11

Метод защиты передаваемой информации с использованием нейросетевого детектирования

© *А.И. Назимов, А.Н. Павлов*

Саратовский государственный университет им. Н.Г. Чернышевского
E-mail: pavlov.alexeyn@gmail.com

Поступило в Редакцию 14 мая 2013 г.

Предлагается метод защиты информации, передаваемой по каналу связи, который предусматривает кодирование информационных сообщений изменением формы последовательностей импульсов и их выделение на основе нейросетевого метода распознавания сигналов. Иллюстрируется эффективность метода при многоканальной передаче графической информации.

Проблема защиты информации, передаваемой по каналу связи, имеет длительную историю и множество возможных решений. Сравнительно новый подход базируется на использовании в качестве несущих сигналов хаотических автоколебаний [1–5]. В таких системах связи выделение информационного сообщения может основываться, например, на явлении хаотической синхронизации [1] или применении специальных приемов цифровой обработки сигналов [6]. При одновременной передаче большого числа сообщений по одному каналу связи эти подходы имеют ограничения. В данной работе мы предлагаем вариант улучшения характеристик многоканальности, который предусматривает кодирование информационных сообщений путем изменения формы передаваемых последовательностей импульсов и нейросетевой принцип детектирования.

Выберем в качестве передаваемого импульса аналоговый сигнал вида

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

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

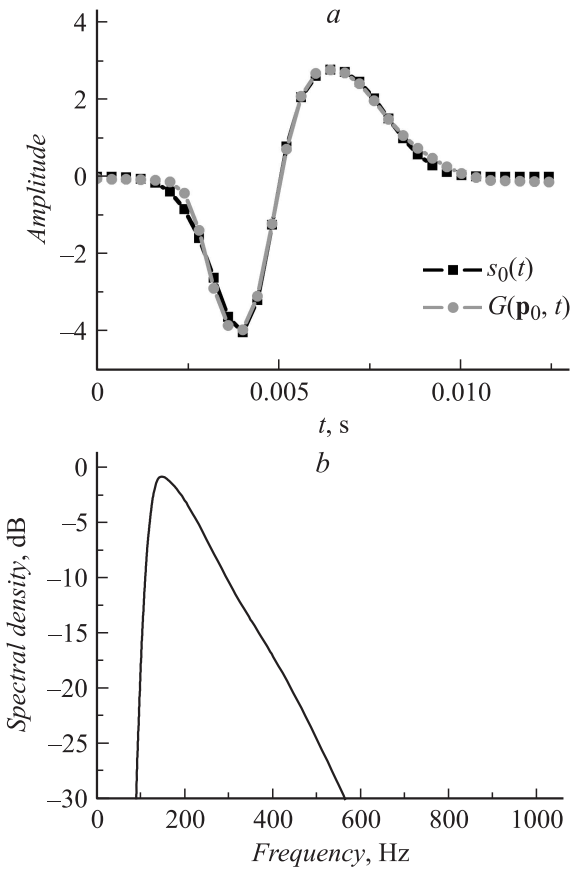

Рис. 1. Импульсные сигналы: a — импульс $G(\mathbf{p}_0, t)$ и экспериментально измеренный потенциал действия нейрона $s_0(i\Delta t)$, b — спектральная характеристика импульса $G(\mathbf{p}_0, t)$.

Функция $G(\mathbf{p}, t)$ характерна для нейронных потенциалов действия $s_0(i\Delta t)$ (рис. 1), для распознавания которых в нейродинамике разработан ряд специальных подходов [7–10]. При соответствующем задании вектора параметров $\mathbf{p}$ функция (1) позволяет осуществить достаточно точную аппроксимацию экспериментального сигнала $s_0(i\Delta t) \approx G(\mathbf{p}_0, t)$. При наличии последовательностей близких по форме импульсов разных

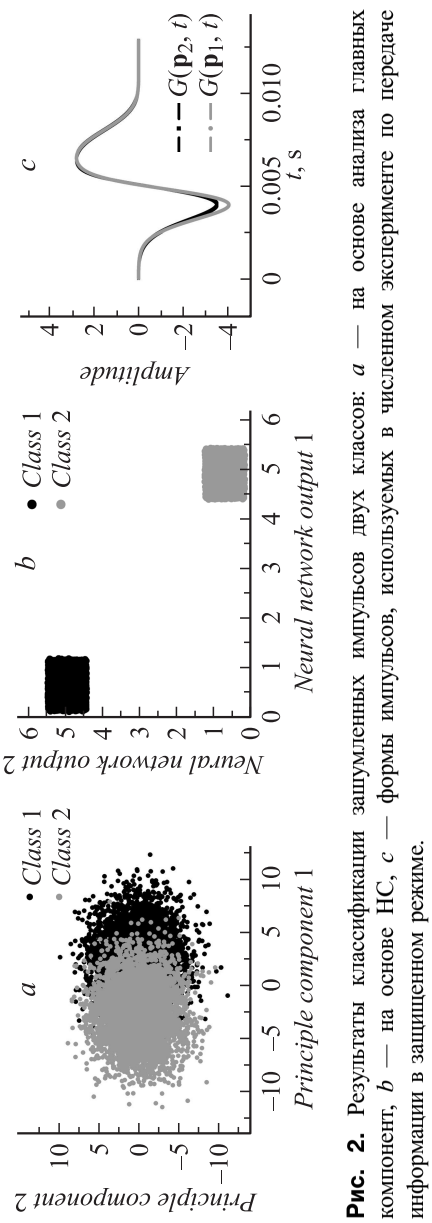

Рис. 2. Результаты классификации зашумленных импульсов двух классов: *a* — на основе анализа главных компонент, *b* — на основе НС, *c* — формы импульсов, используемых в численном эксперименте по передаче информации в защищенном режиме.

классов распознавание формы импульса в присутствии помех может быть реализовано, например, с помощью метода анализа главных компонент [7]. Однако более эффективным инструментом распознавания формы зашумленных сигналов служат искусственные нейронные сети (НС) [11] (рис. 2). Будем использовать вариант построения НС в виде перцептрона

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

где N_k — количество нейронов k-го слоя, M_k — количество синапсов нейрона k-го слоя, $Y(x)$ — функция активации, $\{y_{jk}\}$ — „активность“ нейрона, $\{\theta_{jk}\}$ — пороговый уровень, $\{w_{ijk}\}$ — синаптический коэффициент для i-синапса в j-нейроне на k-слое. Соответственно $x_i = y_{i0}$ — входной вектор, а y_{jL} — выходной вектор. Обучение НС реализуется на основе принципа обратного распространения ошибки [11].

В рамках предлагаемого метода защищенной передачи информации процесс кодирования информационных сообщений в передатчике реализуется следующим образом. Рассмотрим Q_C независимых информационных сообщений, записанных в виде матриц $\{I_k^m\}$, в которых $m \in [1; Q_C]$ — индекс номера сообщения, а $k \in [1; P_I]$ — количество информационных значений в m-сообщении.

Шаг 1. Проводится нормирование информационных сигналов по амплитуде на величину $D_A > 0$ при помощи выражения (3) с получением матрицы $\{v_k^m\}$

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

Шаг 2. Проводится построение отдельных фрагментов кодового сообщения в виде m-матриц $\{B_{ik}^m\}$ согласно (4)

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

Используется дополнительный источник цветного шума $\xi(t) \in [-1.0; 1.0]$ с параметром амплитуды α_ξ и со сплошным спектром в диапазоне $[0; f_\xi]$. Вводятся m импульсов типа (1) с векторами параметров $\mathbf{p}_m$ и одинаковой длительностью T. Устанавливается параметр длины единицы кода $D_S = 2D_A + [T/\Delta t]$.

Шаг 3. Используя отображение (5), состоящее из n итераций ($n \in [1; Q_C P_I]$), по матрицам $\{B_k^m\}$, заданным на основе (4), строится кодовое сообщение в виде сигнала $S(t)$.

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

В ходе итерирования используется случайная величина ξ_{num} с равномерным законом распределения, область значений ξ_{num} ограничена множеством $\{1, 2, \dots Q_C\}$, а также дополнительно введена τ-матрица размерностью $Q_C \times Q_C P_I$. При реализации отображения (5) в качестве начальных условий используются следующие значения: $n = 1$, $\xi_{num}^{(n)} \in \{1, 2, \dots Q_C\}$, $\tau_{\xi_{num}^{(n)} n} = 1$, $\forall k \neq \xi_{num}^{(n)}$, $\tau_{kn} = 0$.

Параметры D_A и D_S являются постоянными (априори заданными) величинами. Кодовый сигнал S для Q_C информационных сообщений будет состоять из $Q_C P_I$ последовательностей отсчетов длиной D_S. Проведение $Q_C P_I$ итераций для передатчика (5) означает необходимость проведения $Q_C P_I$ итераций для приемника. Рассмотрим алгоритм n-й итерации в приемнике.

Шаг 1. Проводятся дискретные измерения значений кодового сигнала, проходящего по каналу связи. В ходе измерений строится дискретизованный сигнал $F^n(i\Delta t)$ длительностью $D_S \Delta t$.

Шаг 2. Сигнал $F^n(i\Delta t)$ подвергается пороговому преобразованию или дискретному вейвлет-преобразованию [8] для локализации импульсов $G(\mathbf{p}_m, i\Delta t)$ длиной T. При локализации импульса определяется его центральная точка — величина t_S.

Шаг 3. С помощью НС (2), адаптированной к распознаванию импульсов типа (1), проводится распознавание входного вектора, представленного в виде $x_i = G(\mathbf{p}_m, t_S + i\Delta t - T/2)$. Выходной вектор y_{jL} НС анализируется при помощи функционала (6), в котором y_j^m — библиотечные вектора (m штук, $m \in [1; Q_C]$), сформированные при обучении НС

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

Шаг 4. На основании условия (7) определяется матрица ν_k^m для приемника

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

Шаг 5. По значениям $\{\nu_k^m\}$ восстанавливается нормированное значение I_k^m (8) для m-го информационного сообщения

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

Таким образом, если на каждой n-й итерации выполняются шаги 1–5 алгоритма для приема сообщений, то в соответствии с формулами (6)–(9) постепенно будет происходить восстановление всех Q_C передаваемых сообщений в виде матриц $\{I_k^m\}$, $m \in [1; Q_C]$, $k \in [1; P_I]$.

Для тестирования предложенного метода защищенной передачи информации был проведен численный эксперимент, в котором проводилось моделирование работы передатчика и приемника. В ходе численного эксперимента алгоритм кодирования работал в режиме передачи двух ($Q_C = 2$) информационных сообщений в виде двух черно-белых изображений (рис. 3), для которых $P_I = 400 \times 600$. В качестве передаваемых импульсов были выбраны импульсы типа (1), изображенные на рис. 2, *c*. Длительность импульсов составляла $T = 0.0128$ s при шаге временно́й дискретизации $\Delta t = 0.0004$ s. Координаты векторов $\mathbf{p}_1$, $\mathbf{p}_2$, задающих формы импульсов, приведены в таблице. Остальные параметры были выбраны следующими: $D_A = 255$, $\alpha_\xi = 0.6$, $f_\xi = 1500$ Hz. Для распознавания использовалась 3-слойная НС со следующей организацией: $N_1 = 32$, $M_1 = 32$, $N_2 = 250$, $N_3 = 2$. Адаптация проводилась на основе выборки из 400 импульсов, зашумленных источником цветного шума ξ

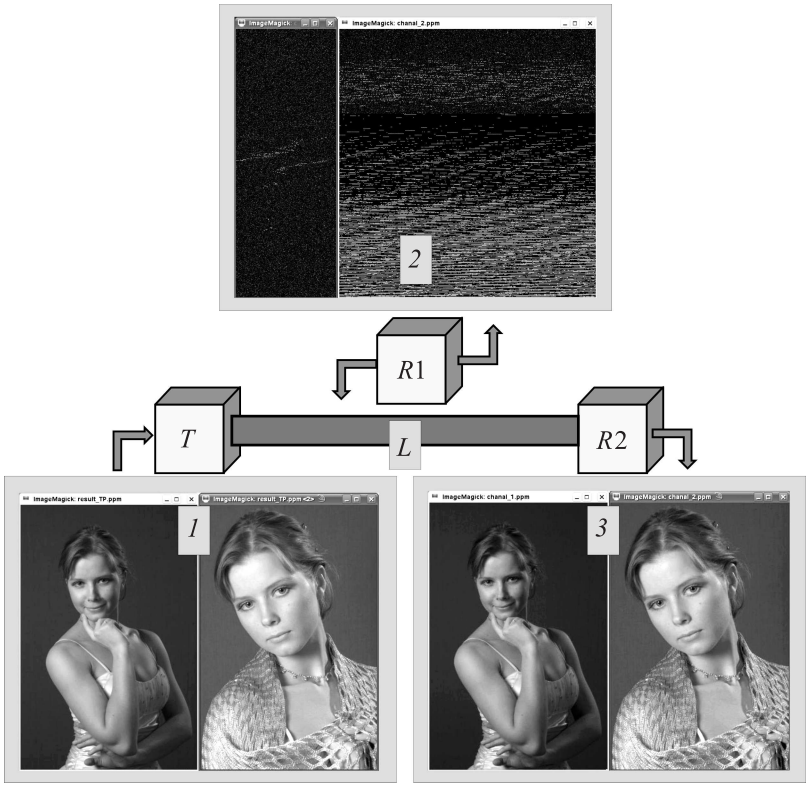

Рис. 3. Результаты численного эксперимента (T — передатчик, $R1$ и $R2$ — приемники, *1* — передаваемые информационные сообщения, *2* — неправильно выделенные сообщения в приемнике $R1$, *3* — правильно выделенные сообщения в приемнике $R2$).

($\alpha_\xi = 0.9$, $f_\xi = 1500\,\mathrm{Hz}$), для двух классов (количество этапов адаптации 10 000, шаг адаптации $h = 0.00025$) с использованием функции активации $Y(x) = 6.0\mathrm{th}(0.4x)$.

В проведенном численном эксперименте была смоделирована работа одного передатчика T и двух приемников $R1$ и $R2$. В первом приемнике применялся алгоритм распознавания формы зашумленных импульсов

Параметры импульсов

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

на основе анализа главных компонент [7], а во втором приемнике — описанный нейросетевой метод. Отсутствие априорной информации о формах незашумленных импульсов (приемник $R1$) приводит к значительным ошибкам распознавания, в результате которых восстановления информационных сообщений не происходит. Прежде всего, это связано с тем, что формы импульсов (рис. $2, c$) и фоновый источник цветного шума подобраны таким образом, чтобы максимально скрыть информацию о принадлежности импульсов к определенному классу. При этом алгоритмы, предварительно адаптированные для распознавания сигналов (рис. $2, c$), сохраняют способности к устойчивой классификации зашумленных импульсов в принимаемом сообщении.

В рассмотренном примере была использована только одна степень защиты, и восстановление информационных сообщений возможно путем простого перебора существующих вариантов (для этого потребуется около $2^{192\,000}$ операций). Однако данный метод можно дополнить следующими элементами: генератор дополнительных классов маскировочных импульсов с хаотическими временны́ми интервалами между следованиями импульсов; добавление одного пустого сообщения, несущего шум; закон распределения состава информационного сообщения по несущим импульсам и т. п. Соответствующие дополнения позволяют существенно повысить степень защищенности системы связи от несанкционированного доступа.

Проводимые исследования были поддержаны Министерством образования и науки РФ в рамках ФЦП „Научные и научно-педагогические кадры инновационной России на 2009–2013 гг.“ (соглашение 14.B37.21.0751).

Список литературы

[1] *Pecora L.M., Carroll T.L.* // Phys. Rev. Lett. 1990. V. 64. P. 821.
[2] *Cuomo K.M., Oppenheim A.V., Strogatz S.H.* // IEEE Trans. Circuits Syst. II Analog Digital Signal Process. 1993. V. 40. P. 626.
[3] *Kocarev L., Parlitz U.* // Phys. Rev. Lett. 1995. V. 74. P. 5028.
[4] *Dmitriev A.S., Panas A.I., Starkov S.O.* // Int. J. Bifurcat. Chaos. 1995. V. 5. P. 1249.
[5] *Короновский А.А., Москаленко О.И., Храмов А.Е.* // УФН. 2009. Т. 179. С. 1281; *Koronovskii A.A., Moskalenko O.I., Hramov A.E.* // Phys. Usp. 2009. V. 52. P. 1213.
[6] *Anishchenko V.S., Pavlov A.N.* // Phys. Rev. E. 1998. V. 57. P. 2455.
[7] *Lewicki M.S.* // Comput. Neural Syst. 1998. V. 9. P. R53.
[8] *Letelier J.C., Weber P.P.* // J. Neurosci. Methods. 2000. V. 101. P. 93.
[9] *Павлов А.Н., Храмов А.Е., Короновский А.А.* и др. // УФН. 2012. Т. 182. № 9. С. 905; *Pavlov A.N, Hramov A.E., Koronovskii A.A.* et al. // Phys. Usp. 2012. V. 55. P. 845.
[10] *Nazimov A.I., Pavlov A.N.* // Proc. SPIE. 2011. V. 7898. P. 789 815.
[11] *Хайкин С.* Нейронные сети: Полный курс. 2-е изд. М.: Вильямс, 2006. 1104 с.; *Haykin S.* Neural Networks: A Comprehensive Foundation. 2nd Ed. New Jersey: Prentice-Hall, 1999. 823 p.