

УДК
378.146

**РАЗРАБОТКА МОДЕЛИ АУТЕНТИФИКАЦИИ ОБУЧАЕМОГО
НА ОСНОВЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ЕГО ПОВЕДЕНИЯ
ПРИ РАБОТЕ С ПЕРСОНАЛЬНЫМ МОБИЛЬНЫМ
УСТРОЙСТВОМ В M-LEARNING**

Мауленов Елжан Серикович
докторант, лектор
y.maulenov@iitu.edu.kz
г. Алматы

Международный университет
информационных технологий

Касымова Айжан Бахытжановна
PhD, ассоциированный профессор
a.kassymova@iitu.edu.kz
г. Алматы

Международный университет
информационных технологий

Гусейн Гурулер
PhD, ассоциированный профессор
hguruler@mu.edu.tr
г. Мугла

Университет Муглы Сытки Кочман

Аннотация. Проблемой исследования является изучение возможности аутентификации обучаемого на основе персональных данных его поведения при работе с персональным мобильным устройством. В рамках исследования был проведен анализ существующих решений для биометрической идентификации. Целью исследования является разработка и апробация модели аутентификации обучаемого на основе персональных данных его поведения при работе с персональным мобильным устройством. В качестве источников данных были использованы показания датчиков акселерометра и гироскопа. Рассматривается корреляционная связь между показаниями датчиков при воспроизведении различных жестов различными пользователями. Для проведения статистического эксперимента была разработана программа для расчета всех необходимых показателей, включая коэффициент корреляции и значение критической точки t -распределения Стьюдента. В результате была доказана потенциальная возможность использования показаний датчиков акселерометра и гироскопа для целей аутентификации пользователей мобильных устройств с уровнем значимости коэффициента корреляции $\alpha = 0,001$. Одновременно данные результаты могут быть использованы в процессе построения обучения по технологии m-learning.

Ключевые слова: m-learning, аутентификация, модель, акселерометр, гироскоп.

Введение

Стремительный прогресс информационных технологий в наш век, привел к тому, что интерес к технологиям возрос в связи с потребностями людей. В то время как технологические устройства и их использование в прошлом были подчинены определенной среде или местоположению, окружающая среда и местоположение теперь имеют свои независимые особенности для прошедшего недавнего времени.

Развитие информационных технологий и технологических устройств в наше время стремительно развивается в сфере образования. Информационные технологии, используемые

в образовании, развивались быстро и надежно таким образом, что традиционные методы обучения уступили свое значение технологическим методам. Этот прогресс выявил понятие электронного обучения. Благодаря поддержке современными мобильными технологиями электронного обучения в рамках концепции d-learning (дистанционного обучения) понятие m-learning обеспечило технологический прогресс в образовании. Хотя электронное обучение имеет гораздо больше преимуществ, чем традиционные методы обучения, некоторые его недостатки сами по себе привели научный мир к новым поискам развития мобильных технологий и необходимость движения технологии в образовании к новым измерениям выявили новое понятие m-learning. Наиболее важным преимуществом m-learning по сравнению с электронным обучением является независимость от времени и окружающей среды. Мобильное обучение – вид обучения, возникший в результате, совместной оценки областей мобильной информатики и электронного обучения, обеспечивающее доступ к электронному учебному контенту независимо от конкретного местоположения, использования, динамично создаваемых сервисов и общение с другими участниками. Мобильное обучение может быть использовано для поддержки традиционного обучения, а также дистанционного обучения [8].

К уникальным преимуществам мобильного обучения можно отнести:

- расширение возможностей и обеспечение равного доступа к образованию;
- персонализацию обучения;
- мгновенную обратную связь и оценку результатов обучения;
- обучение в любое время и в любом месте;
- эффективное использование времени на уроках в классах;
- формирование новых сообществ учащихся;
- поддержку ситуационного обучения;
- развитие непрерывного «бесшовного» обучения;
- обеспечение связи между формальным и неформальным обучением;
- минимизацию последствий разрушения образовательного процесса в зонах военных конфликтов или стихийных бедствий;
- помощь учащимся с ограниченными возможностями, то есть благодаря технологиям масштабирования текста, голосовой транскрипции, геолокации и преобразования текста в речь, мобильные устройства кардинально повышают качество обучения людей с ограниченными возможностями как в сообществах с достаточными ресурсами, так и в менее обеспеченных сообществах;
- повышение качества коммуникации и управления, потому что сообщения с мобильных устройств отправляются быстрее, надежнее, эффективнее и с меньшими затратами по сравнению с обычными каналами связи. Именно поэтому учащиеся и педагоги все чаще используют их для обмена информацией;
- максимизацию эффективности затрат, так как затраты на мобильные технологии выглядят весьма конкурентоспособными в сравнении с затратами на сопоставимые ресурсы.

Статья написана в рамках диссертационного исследования докторанта и является выжимкой одной из глав диссертации, посвященной одной из задач исследования. Этой задачей является изучение возможности аутентификации обучаемого на основе персональных данных его поведения при работе с персональным мобильным устройством.

В настоящее время пароли и личные идентификационные номера (ПИН-коды) являются наиболее часто используемыми механизмами для идентификации пользователей и контроля доступа в мобильных операционных системах. Оба подхода используют явную проверку, но не имеют последовательной проверки. Мы можем использовать распознавание лиц, подписи, сканирование радужной оболочки глаза и другие специальные методы аутентификации. Однако такие специфические методы бесполезны для мобильных пользователей, потому что они позволяют пользователям быть активными с приложением.

Таким образом, повторная аутентификация позволяет пользователям каждый раз сознательно получать доступ к конфиденциальной частной информации. Точно так же эти системы не будут постоянно повторно аутентифицировать пользователей после первоначальной аутентификации, тем самым давая злоумышленникам возможность получить контроль над пользователями смартфонов и действовать как авторизованное лицо. Пароли и ПИН-коды часто уязвимы для таких угроз, как атаки по побочным каналам, спуфинг и атаки на основе предположений. Еще один метод распознавания реального пользователя устройства – это обнаружение лица с помощью мобильной камеры, хотя это непрактично из-за ненадежности технологии в меняющейся среде.

Кроме того, для повторной обработки изображений требуется больше ресурсов, что запрещает использование этой стратегии для непрерывной аутентификации. Аналогичным образом, некоторые проблемы выявляются со стратегиями распознавания жестов на основе камеры, потому что для современных математических моделей, таких как скрытая марковская модель (НММ), сложно получить достаточный обучающий набор для пользовательских жестов. Использование мобильных инерциальных датчиков (акселерометр, гироскоп и магнитометр) для обнаружения пользователя, которое имеет то преимущество, что классификация может выполняться внутри устройства, может потребовать более эффективного метода. Как следствие, емкость и потребляемая мощность меньше [9].

Биометрия на основе смартфона предоставляет широкий спектр потенциальных подходов для решения этих проблем и может использоваться для проверки личности человека и тем самым обеспечивать дополнительную степень защиты и безопасности данных. Многие из этих методов потенциально могут использовать набор встроенных детекторов, таких как гироскопы, для отслеживания стиля ходьбы пользователя. Принимая во внимание тот факт, что у каждого человека есть уникальный подход к ходьбе, в том числе различные модели поведения клиента, датчики, встроенные в мобильные телефоны, могут быть расширены для решения проблемы пошаговой идентификации. Исследователи повсеместно признали походку человека биометрическим признаком, который можно использовать для целей идентификации путем обнаружения людей на основе физиологических или анатомических особенностей. Некоторые из преимуществ походки человека заключаются в том, что она может быть автоматически наблюдаемой, дискретной, неявной, постоянной и последовательной, и ее можно удобно вычислить, пока потребитель перемещается вокруг своей камеры. Когда пользователь идет, телефон может идентифицировать его по походке, и он может сразу получить доступ к мобильным устройствам без дополнительной проверки. Следовательно, в отличие от защиты с помощью кода или PIN-кода, это не требует от человека дополнительной работы [5, 6, 7].

Биометрия – это определенные идентифицирующие переменные. Сегодня отпечатки пальцев и ладони являются наиболее часто используемыми формами биометрии для телефонов и других технологий. На всех устройствах есть сканеры отпечатков пальцев. Хотя биометрия обеспечивает лучшую аутентификацию, она подвержена ошибкам. Есть несколько распространенных типов ошибок:

- уровень ложного отказа (FRR). Это тот случай, когда система отклоняет пользователя, даже если индикаторы известны;
- уровень ложных приемов (FAR). Эта ошибка появляется, когда неизвестный пользователь получает доступ к системе.

Биометрические устройства имеют два основных параметра, которые явно влияют друг на друга. Они отличаются гибкостью и точностью. Понятно, что точность откалибрована по чувствительности.

Ключевые типы биометрических идентификаторов зависят либо от физиологических, либо от поведенческих свойств. На рисунке 1 схематично описаны две формы биометрических идентификаторов.

Поведенческие маркеры обеспечивают определенные аспекты, в которых люди двигаются, включая идентификацию почерка, походки и других движений [4]. Многие из этих

поведенческих сигнатур могут использоваться вместо единственного разового метода безопасности для обеспечения непрерывной безопасности.

Статические детали, такие как распознавание лица, отпечатки пальцев, морфология руки, скрининг сетчатки, идентификация речи и сопоставление ДНК, распознавание радужной оболочки глаза, распознавание вен, обеспечивают анатомические маркеры.

Любой биологический атрибут человека, измеримый и обладающий свойствами универсальности и индивидуальности, будет поддерживать биометрию. Для любого человека универсальность – общее свойство, а индивидуальность – свойство, которое отличает одного человека от другого [2]. Это гарантирует, что не все символы подходят для биометрии.

Чтобы быть биометрическим индикатором, биологические характеристики должны соответствовать требованиям:

- постоянство – биометрические измерения должны быть постоянными с течением времени для каждого человека;
- измеримость – измерение не должно требовать слишком много времени и затрат;
- производительность – скорость, точность и надежность;
- приемлемость – насколько полностью люди принимают биометрию.

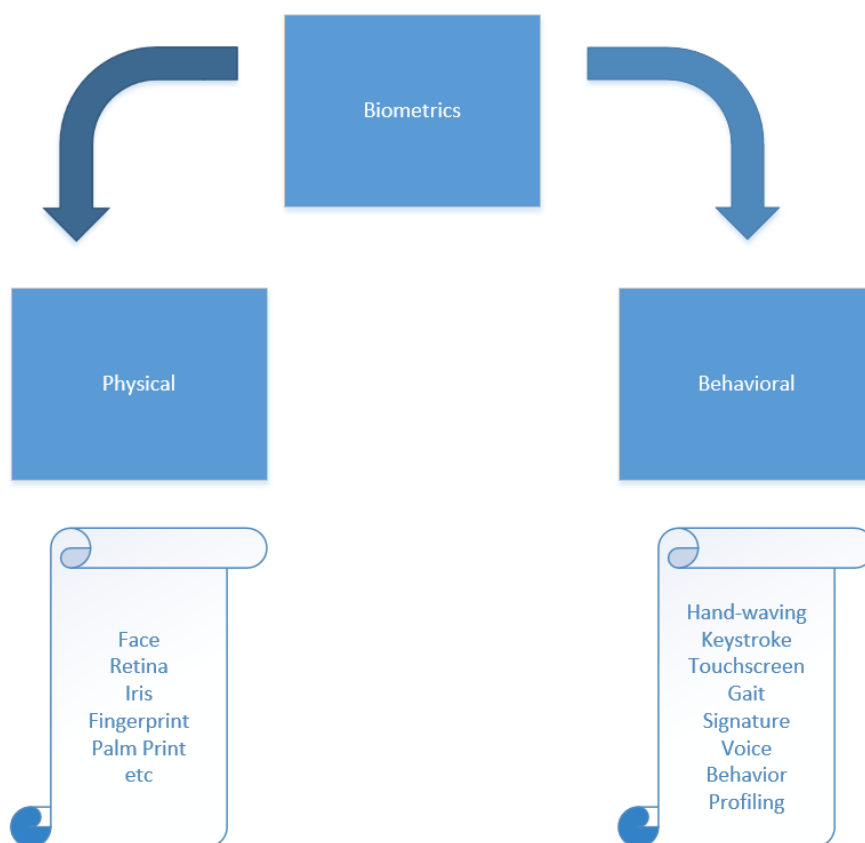


Рис. 1. Типы биометрических идентификаторов

Использование стандартизированных биометрических характеристик при автоматическом распознавании людей не дает оснований надеяться, что конкретные проблемы будут решены таким образом. Ошибки первого типа для схем распознавания отпечатков пальцев по результатам независимого исследования составляют от 10 до 20%. Производители устройств, продающие свои товары, предлагают цифры ошибок первого класса в 2% и ошибок второго класса в 0,0001%.

Таким образом, математическая биометрия не применяется ко второму десятилетию, и в области обнаружения и идентификации объектов на первый план выходит контекстная биометрия, психосемантическая, то есть поведенческая.

Разница между формой человеческого распознавания, основанной на человеческих поведенческих критериях (психосемантических, т.е. ментальных), и альтернативными

формами биометрической идентификации, основанной на обработке лиц, заключается в требовании воспроизведения точно определенного набора действий, специфичных для каждого пользователя [1]. Степень, в которой ранее упомянутая биометрия может использоваться в системе мобильного терминала, в первую очередь зависит от используемого оборудования [3]. Сомнительно, в основном из-за затрат, что многие люди смогут купить дополнительное оборудование, если не будут достигнуты другие практические преимущества, такие как веб-камера, которую можно использовать не только для распознавания лиц, но и для съемки праздничных фотографий. Например, единственный способ сделать транзакции с дополнительным оборудованием, ориентированным на безопасность, будет возможен, когда расходы, связанные с оборудованием, по сравнению с системой, которую она покрывает, будут довольно низкими. В таблице 1 описаны биометрические решения, которые можно применять в портативных приложениях по сравнению с другими инструментами. Этот список далеко не полный, поскольку некоторые продукты различаются по аппаратным требованиям.

Таблица 1.
Применимые биометрические данные для мобильных устройств

Мобильный телефон	ПК	Ноутбук
Распознавание голоса через встроенный микрофон; Динамика нажатия клавиш с помощью уменьшенной клавиатуры; Распознавание лиц с помощью дополнительной или встроенной камеры; Распознавание диафрагмы с помощью дополнительной или встроенной камеры.	Распознавание голоса через встроенный микрофон; Распознавание лиц с помощью дополнительной или встроенной камеры; Распознавание диафрагмы с помощью дополнительной или встроенной камеры; Распознавание подписи через сенсорный дисплей.	Динамика нажатия клавиш с помощью уменьшенной клавиатуры; Распознавание лиц с помощью дополнительной или встроенной камеры; Распознавание диафрагмы с помощью дополнительной или встроенной камеры; Распознавание отпечатков пальцев через встроенную камеру.

Разработка методологии аутентификации

Акселерометр – это новая технология, которая повысила удобство использования интеллектуальных устройств с сенсорным экраном, таких как мобильные телефоны и планшетные ПК. Основная функция — адаптировать изменение ориентации при изменении положения с вертикального на горизонтальное и наоборот. Эта технология фактически измеряет изменение ориентации и позиционирует экран, чтобы пользователь чувствовал себя комфортно во время просмотра.

Акселерометр смартфона содержит цепь, имеющую «Сейсмическую массу» (сделанную из кремния), и она продолжает изменять свое положение в соответствии с изменением ориентации и «корпусом», присоединенным к цепи устройства. Показания датчика акселерометра измеряется по 3-м осям в м/с².

Гироскоп – это устройство со свободной осью вращения, способное реагировать на изменение угла ориентирования тела, в котором оно закрепляется. Ключевая особенность прибора в сохранении неизменного положения, что позволяет его использовать как датчик для определения перемещения и поворота объекта, в котором он расположен. Показания гироскопа измеряются по 3-м осям в рад/с.

Среди пользователей есть мнение, что гироскоп – это тот же акселерометр, и функции, соответствующие. Но это не так: назначение последнего заключается в отслеживании поворотов агрегата в пространстве. Гироскоп же фиксирует перемещения телефона в пространстве, скорость перемещения, определяет стороны света. В целом можно сказать, что функционал у этих двух устройств схож, и гиродатчик – это как бы улучшенный акселерометр.

Последний отвечает за повороты дисплея, а гироскоп за передвижения в 3-х плоскостях. Актуально наличие гироскопа для использования различных приложений.

На мобильных устройствах расположены датчики акселерометра и гироскопа различных моделей и производительности. Частота замеров датчиками показаний может колебаться от 100 до 1000 Гц. Для нивелирования различий в аппаратном обеспечении мобильных устройств необходимо привести показания в одну шкалу. Другими словами, все показания будут группироваться и высчитываться арифметическое среднее для каждой сотой секунды. Таким образом, при 3 секундном интервале для воспроизведения жеста аутентификации мы будем всегда в итоге получать 300 записей.

Следующим вызовом стало то, что каждый пользователь один и тот же жест может начинать в разное время. Так, например, жест круг перед собой в первый раз пользователь может начать воспроизводить в 500 миллисекунде, а вторую попытку уже через 1 секунду после того, как устройство начала считывать показания датчиков. Нам нужен был алгоритм, который определяет момент начала воспроизведения жеста для объективного расчета коэффициента корреляции по данным двух жестов.

Эмпирическим путем было выявлено, что показания гироскопа могут быть использованы для этой цели. В специальном разработанной программе был заложен этот алгоритм, который проверяет последующие 5 замеров с шагом в 1 сотую секунды и, если по 3 осям X , Y и Z абсолютные значения больше 1 рад/с для всех показаний, то можем утверждать, что это начало жеста.

Также нам необходимо было определить момент завершения жеста, чтобы проводить корреляционный анализ на данных в момент исполнения жеста, исключая данные в состоянии покоя. Учитывая то, что жест подразумевается простым и быстрым в исполнении, а также одношаговым, то можем использовать вышеописанный алгоритм для определения завершения действия. Отличие лишь в том, что мы находим последовательный 5 замеров, в котором хотя бы одно из показаний не соответствует условию.

После вышеуказанных действий по приведении данных под одну шкалу и наложении алгоритма для извлечения последовательности показаний датчиков, прямо относящихся к жесту, можем перейти к корреляционному анализу.

Коэффициент корреляции – это мера линейной связи между случайными величинами. Поэтому наш алгоритм принятия решений сильно зависит от коэффициента корреляции. Поскольку у нас есть два индикатора, мы предположили, что общий вес индикатора будет одинаковым, тогда абсолютный вес индикатора в общем весе корреляции будет вычисляться по формуле (1):

$$r = \frac{r_{ax} + r_{ay} + r_{az} + r_{gx} + r_{gy} + r_{gz}}{n}, \quad (1)$$

где

n – общее количество параметров,

r – общий коэффициент корреляции,

r_{ax}, r_{ay}, r_{az} – коэффициент корреляции акселерометра по оси X , Y и Z ,

r_{gx}, r_{gy}, r_{gz} – коэффициент корреляции гироскопа по оси X , Y и Z .

Корреляция каждого параметра рассчитывалась по формуле (2):

$$r_{ax} = \frac{\sum(\bar{X} - X) * (\bar{Y} - Y)}{\sqrt{(\sum(\bar{X} - X)^2 * \sum(\bar{Y} - Y)^2)}} \quad (2)$$

Эта формула является примером расчета корреляции по оси X акселерометра между двумя жестами, где,

r_{ax} – коэффициент корреляции между независимыми величинами X и Y ,

$\bar{X}, \bar{Y}$ – математическое ожидание для независимых величин X и Y ,

X, Y – значения независимых величин X и Y .

После успешного расчета коэффициентов корреляции для каждого параметра в соответствии с формулой (2) для 3-х осей акселерометра и гироскопа, можем рассчитать итоговый коэффициент корреляции по формуле (1).

Алгоритм принятия решения основан на коэффициенте корреляции Пирсона, который имеет значение от +1 до -1, где 1 — полная положительная линейная корреляция, 0 — отсутствие линейной корреляции, а -1 — полная отрицательная линейная корреляция. Это означает, что наш коэффициент корреляции должен быть положительным и ближе к +1, чтобы показать хорошую линейную связь между переменными. Диапазон значений коэффициента корреляции для принятия решения показаны в таблице 2.

Таблица 2.
Принятие решения

Диапазон значений коэффициента корреляции	Принимаемое решение
Если $r > 0.5$	Пользователь прошел аутентификацию
Если $0 < r \leq 0.5$	Сомнительный результат, повторить жест
Если $r \leq 0$	Пользователь не прошел аутентификацию

Все исходные данные с показаниями датчиков для каждого из замеров в наличии и могут быть переданы по запросу.

Апробация разработанного модуля аутентификации и анализ полученных результатов

Для апробации разработанного модуля по аутентификации пользователя мобильного устройства по жесту был проведен эксперимент. Каждое устройство содержит в себе уникальный набор аппаратного обеспечения, что является благоприятным для модели, так как показания будут содержать некоторые отличия. Это в свою очередь, положительно скажется на уникальности показаний с разных устройств и более точной аутентификации пользователей. Поэтому для объективности оценки работы модуля для всех замеров жестов было использовано одно устройство.

В эксперименте приняло участие 2 пользователя (Е и G) и 2 различных жеста (circle и triangle), чтобы показать различия в исполнении одного и того же жеста разными пользователями, а также работу модели, когда один и тот же пользователь воспроизводит 2 различных жеста.

Для каждого уникального жеста и пользователя было проведено от 2 до 6 замеров. Например, пользователь Е воспроизводил жест с кругом (circle) 6 раз, тогда как пользователь G воспроизводила жест с треугольником (triangle) 2 раза.

Помимо расчета коэффициента корреляции по формуле 1 и 2, модель рассчитывает коэффициент Стьюдента для определения статистической значимости полученных результатов по формуле 3.

$$t_{exp} = r_{XY} * \frac{\sqrt{n-2}}{\sqrt{1-r_{XY}^2}} \quad (3)$$

Для того, чтобы сделать выводы статистических исследований, нам нужно выдвинуть и проверить статистическую гипотезу.

В нашем случае нулевой гипотезой выступает утверждение, что корреляционной связи между двумя рассматриваемыми величинами не имеется:

$$H_0: r = 0 \quad (4)$$

Альтернативной гипотезой является обратное утверждение о том, что корреляционная связь существует и обозначается:

$$H_1: r \neq 0 \quad (5)$$

Статистическим критерием будет выступать значение t -критерий Стьюдента по формуле 3, которое будем сопоставлять с табличным значением критических точек распределения Стьюдента (t -распределение) для уровня значимости $\alpha = 0.001$.

Так как минимальное количество времени необходимое для воспроизведения жеста рассчитанное эмпирическим путем равно 0.8 секунд, то всего рассматривается, как минимум, 80 записей (сотых долей одной секунды). Так как корреляционная связь в нашем случае может быть положительной или отрицательной, то мы ищем показания таблицы для двусторонней критической области для значения $n = 160 (80 * 2)$ и больше.

Для поиска необходимого значения критической точки в таблице t -распределения нам нужно вычислить значения числа степеней свободы k по формуле 6:

$$k = n - 2. \quad (6)$$

Таким образом, для наших данных значение k равняется, как минимум, 158, что соответствует критической точке $t_{cr} = 3.29$.

В таблице 3 можно увидеть итоговые результаты эксперимента с парными значениями коэффициента корреляции между всеми замерами.

По анализу полученных результатов можно сделать следующие выводы:

Значение коэффициента корреляции при воспроизведении круга (circle) одним и тем же пользователем было более 0.6 в большинстве случаев, что говорит о высокой положительной корреляционной связи и аутентифицирует пользователя в системе ($r > 0.5$). Это справедливо для обоих пользователей Е и G.

Треугольник (triangle) является более сложной фигурой в сравнении с кругом (circle), поэтому воспроизвести его сложнее, что было доказано расчетами. Коэффициенты корреляции для жестов с треугольником около 0, что говорит об отсутствии корреляционной связи между 2-мя жестами одного и того же пользователя. Это справедливо для всех пользователей, принимавших участие в эксперименте.

Коэффициенты корреляции между воспроизведениями круга различными пользователями также принимает значение около 0. Это означает, что разработанная модель отличает жесты, сделанные различными пользователями.

Также интересно отметить, что круг и треугольник один и тот же пользователь делает с некоторой схожестью, что подтверждается средним значением коэффициента корреляции равным 0.3. Это значение говорит о наличии слабой положительной корреляционной связи, но ожидаемо отклоняется моделью, так как оно меньше 0.5. Это справедливо для всех пользователей, принимавших участие в эксперименте.

Самый последний, но не по значимости это то, что значения коэффициентов корреляции для разных пользователей с разными жестами принимают значения около 0, что ожидаемо, говорит о том, что корреляционной связи между жестами не существует и, согласно модели, не будут аутентифицированы.

Для всех рассчитанных коэффициентов парных корреляции экспериментальное значение критической точки больше табличного значения ($t_{exp} > t_{cr}$, где $t_{cr} = 3.29$ для уровня значимости $\alpha = 0.001$ с $k \geq 158$), что дает основания для опровержения нулевой гипотезы H_0 и принятия альтернативной гипотезы H_1 . Это подтверждает, что рассчитанные коэффициенты корреляция статистически значимы.

Таблица 3.

Результаты эксперимента с парными коэффициентами
корреляции между всеми замерами показаний жестов

#	Dataset names	E_circle_1	E_circle_2	E_circle_3	E_circle_4	E_circle_5	E_circle_6
1	E_circle_1	1.00	0.65	0.63	0.67	0.66	0.70
2	E_circle_2	0.65	1.00	0.25	0.31	0.25	0.40
3	E_circle_3	0.63	0.25	1.00	0.89	0.78	0.68
4	E_circle_4	0.67	0.31	0.89	1.00	0.74	0.60
5	E_circle_5	0.66	0.25	0.78	0.74	1.00	0.76
6	E_circle_6	0.70	0.40	0.68	0.60	0.76	1.00
7	G_circle_1	0.25	0.40	-0.12	-0.01	-0.01	0.06
8	G_circle_2	-0.03	0.21	-0.04	-0.09	-0.04	0.00
9	G_circle_3	0.07	0.20	0.02	0.02	0.04	0.07
10	E_triangle_1	0.28	0.16	0.36	0.29	0.16	0.36
11	E_triangle_2	0.29	0.08	0.48	0.42	0.47	0.36
12	G_triangle_1	0.19	-0.01	0.47	0.40	0.32	0.24
13	G_triangle_2	0.07	0.07	0.01	0.07	0.00	-0.06

Таблица 3 (продолжение).

Результаты эксперимента с парными коэффициентами
корреляции между всеми замерами показаний жестов

#	Dataset names	G_circle_1	G_circle_2	G_circle_3	E_triangle_1	E_triangle_2	G_triangle_1	G_triangle_2
1	E_circle_1	0.25	-0.03	0.07	0.28	0.29	0.19	0.07
2	E_circle_2	0.40	0.21	0.20	0.16	0.08	-0.01	0.07
3	E_circle_3	-0.12	-0.04	0.02	0.36	0.48	0.47	0.01
4	E_circle_4	-0.01	-0.09	0.02	0.29	0.42	0.40	0.07
5	E_circle_5	-0.01	-0.04	0.04	0.16	0.47	0.32	0.00
6	E_circle_6	0.06	0.00	0.07	0.36	0.36	0.24	-0.06
7	G_circle_1	1.00	0.59	0.66	-0.08	-0.21	0.04	0.33
8	G_circle_2	0.59	1.00	0.93	-0.13	-0.01	0.18	0.25
9	G_circle_3	0.66	0.93	1.00	-0.10	0.02	0.22	0.26
10	E_triangle_1	-0.08	-0.13	-0.10	1.00	0.26	0.16	0.11
11	E_triangle_2	-0.21	-0.01	0.02	0.26	1.00	0.22	-0.05
12	G_triangle_1	0.04	0.18	0.22	0.16	0.22	1.00	-0.10
13	G_triangle_2	0.33	0.25	0.26	0.11	-0.05	-0.10	1.00

Заключение

Разработана модель аутентификации обучаемого, отличающаяся принятием решения на основе поведенческих данных, собранных со время пользования персональным мобильным устройством во время обучения. В результате эксперимента выяснилось, что самый стабильно работающий жест – это круг. Следует в дальнейших исследованиях рассмотреть больший набор возможных жестов для последующего использования в модели аутентификации.

Результаты исследования показали, что между воспроизведениями круга одним и тем же пользователем наблюдается значимая корреляционная связь. Обратное тоже верно – один и тот же жест между различными пользователями на одном и том же устройстве, согласно модели, получают коэффициент корреляционной связи менее 0.5, что говорит о слабой или отсутствующей корреляционной связи и не аутентифицирует другого пользователя.

Для всех расчетов также рассчитывался коэффициент Стьюдента, который подтверждал уровень значимости коэффициентов корреляции с $\alpha = 0.001$.

Таким образом, данная модель потенциально может использоваться для аутентификации обучаемого при организации онлайн обучения или тестирования на основе его данных поведения при работе с персональным мобильным устройством.

Список литературы

1. Clarke N., Furnell S., Lines B., Reynolds P. Subscriber Authentication for Mobile Phones using Keystroke Dynamics // Proceedings of the Third International Network Conference (INC2002). Plymouth, UK, 16-18 July 2002. Pp. 347-356.
2. Clarke N., Furnell S., Rodwell P., Reynolds P. Acceptance of Subscriber Authentication for Mobile Telephony Devices // Computers & Security. 2002. Vol. 21, No.3. Pp.220-228.
3. Cho S., Han C., Han D., Kim H. // Web Based Keystroke Dynamics Identity Verification using Neural Networks // Journal of Organisational Computing & Electronic Commerce. 2000. Vol.10. No.4. Pp.295-307.
4. Donald J. B., James C. Using Dynamic Time Warping to Find Patterns in Time Series // AAAIWS'94: Proceedings of the 3rd International Conference on Knowledge Discovery and Data Mining (pp. 359-379). New York, 1994.
5. Jang I.J., Park W.B. Signal processing of the accelerometer for gesture awareness on handheld devices // The 12th IEEE Int. Workshop on Robot and Human Interactive Communication. 2003. Pp. 139-144.
6. Jiayang L., Lin Zh., Jehan W., Venu V. uWave: Accelerometer-based personalized gesture recognition and its ap-plications // Pervasive and Mobile Computing. 2009. Vol. 5. № 6. Pp. 657-675.
7. Little B. Effective and efficient mobile learning: issues and tips for developers // Industrial and Commercial Training. 2012. Vol. 44. No. 7. Pp. 402-407.
8. Wang Y. Context awareness and adaptation in mobile learning // Proceedings - 2nd IEEE International Workshop on Wireless and Mobile Technologies in Education. JungLi: Taiwan, 2004. Pp. 154-158. DOI: 10.1109/WLTE.2004.1281370.
9. Wankel L.A., Blessinger P. Increasing Student Engagement and Retention Using Mobile Applications: Smartphones, Skype and Texting Technologies // Cutting-Edge Technologies in Higher Education. Bingley: Emerald Group Publishing Limited, 2011. Vol. 6. Part D. Pp. 47-82. DOI: 10.1108/S2044-9968(2013)000006D005

DEVELOPMENT OF A STUDENT AUTHENTICATION MODEL BASED ON PERSONAL DATA OF HIS BEHAVIOR WHEN WORKING WITH A PERSONAL MOBILE DEVICE IN M- LEARNING

Y.S. Maulenov
Doctoral student, lector
y.maulenov@iitu.edu.kz
Almaty

International University of Information
Technologies

A.B. Kassymova
PhD, associate professor
a.kassymova@iitu.edu.kz
Almaty

International University of Information
Technologies

H. Guruler
PhD, associate professor
hguruler@mu.edu.tr
Mugla

Mugla Sitki Kocman University

Abstract. The article was written as part of a doctoral student's dissertation research and is an extract of one of the chapters of the dissertation devoted to one of the research tasks. This task is to study the possibility of trainee authentication based on personal data of his behavior when working with a personal mobile device. An analysis of existing solutions for biometric identification was carried out.

The work is devoted to the development and testing of a student's authentication model based on personal data of his behavior when working with a personal mobile device. The readings of the accelerometer and gyroscope sensors were used as data sources. The correlation relationship between the readings of the sensors during the reproduction of various gestures by different users is considered. To carry out a statistical experiment, a program was developed to calculate all the necessary indicators, including the correlation coefficient and the value of the critical point of the Student's t -distribution. As a result, the potential possibility of using the readings of the accelerometer and gyroscope sensors for the purposes of authenticating users of mobile devices with the significance level of the correlation coefficient $\alpha = 0.001$ was proved and can be used as one of the modules in the process of constructing training using the m-learning technology.

Keywords: m-learning, authentication, model, accelerometer, gyroscope.

References

1. Clarke, N. L., Furnell S. M., Lines, B.M., Reynolds, P.L. (2002b). Subscriber Authentication for Mobile Phones using Keystroke Dynamics. Proceedings of the Third International Network Conference (INC2002), Plymouth, UK, 16-18 July 2002. Pp. 347-356.
2. Clarke, N. L., Furnell S. M., Lines, B.M., Reynolds, P.L. (2002a). Acceptance of Subscriber Authentication for Mobile Telephony Devices. *Computers & Security*, 21(3), 220-228.
3. Cho, S., Han, C., Han, D., Kim, H. (2000). Web Based Keystroke Dynamics Identity Verification using Neural Networks. *Journal of Organisational Computing & Electronic Commerce*, 10(4), 295-307.
4. Donald, J. B., James, C. (1994). Using Dynamic Time Warping to Find Patterns in Time Series. In: *AAAIWS'94: Proceedings of the 3rd International Conference on Knowledge Discovery and Data Mining*, New York, July 1994, pp. 359-379.

5. Jang, I.J., Park, W.B. (2003). Signal processing of the accelerometer for gesture awareness on handheld devices. In: *12th IEEE Int. Workshop on Robot and Human Interactive Communication* (pp. 139-144). IEEE Press, Roman.
6. Jiayang, L., Lin, Zh., Jehan, W., Venu, V. (2009). uWave: Accelerometer-based personalized gesture recognition and its applications. *Pervasive and Mobile Computing*, 5 (6), 657-675.
7. Little, B. (2012). Effective and efficient mobile learning: issues and tips for developers. *Industrial and Commercial Training*, 44 (7), 402-407.
8. Wang, Y. (2004). Context awareness and adaptation in mobile learning. In: *2nd IEEE International Workshop on Wireless and Mobile Technologies in Education* (pp.154-158). <https://doi.org/10.1109/WMTE.2004.1281370>.
9. Wankel, L.A., Blessinger, P. (2011). Increasing Student Engagement and Retention Using Mobile Applications: Smartphones, Skype and Texting Technologies. *Cutting-Edge Technologies in Higher Education*, 6, 47-82. [https://doi.org/10.1108/S2044-9968\(2013\)000006D005](https://doi.org/10.1108/S2044-9968(2013)000006D005)