УДК 004.056.52

Нейросетевой преобразователь «Биометрия – код доступа» на основе электроэнцефалограммы в современных криптографических приложениях

С. М. Гончаров, А. Е. Боршевников

Эта статья посвящена использованию средств высоконадежной биометрической аутентификации на основе электроэнцефалограммы в современных криптографических приложениях. В статье описаны 3 вида технологий проведения экспериментов, при которых производится сбор биометрических данных, определена общая структура нейросетевых преобразователей «Биометрия – код доступа» и приведены результаты моделирования работы данного преобразователя. На основе результатов установлена область применения нейросетевых преобразователей «Биометрия – код доступа» в современных криптографических приложениях.

Ключевые слова: аутентификация, биометрия, электроэнцефалограмма, нейросетевой преобразователь «Биометрия – код доступа».

1. Введение

Потребность в защите информации растет совместно с объемом обрабатываемой информации. Средства защиты информации основываются на различных механизмах защиты. Одним из известных механизмов, который используется в средствах защиты информации, является биометрическая аутентификация. Из ряда перспективных видов биометрических данных можно выделить электроэнцефалограмму человека (ЭЭГ). В настоящее время в мире достаточно активно проводятся исследования по разработке методов идентификации человека на основе ЭЭГ. При этом используются как различные технологии проведения экспериментов, так и различные математические методы обработки сигналов ЭЭГ [1]. Эффективность лучших таких технологий, подтвержденных проведением экспериментов, на сегодняшний день невысока: вероятность ошибки 2-го рода (FAR) находится в диапазоне от 10 % до 0.1 %. Одним из решений подобной проблемы является отход от построения классической системы аутентификации на основе ЭЭГ и построение системы высоконадежной биометрической аутентификации в соответствии с серией стандартов ГОСТ Р 52633. Данный подход позволил кардинально повысить эффективность идентификации на основе ЭЭГ и достигнуть значения $FAR = 10^{-12}$.

2. Нейросетевой преобразователь «Биометрия – код доступа» на основе ЭЭГ пользователя с использованием «мысленного пароля»

В качестве метода реализации технологии высоконадежной биометрической аутентификации был выбран подход, основанный на нейросетевых преобразователях «Биометрия – код доступа» [2].

2.1. Технологии проведения экспериментов

На данный момент были проверены экспериментально 3 вида технологий проведения биометрической идентификации на основе ЭЭГ пользователя.

В качестве первой технологии, использованной для выделения сигнала ЭЭГ, была предложена визуальная стимуляция. Для выделения потенциала ЭЭГ в данном эксперименте использовалась стимуляция из поочередно меняющихся цифр от «0» до «9». Пользователь выбирал одну или несколько цифр и при их появлении концентрировался на них. Этот набор цифр считался мысленным паролем [3]. При обнаружении пользователем задуманной цифры возникает сигнал P300, который анализируется в дальнейшем. Недостаток данного метода заключается в том, что данная стимуляция является внешней и злоумышленник может предположить, на каком символе сосредотачивается пользователь. Отдельный интерес представляют технологии проведения экспериментов без воздействия внешней стимуляции.

Второй технологией, которая использовалась для идентификации на основе ЭЭГ, было мысленное исполнение музыкального произведения. В начале эксперимента пользователь находился в расслабленном состоянии. Подавалась команда, после которой он начинал воспроизводить у себя в голове заранее выбранную музыкальную композицию. Далее подавалась вторая команда, после которой пользователь расслаблялся и прекращал мыслительную деятельность.

Третьей технологией, использованной для формирования потенциала ЭЭГ, являлись движения глаз с закрытыми веками. В течение определенного времени пользователь производил определенное движение глазами (влево, вправо, вверх, вниз и т.д.) на каждый удар метронома. В экспериментах использовался алфавит из 7-ми специфических движений глаз с закрытыми веками. Набор таких движений являлся PIN-кодом. На основе обработки ЭЭГ, возникающей в ответ на воспроизведение такого PIN-кода, вырабатывался секретный ключ размером 256 бит.

2.2. Выбор биометрических параметров

На ранних стадиях исследований в качестве биометрической характеристики бралась разность потенциалов ЭЭГ пользователя в состоянии покоя и при воздействии визуальной стимуляции [3]. Далее полученные результаты были улучшены за счет использования дискретного преобразования Фурье для обработки электроэнцефалограммы.

В результате применения быстрого преобразования Фурье к сигналу ЭЭГ 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 векторы:

$$\bar{a}_i = \{a_{ij}\},$$

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

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

В силу высокой сложности математического описания формы сигнала ЭЭГ было принято решение производить выборку нескольких коэффициентов разложения Фурье. Умножение на косинус аргумента комплексного коэффициента введено для получения такой характеристики сигнала, как длительность наибольшего возрастания сигнала.

2.3. Обучение нейросетевого преобразователя

Для построения нейросетевого преобразователя была выбрана структура двухслойной нейронной сети. В качестве алгоритма обучения такого преобразователя использовалась процедура обучения, описанная в стандарте ГОСТ Р 52633.5-2011 [4]. Для реализации обучения необходимо сформировать базу электроэнцефалограмм образов «Чужой», т.е. образов злоумышленника, для которых нейронная сеть будет выдавать случайный криптографический ключ. Формирование такой базы осуществляется из ЭЭГ пользователей, а также специально полученных синтетических образцов ЭЭГ. Также необходимо сформировать набор электроэнцефалограмм образов «Свой» пользователя, который будет считаться легитимным. Данный набор необходимо удалить сразу после обучения преобразователя в целях предотвращения её кражи и использования для компрометации секретного ключа. Результатом выполнения данной процедуры будут являться весовые коэффициенты нейронной сети W_r, где r – номер слоя нейронной сети.

2.4. Структура нейросетевого преобразователя

В общем случае нейросетевой преобразователь «Биометрия – код доступа» может быть описан следующим образом. Работа каждого нейрона определяется следующим соотношением:

$$x = \sum \Delta \cdot W_r \cdot a_{ij} ,$$

где Δ – коэффициент использования вектора $\bar{a}_i$ в нейроне. Если $\bar{a}_i$ используется в данном нейроне, то $\Delta = 1$, и $\Delta = 0$ в противном случае.

Каждый нейрон сети имеет нелинейную передаточную функцию, которую можно описать следующим образом:

$$y = \frac{2}{1+e^x} - 1; \mathrm{f}(y) = \begin{cases} 1, y \geq 0 \\ s, y < 0 \end{cases}; s = \begin{cases} -1, r = 1 \\ 0, r = 2 \end{cases}.$$

Первый слой является вспомогательным. В проведенных экспериментах в первом слое сети использовалось 320 нейронов. Результатом работы второго слоя нейронной сети являлся криптографический ключ длиной 256 бит. Таким образом, во втором слое использовалось 256 нейронов.

2.5. Результаты

Были проведены 3 серии экспериментов по реализации нейросетевого преобразователя «Биометрия – код доступа» на основе «мысленного пароля» с использованием различных технологий проведения эксперимента.

Во всех экспериментах с использованием технологий визуальной стимуляции и движения глаз с закрытыми веками ключ легитимного пользователя размером 256 бит восстанавливался безошибочно. В экспериментах с использованием технологии мысленного исполнения му-

зыкальной композиции в большинстве случаев ключ легитимного пользователя восстанавливался без искажений. В трех случаях восстановленный ключ имел искажение в одном бите. Даже в случае, когда злоумышленник угадывает «мысленный пароль», минимальное расстояние Хэмминга (количество ошибок) до ключа легитимного пользователя во всех экспериментах было равно 18 (табл.). При генерации злоумышленником ошибочного «мысленного пароля» усредненное расстояние Хэмминга до истинного ключа значительно выше.

Для описанных технологий проводились исследования с 10-ю испытуемыми по 20 экспериментов для каждого. Для технологии на основе сигнала P300 проводились исследования по использованию различных символов в «мысленном пароле», а также изменению длины данного пароля. В результате для этой технологии общее количество испытаний составляет около 5000. Предварительная оценка вероятности ошибок 2-го рода для проведенных экспериментов вычислялась на основе методики, специально разработанной для небольшого количества испытаний и приведенной в ГОСТ Р 52633.1 [5]. 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}. Для технологии мысленного исполнения музыкальной композиции была экспериментально подтверждена ее работоспособность. Однако необходимы дополнительные исследования для повышения эффективности аутентификации.

Таблица. Расстояние Хэмминга до секретного ключа пользователя в случае знания злоумышленником мысленного пароля

Номер пользователя	Стимуляция		
	Концентрация на визуальной стимуляции	Мысленное исполнение музыкального произведения	Движение мышц глаз
1	94	84	26
2	88	57	24
3	54	44	82
4	34	83	51
5	27	91	22
6	101	60	44
7	76	21	54
8	116	88	18
9	99	63	93

3. Области применения полученных результатов

Интерпретируя полученные в предыдущей главе результаты, можно сказать, что возможность восстанавливать безошибочно ключ позволяет применять его в современных криптографических приложениях. Этому также способствует выбранный размер второго слоя нейросетевого преобразователя «Биометрия – код доступа». В настоящий момент полученные результаты можно применять для хранения ключа в алгоритме симметричного шифровании по ГОСТ Р 34.12-2015, хранения ключа в алгоритме ключевого хеширования (режим выработки имитовставки в ГОСТ Р 34.13-2015), хранении секретного ключа в алгоритме электронной подписи ГОСТ Р 34.10-2012.

Результаты, полученные для технологии мысленного воспроизведения музыкальной композиции, на данный момент не могут применяться для криптографических приложений из-за нестабильности восстановления ключа и требуют дополнительного исследования.

4. Заключение

Экспериментально отработаны 3 технологии биометрической аутентификации на основе ЭЭГ по методике, описанной в стандарте ГОСТ Р 52633.5-2011. Данный подход позволил повысить эффективность аутентификации пользователей на основе ЭЭГ более чем в миллион раз по сравнению с лучшими зарубежными разработками в этой области.

Нейросетевые преобразователи «Биометрия – код доступа» на основе электроэнцефалограммы являются перспективным направлением исследований в области систем биометрической аутентификации. Данные системы целесообразно использовать в системах ограничения доступа на охраняемые объекты [6], в системах электронного документооборота, в системах, требующих надежной дистанционной аутентификации, а также в криптографических приложениях.

На данный момент можно выделить несколько направлений для дальнейшего развития разработанной технологии: повышение эффективности нейросетевого преобразователя, усовершенствование структуры нейронной сети, получение результатов для преобразователя с 512-битным выходным слоем.

Литература

1. *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: 27.01.2016).
2. 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.
3. *Гончаров С. М., Боршевников А. Е.* Построение нейросетевого преобразователя «Биометрия – код доступа» на основе параметров визуального вызванного потенциала электроэнцефалограммы // Доклады Томского государственного университета систем управления и радиоэлектроники: Научный журнал. Томск: Изд-во ТУСУР, 2014. № 2. С. 51–55.
4. 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.
5. 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.
6. *Гончаров С. М., Боршевников А. Е.* Использование технологий высоконадежной биометрической аутентификации в критически важных объектах // Информационная безопасность регионов. Саратов: Саратовский социально-экономический институт (филиал) РЭУ им. Г.В. Плеханова, 2015. № 4 (21). С. 18–23.

Статья поступила в редакцию 19.01.2016

Гончаров Сергей Михайлович

к.ф.-м.н., профессор кафедры безопасности информации и телекоммуникационных систем МГУ им. адм. Г.И. Невельского (690059, Владивосток, ул. Верхнепортовая, 50а) тел. (423) 2-772-993, e-mail: sgprim@smtp.ru.

Боршевников Алексей Евгеньевич

ассистент кафедры информационной безопасности ШЕН ДВФУ (690950, Владивосток, ул. Суханова, 8) тел. (924) 1-316-797, e-mail: LAdG91@mail.ru.

Neural network transformer «Biometry – access code» based on the electroencephalogram in modern cryptographic applications

S. Goncharov, A. Borshevnikov

This article considers the use of highly reliable biometric authentication based on electroencephalogram in modern cryptographic applications. Three types of technologies to carry out experiments for collecting biometric data are described, the general structure of neural network transformers«Biometry – access code», and the simulation results of this transformer are presented. Based on the results, the range of use of neural network transformers «Biometry – access code» in modern cryptographic applications is identified.

Keywords: authentication, biometry, electroencephalogram, neural network transformer «Biometry – access code».