Компьютерные инструменты в образовании, 2019
№ 3: 52–69
УДК: 004.58[159.91]
http://cte.eltech.ru
doi:10.32603/2071-2340-2019-3-52-69

АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЯ ПО ЭЛЕКТРОЭНЦЕФАЛОГРАФИЧЕСКИМ СИГНАЛАМ ПРИ МОРГАНИИ*

Станкевич Л. А.[1], кандидат технических наук, доцент, stankevich_lev@inbox.ru
Аманбаева С. С.[1], лаборант, sabisha2704@mail.ru
Самочадин А. В.[1], кандидат технических наук, доцент, ✉ samochadin@gmail.com

[1]Санкт-Петербургский политехнический университет Петра Великого,
ул. Политехническая, д. 29, 195251, Санкт-Петербург, Россия

Аннотация

В статье представлены результаты исследования в области применения электроэнцефалографии (ЭЭГ) для аутентификации человека. Разработан и описан алгоритм ЭЭГ-аутентификации на основе морганий. Аутентификация проводится по одному морганию, что занимает 2–5 секунд. Для сбора данных используется электроэнцефалограф Muse. Предобработка данных включает вейвлет-преобразование и выделение морганий. В качестве признаков используются геометрические характеристики ЭЭГ. Распознавание ведется классификатором на основе Случайного леса (*Random Forest*). По результатам тестирования процент верной аутентификации составил 95 %. Имеется возможность фоновой аутентификации. Реализованная система может быть использована для аутентификации студентов при дистанционном образовании.

Ключевые слова: *электроэнцефалограмма, аутентификация, моргание, электроокулограмма, машинное обучение, классификация, Muse Headband, дистанционное образование.*

Цитирование: Станкевич Л. А., Аманбаева С. С., Самочадин А. В. Аутентификация пользователя по электроэнцефалографическим сигналам при моргании // Компьютерные инструменты в образовании. 2019. № 3. С. 52–69. doi:10.32603/2071-2340-2019-3-52-69

1. ВВЕДЕНИЕ

Одним из важных требований к средствам дистанционного обучения является наличие средств проверки личности студента в дистанционном режиме. Необходимость аутентификации студентов при дистанционном обучении включена в некоторые зарубежные образовательные стандарты в качестве обязательной процедуры [1]. При этом средства аутентификации должны обеспечивать проверку не только при начале работы,

*Работа подготовлена в ходе реализации проекта в рамках Постановления Правительства РФ от 09.04.2010 г. № 218 при финансовой поддержке Министерства образования и науки РФ (договор № 03.G25.31.0247 от 28.04.2017 г.)

но и в процессе выполнения учебных заданий. Аутентификация должна осуществляться в фоновом режиме, не отвлекая студента от учебных мероприятий.

В настоящее время наиболее распространенной системой аутентификации является аутентификация на основе паролей. Потенциальный пользователь получает доступ к работе, вводя в компьютер пароль, например в виде заранее определенного для него слова или фразы, чтобы подтвердить свою личность. Пароль должен быть известен только этому пользователю. Надежность пароля определяется его длиной и ограничениями на используемые символы, поэтому пользователям необходимо формировать длинные (например, больше 8 букв, цифр и специальных символов) последовательности, чтобы использовать надежный пароль, что не очень удобно [2]. Применение парольной идентификации с надежным паролем для подтверждения личности студента в процессе выполнения учебных мероприятий нежелательно, в связи с невозможностью реализации фонового, без привлечения внимания студента, режима проверки.

Альтернативой аутентификации на основе паролей является биометрическая аутентификация. Этот метод использует уникальные биологические характеристики каждого человека для распознавания. Часто используются следующие биометрические признаки: отпечаток пальца руки или ладони, рисунок иридиевой оболочки глаза, тембр и спектральный образ голоса, изображение лица, рисунок подписи и пр. Существуют некоторые требования, которые необходимо выполнить, чтобы биометрические признаки можно было применять в реальных приложениях. В частности, признаки должны быть универсальны, постоянны и измеримы, а системы идентификации должны обладать высокой производительностью и распознавать личность с достаточной для практического применения точностью [3].

Существует еще один подход к биометрической аутентификации, который использует сигналы биоэлектрической активности мозга, регистрируемые с помощью электроэнцефалографа в виде электроэнцефалограмм (ЭЭГ). ЭЭГ показывают пространственно-временную картину электрической активности во многих зонах мозга Эта информация специфична для каждого человека и может быть использована для аутентификации. В данном методе аутентификации сигналы ЭЭГ, зарегистрированные на определенном отрезке времени, выступают в роли носителя биометрической информации. В большинстве подходов к аутентификации по ЭЭГ этот отрезок времени должен быть привязан к некоторому типовому событию.

ЭЭГ-аутентификация имеет ряд преимуществ по сравнению с другими биометрическими методами. В частности, сигналы ЭЭГ не могут быть подделаны, поскольку генерируются только тем человеком, который должен быть идентифицирован. Однако имеются существенные трудности при реализации этого метода, в частности, из-за вариативности сигналов ЭЭГ. Они изменяются при работе разных мышц и выполнении различных умственных задач, поэтому систему идентификации требуется привязывать к определенному состоянию человека и долго обучать правильному распознаванию ЭЭГ-паттернов, соответствующих данному состоянию. В отличие от этого, отпечатки пальцев и радужной оболочки являются постоянными, и работать с ними проще.

Генетическая обусловленность информации в ЭЭГ была исследована еще в 1930-х годах [4]. А в 1960-х годах была установлена прямая связь между ЭЭГ человека и его генетической информацией [5]. Помимо уникальности, ЭЭГ обладает еще одним важным для аутентификации свойством — данные ЭЭГ визуально не наблюдаемы, следовательно, их более сложно зафиксировать и подделать. Последнее дает значительное преимущество методу ЭЭГ-аутентификации в сравнении с другими.

Данная работа посвящена исследованию и разработке средств аутентификации человека по ЭЭГ-паттернам, соответствующим состоянию моргания. Это самое простое дей-

ствие, которое довольно четко отображается в сигналах ЭЭГ, регистрируемых в определенных зонах мозга. Моргание относится к таким реакциям организма, которые необходимы для поддержания его состояния. Рефлекторно человек моргает 10–20 раз в минуту (в среднем), и поэтому моргания могут использоваться для аутентификации в фоновом режиме, без отвлечения человека на процесс проверки.

Материал остальной части статьи изложен в нескольких разделах. В первом разделе приводится описание методики и системы ЭЭГ-аутентификации. Второй — содержит описание алгоритмов процесса аутентификации. В третьем разделе рассмотрены вопросы практической реализации предложенного метода, в четвертом приведены результаты экспериментального исследования системы и ее эффективности.

2. МЕТОДИКА И СИСТЕМЫ ЭЭГ-АУТЕНТИФИКАЦИИ

При дистанционном обучении часто требуется аутентификация, которая может использоваться для узнавания человека при доступе в рабочую зону или его аутентификации в процессе работы, например, при ограниченном доступе к защищенным документам [6]. ЭЭГ-аутентификация часто является предпочтительной, поскольку может быть реализована с использованием распространенного оборудования.

При разработке методики ЭЭГ-аутентификации прежде всего требуется определить, какие сигналы ЭЭГ могут быть использованы. Для решения этой проблемы был проведен анализ существующих работ в данной области.

Исследования, описанные в работе [7], основаны на использовании для идентификации субъектов сигналов ЭЭГ, полученных в фоновом режиме, то есть при отдыхе и отсутствии целенаправленной мыслительной активности. Полученные сигналы ЭЭГ обрабатывались с целью вычисления коэффициентов авторегрессии. Идентификация проводилась с использованием предварительно обученной на коэффициентах авторегрессии соревновательной нейронной сети. В эксперименте приняли участие 10 человек с оценкой точности для каждого человека отдельно. При этом минимальная точность идентификации была 80 %, а максимальная — 90 %.

В работе [8] проводилось исследование по точности распознавания слов на основе вызванного потенциала N400. Это отрицательное отклонение на ЭЭГ, которое достигает пика приблизительно через 400 миллисекунд после начала стимула. N400 является частью нормальной реакции мозга на слова (изображенные и произнесенные). Запись длилась в течение 50 секунд, каждую секунду на экране менялось слово. В эксперименте приняли участие 45 человек, точность распознавания набора изображенных слов каждым человеком составила около 83 %.

В исследовании [9] приняло участие 10 человек, в течение 40 секунд каждому предъявляли фотографии лиц. Периодически перед собой они видели свою фотографию, что создавало особую форму волны, по которой и велось распознавание своего лица. Точность распознавания своего лица составила 86 %.

В работе [10] велась запись сигнала ЭЭГ по 4 минуты. В это время человек, сидя в расслабленном состоянии, должен был воображать движения сначала левой рукой, потом правой. В эксперименте принимали участие 9 человек, при этом точность классификации движений рук составила 80 %.

Работа [11] основывалась на состоянии покоя. 23 человека в течение одной минуты должны были находиться в расслабленном состоянии. Результаты классификации показали лишь 79 % точности. Общая ошибка аутентификации 42 %.

Работа [12] аналогична работе [9] с фотографиями самого себя. Точность распознавания своего лица была около 85 %, но время записи стало намного короче.

Статья [13] описывает эксперимент по аутентификации с участием 10 человек, которым в момент записи предлагалось совершать естественные моргания длительностью 20 секунд, Точность аутентификации личности путем распознавания морганий составила 93–98 %.

Опираясь на результаты этих исследований, можно сделать ряд выводов о возможных системах аутентификации и их особенностях.

1. Аутентификация на основе визуальных стимулов дает хорошие результаты и может происходить быстро, но невозможна без привлечения внимания пользователя.
2. Чтение текста требует длительной записи для усреднения результатов по причине низкой, сложно распознаваемой амплитуды отклика.
3. Моторные образы занимают много времени и дают плохие результаты.
4. Состояние покоя также требует много времени и трудно уловимо в фоне.
5. Моргания — являются естественным процессом, что дает возможность использовать их в фоновом режиме. Рекомендуемая длительность записи составляет около 20 секунд, за это время совершается 4–6 морганий, которые далее усредняются для компенсации случайных шумов и выделения более четких пиков морганий (шаблонов).

Вариант системы ЭЭГ-аутентификации на основе морганий имеет преимущества, поскольку относительно просто реализуется и, как показано в работе [13], может дать хорошие результаты по точности.

Движения глаз сопровождает биоэлектрическая активность (глазодвигательный артефакт), которую можно зарегистрировать посредством накожных электродов вблизи глаз. Графическое изображение зафиксированной активности называется электроокулограммой (ЭОГ) [14]. Электроды электроэнцефалографа способны зафиксировать движение глаз. В теории ЭЭГ данный вид активности считается артефактом, то есть дефектом, так как не является истинной биоэлектрической активностью головного мозга, который устраняется из записи. Исследования показали, что моргания с интервалом не менее 300 миллисекунд генерируют уникальный сигнал ЭОГ для каждого человека [15].

Учитывая сказанное, для ЭЭГ-аутентификации в данной работе выбран последний вариант системы аутентификации с использованием шаблона морганий и уменьшенным количеством их повторений и длительность записи.

3. АЛГОРИТМЫ ПРОЦЕССА ЭЭГ-АУТЕНТИФИКАЦИИ

Процесс аутентификации, основанный на естественных морганиях, которые фиксируются на ЭЭГ, включает 4 этапа (рис. 1):

1. Сбор данных путем регистрации сигналов ЭЭГ в выбранных каналах.
2. Предобработка для фильтрации шумов и выделения ЭОГ (ЭЭГ-паттернов морганий).
3. Формирование признаков по шаблону.
4. Аутентификация на основе классификации разных пользователей.

Сбор данных. На данном этапе происходит запись ЭЭГ при помощи электроэнцефалографа. Записываются «сырые» данные, содержащие сигналы ЭЭГ с выбранных каналов с указанием времени их появления. Предполагается, что данные содержат моргания.

Предобработка. Цель данного этапа — выделить сигналы ЭОГ из сигнала ЭЭГ. Для этого сначала записанные сигналы ЭЭГ подвергаются разложению до третьего уровня

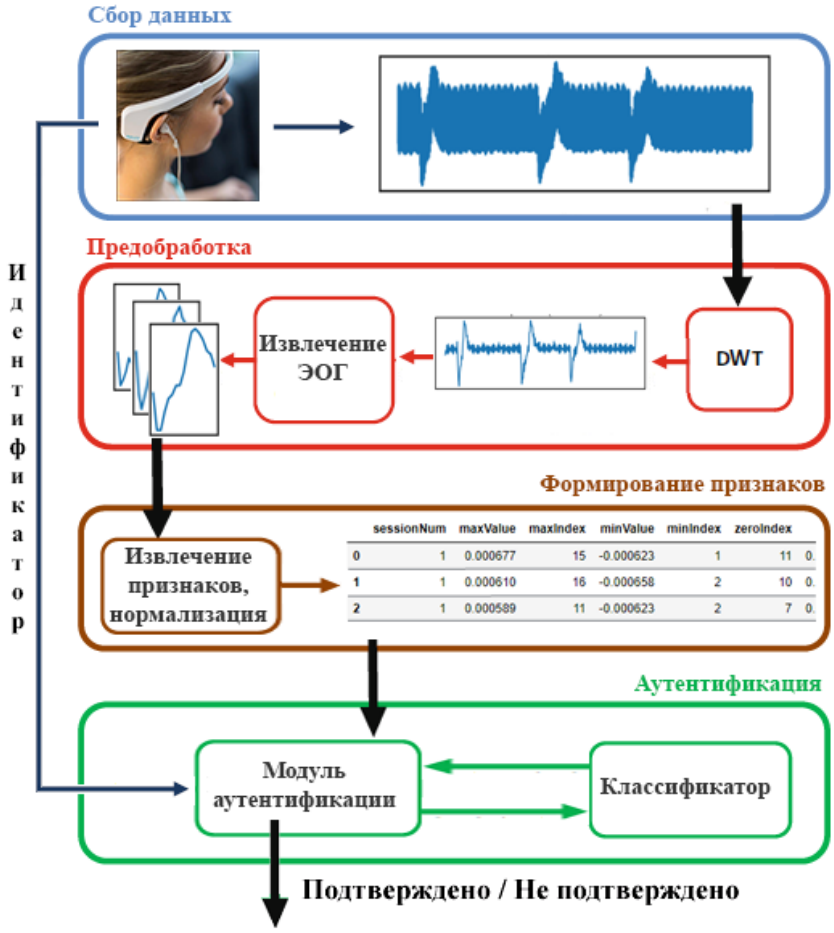


Рис. 1. Этапы процесса аутентификации на основе ЭЭГ

с использованием дискретного вейвлет-преобразования, в результате чего выделяются пики на имеющейся записи. При этом сигнал разбивается на две составляющие — аппроксимирующую и детализирующую. Аппроксимирующая часть содержит информацию, которую необходимо извлечь, детализирующая — маловажные элементы сигнала. Осуществляется это путем вычисления скалярного произведения анализируемого сигнала и анализирующего вейвлета на заданном масштабе.

В зависимости от того, какую именно информацию необходимо извлечь из сигнала, могут быть использованы вейвлеты разного типа. В нашем случае для разложения оказалось лучше использовать в качестве материнского Вейвлет Добеши второго порядка (db2), поскольку по форме он близок к паттерну моргания рис. 2. Графики аппроксимирующей и детализирующей составляющих вейвлета показаны в осях «условная амплитуда-условное время».

Для данной процедуры требуется разбить исходный сигнал S на группы по четыре элемента, смещаясь каждый раз на два. Элементы аппроксимирующей последовательности вычисляются по формуле

$$a_i = c_0 + c_1 \cdot s_{2i} + c_2 \cdot s_{2i+1} + c_3 \cdot s_{2i+2} + c_4 \cdot s_{2i+3},$$

где c_0–c_3 — табличные коэффициенты вейвлета:

$$c_0 = 0,4829629131;\ c_1 = 0,2241438680;\ c_2 = 0,8365163037; c_3 = -0,1294095226.$$

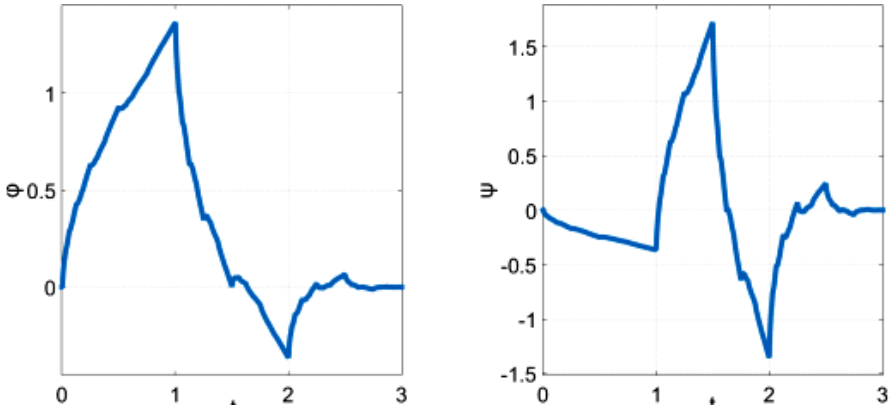


Рис. 2. Аппроксимирующая и детализирующая составляющие вейвлета Добеши второго порядка

Коэффициенты второго фильтра должны быть ортогональны первому, для чего берутся те же коэффициенты, но переставляются и меняются знаки. Элементы детализирующей последовательности вычисляются по следующей формуле:

$$d = c_0 + c_4 \cdot s_{2i} - c_3 \cdot s_{2i+1} + c_2 \cdot s_{2i+2} - c_1 \cdot s_{2i+3} \, .$$

Матрица преобразования имеет вид:

$$\begin{bmatrix} c_1 & c_2 & c_3 & c_4 & & & & \\ c_4 & -c_3 & c_2 & -c_1 & & & & \\ & & c_1 & c_2 & c_3 & c_4 & & \\ & & c & -c_3 & c_2 & -c_1 & \bullet & \bullet \end{bmatrix}$$

После вычисления скалярного произведения анализируемого сигнала и данной матрицы получаются два набора коэффициентов. На аппроксимирующем наборе данное преобразование повторяется еще дважды, в результате получим разложение сигнала до третьего уровня с уменьшенным шумом и выделенными морганиями. Далее происходит извлечение морганий из полученных сигналов. Для этого каждый сигнал подвергается следующей поэтапной обработке (рис. 3).

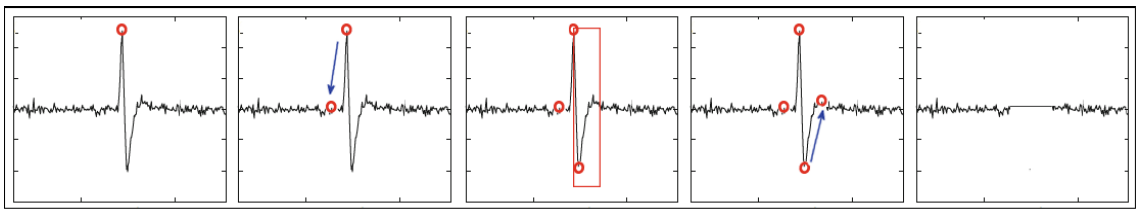


Рис. 3. Этапы процесса извлечения морганий

1. Определяется максимальное положительное значение сигнала. Ожидается, что это будет положительный пик одного из морганий.
2. Идет поиск начала положительного пика путем уменьшения индекса сигналов, пока значение амплитуды не станет меньше 5 % от обнаруженного положительного пика на этапе 1.

3. Находится максимальное отрицательное значение в течение 400 мс от положения положительного пика, обнаруженного на этапе 1. Предполагается, что это будет отрицательный пик моргания.
4. Обнаруживается завершение отрицательного пика путем увеличения индекса сигналов до тех пор, пока значение амплитуды не станет менее 5 % от обнаруженного отрицательного пика на этапе 3.
5. Если значение обнаруженного отрицательного пика (на этапе 3) составляет менее 35 % от обнаруженного положительного пика (на этапе 1), то этот сигнал отбрасывается, поскольку обнаруженная форма не соответствует шаблону моргания. В противном случае сигнал от начала до завершения (этапы 3 и 4) сохраняется, а в исходном сигнале этот участок обнуляется.
6. Этапы 1–5 повторяются до тех пор, пока значение обнаруженного положительного пика не станет менее 50 % от первого обнаруженного положительного пика.

После последовательного выполнения всех этапов процесса получаются выделенные моргания, подготовленные для дальнейшего анализа и извлечения уникальных признаков. Формирование признаков. В качестве признаков выбраны геометрические характеристики каждого выделенного моргания, так как он является уникальным. Выделенные моргания обрабатываются для получения признаков, таких как: амплитуда максимального позитивного или негативного пика, позиция максимального позитивного или негативного пика и т. д. При построении шаблона морганий вычисляются следующие признаки:

M_p — амплитуда позитивного пика;
I_p — позиция позитивного пика;
M_n — амплитуда негативного пика;
I_n — позиция негативного пика;
I_z — позиция точки пересечения нуля;
S_p — площадь под позитивным импульсом;
S_n — площадь под негативным импульсом;
Av_p — среднее значение позитивного импульса;
Av_n — среднее значение негативного импульса;
D_p — длительность позитивного импульса;
D_n — длительность негативного импульса;
Tg_{sp} — угол наклона от начала позитивного импульса;
Tg_{ep} — угол наклона от конца позитивного импульса;
Tg_{sn} — угол наклона от начала негативного импульса;
Tg_{en} — угол наклона от конца негативного импульса;
M_{p1} — амплитуда позитивного пика первой производной волны;
I_{p1} — позиция позитивного пика первой производной волны;
M_{n1} — амплитуда негативного пика первой производной волны;
I_{n1} — позиция негативного пика первой производной волны;
N_{z1} — количество пересечений нуля первой производной волны.

Исходные значения признаков могут изменяться в большом диапазоне, поэтому работа классификатора с такими данными может оказаться некорректной. Для решения этой проблемы производится нормализация признаков, то есть значения признаков, приводятся к некоторому заданному диапазону. В нашем случае каждый признак приводится к единичному среднеквадратичному отклонению и нулевому среднему. Для этого среднее значение столбца (признака) μ вычисляется по формуле

$$\mu = \frac{1}{N}\sum_{i=1}^{N} x_i,$$

где N — количество элементов в столбце, x_i — элемент столбца.

Выражение для вычисления стандартного отклонения σ имеет вид

$$\sigma = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(x_i - \mu)^2}.$$

Для получения нормализованного значения признака используем вычисленные среднее значение и стандартное отклонение величины и применим к ним выражение

$$z_i = \frac{x_i - \mu}{\sigma},$$

где z_i — новое нормализованное значение признака.

Аутентификация. Процесс аутентификации производится‘с использованием машинного обучения, которое позволяет создавать модели распознавания и классификации путем обучения на основе накопленных данных. В нашем случае создается модель классификации ЭЭГ-паттернов, соответствующих процессам моргания разных людей.

Модель классификации имеет на входе вектор признаков ЭЭГ-паттерна, соответствующий морганиям тестируемого человека и, используя векторные шаблоны признаков нескольких людей (в том числе и тестируемого), полученные путем обучения, выдает на выходе метку класса этого человека. Формально задача классификации ставится следующим образом. Если $X = (X_1, \ldots, X_m)$ —- конечное множество векторных шаблонов признаков, а $Y = (y_1, \ldots, y_m)$ — соответствующее ему конечное множество меток классов (номеров или имен людей), то модель классификации описывается отношением $X \to Y$, которое может быть найдено путем обучения. Для этого используется обучающая выборка, содержащая множество примеров правильного отображения отношения классификации $\{(X_1 \to y_1), \ldots, (X_m \to y_m)\}$. Найденное с использованием обучающей выборки отношение $X \to Y$ применяется для определения класса ЭЭГ-паттерна y_i, если он является (или близок) элементом множества X, то есть $X_i \in X$. Таким образом, для аутентификации необходим обученный классификатор, способный предсказать класс ЭЭГ-паттерна конкретного человека по его признакам.

В данной работе исследовались несколько классификаторов: на методе ближайших соседей, методе опорных векторов, деревьях решений и наивной Байесовской классификации. Для практического использования в предлагаемой системе аутентификации выбран классификатор *Random Forest* (Случайный лес) [16].

Random Forest является классификатором, основная идея которого заключается в построении как можно менее зависимых друг от друга деревьев решений с последующим принятием решения путем голосования. Деревья принятия решений (*Decision trees*) имеют листы, внутренние узлы и ребра. В листах записаны значения классов, а в узлах — признаки, по которым различаются случаи при спуске по дереву. Чтобы вычислить значение класса для набора признаков, надо спуститься по дереву до листа и выдать соответствующую метку. *Random Forest* использует ансамбль решающих деревьев. Он сочетает метод случайных подпространств и усреднений решений локальных классификаторов по методу бутстрэпа. Будстреп — статистический метод формирования m новых выборок размером n из n объектов исходной выборки. При этом производится n

раз выбор объекта в одну из m выборок с возвратом предмета в исходное множество, то есть некоторые предметы могут попасть в выборку несколько раз, некоторые могут не попасть вообще. При классификации выборки формируются описанным подходом, на каждой выборке обучается свой (локальный) классификатор, а итоговый классификатор усредняет решения всех локальных классификаторов.

Для снижения корреляции между деревьями при их обучении на случайно выбранных признаках вместо всего набора используется метод случайных подпространств.

Выбор признака для разбиения может осуществляться различными способами. Для этого может использоваться критерий Гини [16], но в некоторых реализациях алгоритма построения деревьев вместо него используется критерий прироста информации. Дерево строится до полного исчерпания подвыборки.

Классификация объектов проводится путём голосования: каждое дерево комитета решающих деревьев относит классифицируемый объект к одному из классов, и побеждает класс, за который проголосовало наибольшее число деревьев.

Обучение и тестирование. Перед аутентификацией производится обучение и тестирование классификаторов на имеющемся наборе записей сигналов ЭЭГ. Общий набор данных необходимо поделить на обучающую и тестовую выборки, например, в процентном соотношении 70/30. Одним из полезных инструментов, дающим наиболее равномерное использование имеющихся данных, является кросс-валидация [17]. При этом данные разбиваются на k частей. Затем на $k-1$ частях данных производится обучение классификатора, а оставшаяся часть данных используется для тестирования. Процедура повторяется k раз; в итоге каждая из k частей данных используется для тестирования. В данной работе рассмотрено несколько подходов к делению исходных данных:

1. Стандартный, где записанные данные поделены в соотношении 70/30: для обучения используется 70 % данных, для тестирования — 30 %.
2. *KFold* — кросс-валидация при $k = 5$. Данные перемешиваются 1 раз в начале, делятся на 5 групп: 4 для обучения, 1 для тестирования. Производится 5 тестирований, каждый раз с заменой тестовой группы. Данные в тестовых группах не повторяются. За оценку берется среднее значение по 5 тестированиям.
3. *ShuffleSplit* — кросс-валидация с перемешиванием, $k = 5$. Производится 5 тестирований, перед каждым данные перемешиваются, делятся на 5 групп: 4 для обучения, 1 для тестирования. Данные в тестовых группах могут повторяться. За оценку берется среднее значение по 5 тестированиям.

Результаты классификации можно разбить на четыре категории, сопоставив истинные ответы и ответы классификатора

Карина9370 <students3970@yandex.ru>,
Примакова Екатерина <spbetu9301@gmail.com>,
Ширин Кирилл 9302 <k.shirin@gmail.com>,
Andrey Taubin <andrey.taubin@gmail.com>,
9371 <asta2001@inbox.ru>,
KiShiVi <k.shirnin@gmail.com>,

следующим образом:

TP — истинно-положительное решение;
TN — истинно-отрицательное решение;
FP — ложно-положительное решение;
FN — ложно-отрицательное решение.

Качество классификации можно определить по следующим метрикам:

1. Доля верных ответов (оценка *Accuracy*):
   Accuracy= (TP + TN)/(TP + TN + FP + FN).
2. Точность (*Precision*) в пределах класса — это доля записей, действительно принадлежащих данному классу относительно всех записей, которые классификатор отнес к этому классу:
   Precision= TP/(TP + FP).
3. Полнота (*Recall*) в пределах класса — это доля найденных классификатором записей, принадлежащих классу относительно всех записей этого класса в тестовой выборке:
   Recall= TP/(TP + FN).
4. *F*-мера — представляет собой гармоническое среднее между точностью и полнотой:
   F=(*Precision* · *Recall*)/(*Precision* + *Recall*).

Лучший из классификаторов используется в системе аутентификации. Аутентификация проходит по алгоритму, представленному на рис. 4.

1. Модуль аутентификации получает идентификатор пользователя (id) и набор векторов признаков 5-ти морганий (*DataSet*), сформированный из ЭЭГ пользователя.
2. Модуль аутентификации осуществляет запрос к обученному классификатору, для получения вероятности p — соответствия биометрических данных имеющемуся идентификатору.
3. Решение (V) принимается согласно следующему выражению
   $V = 1$ ***if*** $(p(id, DataSet) / (1-p(id, DataSet)) \geq T) \vee 0$ ***if else*** ,
   где T— порог подобия, определяющий степень безопасности системы. Пользователь подтвержден, если $V = 1$, или не подтвержден, если $V = 0$.

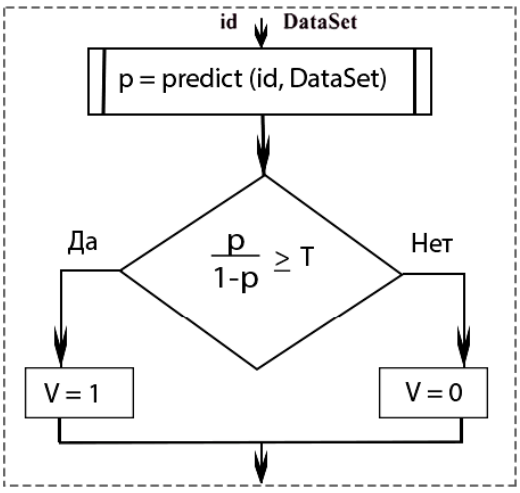


Рис. 4. Алгоритм аутентификации

При аутентификации возможно возникновение ошибок двух типов:

1. Ошибка первого рода FRR (False Reject Rate) — коэффициент ложного отказа, истинный пользователь не допущен.
2. Ошибка второго рода FAR (False Acceptance Rate) — коэффициент ложного допуска, допущен не истинный пользователь.

Значение ошибок напрямую зависит от порога подобия системы (T). При увеличении порога система становится более безопасной, FAR уменьшается, но FRR увеличивается.

При уменьшении порога, наоборот, FAR увеличивается, а FRR уменьшается, система становится уязвимой. Необходимо подобрать такой порог для системы, чтобы свести ошибки к минимуму. Равный уровень ошибок EER (Equal Error Rate) — это коэффициент, при которых обе ошибки (ошибка приёма и ошибка отклонения) эквивалентны, служит для комплексной оценки алгоритма.

4. РЕАЛИЗАЦИЯ СИСТЕМЫ ЭЭГ-АУТЕНТИФИКАЦИИ

Система ЭЭГ-аутентификации состоит из модулей, реализующих обозначенные в секции 2 этапы: сбора данных, предобработки, формирования признаков и аутентификации. Разработка системы велась с использованием языка *Python* [18] и интерактивной оболочки для него — *Jupyter Notebook* [19]. Выбор обусловлен наличием большого количества научных и технических библиотек.

Для регистрации ЭЭГ в системе используется широко доступный и дешевый миниатюрный электроэнцефалограф Muse Headband компании *Interaxon* [20]. Он оснащен четырьмя сухими (безгелиевыми) электродами, размещенными по системе 10–10, и не требует предварительной подготовки. Muse оборудован индикатором, который отображает режимы его работы, статус соединения с компьютером или смартфоном. Устройство является беспроводным, для передачи данных используется Bluetooth. Соединение с компьютером устанавливается через приложение для Windows — *BlueMuse* для потоковой передачи данных или с использованием Muse SDK [21].

Предобработка, формирование признаков и аутентификация реализуются программно на удаленном компьютере. При запуске программы перед пользователем появляется окно, в котором отображаются моргания человека в режиме реального времени. Система распознает моргание одним и двумя глазами, используя поступающие сигналы с Muse, и выводит соответствующую картинку. Запись длится некоторое (регулируемое) время.

Для работы с устройством Muse на языке *Python* предназначен пакет *pyMuse* [22] с набором библиотек. Например, библиотека *muselsl* позволяет устанавливать соединение, снимать информацию с датчиков, сохранять ее в файл в формате .cvs. Сохраненные записи с 4-х электродов: TP9, AF7, AF8, TP10 загружаются в программу, формируя многомерный массив, предоставленный библиотекой numpy. Далее «сырые» данные отправляются на предобработку.

В процессе предобработки сигналы ЭЭГ подвергаются вейвлет-преобразованию, которое реализуется средствами библиотеки *pywavelets*. Разложение до третьего уровня вейвлетом Добеши второго порядка (db2) по всем 4-м каналам показано на рис. 5.

ЭЭГ-паттерны морганий извлекаются из преобразованных сигналов согласно алгоритму, приведенному ранее в секции 2. Примеры ЭЭГ-паттернов моргания, извлеченных из сигналов по 4-м каналам, приведены на рис. 6.

Нормализация ЭЭГ-паттерном проводилась функцией *scale ()* библиотеки *scikit-learn*.

Перед аутентификацией проводился отбор лучшего классификатора, для этого использовалось четыре указанных здесь ранее классификатора из библиотеки *scikit-learn*. Как было ранее показано, использовались три различных подхода к делению данных на обучающую и тестовую выборки: стандартное деление 70/30, *KFold* и *ShuffleSplit*.

Для машинного обучения использовалась библиотека *scikit-learn*, а для построения визуализации результатов — *matplotlib*, *seaborn*.

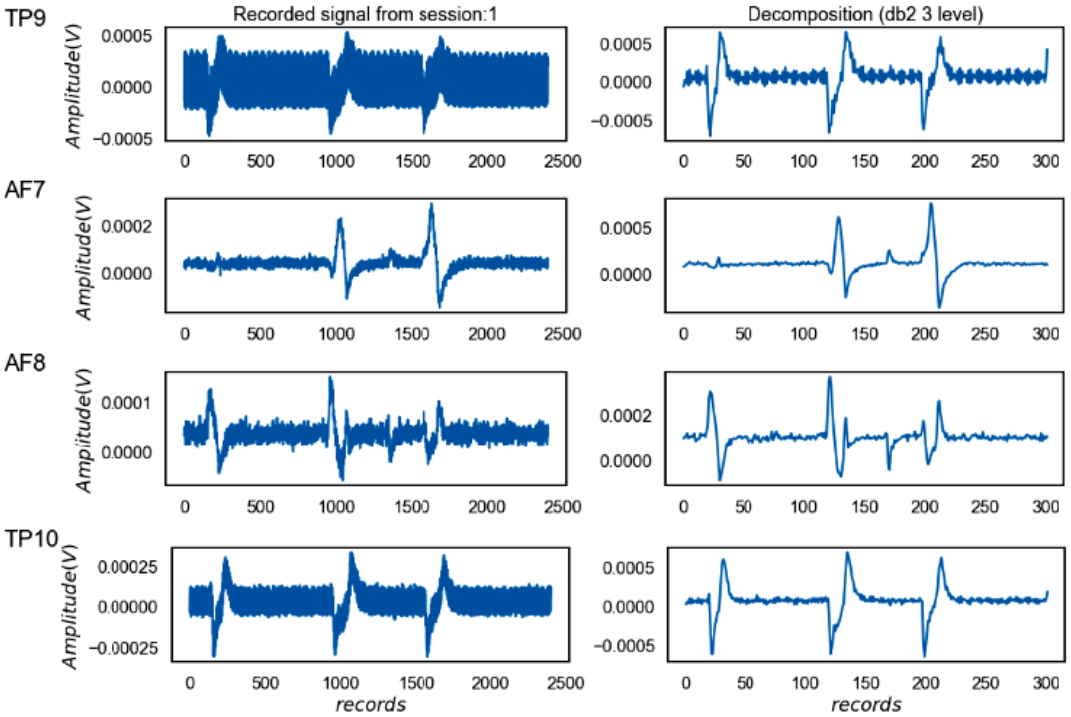


Рис. 5. Разложение вейвлетом Добеши второго порядка

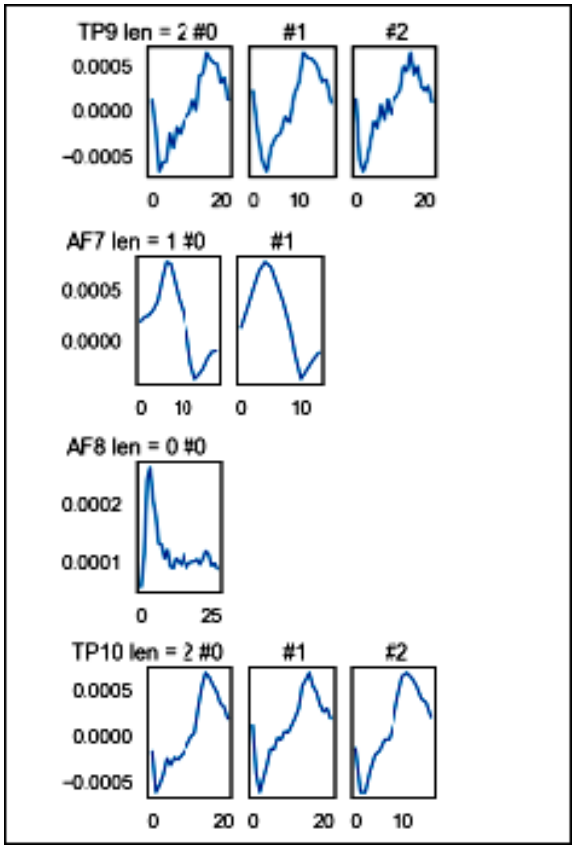


Рис. 6. ЭЭГ-паттерны морганий

5. ОЦЕНКА ЭФФЕКТИВНОСТИ СИСТЕМЫ АУТЕНТИФИКАЦИИ

Для оценки длительности и точности аутентификации был проведен эксперимент с участием 10 человек. На этапе регистрации каждый участник проходил запись ЭЭГ в течение двух минут с помощью устройства Muse. За это время он совершал примерно 30-40 естественных морганий. Далее собранные данные проходили этап предобработки и формирования признаков. В результате формировалась таблица по признаковым данным, полученным при обработке сигналов с каждого электрода (AF7, AF8, TP9, TP10). Строки этой таблицы соответствуют морганиям определенного человека (10 строк, каждая определяет класс), столбцы содержат геометрические характеристики (20 признаков) сигнала ЭЭГ текущих морганий всех испытуемых. Полученная таблица содержала наборы значений признаков морганий (обученные шаблоны) для каждого их испытуемых. Эти шаблоны далее использовались для классификации испытуемых при тестировании системы.

Для подбора классификатора в систему аутентификации было проведено тестирование классификаторов. Использовались четыре различных классификатора [23]:

1. KNN — метод k ближайших соседей.
2. SVC — метод опорных векторов.
3. RF — метод случайных деревьев решений.
4. NBC — метод наивной Байесовской классификации.

Для разделения данных на обучающую и тестовую выборки применялись подходы: стандартный (*Default*) 70/30, *KFold*, *ShuffleSplit*, кратко описанные ранее в секции 3.

Были вычислены метрики: доля верных ответов, точность, полнота, F-мера. Для примера на рис. 7 показаны результаты по каналу TP10.

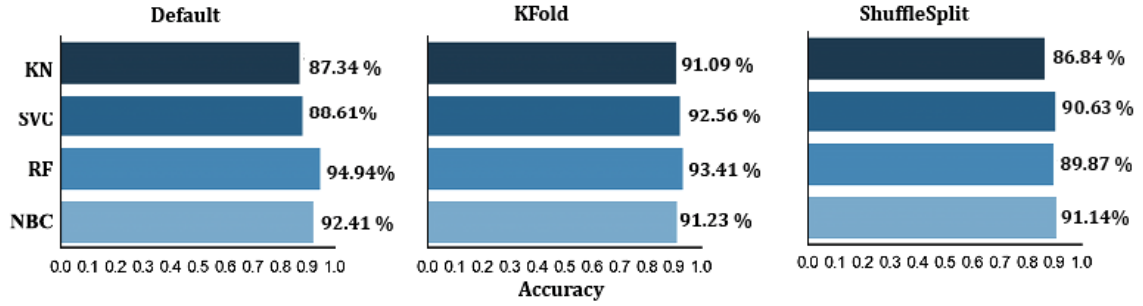
Необходимо отметить, что имеют место случаи, когда у некоторых людей на определенном канале не удается зафиксировать моргания. Причиной может быть неправильно надетое регистрирующее устройство, особенности человека или высокий уровень помех. Например, в этом эксперименте на электроде T10 не были зафиксированы моргания класса 3, 4, но на электроде TP9 они имелись.

Сравнение классификаторов проводилось по метрике *Accuracy* — доля верных ответов, где лучшие результаты классификации показал *Random Forest* 89–95 % при различных подходах к делению данных, поэтому именно он был использован в финальном варианте системы аутентификации.

Тестирование производилось в соответствии с алгоритмом, представленным на рис. 8. Для оценки качества из имеющегося набора данных с канала TP10, где зафиксировано 8 различных классов, было извлечено 8 произвольных морганий каждого класса для тестирования, остальные данные использовались для обучения классификатора *Random Forest*. Всего использовано 64 моргания для тестирования и 197 — для обучения.

Далее каждое моргание тестировалось на предмет входа в систему по каждому из 8-ми классов (64*8), то есть всего использовано 512 попыток входа. Ошибки ложного отказа (FRR) и ложного допуска (FAR) фиксировались согласно алгоритму:

Так как значение ошибок напрямую зависит от порога подобия, который для нашей системы еще не определен, было выполнено несколько итераций вышеприведенного алгоритма с различными порогами T. Полученная диаграмма FAR-FRR использовалась для поиска EER и оптимального порога подобия T (рис. 9а). Для общей картины на рис. 9б приведена ROC-кривая («кривая ошибок»). По результатам вычисления оптимальный порог подобия составил 0.52.



KNeighbors Default Version

	precision	recall	f1-score
1	0.83	0.94	0.88
2	0.78	1.00	0.88
5	0.92	0.86	0.89
6	0.92	0.79	0.85
7	1.00	1.00	1.00
8	1.00	0.40	0.57
9	1.00	0.50	0.67
10	0.80	1.00	0.89

KNeighbors KFold Version

	precision	recall	f1-score
1	1.00	0.84	0.92
2	0.86	0.86	0.86
5	0.98	0.88	0.92
6	0.80	0.94	0.87
7	1.00	1.00	1.00
8	0.79	0.92	0.85
9	1.00	0.85	0.92
10	0.91	1.00	0.95

KNeighbors Shufflesplit Version

	precision	recall	f1-score
1	0.95	0.76	0.84
2	0.81	0.78	0.80
5	0.90	0.88	0.89
6	0.79	0.92	0.85
7	1.00	0.98	0.99
8	0.65	0.75	0.70
9	0.89	0.85	0.87
10	0.90	0.93	0.92

SVC Default Version

1	1.00	0.94	0.97
2	0.70	1.00	0.82
5	1.00	0.79	0.88
6	0.87	0.93	0.90
7	1.00	1.00	1.00
8	1.00	0.40	0.57
9	1.00	0.50	0.67
10	0.80	1.00	0.89

SVC KFold Version

1	0.97	0.88	0.92
2	0.93	0.95	0.94
5	0.96	0.90	0.92
6	0.84	0.96	0.89
7	0.98	1.00	0.99
8	0.90	0.75	0.82
9	1.00	0.77	0.87
10	0.91	1.00	0.95

SVC Shufflesplit Version

1	0.93	0.84	0.88
2	0.90	0.92	0.91
5	0.96	0.89	0.92
6	0.80	0.96	0.87
7	0.97	0.98	0.98
8	0.80	0.60	0.69
9	1.00	0.80	0.89
10	0.94	1.00	0.97

RandomForest Default Version

1	1.00	0.94	0.97
2	0.88	1.00	0.93
5	1.00	1.00	1.00
6	0.92	0.86	0.89
7	1.00	1.00	1.00
8	1.00	1.00	1.00
9	1.00	0.50	0.67
10	0.80	1.00	0.89

RandomForest KFold Version

1	1.00	0.84	0.92
2	0.89	0.98	0.93
5	0.96	0.92	0.94
6	0.90	0.96	0.93
7	0.98	1.00	0.99
8	0.83	0.83	0.83
9	1.00	0.85	0.92
10	0.91	0.95	0.93

RandomForest Shufflesplit Version

1	1.00	0.78	0.88
2	0.84	0.89	0.87
5	0.97	0.92	0.94
6	0.82	0.93	0.87
7	0.98	0.98	0.98
8	0.70	0.70	0.70
9	0.86	0.95	0.90
10	0.93	0.90	0.92

NBC Default Version

1	0.94	0.94	0.94
2	0.82	1.00	0.90
5	1.00	0.86	0.92
6	0.93	1.00	0.97
7	1.00	1.00	1.00
8	1.00	0.80	0.89
9	1.00	0.50	0.67
10	0.75	0.75	0.75

NBC KFold Version

1	0.93	0.88	0.90
2	0.80	0.95	0.87
5	0.98	0.88	0.92
6	0.89	1.00	0.94
7	1.00	0.95	0.98
8	0.89	0.67	0.76
9	1.00	0.77	0.87
10	0.86	0.90	0.88

NBC Shufflesplit Version

1	0.95	0.84	0.89
2	0.80	0.92	0.86
5	0.94	0.85	0.89
6	0.90	1.00	0.95
7	1.00	0.98	0.99
8	0.80	0.60	0.69
9	1.00	0.90	0.95
10	0.91	1.00	0.95

Рис. 7. Результаты классификации по каналу TP10

6. ЗАКЛЮЧЕНИЕ

ЭЭГ-аутентификация является эффективным средством идентификации студента в дистанционном образовании. Она выполняется за приемлемое время и обеспечивает высокую точность, а также не требует очень дорогих технических средств для каждого пользователя.

Моргание является естественным процессом, и представленный метод ЭЭГ-аутентификации не требует использования сложной аппаратуры и алгоритмов.

Реализованный алгоритм аутентификации включает в себя четыре этапа: сбор данных, предобработку, формирование признаков, аутентификацию. Для сбора данных оказалось возможным использование относительно простого и дешевого электроэнцефало-

графа типа Muse headband. Предобработка с использованием вейвлет-преобразования позволяет избавиться от ненужных частот в сигнале ЭЭГ, а также произвести выделение морганий согласно существующему шаблону морганий. По выделенным участкам моргания снимаются геометрические характеристики, которые применяются для аутентификации с использованием заранее обученного классификатора, предсказывающего вероятность соответствия полученных признаков шаблону признаков, соответствующих пользователю, пытающемуся войти в систему. Пользователь получает доступ, если эта вероятность удовлетворяет пороговому значению, установленному в системе.

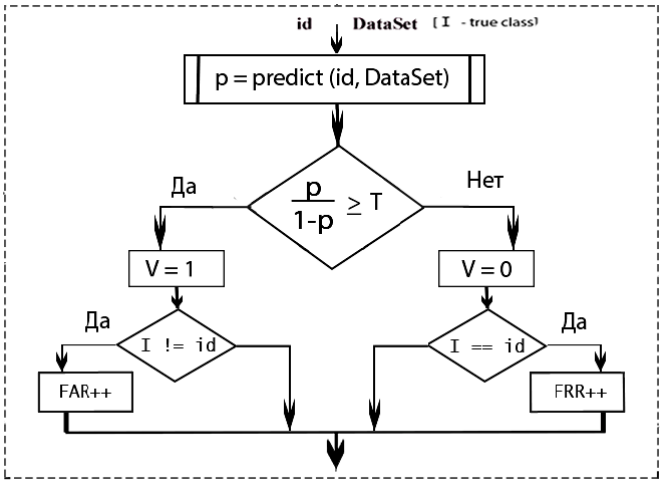
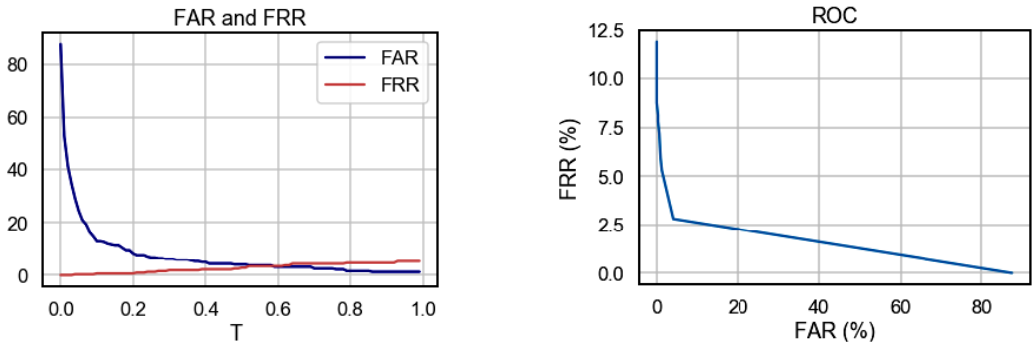


Рис. 8. Алгоритм аутентификации для тестирования



(а) **(б)**

Рис. 9. Диаграмма FAR-FRR и кривая ROC

Метод ЭЭГ-аутентификации по морганию оказался достаточно эффективным. Так, процесс тестирования показал, что из 512 попыток входа, программа корректно отвечает на 487 запросов, что составляет 95,12 %. Аутентификация реализована по одному морганию, что занимает всего 2–5 секунд. Поскольку в эксперименте участвовало 10 испытуемых и все они были идентифицированы программой, можно утверждать, что программа может уверенно различать минимум 10 человек. Для оценки максимальной различительной способности программы планируется провести дополнительные исследования со значительно большим количеством испытуемых. По предварительным оценкам программа сможет различать более 50 человек, что вполне достаточно для контроля группы учащихся при дистанционном обучении.

Таким образом, была реализована система ЭЭГ-аутентификации на основе морганий с использованием прибора Muse headband, соответствующая требованиям к точности аутентификации — не менее 85 % и времени реализации — не более 5 секунд. Возможность фоновой аутентификации тоже имеется, если отключить визуализацию и назначить интервал запуска.

Представленная система аутентификации по морганиям может быть эффективно использована для определения личностей студентов и допуске их, например, к контрольным работам в аудитории в рамках дистанционного образования.

Список литературы

1. Higher Education Opportunity, Act 122 Stat. 3078. Public Law 110–315. Aug. 14, 2008. USA.
2. *Matsumoto T.* Impact of Artificial “Gummy” Fingers on Fingerprint Systems // Proc. of SPIE, Optical Security and Counterfeit IV. San Jose, 2002. Vol. 4677. P. 275–289. doi: 10.1117/12.462719
3. *Nixon K. A. et al.* Handbook of Biometrics, chap. Spoof detection schemes, Boston: Springer, 2008. P. 403–423. doi: 10.1007/978-0-387-71041-9_20
4. *Anoklin A. et al.* A genetic study of the human low-voltage electroencephalogram // Human Genetic. 1992. Vol. 90. № 1–2. P. 99–112. doi: 10.1007/BF00210751
5. *Vogel F.* The genetic basis of the normal EEG // Human Genetic. 1970. Vol. 10. № 2. P. 91–114.
6. *Тимофеев Д. А., Маслов М. Ю.* Архитектура системы сбора и обработки данных для повышения производительности труда разработчиков программного обеспечения // Научно-технические ведомости СПбПУ. Информатика. Телекоммуникации. Управление. 2018. Т. 11. № 4. С. 71–81.
7. *Gelareh Mohammadi et al.* Person Identification by Using AR Model for EEG Signals // Proceedings of World Academy of Science, Engineering and Technology. 2006. Vol. 11. № 3. P. 281–285.
8. *Armstrong B. C. et al.* Assessing the uniqueness, collectability, and permanence of a novel method for erp biometrics // Neurocomputing. 2015. Vol. 156. P. 59–67. doi: 10.1016/j.neucom.2015.04.025
9. *Yeom S. K. et al.* Person authentication from neural activity of face-specific visual self-representation // Pattern Recognition. 2013. Vol. 46. № 4. P. 1159–1169.
10. *Marcel S., Millan J. D. R.* Person authentication using brainwaves (eeg) and maximum a posteriori model adaptation // IEEE Trans. Pattern Anal. Mach. Intell. 2007. Vol. 29. № 4. P. 743–752.
11. *Miyamoto C. et al.* Biometric person authentication using new spectral features of electroencephalogram (EEG) // Proceedings of the 2008 International Symposium on Intelligent Signal Processing and Communications Systems. Bangkok. Thailand. 8–11 February. 2009.
12. *Mu Z., Hu J., Min J.* EEG-Based Person Authentication Using a Fuzzy Entropy-Related Approach with Two Electrodes // Entropy. 2016. Vol. 18. № 12. doi: 10.3390/e18120432
13. *Abo-Zahhad M. et al.* A new multi-level approach to eeg based human authentication using eye blinking // Pattern Recognition. Lett. 2016. Vol. 32. № 2. P. 216–225. doi: 10.1016/j.patrec.2015.07.034
14. *Denney D., Denney C.,* The eye blink electro-oculogram // Br. J. Ophthalmology. 1984. Vol. 68. № 4. P. 225–228. doi: 10.1136/bjo.68.4.225
15. *Ohya T. et al.* Research of Operation Method of Accessibility Equipment for Severely Handicapped Based on Voluntary Eye Blink / Goh J. (eds.) // The 15th International Conference on Biomedical Engineering. IFMBE Proceedings. Cham: Springer. 2001. Vol. 43. P. 928–929.
16. *L. Breiman.* Random Forest // Machine Learning. 2001. Vol. 45. № 1. P. 5–32.
17. Cross-validation: evaluating estimator performance. Scikit-learn. Machine Learning in Python. URL: https://scikit-learn.org/stable/modules/cross_validation.html#cross-validation
18. *Д. Бизли.* Python. Подробный справочник. Программирование. Перевод с англ. СПб.: Символ-Плюс, 2010, 864 с.
19. Jupyter-Notebook. Real Python. https://realpython.com/jupyter-notebook-introduction/
20. *Krigolsan, O. E. et al.* (2017). Choosing MUSE validation of Low-Cost, Portable EEG System for ERP Research // Frontiers in Neuroscience. 2017. Vol. 11. P. 109. doi: 10.3389/fnins.2017.00109
21. Muse SDK. URL: https://choosemuse.com/development/ (дата обращения: 09.10.19).
22. PyMuse package. URL: http://polycortex.polymtl.ca/ (дата обращения: 09.10.19).
23. Scikit-learn. Machine Learning in Python. URL: http://scikit-learn.org/ (дата обращения: 09.10.19).

Поступила в редакцию 11.05.2019, окончательный вариант — 20.09.2019.

Станкевич Лев Александрович, кандидат технических наук, доцент, ведущий программист лаборатории «Системы управления мобильными устройствами» Института компьютерных наук и технологий СПбПУ, stankevich_lev@inbox.ru

Аманбаева Сабина Сергеевна, лаборант лаборатории «Системы управления мобильными устройствами» Института компьютерных наук и технологий СПбПУ, sabisha2704@mail.ru

Самочадин Александр Викторович, кандидат технических наук, доцент, заведующий лаборатории «Системы управления мобильными устройствами» Института компьютерных наук и технологий СПбПУ, ✉ samochadin@gmail.com

Computer tools in education, 2019
№ 3: 52–69
http://cte.eltech.ru
doi:10.32603/2071-2340-2019-3-52-69

User Authentication by Electroencephalographic Signals when Blinking

Stankevich L. A.[1], PhD, associate professor, stankevich_lev@inbox.ru
Amanbaeva S. S.[1], laboratory assistant, sabisha2704@mail.ru
Samochadin A. V.[1], PhD, associate professor, ✉ samochadin@gmail.com

[1]Peter the Great St. Petersburg Polytechnic University,
Polytechnicheskaya st., 29, 195251, Saint Petersburg, Russia

Abstract

The article presents the results of a study in the field of applying electroencephalography (EEG) for human authentication. An algorithm for EEG authentication based on blinks has been developed and described. Authentication is carried out by one blink, which takes 2-5 seconds. The data is collected using a Muse electroencephalograph. Data preprocessing includes wavelet transform and blink detection. Geometric characteristics of the EEG signals are used as features. Recognition is conducted by the Random Forest classifier. According to the test results, the percentage of correct authentication was 95 %. There is the possibility of background authentication. The implemented system may be used to authenticate students at distant education.

Keywords: *electroencephalogram, authentication, blinking, electrooculogram, machine learning, classification, Muse Headband, distance education.*

Citation: L. A. Stankevich, S. S. Amanbaeva, and A. V. Samochadin, “User Authentication by Electroencephalographic Signals when Blinking,” *Computer tools in education*, no. 3, pp. 52–69, 2019 (in Russian); doi:10.32603/2071-2340-2019-3-52-69

References

1. Higher Education Opportunity, Act 122 Stat. 3078, Public Law 110–315, Aug. 14, 2008.
2. T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino, “Impact of Artificial "Gummy"Fingers on Fingerprint Systems,” in *Proc. of SPIE, Optical Security and Counterfeit Deterrence Techniques IV*, vol. 4677, San Jose, CA, 2002, pp. 275–289; doi: 10.1117/12.462719

3. K. A. Nixon et al., “Spoof detection schemes,” in *Handbook of Biometrics*, A. K. Jain, P. Flynn, and A. A. Ross eds., Boston, MA: Springer, 2008, pp. 403–423; doi: 10.1007/978-0-387-71041-9_20
4. A. Anoklin et al., “A genetic study of the human low-voltage electroencephalogram,” *Human Genetic*, vol. 90, no. 1–2, pp. 99-112, 1992; doi: 10.1007/BF00210751
5. F. Vogel, “The genetic basis of the normal EEG,” *Human Genetic*, vol. 10, no. 2, pp. 91–114, 1970.
6. D. A. Timofeev and M. Yu. Maslov, “Architecture of data acquisition and processing system for improving productivity of software developers,” *St. Petersburg State Polytechnical University Journal. Computer Science. Telecommunications and Control Systems*, vol. 11, no. 4, pp. 71–81, 2018.
7. G. Mohammadi, P. Shoushtari, A. B. Molaee, and M. B. Shamsollahi, “Person Identification by Using AR Model for EEG Signals,” in *Proc. of World Academy of Science Engineering and Technology*, vol. 11, no. 2, pp. 281–285, 2006.
8. B. C. Armstrong et al., “Assessing the uniqueness, collectability, and permanence of a novel method for erp biometrics,” *Neurocomputing*, vol. 156, pp. 59–67, 2015; doi: 10.1016/j.neucom.2015.04.025
9. S.-K. Yeom, H.-I. Suk, and S.-W. Lee, “Person authentication from neural activity of face-specific visual self-representation,” *Pattern Recognition*, vol. 46, no. 4, pp. 1159–1169, 2013.
10. S. Marcel and J. D. R. Millan, “Person authentication using brainwaves (eeg) and maximum a posteriori model adaptation,” *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 4, pp. 743–752, 2007; doi: 10.1109/TPAMI.2007.1012
11. C. Miyamoto, S. Baba, and I. Nakanishi, “Biometric person authentication using new spectral features of electroencephalogram (EEG),” in *Proc. of the 2008 International Symposium on Intelligent Signal Processing and Communications Systems*, Bangkok, Thailand, 2009; doi: 10.1109/ISPACS.2009.4806762
12. Z. Mu, J. Hu, and J. Min, “EEG-Based Person Authentication Using a Fuzzy Entropy-Related Approach with Two Electrodes,” *Entropy*, vol. 18, no. 12, 2016; doi: 10.3390/e18120432
13. M. Abo-Zahhad, S. M. Ahmed, and S. N. Abbas, “A new multi-level approach to eeg based human authentication using eye blinking,” *Pattern Recognition. Lett.*, vol. 82, no. 2, 216–225, 2016; doi: 10.1016/j.patrec.2015.07.034
14. D. Denney and C. Denney, “The eye blink electro-oculogram,” *Br. J. Ophthalmology*, vol. 68, no. 4, pp. 225–228, 1984; doi: 10.1136/bjo.68.4.225
15. T. Ohya, Y. Nomoto, H. Koyama, and M. Kawasumi, “Research of Operation Method of Accessibility Equipment for Severely Handicapped Based on Voluntary Eye Blink,” in *The 15th International Conference on Biomedical Engineering. IFMBE Proc.*, J. Goh ed., vol. 43, pp. 928–929, Springer, 2013
16. L. Breiman, “Random Forest,” *Machine Learning*, vol. 45, no. 1, pp. 5–32, 2001.
17. Cross-validation: evaluating estimator performance, in *Scikit-learn. Machine Learning in Python*, [Online], Available: https://scikit-learn.org/stable/modules/cross_validation.html#cross-validation
18. D. Beazley, “Python. Podrobnyi spravochnik” [Python. Essential Reference], Saint Petersburg, Russia: Simvol-Plyus, 2010. (in Russian).
19. “Jupyter-Notebook,” *Real Python*, [Online], Available: https://realpython.com/jupyter-notebook-introduction/
20. O. E. Krigolsan et al., “Choosing MUSE validation of Low-Cost, Portable EEG System for ERP Research,” *Frontiers in Neuroscience*, vol. 11, p. 109, 2017; doi: 10.3389/fnins.2017.00109
21. *Muse SDK*, [Online], Available: https://choosemuse.com/development/
22. *PyMuse package*, [Online], Available: http://polycortex.polymtl.ca/
23. *Scikit-learn. Machine Learning in Python*, [Online], Available: https://scikit-learn.org/stable/

Received 11.05.2019, the final version — 20.09.2019.

Lev A. Stankevich, PhD, associate professor, Lead Programmer, Mobile Device Management laboratory, Institute of Computer Science and Technology, Peter the Great St. Petersburg Polytechnic University, stankevich_lev@inbox.ru

Sabina S. Amanbaeva, laboratory assistant, Mobile Device Management laboratory, Institute of Computer Science and Technology, Peter the Great St. Petersburg Polytechnic University, sabisha2704@mail.ru

Aleksandr V. Samochadin, PhD, Head of laboratory, Mobile Device Management laboratory, Institute of Computer Science and Technology, Peter the Great St. Petersburg Polytechnic University, ✉ samochadin@gmail.com