УДК 004.056.52

ИСПОЛЬЗОВАНИЕ ВЕЙВЛЕТ-ПРЕОБРАЗОВАНИЯ ДЛЯ ВЫДЕЛЕНИЯ БИОМЕТРИЧЕСКИХ ХАРАКТЕРИСТИК ПОТЕНЦИАЛА P300 В ЗАДАЧАХ ВЫСОКОНАДЕЖНОЙ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ

С.М. Гончаров, А.Е. Боршевников

В статье рассматривается эксперимент по восстановлению криптографического ключа нейросетевым преобразователем «Биометрия - код доступа» из набора коэффициентов вейвлет-преобразования сигнала электроэнцефалограммы. Приводится сравнение эффективности применения вейвлет-преобразования и преобразования Фурье для выделения параметров биометрических данных

Ключевые слова: информационная безопасность, нейросетевой преобразователь «Биометрия - код доступа», электроэнцефалограмма, восстановление ключа, вейвлет-преобразование, P300

Современное состояние информационного общества подразумевает рост востребованности в более надежных средствах защиты информации. В частности, растет потребность в технологиях биометрической аутентификации.

Особый интерес среди всего рынка биометрических технологий вызывают технологии высоконадежной биометрической аутентификации. Под средствами высоконадежной высоконадежной биометрической аутентификацией понимается биометрическая аутентификация с приемлемой вероятностью ошибок первого рода и гарантированно малой вероятностью ошибок второго рода, сопоставимой по своему значению с вероятностью случайного подбора кода неизвестного криптографического ключа при малом числе попыток подбора [1].

По данным, приведенным в открытых источниках, подход, основанный на использовании больших и сверхбольших нейронных сетей, обеспечивает более низкую ошибку второго рода, хотя для практического использования реализованы, в основном, системы, использующие в качестве биометрической характеристики рукописный почерк.

Гончаров Сергей Михайлович – МГУ им. Г.И. Невельского, канд. физ.-мат. наук, профессор, e-mail: sgprim@smtp.ru

Боршевников Алексей Евгеньевич - ДВФУ, аспирант, e-mail: LAdG91@mail.ru

Большую значимость в вопросе разработки технологии биометрической аутентификации имеет выбор биометрической характеристики, а также выбор метода ее обработки. Одной из перспективных биометрических характеристик является электроэнцефалограмма (ЭЭГ) [2,3].

Принято считать, что ЭЭГ является нестационарным сигналом. Это делает использование преобразования Фурье для анализа сигнала ЭЭГ проблематичной, так как классический Фурье-анализ предполагает стационарность сигнала. В отличие от дискретного преобразования Фурье, непрерывное вейвлет-преобразование позволяет отследить динамику изменения гармонических составляющих сигнала с течением времени [4].

Непрерывное вейвлет-преобразование определяется как скалярное произведение исходного сигнала $x(t)$ и дочерней вейвлет-функции $\psi_{\tau,\alpha}(t)$:

$$V(\tau,\alpha) = \langle x(t), \psi_{\tau,\alpha}(t) \rangle = \int_{-\infty}^{\infty} x(t)\psi^{*}_{\tau,\alpha}(t)dt$$

$$\tau \in R, \alpha \in R^{+}.$$

Здесь $V(\tau,\alpha)$– коэффициенты вейвлет-разложения; τ , α – параметры временного сдвига и масштаба соответственно; оператор * означает комплексное сопряжение.

Дочерние вейвлет-функции $\psi_{\tau,\alpha}(t)$ образуются путем операций сдвига и масштабирования материнской вейвлет-

функции $\psi(t)$ и связаны с ней соотношением:

$$\psi_{\tau,\alpha}(t) = \frac{1}{\sqrt{\alpha}}\psi\left(\frac{t-\tau}{\alpha}\right).$$

В качестве материнской вейвлет-функции был выбран комплексный вейвлет Морле, который представляет собой произведение комплексной синусоиды на гауссиан. Аналитическое выражение вейвлета Морле имеет вид:

$$\psi(t) = \frac{1}{\sqrt[4]{\sigma^2\pi}} \cdot e^{-\frac{t^2}{\sigma^2}} \cdot e^{j\omega_0 t},$$

где ω_0 – центральная частота материнского вейвлета; σ – стандартное отклонение огибающей материнского вейвлета.

На практике расчет коэффициентов вейвлет-разложения осуществляется в узлах некоторой дискретной сетки, заданной на плоскости (τ,α). Пусть $V\{v_{ij}\}$ – матрица коэффициентов вейвлет-разложения для сигнала $x(t)$, представленного в виде последовательности отсчетов, взятых с частотой дискретизации F_s в моменты времени с номерами $n = \overline{0, N-1}$. Тогда элементы матрицы V определяются, исходя из выражения:

$$\bar{v}_{ij} = \sum_{n=0}^{N-1} x(n) \cdot \psi^*\left(\frac{n\Delta t - t_i}{\alpha_j}\right),$$
$$i = \overline{0, N_\tau - 1}; j = \overline{0, N_\alpha - 1},$$

где $x(n)$ – измеренное значение сигнала в момент времени с номером $n; \tau_i, \alpha_j$ – значения временного сдвига и масштаба в узле сетки с номером $(i, j); N_\tau$ – разрешение матрицы V по времени; N_α – разрешение матрицы V по масштабу; Δt – интервал дискретизации.

Для выделения потенциала Р300 был проведен следующий эксперимент [3]. Была использована зрительная стимуляция из поочередно меняющихся цифр от «0» до «9». Пользователь выбирал 1, 2 или 4 символа и при их появлении на экране поочередно концентрировался на них. Запись данных производилась в течение 10 секунд. Набор символов, на которых концентрировался пользователь, составляет «мысленный пароль» пользователя.

В результате применения вейвлет-преобразования мы получаем набор комплексных коэффициентов a_q. Из оставшихся значений выбираются R максимальных по амплитуде значений коэффициентов и формируются следующие вектора:

$$\bar{a}_q = \left\{ \max_{v_{ij}} v_{qr} \right\}, 1 \le q \le Q, 1 \le r \le R,$$

где $\bar{a}_q$ – вектор биометрических данных, используемый в нейросетевом преобразователе; Q - общее количество электродов электроэнцефалографа; R - количество выбираемых коэффициентов.

Для обработки полученных данных в качестве структуры преобразователя выбрана двухслойная нейронная сеть с сигмоидальными передаточными функциями.

Для обучения выбрана стандартная процедура обучения нейросетевых преобразователей «Биометрия - код доступа», описанная в стандарте ГОСТ Р 52633.5-2011 [5]. Результатом выполнения данной процедуры будут являться весовые коэффициенты нейронной сети:

$$\bar{w}_q = \{w_{qr}\}, 1 \le q \le Q, 1 \le r \le R,$$
$$\bar{W} = \{W_k\}, 1 \le k \le K,$$

где $\bar{w}_q$ – вектор весовых коэффициентов первого слоя нейронной сети, соответствующий вектору $\bar{a}_q$; $\bar{W}$ – вектор весовых коэффициентов второго слоя нейронной сети; K – количество нейронов первого слоя.

Для описания работы первого слоя введем следующую величину:

$$n_q = \bar{a}_q \cdot \bar{w}_q, 1 \le q \le Q.$$

Это нормированная величина, которая подается на входы сумматоров с электрода i. Составим вектор таких значений:

$$\bar{n} = \{n_q\}, 1 \le q \le Q.$$

Работу каждого нейрона первого слоя можно описать следующим образом:

$$x_{1,k} = \overline{n} \cdot \overline{net}_k,$$

$$\overline{net}_k = \{\Delta_q\}, 1 \le q \le Q,$$

$$y_{1,k} = \frac{2}{1+e^{x_{1,k}}} - 1,$$

$$t_k = \mathrm{f}_1(y_{1,k}) = \begin{cases} 1, y_{1,k} \ge 0 \\ -1, y_{1,k} < 0 \end{cases}, 1 \le k \le K,$$

где $x_{1,k}$ – это результат работы сумматора нейрона k первого слоя; $\overline{net}_k$ - вектор связей нейрона k; Δ_q – коэффициент использования данных электрода q в нейроне. Если электрод используется в данном нейроне, то $\Delta_q = 1$ и $\Delta_q = 0$ в противном случае; $y_{1,k}$ – передаточная функция первого слоя нейронной сети; $\mathrm{f}_1(y_{1,k})$ – решающее правило для нейрона первого слоя.

Каждый нейрон второго слоя можно описать следующим образом:

$$x_{2,l} = \sum_{k=1}^{K} W_k t_k \Delta_l, 1 \le k \le K,$$

$$y_{2,l} = \frac{2}{1+e^{x_{2,l}}} - 1,$$

$$k_l = \mathrm{f}_2(y_{2,l}) = \begin{cases} 1, y_{2,l} \ge 0 \\ 0, y_{2,l} < 0 \end{cases}, 1 \le l \le L,$$

где $x_{2,l}$ – это результат работы сумматора нейрона второго слоя; Δ_l – коэффициент использования компонента t_k в нейроне. Если t_k используется в данном нейроне, то $\Delta_l = 1$ и $\Delta_l = 0$ в противном случае; $y_{2,l}$ – передаточная функция второго слоя нейронной сети; $\mathrm{f}_2(y_{2,l})$ – решающее правило для нейрона второго слоя; L - длина восстанавливаемого криптографического ключа.

Результат работы каждого нейрона второго слоя k_l является битом восстанавливаемого секретного криптографического ключа.

В проведенном эксперименте использовались следующие параметры. Количество электродов $Q = 14$. Было опытно установлено, что для корректной работы преобразователя требуется выборка из $R = 15$ коэффициентов вейвлет-преобразования. Количество нейронов первого слоя $K = 320$. Размер восстанавливаемого ключа был выбран $L = 256$, что означает во втором слое нейронной сети использовалось 256 нейронов. Количество входов на нейрон было взято 4.

Для проведения исследования построенного преобразователя была создана база из 10 различных биометрических образов, для каждого из которых было снято 20 примеров ЭЭГ. Один образ был выбран в качестве образа «Свой», остальные девять сформировали базу образов «Чужой».

Был проведен опыт по возможности получения злоумышленником секретного ключа при условии знания злоумышленником мысленного пароля. Сравнение результатов выделения параметров с помощью преобразования Фурье и вейвлет-преобразования приведены в таблице (табл. 1).

Табл. 1

Расстояние Хэмминга до секретного ключа пользователя в случае знания злоумышленником «мысленного пароля»

Номер пользователя	Расстояние Хэмминга до секретного ключа					
	Вейвлет-преобразование			Преобразование Фурье		
	1 символ в пароле	2 символа в пароле	4 символа в пароле	1 символ в пароле	2 символа в пароле	4 символа в пароле
1	134	142	101	59	79	60
2	114	149	41	51	73	75
3	94	126	132	61	70	64
4	93	77	111	60	87	63

5	59	97	143	70	95	88
6	35	85	84	69	67	85
7	108	81	129	77	95	79
8	29	73	91	68	85	90
9	28	75	67	86	81	65

Наиболее интересными являются следующие результаты:

1. Расстояние Хэмминга для данных полученных при использовании вейвлет-преобразования в среднем лучше, чем при использовании преобразования Фурье.
2. Во всех опытах по восстановлению ключа пользователем преобразователь безошибочно восстанавливал секретный ключ для данных, полученных из преобразования Фурье.
3. Отмечены случаи ошибочного восстановления секретного ключа для данных, полученных из вейвлет-преобразования (максимальное расстояние Хэмминга в этих случаях составляло 4).

Вейвлет-преобразование является перспективной технологией для выделения параметров биометрических данных, однако требуется дальнейшая доработка процедуры ее применения для ЭЭГ.

Литература

1. Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации: ГОСТ Р 52633.0-2006. – Введен впервые; Введ. 27.12.2006. – М.: Стандартинформ, 2007. – 25 с.
2. Yang, S. The Use of EEG Signals For Biometric Person Recognition. Doctor of Philosophy (PhD) thesis // Kent Academic Repository. University of Kent. URL: https://kar.kent.ac.uk/53681/1/235Thesis%20(Su%20Yang).pdf (дата обращения: 20.06.2016).
3. Гончаров, С.М. Построение нейросетевого преобразователя «Биометрия - код доступа» на основе параметров визуального вызванного потенциала электроэнцефалограммы / С.М. Гончаров, А.Е. Боршевников // Доклады Томского государственного университета систем управления и радиоэлектроники: Научный журнал. – Томск: Изд-во ТУСУР, 2014. – № 2. – С. 51–55.
4. Блаттер, К. Вейвлет-анализ. Основы теории [Текст] / К. Блаттер. - М.: РИЦ «Техносфера», 2004. -280 с.
5. Защита информации. Техника защиты информации. Автоматическое обучение нейросетевых преобразователей биометрия - код доступа: ГОСТ Р 52633.5-2011. – Введен впервые; Введ. 01.12.2011. – М.: Стандартинформ, 2012. – 20 с.

ФГБОУ ВО «Морской государственный университет имени адмирала Г.И. Невельского»
Maritime state university named after admiral G.I. Nevelskoy
ФГАОУ ВО «Дальневосточный федеральный университет»
Far eastern federal university

HIGHLY RELIABLE BIOMETRIC AUTHENTICATION USING WAVELET TRANSFORM FOR ALLOCATION FROM P300

S.M. Goncharov, A.E. Borshevnikov

The article discusses an experiment to restore the cryptographic key using neural network transformer «Biometrics - access code» from the set of the wavelet transform coefficients of electroencephalogram signal. The paper compares the effectiveness of the wavelet transform and Fourier transform to extract the biometric parameters

Key words: information security, neural network transformer «Biometry - access code», electroencephalogram, key recovery, wavelet transform, P300