УДК 004.056.52

ВОССТАНОВЛЕНИЕ СЕКРЕТНОГО КЛЮЧА НА ОСНОВЕ ЭЛЕКТРОЭНЦЕФАЛОГРАММЫ ПРИ ДВИЖЕНИИ ГЛАЗ С ЗАКРЫТЫМИ ВЕКАМИ

С.М. Гончаров, А.Е. Боршевников, А.Г. Михайлов, А.Ю. Апальков

В статье рассматривается возможность построения нейросетевого преобразователя "Биометрия - код доступа" на основе потенциала движения мышц глаз. Описывается структура нейросетевого преобразователя "Биометрия - код доступа", используемого для восстановления ключа. Рассчитаны характеристики данного преобразователя и сравнены с характеристиками нейросетевого преобразователя "Биометрия - код доступа" на основе потенциала P300

Ключевые слова: нейросетевой преобразователь "Биометрия - код доступа", криптографический ключ, восстановление ключа, электроэнцефалограмма, потенциал движения глаз, биометрическая аутентификация

Стремительное развитие технологий позволяет обеспечивать более высокий уровень безопасности. Не является исключением и биометрия. Одной из многообещающих технологий этой области является технология биометрической аутентификации на основе электроэнцефалограммы (ЭЭГ).

Современные исследования в указанной области показывают недостаточно высокие результаты. Значения вероятности ошибок второго рода для технологий аутентификации на основе ЭЭГ варьируется от 10^{-1} до 10^{-3}.

Решением, позволяющим повысить характеристики систем биометрической аутентификации на основе ЭЭГ, может послужить использование аппарата больших и сверхбольших нейронных сетей для восстановления секретного ключа. Упомянутые нейронные сети получили название нейросетевых преобразователей "Биометрия - код доступа". Данная технология принята в качестве государственного стандарта Российской Федерации по высоконадежной биометрии и описана в линейке стандартов ГОСТ Р 52633 [1,2,3].

На начальном этапе исследований по биометрической идентификации на основе ЭЭГ нарабатывался опыт использования технологий «интерфейс мозг-компьютер» [4]. Далее проводились исследования по построению нейросетевого преобразователя "Биометрия - код доступа" с использованием вызванных потенциалов мозга [5]. В качестве биометрических параметров бралась разность потенциалов ЭЭГ пользователя в состоянии покоя и при его стимулировании. Для выделения потенциала P300 в данной работе использовалась стимуляция из поочередно меняющихся на экране цифр от "0" до "9". Пользователь выбирал одну или несколько цифр и при их появлении концентрировался на них. Этот набор цифр считался мысленным паролем.

Отдельный интерес представляет разработка нейросетевого преобразователя на основе ЭЭГ без использования внешней стимуляции. Было решено провести эксперименты по построению нейросетевого преобразователя на основе движения глаз с закрытыми веками. С целью повышения эффективности работы преобразователя в качестве входных параметров при этом использовались коэффициенты дискретного преобразования Фурье соответствующих ЭЭГ пользователей.

Для упрощения проведения эксперимента использовалась звуковая стимуляция метрономом, с интервалом 2 секунды. Запись данных производилась в течение 8 секунд. На каждый удар метронома

Гончаров Сергей Михайлович - МГУ им. Г.И. Невельского, к.ф.-м.н., профессор,
e-mail: sgprim@smtp.ru
Боршевников Алексей Егеньевич - ДВФУ, аспирант,
e-mail: LAdG91@mail.ru
Михайлов Андрей Геннадьевич - ДВФУ, студент,
e-mail: quantum722@gmail.com
Апальков Артем Юрьевич - ДВФУ, студент,
e-mail: apalkov995@gmail.com

испытуемый производил соответствующие движения глазами (влево, вправо, вверх, вниз, вращение по кругу и т.д.). Движение глаз производилось с закрытыми веками. Последовательность движений составляет мысленный пароль пользователя.

Описанные условия выбирались по следующим причинам. Запись в течение 8 секунд производилась для того, чтобы получить набор дискретных значений ЭЭГ. С этой целью использовался алгоритм быстрого преобразования Фурье. Произведение движений с закрытыми веками обеспечивает невозможность зрительного определения вводимого пароля злоумышленником.

В результате применения быстрого преобразования Фурье мы получаем набор комплексных коэффициентов a_i, где i – номер электрода, с которого снята ЭЭГ. После этого отбрасываются коэффициенты, не удовлетворяющие условию $10° < \arg a_i < 90°$. Наложив это условие, мы подразумеваем то, что мы анализируем только неубывающие всплески ЭЭГ. Из оставшихся значений выбираются j максимальных по амплитуде значений коэффициентов и формируются следующие вектора:

$$\overline{a}_i = \{a_{ij}\}, \quad (1)$$

$$a_{ij} = \max_{a_i} |a| \cdot \cos(\arg a), 1 \le i \le I, 1 \le j \le J, \quad (2)$$

где $\overline{a}_i$ – вектор биометрических данных, используемый в нейросетевом преобразователе; I - общее количество электродов электроэнцефалографа; J - количество выбираемых коэффициентов.

В связи с тем, что количество входов должно быть значительно больше количества нейронов в первом слое [2], было принято решение производить выборку 74 коэффициентов разложения Фурье.

Умножение на косинус аргумента комплексного коэффициента введено для получения такой характеристики сигнала, как время наибольшего возрастания сигнала.

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 [2]. Для обучения необходимо сформировать базу электроэнцефалограмм при воздействии стимуляции образов "Чужой", т.е. образов злоумышленника, для которых нейронная сеть будет выдавать случайный криптографический ключ, а также необходимо сформировать базу электроэнцефалограмм образов "Свой" - пользователя, который будет считаться законным. Результатом выполнения данной процедуры будут являться весовые коэффициенты нейронной сети:

$$\overline{w}_i = \{w_{ij}\}, 1 \le i \le I, 1 \le j \le J, \quad (3)$$

$$\overline{W} = \{W_k\}, 1 \le k \le K, \quad (4)$$

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

Нейроны первого и второго слоя сходны по строению, но имеют различие в обрабатываемых данных и получаемых результатах. Для описания работы первого слоя введем следующую величину:

$$v_i = \overline{a}_i \cdot \overline{w}_i, 1 \le i \le I. \quad (5)$$

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

$$\overline{v} = \{v_i\}, 1 \le i \le I. \quad (6)$$

Работу каждого нейрона первого слоя можно описать следующим образом:

$$x_{1,k} = \overline{v} \cdot \overline{net}_k, \quad (7)$$

$$\overline{net}_k = \{\Delta_i\}, 1 \le i \le I, \quad (8)$$

$$y_{1,k} = \frac{2}{1 + e^{x_{1,k}}} - 1, \quad (9)$$

$$t_k = f_1(y_{1,k}) = \begin{cases} 1, y_{1,k} \ge 0 \\ -1, y_{1,k} < 0 \end{cases}, 1 \le k \le K, \quad (10)$$

где $x_{1,k}$ – это результат работы сумматора нейрона k первого слоя; $\overline{net}_k$ - вектор связей нейрона k; Δ_i – коэффициент использования данных электрода i в нейроне. Если электрод используется в данном нейроне, то $\Delta_i = 1$ и $\Delta_i = 0$ в противном случае; $y_{1,k}$ –

передаточная функция первого слоя нейронной сети; $f_1(y_{1,k})$ – решающее правило для нейрона первого слоя.

Используемые в сумматорах нейрона вектора нормированных биометрических данных определяются следующим образом. В любом сумматоре обязательно используется один из нескольких векторов, соответствующих векторам данных, характеризующим наиболее сильный потенциал движения глаз. Для оставшихся входов сумматора используются не использованные вектора нормированных биометрических данных.

Каждый нейрон второго слоя можно описать следующим образом:

$$x_{2,l} = \sum_{k=1}^{K} W_k t_k \Delta_l \ , 1 \le k \le K \ , \qquad (11)$$

$$y_{2,l} = \frac{2}{1+e^{x_{2,l}}} - 1 , \qquad (12)$$

$$k_l = f_2(y_{2,l}) = \begin{cases} 1, y_{2,l} \ge 0 \\ 0, y_{2,l} < 0 \end{cases}, 1 \le l \le L \ , \qquad (13)$$

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; $f_2(y_{2,l})$ – решающее правило для нейрона второго слоя; L - длина восстанавливаемого криптографического ключа.

Используемые в сумматорах нейрона выходы первого слоя определяются согласно процедуре, описанной в ГОСТ Р 52633.5-2011 [2].

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

В проведенном эксперименте использовались следующие параметры. Количество электродов $I = 14$. Количество выбираемых коэффициентов Фурье для одного $J = 74$. Количество нейронов первого слоя $K = 320$. Размер восстанавливаемого ключа был выбран $L = 256$, что означает использование во втором слое нейронной сети 256 нейронов. Количество входов на нейрон было взято 4.

Для проведения исследования характеристик построенного преобразователя была создана база биометрических образов для 10 различных испытуемых, для каждого из которых было снято 20 примеров ЭЭГ. Образы одного пользователя были выбраны в качестве базы образов "Свой", остальные девять испытуемых сформировали базу "Чужой".

Был проведены исследования по возможности получения злоумышленником секретного ключа при условии знания мысленного пароля (табл. 1).

Табл. 1

Расстояние Хэмминга до секретного ключа пользователя в случае знания злоумышленником пароля

Номер пользователя	Расстояние Хэмминга
1	26
2	24
3	82
4	51
5	22
6	44
7	54
8	18
9	93

Приведем схему приблизительной оценки ошибки второго рода на основе полученных результатов.

Вероятность ошибки второго рода P_2 можно вычислить приближенно, исходя из гипотезы нормального закона распределения значений вероятности ошибок, по формуле [3]:

$$P_2 \approx \frac{1}{\sqrt{2\pi}} \int_{\sqrt{n}E(q(v))}^{\infty} e^{-\frac{x^2}{2}} dx , \qquad (14)$$

где n – число учитываемых преобразователем биометрических параметров; $E(q(v))$ – среднее качество всех учитываемых преобразователем биометрических параметров.

В построенном преобразователе использовались 1036 параметров. Производя вычисления по формуле (14), получим

приблизительную оценку вероятности ошибки второго рода $P_2 \le 10^{-12}$.

Приведем основные результаты проведенных исследований:

1. Предварительные оценки вероятности ошибки 2-го рода при аутентификации с использованием технологий визуальной стимуляции и движения глаз с закрытыми веками дают значение ниже 10^{-12}. Таким образом, эффективность разработанного метода биометрической идентификации на основе ЭЭГ, по крайней мере, в 10^6 раз выше известных зарубежных аналогов.

2. Во всех опытах по восстановлению ключа легитимным пользователем секретный ключ восстанавливался безошибочно.

3. Даже в случае, когда злоумышленник угадывает "мысленный пароль", минимальное расстояние Хэмминга от полученного злоумышленником ключа до секретного ключа пользователя было равно 18. При генерации злоумышленником ошибочного «мысленного пароля» усредненное расстояние Хэмминга до истинного ключа значительно выше.

4. Результаты работы нейросетевого преобразователя на основе движения глаз с закрытыми веками сравнимы по эффективности с результатами на основе визуального вызванного потенциала с использованием сигнала P300 [5].

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. 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.

3. Защита информации. Техника защиты информации. Требования к формированию баз естественных биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации: ГОСТ Р 52633.1–2009. – Введен впервые; Введ. 15.12.2009. – М.: Стандартинформ, 2010. – 24 с.

4. Гончаров С.М. Использование потенциалов коры головного мозга для парольной идентификации на основе технологии «ИМК» / С.М. Гончаров, М.С. Вишняков, М.Е. Маркин // Журнал «Информация и безопасность». Вып. 3. Воронеж: ВГТУ, 2012. - С. 404-409.

5. 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.

Дальневосточный федеральный университет, Морской государственный университет имени адмирала Г.И. Невельского
Far Eastern Federal University, Admiral G.I. Nevelskoy Maritime State University

KEY RECOVERY BASED ON A ELECTROENCEPHALOGRAM WHILE MOVING THE CLOSED EYE

S.M. Goncharov, A.E. Borshevnikov, A.G. Mikhailov, A. Yu. Apalkov

Researched the construction of neural net transformer "Biometry - access code" based on the movement potential of eye muscles. Describes the structure of neural net transformer "Biometry - access code" to be used for key recovery. The characteristics of this transformer computed and compared with the characteristics of neural net transformer "Biometry - access code" based on P300

Key words: neural net transformer "Biometrics - access code", a cryptographic key, key recovery, electroencephalogram, movement potential of eye muscles, biometric authentication