УДК 004.056.5

С. М. Гончаров, Г. А. Квачук, А. Е. Боршевников

АНАЛИЗ ТРЕБОВАНИЙ К БАЗАМ МЫСЛЕННЫХ ОБРАЗОВ НА ОСНОВЕ ЭКСПЕРИМЕНТОВ, ПРОВЕДЕННЫХ С ИСПОЛЬЗОВАНИЕМ РАЗЛИЧНЫХ МЕТОДОВ ФОРМИРОВАНИЯ МЫСЛЕННЫХ ОБРАЗОВ

Практическое применение криптографии стало неотъемлемой частью жизни современного общества. На сегодняшний день стандартными способами идентификации де-факто являются пароли и уникальные идентификаторы или документы, удостоверяющие личность владельца (паспорт, водительские права и прочее). Но все эти способы идентификации могут стать предметом подделки или потери. Оптимальной альтернативой им является генерация секретного ключа из биометрических данных пользователя. Однако использование биометрических данных для генерации криптографических ключей осложняется тем, что эти данные неточно воспроизводимы и имеют ряд особенностей:

– биометрические характеристики могут изменяться со временем, а некоторые зависят от физического и эмоционального состояния их владельца;

– проблема смены ключей – биометрические данные неотзываемы;

– невозможность держать многие биометрические данные в тайне (например: отпечатки пальцев могут быть оставлены на различных поверхностях).

На данный момент существует два подхода к генерации секретных ключей на основе биометрических данных, удовлетворяющие требованиям современной криптографии: использование специально обученных искусственных нейронных сетей и применение «нечетких экстракторов».

1. *Нейронные сети*. Нейросетевой преобразователь «Биометрия-код доступа» – заранее обученная искусственная нейронная сеть с большим числом входов и выходов, преобразующая частично случайный вектор входных биометрических параметров «СВОЙ» в однозначный код криптографического ключа и преобразующая любой иной случайный вектор входных данных «ЧУЖОЙ» в случайных выходной код. Описанию данного подхода посвящена линейка стандартов ГОСТ Р 52633.

2. *Нечеткие экстракторы*. Этот подход позволяет однозначно восстанавливать секретный ключ из неточно воспроизводимых биометрических данных при участии так называемых вспомогательных данных, являющихся открытыми.

В проведенных экспериментах используется нейросетевой преобразователь «Биометрия-код доступа», а в качестве биометрических данных пользователя выступают данные, основанные на деятельности головного мозга. Использование электроэнцефалограммы (ЭЭГ) головного

мозга в качестве биометрической характеристики является новым направлением в области высокоточной биометрической аутентификации. Из-за этого возникает вопрос формирования баз мысленных образов [1].

Была поставлена задача – проанализировать ряд основных типов мысленных образов и сформулировать требования, которым они должны будут соответствовать методы их сбора/обработки. В ходе решения данной задачи были произведены 3 серии экспериментов, в которых использовались различные методы формирования мысленных образов.

1. Здесь стимуляция вызывает VEP потенциал. Используемый метод заключается в следующем: стимуляция выглядит в виде поочередно меняющихся на экране цифр от «0» до «9». Пользователи выбирают 1, 2 или 4 символа и при их появлении на экране концентрирует свое внимание на них. Данные символы являются «мысленным паролем».

Съем ЭЭГ производился в течение 10 секунд в случае, когда пользователь запоминает 1 или 2 символа. Для 4 символов съем длится 20 с. Для каждой секунды было использовано разбиение на 128 частей, что соответствует синхронизации с нейрогарнитурой, используемой для съема ЭЭГ [2].

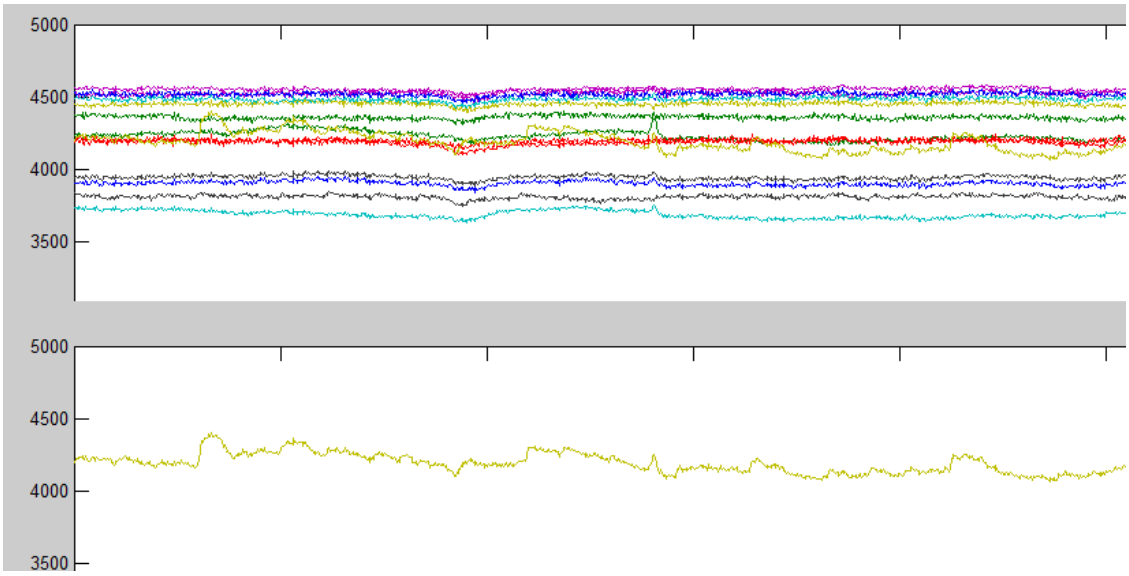

Рис. 1. ЭЭГ при визуальной стимуляции

2. В рамках следующей серии экспериментов была выбрана задача - мысленно проиграть музыкальную мелодию. Проигрываемая мелодия является «мысленным паролем». Данная задача была выбрана не случайно. В структуре головного мозга Корбинианом Бродманом были выделены отделы (поля Бродмана), отличающиеся по клеточному строению и отвечающие за определённые функции. Локализация мысленного образа в одном поле в дальнейшем увеличивает точность распознавания полученных ЭЭГ пользователей.

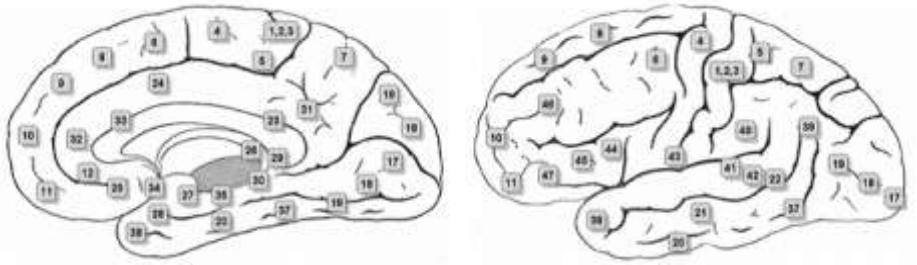

Рис. 2. Локализация полей Бродмана

В начале эксперимента пользователь находится в расслабленном состоянии. Подается команда, после которой он начинает воспроизводить у себя в голове заранее выбранную музыкальную композицию. Далее подается вторая команда, после которой пользователь расслабляется и прекращает мыслительную деятельность. Эксперимент длится в течение 8 секунд. Время рассчитано из тех соображений, что частота дискретизации ЭЭГ составляет 1/128, а для удобства последующей обработки полученных данных методом быстрого преобразования Фурье необходимо, чтобы количество выборок было пропорционально 2^k.

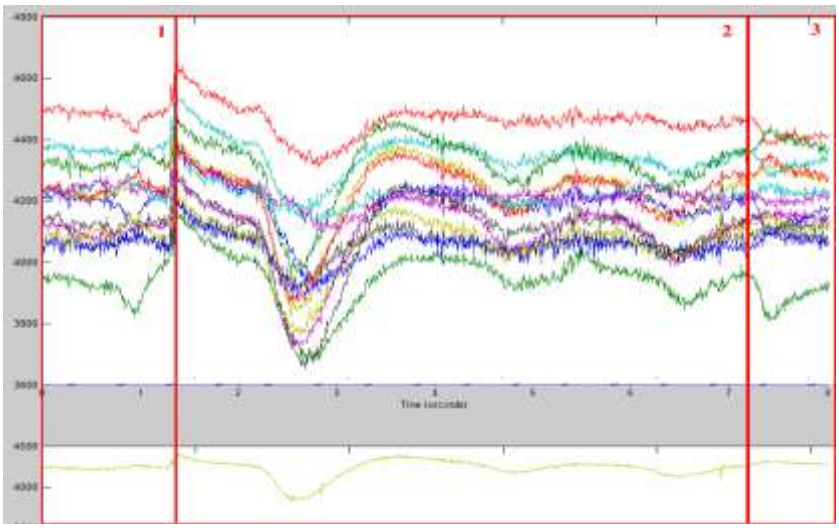

Рис. 3. ЭЭГ, полученная в результате второго эксперимента: 1 – пользователь расслаблен; 2 – пользователь мысленно воспроизводит музыкальную композицию; 3 – пользователь расслаблен

3. В третьей серии экспериментов мысленные образы формируются на основе реакции движении глаз [3]. Опыт состоит в следующем:в течение 8 секунд у пользователя снимают ЭЭГ, каждую секунду пользователь ориентирует закрытые глаза в определенную сторону (лево-право-вверх-вниз). Такая последовательность движений глаз является «мысленным паролем».

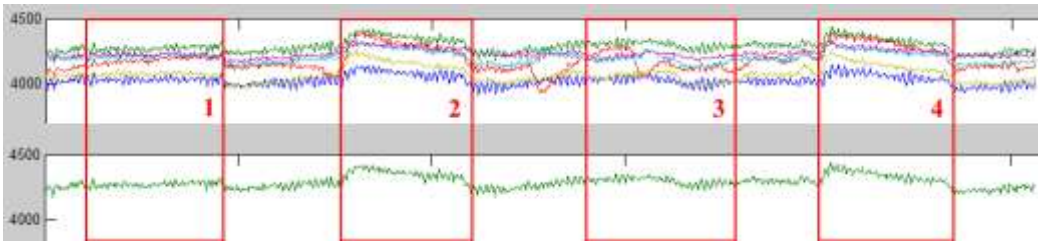

Рис. 4. ЭЭГ, полученное в результате третьего эксперимента: 1 –взгляд влево; 2 – взгляд вправо; 3 – взгляд вверх; 4 – взгляд вниз

Полученные результаты показывают, что для каждого из методов формирования мысленных образов существуют свои требования. Придерживаясь этих требований возможно получить весьма четкие мысленные образы, которые в дальнейшем можно использовать для высокоточной биометрической аутентификации.

Список литературы

1. Перцев А.О. Использование устойчивых мысленных образов в качестве элементов словаря для аутентификации / А.О. Перцев, М.Е. Маркин, Г.А. Любавский // 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. 139-142.

2. Боршевников А.Е. Результат эксперимента по восстановлению секретного ключа по ЭЭГ с использованием нейросетевого преобразователя "Биометрия - код доступа" / А.Е. Боршевников, 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.

3. Киктев С.В. Создание интерфейса управления р/у моделью автомобиля, посредством движения глаз и бровей / С.В. Киктев, С.Я. Горишный, М.А. Шинкоренко // Сборник докладов 58-й международной молодежной научно-технической конференции «МОЛОДЕЖЬ-НАУКА-ИННОВАЦИИ», 24-25 ноября 2010 г. в 2-х т. – Владивосток: Мор. гос. ун-т, 2010.- Т. 1.- С. 150-153.