. Let us consider the algorithm of the nth iteration in the receiver.

Step 1. Discrete measurements of values of the coded signal passing through the communication channel are performed. In the course of the measurements, discretized signal $F^n(i\Delta t)$ with duration $D_S \Delta t$ is constructed.

Step 2. Signal $F^n(i\Delta t)$ is subjected to a threshold transform or a discrete wavelet-transform [8] to localize pulses $G(\mathbf{p}_m, i\Delta t)$ with length T. In the process of pulse localization, its central point is determined (the value t_S).

Step 3. Using NN (2) adapted to recognizing pulses of type (1), the input vector represented in the form

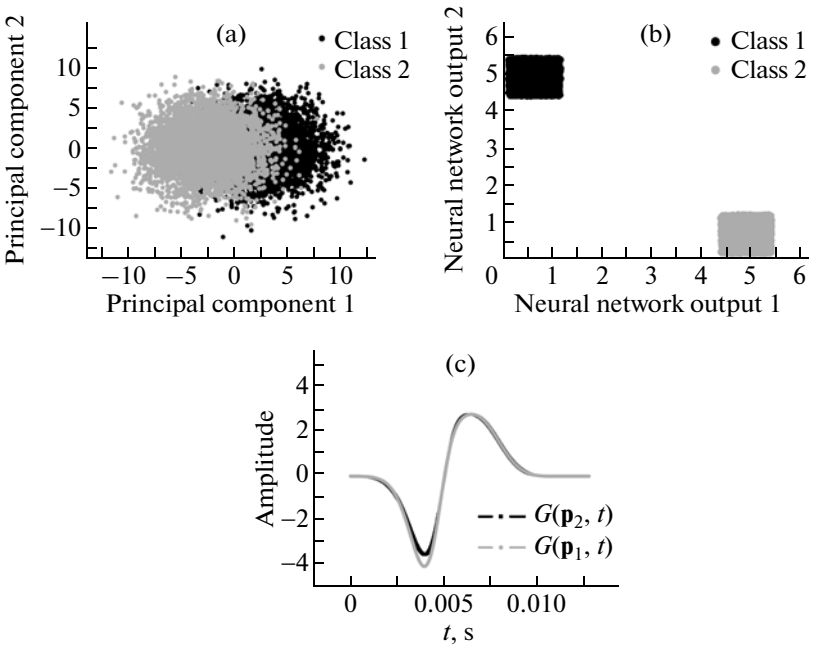

Fig. 2. Results of the classification of noised pulses of two classes: (a) based on the analysis of principal components, (b) based on the NN, and (c) shapes of pulses used in the numerical experiment on information transfer in the protected mode.

$x_i = G(\mathbf{p}_m, t_S + i\Delta t - T/2)$ is recognized. Output vector y_{jL} of the NN is analyzed using functional (6) in which y_j^m are library vectors (m vectors, $m \in [1; Q_C]$) formed in the course of NN learning:

$$R(m) = \sqrt{\sum_{j=1}^{N_L} (y_{jL} - y_j^m)^2}. \quad (6)$$

Step 4. Based on condition (7), the matrix ν_k^m for the receiver is determined:

$$\exists m \in Z: R(m) = \min \Rightarrow \nu_k^m = \frac{t_S}{\Delta t}, \quad k = k(n). \quad (7)$$

Step 5. In accordance with values $\{\nu_k^m\}$, normalized value I_k^m (8) for the mth information message is reconstructed:

$$I_k^m = \frac{\nu_k^m - D_A}{D_A}, \quad k = k(n). \quad (8)$$

Thus, if steps 1–5 of the algorithm for message receiving are executed at each nth iteration, then, in correspondence with formulas (6)–(9), all Q_C transmitted messages are gradually reconstructed in the form of matrices $\{I_k^m\}$, $m \in [1; Q_C]$, $k \in [1; P_I]$.

A numerical experiment in which the operation of the transmitter and receiver was simulated was carried out to test the proposed method of protected information transfer. In the course of the numerical experiment, the encoding algorithm operated in the regime of transferring two ($Q_C = 2$) information messages in the form of two black-and-white images (Fig. 3) for which $P_I = 400 \times 600$. Pulses of type (1) presented in Fig. 2c were chosen for the transmitted pulses. The duration of the pulses was $T = 0.0128$ s and the time discretization step was $\Delta t = 0.0004$ s. Coordinates of vectors p_1 and p_2 assigning the pulse shapes are presented in the table. Other parameters were chosen as follows: $D_A = 255$, $\alpha_\xi = 0.6$, and $f_\xi = 1500$ Hz. The recognition involved a three-layer NN organized as follows: $N_1 = 32$, $M_1 = 32$, $N_2 = 250$, and $N_3 = 2$. The adaptation was performed based on a sample of 400 pulses noised by colored noise source ξ ($\alpha_\xi = 0.9$ and $f_\xi = 1500$ Hz) for two classes (the number of adaptation stages was 10000 and the adaptation step $h = 0.00025$) by use of the activation function $Y(x) = 6.0\tanh(0.4x)$.

The performed numerical experiment simulated the operation of one transmitter T and two receivers $R1$ and $R2$. In the first receiver, the applied algorithm for recognizing the shape of noised pulses was based on the principal component analysis [7]; in the second case, it was based on the described neural network method. The absence of a priori information on the shapes of noise-free pulses (received $R1$) leads to considerable recognition errors; as a result, the information messages remain unreconstructed. This is connected, first of all, with the fact that pulse shapes (Fig. 2c) and the background source of colored noise were chosen so that the information about definite classes to which the pulses belong was maximally hid-

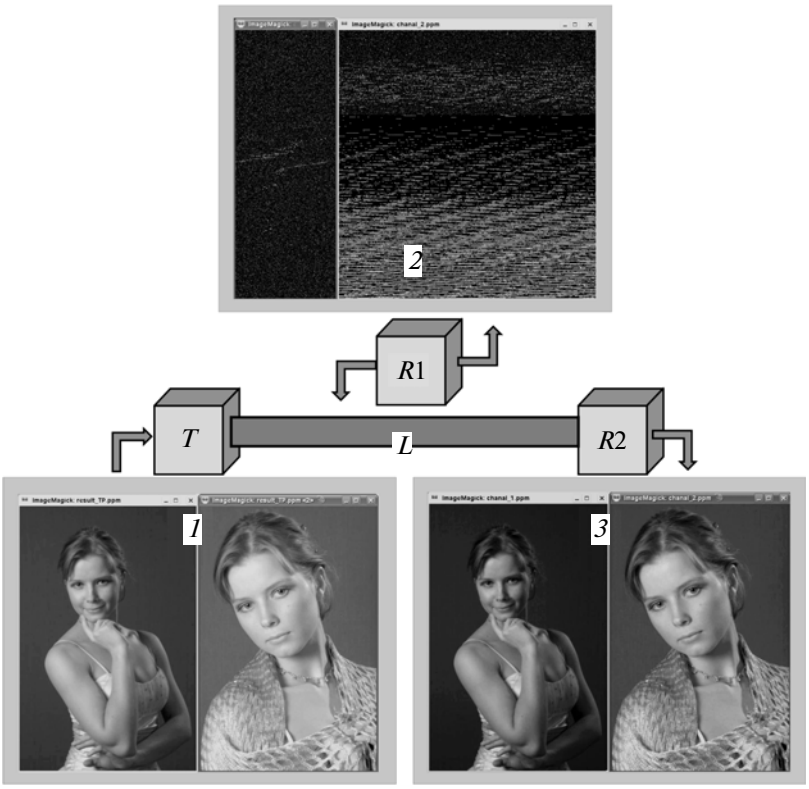

Fig. 3. Results of the numerical experiment (*T* is the transmitter, *R*1 and *R*2 are the receivers, *1* are the transmitted information messages, *2* are incorrectly segregated messages in receiver *R*1, and *3* are correctly segregated messages in receiver *R*2).

den. Algorithms that were preliminarily adapted for signal recognition (Fig. 2c) preserve their capabilities for stable classification of noisy pulses in the received message.

In the considered example, only one degree of defense was used and the information message can be reconstructed by simple exhaustion of existing variants (this needs about 2^{192000} operations). However, this method can be completed using the following elements: a generator of additional classes of masking pulses with chaotic time intervals between repetitions of the pulses, adding one empty message carrying the noise, the distribution of the composition of the information message with respect to carrying pulses, etc. The corresponding additions make it possible to significantly increase the degree of protection of a communication system from unauthorized access.

Pulse parameters

	$\mathbf{p}_1$	$\mathbf{p}_2$
a_t	3.626004	3.004003
b_t	2.988912	2.155355
ρ_t	-9.849386×10^2	-1.088808×10^3
q_t	4.759452×10^{-3}	5.128043×10^{-3}
a_e	−4.591491	−3.559475
ρ_e	4.844415×10^2	4.621989×10^2
q_e	6.303474×10^{-3}	6.194369×10^{-3}
f_s	1.153357	1.188738
φ_s	2.919729×10^{-1}	1.986695×10^{-1}
T	0.01280	0.01280

Acknowledgments. The performed investigations were supported by the Ministry of Education and Science of the Russian Federation in the framework of the federal targeted program "Scientific and Scientific-Pedagogic Staff of Innovative Russia (2009–2013)," agreement no. 14.V37.21.0751.

REFERENCES

1. L. M. Pecora and T. L. Carroll, Phys. Rev. Lett. **64**, 821 (1990).
2. K. M. Cuomo, A. V. Oppenheim, and S. H. Strogatz, IEEE Trans. Circuits Syst. II Analog Digital Signal Process. **40**, 626 (1993).
3. L. Kocarev and U. Parlitz, Phys. Rev. Lett. **74**, 5028 (1995).
4. A. S. Dmitriev, A. I. Panas, and S. O. Starkov, Int. J. Bifurcation Chaos Appl. Sci. Eng. **5**, 1249 (1995).

5. A. A. Koronovskii, O. I. Moskalenko, and A. E. Hramov, Phys. Usp. **52**, 1213 (2009).

6. V. S. Anishchenko and A. N. Pavlov, Phys. Rev. E: Stat., Nonlinear, Soft Matter Phys. **57**, 2455 (1998).

7. M. S. Lewicki, Comput. Neural Syst. **9**, R53 (1998).

8. J. C. Letelier and P. P. Weber, J. Neurosci. Methods **101**, 93 (2000).

9. A. N. Pavlov, A. E. Khramov, A.A. Koronovskii, et al., Phys. Usp. **55**, 845 (2012).

10. A. I. Nazimov and A. N. Pavlov, Proc. SPIE—Int. Soc. Opt. Eng. **7898**, 789815 (2011).

11. S. Haykin, *Neural Networks: A Comprehensive Foundation*, 2nd ed. (Prentice Hall, New Jersey, 1999).

Translated by A. Nikol'skii