

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ
Федеральное государственное автономное образовательное учреждение
высшего образования

**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

Институт кибернетики

Молодёжь и современные информационные технологии

Том I

**Сборник трудов
XIII Международной научно-практической
конференции студентов, аспирантов
и молодых учёных**

9–13 ноября 2015 г.

Томск 2016

УДК 378:004
ББК Ч481.23
М75

Молодежь и современные информационные технологии. Сборник трудов XIII Международной научно-практической конференции студентов, аспирантов и молодых ученых «Молодежь и современные информационные технологии». Томск, 9-13 ноября 2015 г. – 2016 – Томск: Изд-во ТПУ. – Т. 1 – 330 с.

Сборник содержит доклады, представленные на XIII Международной научно-практическую конференцию студентов, аспирантов и молодых ученых «Молодежь и современные информационные технологии», прошедшей в Томском политехническом университете на базе Института кибернетики. Материалы сборника отражают доклады студентов, аспирантов и молодых ученых, принятые к обсуждению на секциях: «Микропроцессорные системы, компьютерные сети и телекоммуникации», «Математическое моделирование и компьютерный анализ данных», «Автоматизация и управление в технических системах», «Информационные и программные системы в производстве и управлении», «Компьютерная графика и дизайн», «Информационные технологии в гуманитарных и медицинских исследованиях».

Сборник предназначен для специалистов в области информационных технологий, студентов и аспирантов соответствующих специальностей.

УДК 378:004
ББК Ч481.23
М 75

Редакционная коллегия сборника:

Мамонова Т.Е., к.т.н., доцент каф. ИКСУ ИК ТПУ, ученый секретарь конференции;
Ботыгин И.А., к.т.н., доцент каф. ИПС ИК ТПУ, председатель секции № 1;
Зимин В.П., к.т.н., доцент каф. ПМ ИК ТПУ, председатель секции № 2;
Рудницкий В.А., к.т.н., доцент каф. ИКСУ ИК ТПУ, председатель секции № 3;
Шерстнев В.С., к.т.н., доцент каф. ВТ ИК ТПУ, председатель секции № 4;
Винокурова Г.Ф., к.т.н., доцент каф. ИГПД ИК ТПУ, председатель секции № 5;
Берестнева О.Г., д.т.н., профессор каф. ПМ ИК ТПУ, председатель секции № 6.

Редакционная коллегия предупреждает, что за содержание представленной информации ответственность несут авторы.

© ГАОУ ВО «Национальный исследовательский
Томский политехнический университет», 2016
© Оформление. Издательство Томского
политехнического университета, 2016

СОДЕРЖАНИЕ

СЕКЦИЯ 1 МИКРОПРОЦЕССОРНЫЕ СИСТЕМЫ, КОМПЬЮТЕРНЫЕ СЕТИ И ТЕЛЕКОММУНИКАЦИИ	15
КОНЦЕПЦИЯ ПРИМЕНЕНИЯ ГИБРИДНОГО МОДЕЛИРОВАНИЯ ПРИ РАЗРАБОТКЕ ПРОГРАММНЫХ СИСТЕМ РЕАЛЬНОГО ВРЕМЕНИ	
Погребной А. В.....	16
ПРИМЕНЕНИЕ СОБЫТИЙНО-ОРИЕНТИРОВАННОГО ПОДХОДА К ПОСТРОЕНИЮ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ПРИ ДЛИТЕЛЬНОМ ВРЕМЕНИ ОБРАБОТКИ СОБЫТИЯ	
Пономарева А.В., Шамин А.А.	18
ОБОСНОВАНИЕ ВЫБОРА ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ ДЛЯ УМНОГО ДОМА	
Ракитин Д.А., Железнов А.А., Коцубинский В.П.	20
ЭКСПЕРИМЕНТ ПО УВЕЛИЧЕНИЮ КОЛИЧЕСТВА ВХОДОВ НЕЙРОСЕТЕВОГО ПРЕОБРАЗОВАТЕЛЯ, ПОСТРОЕННОГО НА ОСНОВЕ ЭЭГ	
Михайлов А.Г., Апальков А.Ю., Боршевников А.Е.	22
ИНТЕЛЛЕКТУАЛЬНОЕ УСТРОЙСТВО ДИАГНОСТИКИ СОСТОЯНИЯ ПЛОТИНЫ	
Першин Е.А., Мейта Р.В., Шамин А.А.	24
СИНХРОНИЗАЦИЯ ВРЕМЕНИ ВО ВСТРАИВАЕМЫХ СИСТЕМАХ	
Мейта Р.В., Першин Е.А., Шамин А.А.	26
РАЗРАБОТКА ОНЛАЙН-СЕРВИСА РЕКОМЕНДАЦИИ ХУДОЖЕСТВЕННОЙ ЛИТЕРАТУРЫ	
Никитина К.С., Дорофеев В.А.	28
ГЕНЕРАТОР СИГНАЛОВ ПРОИЗВОЛЬНОЙ ФОРМЫ НА NI FPGA Board	
Ершов И.А., Рыбин Ю.К.	30
ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ДЛЯ РАСЧЕТА ЦЕНТРА МАСС ЗЕМЛИ С ПОМОЩЬЮ ЕИЭМПЗ	
Горемыкина Д.С., Петрик И.М.	32
THE UNDERSTANDING OF CONSISTMENT HASHING	
N.S. Gukov	34
ОЦЕНКА ЭФФЕКТИВНОСТИ РАСПРЕДЕЛЕННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ЗАЯВКАМИ НА ОСНОВЕ ПРОГРАММНОГО ЭКСПЕРИМЕНТА	
Нагиев А.Е.	38
АНАЛИЗ ИНФОРМАТИВНОСТИ ДЕМАСКИРУЮЩИХ ПРИЗНАКОВ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ И МЕТОДОВ ЗАЩИТЫ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА	
Клостер С.А.	40
МЕТОДЫ КОНТРОЛЯ УСТРОЙСТВА НАГРУЗОЧНО-РЕГИСТРИРУЮЩЕГО «ГАММА-500»	

ЭКСПЕРИМЕНТ ПО УВЕЛИЧЕНИЮ КОЛИЧЕСТВА ВХОДОВ НЕЙРОСЕТЕВОГО ПРЕОБРАЗОВАТЕЛЯ, ПОСТРОЕННОГО НА ОСНОВЕ ЭЭГ

Михайлов А.Г., Апальков А.Ю., Боршевников А.Е

Научный руководитель: к.ф.-м.н., доцент, С.М. Гончаров
Дальневосточный федеральный университет, г. Владивосток
quantum722@gmail.com

Введение

В настоящее время биометрия, как отрасль науки, развивается в нескольких направлениях, каждое из которых имеет свое предпочтительное аппаратное и программное обеспечение. Одним из направлений развития являются биометрические методы аутентификации человека. Привлекательной в данной области является такая биометрическая характеристика, как электроэнцефалограмма (ЭЭГ).

Стоит выделить положительные черты данной характеристики. Дашные электроэнцефалограммы конфиденциальны, эти данные крайне сложно подделать; снятие ЭЭГ возможно на расстоянии не более 0,001 м от головы, что обеспечивает дополнительную защищенность от перехвата злоумышленником и невозможность незаметного для пользователя съема данных.

Данные ЭЭГ используются для генерации уникального ключа пользователя. Одним из вариантов выработки такого ключа является использование нейросетевых преобразователей «Биометрия — код доступа», описанных в линейке стандартов ГОСТ Р 52633 [1].

Формирование базы ЭЭГ

Ранее уже проводились исследования по использованию ЭЭГ в качестве биометрической характеристики для нейросетевого преобразователя "Биометрия - код доступа". Была построена модель такого преобразователя, построенного на основе ЭЭГ зрительных вызванных потенциалов [2]. Для выделения визуального вызванного потенциала 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.

У работы данной модели существует недостаток в том, что для выделения вызванного потенциала требуется внешняя стимуляция. Устранить этот недостаток можно, проводя эксперименты без дополнительной стимуляции. В данном исследовании было решено использовать в качестве входных данных параметры ЭЭГ, полученные при проведении экспериментов с движением глаз при сомкнутых веках. Заметим, что разные виды работы глазных мышц неплохо распознаются на ЭЭГ.

Приведем краткое описание эксперимента. Для простоты синхронизации при проведении

испытаний использовалась звуковая стимуляция метрономом с интервалом 2 секунды. Запись данных производилась в течение 8 секунд. На каждый удар метронома испытуемый фиксировал глаза в определенном положении (влево – вправо – вверх – вниз). Движение глаз производилось с закрытыми веками. Последовательность движений глаз составляет пароль. Для построения модели преобразователя была сформирована база ЭЭГ из 10 образов, по 20 записей на каждый образ. Один из 10 образов был выбран как образ «свой», остальные 9 образов – «чужой».

Полученные результаты

Используемая в данном исследовании для снятия ЭЭГ нейрогабитура имеет 14 электродов, поэтому изначально было решено использовать 14 входов у нейросетевого преобразователя. Структурой данного преобразователя выбрана двухслойная нейронная сеть сигмоидального типа. Количество нейронов первого слоя равно 320, второго – 256. То есть длина двоичного выходного ключа – 256 бит.

Ранее проводимые исследования показали, что использование дискретного преобразование Фурье улучшает характеристики работы преобразователя. Поэтому перед подачей данных на вход преобразователя к сигналу ЭЭГ применялось быстрое преобразование Фурье [3]. После данного преобразования мы получаем набор комплексных коэффициентов a_{ij} , где i – номер электрода, с которого снята ЭЭГ. Среди данных коэффициентов выбираются удовлетворяющие условию: $15^\circ \leq \arg a_{ij} \leq 90^\circ$. Наложив это условие, мы подразумеваем, что анализируем только неубывающие всплески ЭЭГ. Затем модуль полученных значений умножается на косинус аргумента. По каждому информационному каналу ЭЭГ полученные значения $v_{ij} = |a_{ij}| \cos(\arg a_{ij})$ сортируются по убыванию. Экспериментально было установлено, что для корректной работы преобразователя входные данные достаточно сформировать, используя $j = 10$ максимальных значений v_{ij} по соответствующему каналу ЭЭГ с номером i . Поэтому на вход преобразователя было

$$q_i = \sum_{j=1}^{10} v_{ij} * w_{ij}$$

где v_{ij} – отсортированные по убыванию полученные ранее значения, w_{ij} – вычисленные по

стандарту весовые коэффициенты первого слоя для о Автомат обучения первого и второго слоя преобразователя построен по ГОСТ Р 52633.5. т После построения модели преобразователя были проведены исследования по его работе. Для всех образов «свой» преобразователь безошибочно восстанавливал ключ. Результаты исследования по получению злоумышленником секретного ключа с помощью преобразователя при известных весовых коэффициентах и при условии знания пароля приведены в таблице 1.

Таблица 1. Расстояние Хэмминга до секретного ключа пользователя (14*10=140 входов)

Номер пользователя	Расстояние Хэмминга
1	18
2	37
3	118
4	87
5	8
6	125
7	119
8	125
9	125

Для данной модели общий подход формирования данных подаваемых на вход преобразователя был такой же, как и в исследовании модели, построенной на вызванном потенциале [2]. Было решено попробовать изменить конструкцию преобразователя, увеличив количество входов, и проанализировать работу полученного преобразователя.

Наиболее оптимальным на данном этапе исследования было выбрано количество входов равное 1036, так как при таком количестве не придется существенно изменять процедуру формирования нейронной сети и ее обучения. В итоге у полученной нейронной сети следующие характеристики: количество входов – 1036, количество нейронов первого слоя – 320, второго слоя – 256.

Входные данные формировались следующим образом. Была сформирована матрица, состоящая из 14 строк, в каждой из которых содержатся первые 74 отсортированных значений v_{ij} по соответствующему каналу ЭЭГ с номером $i = 1, 14$. Было решено объединить строки полученной матрицы в единый вектор, состоящий из $1036=14*74$ значений. Этот вектор и подается на вход преобразователя.

Автомат обучения первого слоя был изменен, исходя из изменившегося формата входных данных. Автомат обучения второго слоя остался без изменений.

После изменения структуры преобразователя были проведены исследования по его работе. Для всех образов «свой» преобразователь безошибочно

восстанавливал ключ. Результаты исследования по получению злоумышленником секретного ключа с помощью преобразователя при известных весовых коэффициентах и при условии знания пароля приведены в таблице 2.

Таблица 2. Расстояние Хэмминга до секретного ключа пользователя (1036 входов)

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

Заключение

Видно, что для некоторых образов результаты работы преобразователя при использовании одной и той же базы при увеличении количества входов и объема входных данных ухудшились, но общая картина работы относительно всех образов базы «чужой» стала более стабильной.

Результаты показывают, что увеличение количества входов и общего объема входных данных улучшает стабильность работы нейросетевого преобразователя «Биометрия – код доступа», но необходимо дальнейшее исследование по выбору наиболее оптимальных параметров входных данных для улучшения характеристик работы преобразователя.

Список литературы

1. 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.–20с.
2. 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.
3. Лопатеев И.Н. Эксперимент по использованию быстрого преобразования Фурье в преобразователе «биометрия- код доступа» на основе ЭЭГ/ И.Н. Лопатеев, А.Е. Боршевников// Сборник докладов 62-й международной молодежной научно-технической конференции «Молодежь. Наука. Инновации», 18-25 ноября 2014 г. – Владивосток: Мор. гос. ун-т, 2014. - с. 153-156.