Вестник Морского государственного университета им. адм. Г. И. Невельского. Серия : Автоматическое управление, математическое моделирование и информационные технологии. Вып. 65/2014. – Владивосток : Мор. гос. ун-т, 2014 – 125 с.

ISBN 978-5-8343-0902-4

Учредитель журнала – Морской институт
информационных технологий
МГУ имени адмирала Г. И. Невельского

ISBN 978-5-8343-0902-4

ОГЛАВЛЕНИЕ

Междуведомственного совета по управлению движением судов и специальных аппаратов. – М.: Ин-т проблем управления РАН, 2002. – С. 12-25.

4. Веремей Е.И. [и др.]. Компьютерное моделирование систем управления движением морских подвижных объектов. - СПб.: НИИ Химии СПбГУ, 2002. - 370 с.

УДК 681.322.067

С.М. Гончаров, А.Е. Боршевников, В.С. Горев, А.О. Перцев

РАСЧЕТ ХАРАКТЕРИСТИК НЕЙРОСЕТЕВОГО ПРЕОБРАЗОВАТЕЛЯ "БИОМЕТРИЯ - КОД ДОСТУПА" НА ОСНОВЕ ЭЛЕКТРОЭНЦЕФАЛОГРАММЫ

В настоящее время наиболее эффективными средствами обеспечения безопасности данных пользователей являются криптографические средства защиты информации. Использование подобных средств подразумевает использование некоторого секрета (криптографического ключа, пароля и т.д.). Наиболее удобным способом связывания секретной информации пользователем была бы привязка информации к биометрическим характеристикам пользователя. Именно подобной технологией является технология восстановления ключа.

Один из эффективных подходов надежного хранения и восстановления секретного ключа используется в России. Для хранения секретных ключей (паролей) была предложена идея использования нейросетевых преобразователей "Биометрия - код доступа". Описанию данных преобразователей посвящена линейка стандартов ГОСТ Р 52633. Данные преобразователи обеспечивают выбранный уровень вероятности ошибки первого рода, а также хороший результат по уровню ошибки второго рода [2,3].

Высокий уровень безопасности таких преобразователей в первую очередь определяется выбором биометрической характеристики, которая используется для восстановления ключа. Для использования в качестве биометрической характеристики большой интерес представляют параметры электроэнцефалограммы мозга (ЭЭГ). Использование ЭЭГ в качестве биометрической характеристики дает несколько преимуществ. Данные ЭЭГ конфиденциальны, их сложно подделать, а также они обеспечивают дополнительную меру защищенности от перехвата злоумышленником. Данная мера заключается в том, что снятие электроэнцефалограммы возможно на расстоянии не более 1 миллиметра от головы, что означает невозможность незаметного для пользователя съема данных. Помимо указанных преимуществ внедрение технологии восстановления ключа из нечетких данных может обеспечить легкую смену "мысленного пароля" [1].

Учитывая данные факторы, было решено смоделировать работу нейросетевого преобразователя "Биометрия - код доступа" на основе электроэнцефалограммы и рассчитать вероятности ошибок первого и второго рода.

Опишем процедуру стимуляции деятельности мозга, при которой снимается электроэнцефалограмма для восстановления секретного ключа.

Используемая стимуляция для создания выглядит, как поочередно меняющиеся цифры от «0» до «9». Стимуляция для эксперимента вызывает визуальный вызванный потенциал [4]. Фрагмент стимуляции изображен на рисунке (рис. 1).

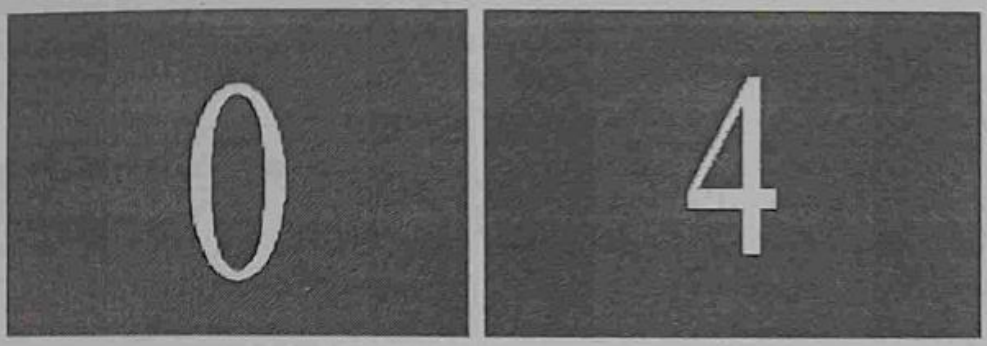

Рис. 1. Фрагмент визуальной стимуляции

Пользователи выбирают 1, 2 или 4 символа, и при их появлении на экране концентрируются на них. Данные символы являются "мысленным паролем".

Съем ЭЭГ для 1-2 символов производился в течение 10 секунд, а для 4 символов в течение 20 секунд. Для каждой секунды было использовано разбиение данной секунды на 128 частей, что соответствует синхронизации с нейрогарнитурой Epoc Emotiv Neuroheadset, используемой для съема ЭЭГ и обеспечивает съем в реальном времени. Для случая, когда пользователь запоминает 2 или 4 символа, съем ЭЭГ разбивается на два, или четыре этапа соответственно, по 5 секунд. В течение первого этапа пользователь концентрируется на одном символе, в течение второго - на втором символе и т.д.

В качестве биометрической характеристики a используется разница между уровнем ЭЭГ при стимуляции и усредненного значения ЭЭГ в состоянии покоя. Обозначим уровень электроэнцефалограммы при стимуляции через $a_{\text{стим}}$, а усредненный уровень электроэнцефалограммы в состоянии покоя через $\bar{a}_{\text{покой}}$. Тогда:

$$a = a_{\text{стим}} - \bar{a}_{\text{покой}}. \quad (1)$$

Однако в силу высокой сложности математического описания формы сигнала ЭЭГ [4] было принято решение производить выборку пятнадцати максимальных значений, вычисляемых по формуле (1). Целесообразно говорить об использовании характеристики a в векторном виде:

$$\bar{a}_i = \{a_{ij}\}, i = 1,...,14, j = 1,...,15, \quad (2)$$

где $\bar{a}_i$ – вектор биометрических данных, используемый в нейросетевом преобразователе; i – номер электрода, с которого снята электроэнцефалограмма; j – номер максимального значения a с канала i.

В качестве структуры данного преобразователя выбрана двухслойная нейронная сеть сигмоидального типа. Также была построена нейронная сеть сигмоидального типа, использующая во втором слое линейную передаточную функцию. Для этих сетей первый слой нейронной сети содержит 320 нейронов, а второй слой содержит 256 нейронов [5]. Моделирование работы нейронных сетей было произведено с помощью пакета Simulink среды Matlab.

Для обучения нейронов сети была выбрана стандартная процедура обучения нейросетевых преобразователей "Биометрия - код доступа", описанная в стандарте ГОСТ Р 52633.5-2011 [2].

Расчет вероятностей ошибки второго рода был проведен для случая знания злоумышленником весовых коэффициентов, а также знания "мысленного пароля", т.е. знания символов на которых концентрируется пользователь для восстановления ключа. Наиболее интересными являются следующие результаты:

1. В случае использования "мысленного пароля" состоящего из одного или двух символов и обработке его двухслойной сетью сигмоидального типа, минимальное расстояние Хэмминга от полученного злоумышленником ключа до секретного ключа пользователя было равно 7.

2. В случае использования "мысленного пароля" состоящего из одного или двух символов и обработке его двухслойной сетью со вторым линейным слоем, минимальное расстояние Хэмминга от полученного злоумышленником ключа до секретного ключа пользователя было равно 21.

3. В случае использования "мысленного пароля" состоящего из четырех символов и обработке его двухслойной сетью сигмоидального типа, минимальное расстояние Хэмминга от полученного злоумышленником ключа до секретного ключа пользователя было равно 27.

4. В опытах по восстановлению ключа пользователем (во всех случаях), преобразователь безошибочно восстанавливал секретный ключ. В результате 5 опытов расстояние Хэмминга от восстановленного ключа до ключа пользователя было равно 0.

Приведем расчет ошибок первого и второго рода на основе результатов полученных в ходе проведения опытов.

Для случаев, когда тестирующая выборка является небольшой, и ошибка первого рода не была выбрана, данную ошибку можно вычислить по следующей формуле [5]:

$$P_1 \approx \int_1^{\infty} \frac{1}{2^{\frac{\Omega}{2}} \cdot \Gamma\left(\frac{\Omega}{2}\right)} \cdot x^{\frac{\Omega}{2}-1} \cdot e^{-\frac{x^2}{2}} \cdot dx, \qquad (3)$$

где Ω – количество степеней свободы в распределении X^2.

В случае, когда в проведенной серии испытаний по предъявлению биометрической характеристики образа «Свой», состоящей из m опытов,

не обнаружен факт отказа в доступе, число степеней свободы в распределении X^2 вычисляется по формуле:

$$\Omega = \frac{1}{m+1}. \quad (4)$$

Прогноз вероятности ошибок второго рода P_2 вычисляют приближенно, исходя из гипотезы нормального закона распределения значений вероятности ошибок по формуле [2]:

$$P_2 \approx \frac{1}{\sqrt{2\pi}} \int_{\sqrt{n}E(q(v))}^{\infty} e^{-\frac{x^2}{2}} dx, \quad (5)$$

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

В построенном преобразователе использовались 210 параметров. Для пароля, состоящего из 1-2 символов, среднее качество составляло 2,3. Для пароля, состоящего из 1-2 символов, среднее качество составляло 3,6.

По формулам (3) и (5) рассчитаем вероятности ошибок первого и второго рода (таблица 1).

Как видно из полученных результатов, нейросетевой преобразователь "Биометрия - код доступа" является высоконадежной технологией восстановления ключа.

Таблица 1

Вероятности ошибок первого и второго рода

Ошибка	Количество символов "мысленного пароля"					
	Двухслойная нейронная сеть сигмоидального типа			Двухслойная нейронная сеть сигмоидального типа с линейным вторым слоем		
	1	2	4	1	2	4
P_1	$6 \cdot 10^{-4}$	$6 \cdot 10^{-4}$	$6 \cdot 10^{-4}$	$6 \cdot 10^{-4}$	$6 \cdot 10^{-4}$	-**
P_2	$<\cdot 10^{-50}$	$<\cdot 10^{-50}$	$<\cdot 10^{-50}$*	$<\cdot 10^{-50}$	$<\cdot 10^{-50}$	-**

* - Стандартные средства расчета округляют результат до 0.

** - Не было проведено соответствующего опыта.

Список литературы

1. Гончаров С.М. Идентификация пользователей на основе электроэнцефалографии с использованием технологий «Интерфейс мозг-компьютер» / С.М. Гончаров, М.С. Вишняков // Доклады Томского государственного университета систем управления и радиоэлектроники: Научный журнал. - Томск: Изд-во ТУСУР, 2012. - №1-2. - С.166-170.

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. Гнездицкий В.В. Обратная задача ЭЭГ и клиническая электроэнцефалография (картирование и локализация источников электрической активности мозга) / В.В. Гнездицкий. - М.: МЕДпрессинформ, 2004. - 624 с.

5. Борщевников А.Е. Результат эксперимента по восстановлению секретного ключа по ЭЭГ с использованием нейросетевого преобразователя "Биометрия - код доступа" / А.Е. Борщевников, М.Е. Маркин // Сборник докладов 61-й международной молодежной научно-технической конференции «Молодежь. Наука. Инновации», 21-22 ноября 2013 г. – Владивосток: Мор. гос. ун-т, 2013. - Т. 1. - С. 126-128.

6. Ахметов Б.С. Оценка вероятностей появления ошибок нейросетевых преобразователей биометрия-код на основе малых выборок / Б.С. Ахметов, А.И. Иванов, А.Ю. Малыгин, Т.С. Картбаев // Труды II Международной научной конференции "Высокие технологии - залог устойчивого развития" - 2013. - том №1. - С. 234-237

УДК 37.01:007

А. И. Дешнер

ОСНОВНЫЕ НАПРАВЛЕНИЯ И ПРОБЛЕМЫ РАЗВИТИЯ СОВРЕМЕННЫХ ТЕХНОЛОГИЙ ДИСТАНЦИОННОГО ОБРАЗОВАНИЯ

Большое число учебных заведений, включая центры повышения квалификации, а также онлайн-сертификации успешно применяют технологии дистанционного образования в учебном процессе и для выполнения итогового контроля обучения. В настоящее время основными направлениями развития являются следующие технологии:

- видеоконференции;
- системы обмена данными различных форматов;
- онлайновые потоковые видео-курсы по запросу;
- сложные интерактивные системы организации и управления дистанционным учебным процессом.

Следует отметить, что ввиду значительной сложности любой системы организации и управления учебным процессом, практически каждое учебное заведение с мировым именем разрабатывает и внедряет системы данного типа индивидуальной разработки, и, как правило, исследования учебных процессов и создание инструментов и средств управления учебным процессом выполняется в рамках самого учебного заведения.

Как правило, собственно обучение в системах управления учебным процессом организовано в виде учебных курсов, для создания которых предусмотрено специальное программное средство, выполняющее следующие функции [1]:

- объявление о начале нового учебного курса;
- предоставление он-лайн учебно-методических материалов;
- создание динамических планов и расписаний;