УДК 004.056.52

Гончаров Сергей Михайлович,
к. ф.-м. н., доцент, МГУ им. адм. Г.И. Невельского,
e-mail: sgprim@smtp.ru
Михайлов Андрей Геннадьевич,
студент, ДВФУ,
e-mail: quantum722@gmail.com
Боршевников Алексей Евгеньевич,
ассистент кафедры ИБ, ДВФУ,
e-mail: LAdG91@mail.ru

ОБ ИСПОЛЬЗОВАНИИ МЕТОДА ЛОКАЛИЗАЦИИ СИМВОЛОВ МЫСЛЕННОГО ПАРОЛЯ В ЗАДАЧАХ БИОМЕТРИЧЕСКОЙ ИДЕНТИФИКАЦИИ

Область технологий биометрической идентификации является динамично развивающейся областью. Это связано с тем, что биометрическая идентификация основывается на неотъемлемых психофизиологических особенностях человека, что обеспечивает относительно удобное их использование в качестве идентификаторов. Различные биометрические характеристики обеспечивают различный уровень безопасности.

Из ряда перспективных видов биометрических характеристик можно выделить электроэнцефалограмму человека (ЭЭГ). На текущий момент 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]. Вероятность ошибки 2-го рода находится в диапазоне от 10% до 0.1% для лучших из этих экспериментов. Одним из решений подобной проблемы является отход от построения классической системы идентификации на основе ЭЭГ и построение системы высоконадежной биометрической идентификации в соответствии с серией стандартов ГОСТ Р 52633 [2].

Ранее уже проводились исследования по построению подобных систем биометрической идентификации [3,4]. При обучении нейросетевого преобразователя из сигнала требуется выделить информативную часть, однако большинство методов обработки сигналов для выделения параметров основаны на том факте, что обрабатываемый сигнал является стационарным. Так как ЭЭГ не является стационарным сигналом, то выделение параметров сигнала в данном случае затруднено.

Для эксперимента было решено использовать потенциал движения мышц глаз [4]. Для обработки полученного сигнала (матрица 14×1025, где 14 – количество каналов нейрогарнитуры), было решено определить локализацию точек в моменты движения глаз. Значения, полученные с электрода, были пропущены через фильтр Баттерворта с полосой

пропускания 0,16 – 0.6 Гц. Затем полученный массив y было решено численно продифференцировать. Для этого были составлены конечные разности вида:

$$\Delta y_k = y_k - y_{k+1}, \qquad k = \overline{1,1024} \tag{1}$$

Искомыми точками, в моменты движения глаз, будут те значения k, для которых выполняется:

$$\begin{cases} \Delta y_k \le 0 \\ \Delta y_{k+1} \ge 0 \end{cases} \text{ или } \begin{cases} \Delta y_k \ge 0 \\ \Delta y_{k+1} \le 0 \end{cases} \tag{2}$$

Так как за 1 секунду с нейрогарнитуры регистрируется 64 значений, а PIN-код в данной работе длиной 7 символов, то вектор входных параметров было решено сформировать следующим образом: в информативном канале 2 в окрестностях точек, полученных из информативного канала 1, применялось дискретное преобразование Фурье на интервалах *k-63* до *k+64* (Рисунок 1). Модуль полученных комплексных коэффициентов для каждого символа пароля объединяется в единый вектор. Данный вектор подается на входы нейросетевого преобразователя.

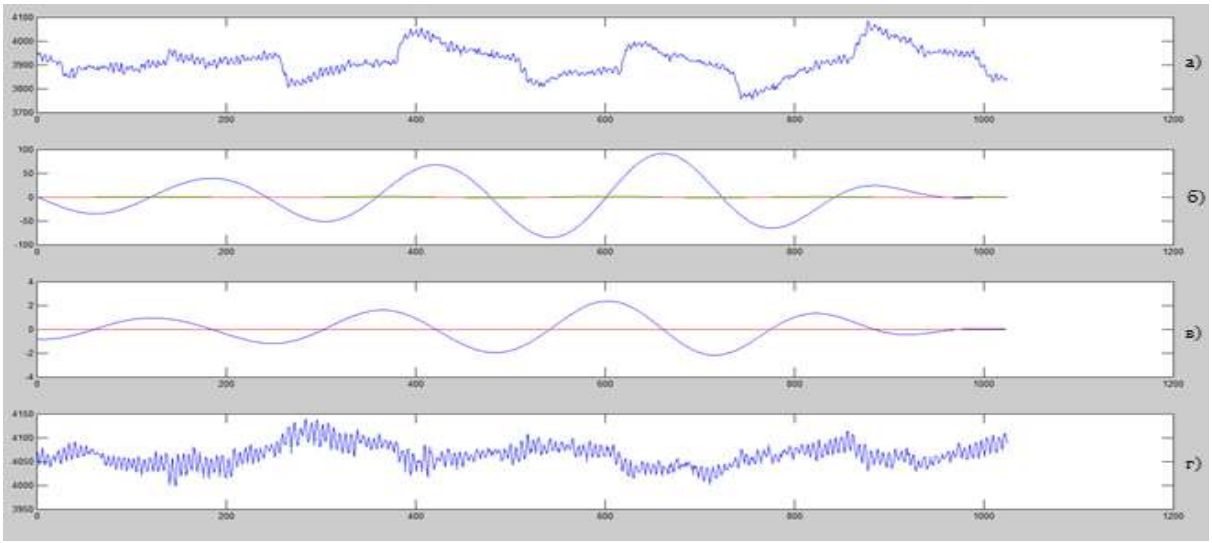

Рис. 1. а) информативный канал 1 б) информативный канал после фильтрации в) производная г) Информативный канал 2

Процедура построения и обучения нейросетевого преобразователя полностью основана на ГОСТ Р 52633.5 с учетом параметров получившихся входных данных [2].

После построения модели преобразователя были проведены исследования по его работе. Исследования по получению злоумышленником секретного ключа длиной 256 бит с помощью преобразователя при известных весовых коэффициентах и при условиях знания истинного или некоторого ложного пароля показывают, что минимальное полученное расстояние

Хэмминга составляет 47 (таблица 1). Как показано в таблице удалось увеличить расстояние Хэмминга по сравнению с экспериментом без выделения символа мысленного пароля.

Таблица 1

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

Номер пользователя	Расстояние Хэмминга в эксперименте без выделения символа мысленного пароля	Расстояние Хэмминга в эксперименте с выделением символа мысленного пароля
1	26	103
2	24	83
3	82	71
4	51	47
5	22	70
6	44	67
7	54	83
8	18	90
9	93	56

При этом для всех тестовых образов «свой» преобразователь безошибочно восстанавливал ключ.

Полученные результаты показывают, что обработка данных части биометрического сигнала для выбора биометрических параметров показывает качественно лучший результат по сравнению с обработкой целого сигнала. Дальнейшее исследование в этой области открывает возможности по улучшению качества работы нейросетевого преобразователя "Биометрия - код доступа на основе ЭЭГ.

Список литературы

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. Автоматическое обучение нейросетевых преобразователей биометрия - код доступа: ГОСТ Р 52633.5-2011. – Введен впервые; Введ. 01.12.2011. – М.: Стандартинформ, 2012. – 20 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. Гончаров С. М., Боршевников А. Е. Нейросетевой преобразователь «Биометрия – код доступа» на основе электроэнцефалограммы в современных криптографических приложениях. // Вестник СИБГУТИ: – Новосибирск: Изд-во СИБГУТИ, 2016. – № 1. – С. 17–22.