**0. Abstract:**

В течение последних трех десятилетий проводились научные исследования в области биометрических данных о динамике нажатия клавиш на физических клавиатурах (настольных компьютерах или обычных мобильных телефонах). Однако, с точки зрения биометрии сенсорной динамики на виртуальных клавиатурах (современные сенсорные мобильные устройства), было опубликовано мало работ. В частности, отсутствует обширный обзор и оценка методологий, принятых в этой области. Из-за широкого использования сенсорных мобильных устройств нам необходимо изучить методы и их эффективность в области биометрии сенсорной динамики. Цель этой статьи - дать некоторые идеи и сравнительный анализ современного состояния дел в тематической области, включая протоколы сбора данных, представления данных о характеристиках, методы принятия решений, а также экспериментальные настройки и оценки. Благодаря такому обзору мы сможем лучше понять современное состояние искусства, определив тем самым сложные проблемы и пробелы в знаниях для дальнейших исследований

**1. Introduction**

Технологическое продвижение в вычислительной технике, коммуникационных устройствах, а также подключение к сети - это переход от использования обычных настольных компьютеров к мобильным устройствам. По прогнозам, к 2016 году будет насчитываться более 2 миллиардов пользователей смартфонов (emarketer, 2014). Возрастающая зависимость от этих устройств неизбежно подразумевает увеличение чувствительных данных, хранящихся на этой платформе. К сожалению, переносимость мобильных устройств также делает их уязвимыми для краж (Raghunathan et al., 2003). Утечка данных и неправильное использование украденного устройства потенциально более опасны, чем стоимость самого устройства (Crawford et al., 2013)

Методы аутентификации на основе знаний, такие как пароли, PIN-коды или блокировки паттерна (далее именуемые как код доступа), по-прежнему остаются основными методами, используемыми для аутентификации мобильных пользователей (Khan et al., 2014). Однако эти методы уязвимы для ряда угроз безопасности или атак, включая грубую атаку (Kim, 2012), серфинг на плечах (Zakaria et al., 2011) и нападения с использованием smudge (Giuffrida et al., 2014). Кроме того, шаблон использования мобильных устройств обычно находится в коротких очередях интервалов (Frank et al., 2013), и это значительно увеличивает частоту проверки подлинности, которая требуется по сравнению со случаями настольных компьютеров. Более высокая частота аутентификации снижает удобство использования (Harbach et al., 2014). Чтобы сбалансировать конфликт между безопасностью и удобством использования, такие меры, как отсроченная проверка подлинности, например. Устройство настроено на то, чтобы иметь некоторое время простоя до того, как потребуются запросы на повторную аутентификацию, можно использовать (Sen and Muralidharan, 2014). Тем не менее, вопрос о том, как повысить безопасность, в то же время все еще способен поддерживать минимальное вмешательство пользователя или максимальное удобство использования, остается нерешенным

Альтернативой подходу к аутентификации по паролю является проверка подлинности биометрических данных. Последний идентифицирует человека на основе его / ее физиологических или поведенческих характеристик. Физиологическая биометрия - относительно стабильная физическая особенность человеческого тела, такая как отпечатки пальцев, черты лица и узор радужной оболочки. Поведенческая биометрия, с другой стороны, это черты, которые приобретаются от человеческого поведения или привычек, таких как подпись, голос, походка и динамика нажатия клавиш. Методы аутентификации биометрии считаются более безопасными, чем другие методы аутентификации (например, код доступа), потому что биометрические данные нельзя потерять или украсть (если они используются безопасно), и их труднее подделать (Jain et al., 2008). Чтобы метод биометрической аутентификации был эффективным, этот метод должен быть не только безопасным, но и полезным. Hanul Sieger et al. (2010) провели опрос, чтобы изучить, как участники оценили воспринятую защиту безопасности и удобство использования (готовность использовать этот метод) различных типов методов проверки подлинности биометрических данных на мобильных устройствах. Опрос показал, что методы аутентификации ирисовой и голосовой биометрики были ранжированы Самый высокий с точки зрения воспринимаемой защиты, но самый низкий с точки зрения удобства использования. Это показывает, что метод аутентификации биометрических данных, рассматриваемый как обеспечивающий более высокий уровень защиты безопасности, может быть не самым приемлемым методом.

Согласно результатам исследования, представленным De Luca et al. (2015 г.), одним из важных факторов, влияющих на выбор участников, в отношении того, какой метод аутентификации по биометрии, который они предпочитают использовать на мобильном устройстве, является коэффициентом удобства использования. Они определили две основные проблемы юзабилити, которые откладывают адаптацию участников метода биометрической аутентификации, а именно: (i) медленную скорость аутентификации и неудобства, и (ii) социальную неловкость. В первом выпуске, например, в случае биометрии лица участники считали, что было сложно и отнимало много времени, чтобы правильно выровнять лицо перед камерой устройства. В случае с биометрией отпечатков пальцев участники считали, что было трудно отсканировать отпечаток пальца, когда пальцы были слишком жирными или сухими, или когда устройство было покрыто защитным кожухом. Например, по второму вопросу (например, социальная неловкость) участники считали неудобным удерживать устройство перед лицом для выполнения задачи аутентификации в публичной зоне. Это в большей степени относится к мобильным устройствам, где использование этих устройств в общественных местах очень распространено и часто

Сенсорная динамика - это поведенческая биометрия, которая фиксирует, как человек прикасается к сенсорному устройству. Подобно другим биометрическим данным, биометрия сенсорной динамики может использоваться для идентификации человека / пользователя, а также может использоваться в сочетании с методом аутентификации пароля, чтобы достичь повышенного уровня безопасности при аутентификации пользователя и в защите мобильных устройств. Этот метод может быть реализован путем использования существующих датчиков, встроенных в мобильное устройство, поэтому он сравнительно дешевле, чем другой метод аутентификации биометрических данных. Кроме того, этот метод неинтрузивен и может работать параллельно с обычными действиями пользователя по использованию мобильных устройств (Shen et al., 2016). Существующий метод аутентификации кода доступа имеет широкое общественное признание, и ожидается, что метод аутентификации касания Быть широко приемлемым для широкой общественности (Campisi et al., 2009).

Из-за потенциальной биометрии сенсорной динамики в этой тематической области предпринимаются все более активные усилия, как показано на рис. 1. В настоящем документе приводится обзор этих усилий, в которых обсуждается их важный вклад и определяются вопросы для дальнейших исследований. Основной вклад этой статьи в три аспекта. Во-первых, он представляет собой исчерпывающий обзор опубликованных работ в тематической области биометрии сенсорной динамики, в которой подчеркивается их вклад и технический прогресс в тематической области. Во-вторых, он критически анализирует эти связанные работы из ряда перспектив, приводя к выявлению пробелов в знаниях и вопросов для дальнейших исследований. Наконец, ссылки, приведенные в этом документе, являются полезными примерами для этой темы.

Подробно структура статьи выглядит следующим образом. В разделе 2 дается обзор биометрии сенсорной динамики в целом. В разделах 3-8, соответственно, сравниваются соответствующие работы с точки зрения их экспериментальных конструкций, методов сбора данных, стратегий выбора признаков, методов принятия решений, подходов к слиянию и подходов к адаптации данных. Их характеристики обсуждаются в разделе 9. Определенные пробелы в знаниях И вопросы для дальнейших исследований изложены в разделе 10. Наконец, раздел 11 завершает работу. Насколько нам известно, подобного документа, опубликованного в литературе на момент написания статьи, не было.

**2. Touch dynamics biometics**

*2.1 Overview*

Биометрика сенсорной динамики относится к процессу измерения и оценки человеческого сенсорного ритма на мобильных устройствах с сенсорным экраном (например, смартфонах и цифровых планшетах). Форма цифровых подписей создается при взаимодействии человека с этими устройствами. Эти подписи считаются дискриминационными и уникальными для каждого человека, поэтому их можно использовать в качестве личного идентификатора

В 1860-е годы, когда телеграф был основным методом для междугородной связи, операторы «идентифицировали» друг друга посредством способов, которыми они пользовались телеграфными ключами (Bryan and Harter, 1897). Сегодня телеграфные ключи были заменены компьютерными клавиатурами, Мобильных клавиатур и виртуальных клавиатур. Компьютерные клавиатуры были наиболее распространенными устройствами ввода с конца 20 века. Хорошо известно, что шаблоны типирования человеческой клавиатуры уникальны, поэтому их можно использовать в качестве личного идентификатора (Obaidat and Sadoun, 1996).

Одна из самых ранних исследований по проверке динамики нажатия клавиш была проведена Gaines et al. (1980 год). Они провели эксперимент, чтобы попытаться признать 6 профессиональных секретарей, проанализировав способ, которым они набрали три отрывка текстов, состоящих из 300-400 слов каждый. С тех пор было предпринято много смежных усилий. Кроуфорд, Карнан и др. И Teh et al. Провели независимые письменные обзоры опубликованных работ по аутентификации динамики нажатия клавиш (Crawford, 2010; Karnan et al., 2011; Teh et al., 2013). Тем не менее, эти ранние работы в основном были сосредоточены на проверке динамики нажатия клавиш на компьютерных клавиатурах. С быстрым развитием технологий мобильной связи последние исследования в этой области были сосредоточены на мобильных устройствах с физическими клавиатурами (Campisi et al., 2009; Clarke and Furnell, 2007; McLoughlin and Naidu, 2009). Совсем недавно исследовательская деятельность в основном проводилась в контексте мобильных устройств с сенсорным экраном. Инжир. 2 кратко излагаются временные рамки исследования биометрии сенсорной динамики под влиянием технологических изменений в секторе

Биометрия сенсорной динамики обладает уникальными достоинствами или полезными функциями, в то же время они также создают сложные проблемы. В нижеследующих разделах представлены функции и сложные проблемы

*2.2 Features*

Система аутентификации сенсорной динамики может предложить ряд полезных функций по сравнению с другими типами системы аутентификации биометрических данных. Это следующие.

* Отличительная особенность: модели с сенсорной динамикой способны создавать многомерные объекты, такие как временные, пространственные и движущиеся объекты. Эти многомерные характеристики могут измеряться с точностью до уровня, значительно превышающего человеческое восприятие (Zheng et al., 2014). Эти уникальные функции трудно реплицировать последовательно и, следовательно, могут использоваться для аутентификации.
* Повышенная безопасность. Несмотря на свои недостатки, коды доступа были наиболее распространенным и развернутым методом аутентификации (Schlöglhofer and Sametinger, 2012). Интегрируя биометрию сенсорной динамики в метод аутентификации пароля, можно повысить общий уровень достоверности
* Непрерывный мониторинг: биометрия сенсорной динамики может использоваться для проверки подлинности пользователя за пределами первоначальной проверки подлинности, постоянно отслеживая шаблоны сенсорной динамики пользователя. Другими словами, повторная аутентификация пользователя может выполняться легко и ненавязчиво в течение активного сеанса входа в систему. Таким образом, защита безопасности выходит за рамки первоначальной регистрации без ущерба для удобства использования. Это одно из самых заметных преимуществ биометрии сенсорной динамики по сравнению с другими физиологическими биометрическими данными.
* Отказоустойчивость: в случае нарушения кода доступа, связанного с шаблоном динамики касания, новый шаблон динамики касания может быть легко создан при создании нового кода доступа. Это не относится к другим физиологическим биометрическим данным. Например, с биометрией радужной оболочки или лица, после того как они будут скомпрометированы, не будет никакой замены, а для биометрических данных отпечатков пальцев количество замен ограничено (в конце концов, у людей всего 10 пальцев).
* Независимость: мобильное устройство обычно работает в режиме «на ходу», поэтому окружающее освещение и уровень фонового шума в большинстве случаев постоянно меняются. По сравнению с другими биометрическими характеристиками, такими как биометрия лица и голоса, функция обнаружения биометрии сенсорной динамики менее чувствительна к этим факторам окружающей среды. Таким образом, он больше подходит для и может быть легче развернут на мобильном устройстве
* Прозрачность. Система аутентификации Touch Dynamics требует практически никаких дополнительных вмешательств от пользователя мобильного устройства. Это происходит потому, что получение и обработка шаблонов динамики касания могут выполняться в фоновом режиме, пока пользователь использует устройство. Пользователи могут не знать, что их диаграммы динамики касания захватываются, захваченные данные используются для аутентификации, а аутентификация выполняется периодически или они защищены дополнительным уровнем аутентификации. Это резко контрастирует с другими системами аутентификации биометрических систем, которые обычно требуют явного согласования биометрической функции с конкретным датчиком. Например, в случае проверки подлинности радужной оболочки, пользователь должен смотреть прямо в камеру, чтобы сделать изображение радужной оболочки, а в случае аутентификации по отпечаткам пальцев пользователю нужно поместить один из его пальцев в датчик отпечатков пальцев.
* Знакомство: данные о динамике касания, используемые для аутентификации, приобретаются во время рутинной активности мобильных пользователей. Это процесс, с которым уже знакомы мобильные пользователи, поэтому операция сбора данных имеет тенденцию к более мягкой кривой обучения с более высоким уровнем практичности, чем другие случаи сбора данных биометрических данных
* Эффективность затрат: в отличие от других физиологических методов биометрической аутентификации, таких как диафрагма и биометрическая идентификация отпечатка пальца, которые обычно требуют использования специализированного оборудования, система аутентификации сенсорной динамики использует только встроенные мобильные датчики. Это позволяет снизить затраты на устройство и идеально подходит для крупномасштабных развертываний

*2.3 Challenging issues*

Конструкция системы аутентификации сенсорной динамики накладывает ряд сложных проблем следующим образом:

* Минимизация вычислительных и коммуникационных затрат: вычислительные возможности мобильных устройств обычно ниже, чем у настольных компьютеров. Это означает, что определенные критерии, такие как сложность алгоритма, стоимость связи и задержка аутентификации, важны и должны учитываться при разработке решений аутентификации касания динамики. Другими словами, затраты на алгоритм и связь, возникшие в результате развертывания этого средства аутентификации, должны быть минимальными
* Минимизация потребления энергии. Мобильные устройства, в отличие от настольных компьютеров, работают от батарей. Чем меньше потребляет энергии приложение, тем дольше устройство может работать. Хотя связь является основным потребителем энергии аккумулятора мобильного устройства (Perrucci et al., 2009), количество и частота использования различных датчиков, встроенных в мобильное устройство, которые используются для извлечения данных о динамике касания, также имеют прямой Влияние на потребление аккумулятора мобильного устройства. Для снижения энергопотребления мобильного устройства были предложены различные меры, такие как снижение частоты дискретизации (Niu and Chen, 2012) или выполнение сложных вычислений только при перезарядке устройства (Crawford et al., 2013).
* Максимизация точности: точность системы проверки подлинности сенсорной динамики относительно низка по сравнению с другими физиологическими системами аутентификации биометрических данных (например, отпечатков пальцев и диафрагмы). Это связано с тем, что характеристики биометрии сенсорной динамики (или данные о характеристиках), приобретенные в разное время, могут проявлять определенную степень вариации из-за внешних факторов, таких как усталость, настроение или отвлечение внимания. Поэтому следует рассмотреть вопрос о том, как повысить точность работы системы проверки подлинности сенсорной динамики при разработке метода
* Способность адаптации. Поведенческие характеристики человека обычно меняются со временем, и они обычно меняются чаще, чем физиологические. Паттерны сенсорной динамики пользователя могут постепенно меняться по мере того, как пользователь более подробно знаком с кодом доступа, методом ввода, устройством и другими внешними факторами. Система аутентификации сенсорной динамики должна быть способна адаптироваться к любым изменениям в шаблоне сенсорной динамики пользователя

*2.4 Operational process*

Типичная система аутентификации сенсорной динамики показана на рис. 3. Из рисунка видно, что работа этой системы может быть в значительной степени отражена в трех основных этапах: (i) регистрация пользователей, когда данные (или образцы) динамики касания приобретаются, обрабатываются и сохраняются в качестве эталонного шаблона; (Ii) Аутентификация пользователя, в которой сравнительный образец динамики касания сравнивается с сохраненным эталонным шаблоном (ами) для определения сходства или несходства; И (iii) переобучение данных, при котором эталонный шаблон обновляется, чтобы отражать любые изменения в последних данных о динамике касания. Три эксплуатационных этапа выполняются рядом функциональных блоков (то есть архитектурных компонентов), каждый из которых выполняет четко определенную функцию, и эти компоненты и их соответствующие функции описаны ниже

*2.4.1. Data acquisition*

Сбор данных - это операция, с помощью которой собираются данные динамической обработки касания. Обычно это выполняется как первый шаг и на этапе установки системы аутентификации касания касания. Приобретенные необработанные данные обычно представляют собой набор повторяющихся (множественных) входных выборок, полученных за определенный период времени. Устройства, обычно используемые для сбора данных, являются коммерческими готовыми смартфонами (Buschek et al., 2015; Trojahn et al., 2013; Zheng et al., 2014), или, в некоторых случаях, цифровыми таблетками (Saravanan et al. 2014)

*2.4.2 Data preprocessing*

Предварительная обработка данных выполняется для удаления выбросов в исходных данных, улучшения качества данных и повышения точности. Используемые в этой операции методы включают обнаружение и удаление выбросов (Zheng et al., 2014). Для уменьшения вычислительной эффективности на ограниченных ресурсом мобильных устройствах (de Mendizabal-Vazquez et al., 2014) может быть также использован метод уменьшения размера, чтобы гарантировать, что необработанные данные остаются небольшими, но представляемыми,

*2.4.3 Feature Extraction*

Извлечение признаков является обязательной операцией, выполняемой на этапах регистрации и аутентификации пользователей. Основная задача этой операции - идентифицировать и извлечь отличительные черты, общие для пользователя, от полученных необработанных данных. Эти функции будут позже использоваться для создания шаблонов. Возможные функции, извлеченные из данных о динамике сенсорной информации человека, можно разделить на три широкие категории: временные, пространственные и динамические (дальнейшее обсуждение в разделе 5).

*2.4.4 Template generation*

Генерация шаблона - это операция, выполняемая для преобразования извлеченного объекта в компактную форму, которая однозначно представляет характеристику сенсорной динамики пользователя. Обычно несколько различных типов объектов объединяются в последовательность n-мерных векторов признаков, где n - количество элементов-признаков (Cai et al., 2013; Serwadda et al., 2013). Эти уникальные эталонные шаблоны затем сохраняются для Аутентификация пользователя или цель переобучения данных.

*2.4.5 Data classification*

Классификация данных является основной операцией для большинства методов проверки подлинности биометрических данных, где данные о характеристиках классифицируются и сравниваются с эталонными шаблонами. Результат этого этапа обычно ассоциируется с совпадающим счетом, используемым для принятия решения. Классификация данных обычно осуществляется с использованием методов машинного обучения (также называемых алгоритмами классификации данных или классификаторами), и для этой цели в литературе по биометрии сенсорной динамики использовался ряд методов машинного обучения (дальнейшее обсуждение в разделе 6)

*2.4.6 Decision making*

Принятие решения - это операция, выполняемая для определения того, были ли данные о динамике касания, представленные пользователем, действительно получены от целевого пользователя. Это решение принято путем сравнения оценки сходства или несходства, полученной с помощью техники машинного обучения, с заранее заданным порогом (Bo et Al., 2014, Kolly et al., 2012). Прежде чем принять окончательное решение, можно применить подход слияния, чтобы комбинировать либо информацию из нескольких функций (Buschek et al., 2015; Jeanjaitrong and Bhattarakosol, 2013), либо объединить совпадающие оценки из разных методов машинного обучения (Samura et al. ., 2014), для повышения точности.

*2.4.7 Data adaptation*

Адаптация данных - это операция, выполняемая для перекомпоновки или обновления эталонного шаблона с последними шаблонами динамики касания от пользователя. Эта операция требуется, потому что шаблоны динамики касания пользователя могут постепенно меняться со временем, в результате исходный зарегистрированный шаблон ссылки отклоняется от Самые последние шаблоны динамики касания от одного и того же пользователя. Путем добавления адаптивного компонента, который выполняет операцию адаптации данных после каждой успешной аутентификации, эти постепенные изменения могут быть зафиксированы и приняты во внимание (Crawford et al., 2013)

*2.5 Evaluation creteria*

Система аутентификации сенсорной динамики может быть развернута в одном из двух режимов: режиме верификации (или аутентификации) и режиме идентификации (или распознавания). Эти режимы служат для различных целей и сценариев использования. Режим проверки используется для проверки заявленного идентификатора . Он используется для ответа на вопрос «является ли это лицо кем он / она претендует быть». Аутентификация мобильного пользователя или мобильного устройства вписывается в этот режим. С другой стороны, режим идентификации используется для классификации и идентификации некоторой неизвестной идентичности. Он используется для ответа на такие вопросы, как «кто этот человек» или «этот человек в базе данных». Этот режим обычно используется для судебных расследований или обнаружения вторжений. Как показано на фиг. 4, фундаментальное различие между двумя режимами состоит в том, что в режиме проверки проверка между данными динамической чувствительности, представленными пользователем, и эталонным шаблоном является 1-к-1, тогда как в режиме идентификации эта проверка равна 1 -томания. По данным нашего обзора литературы, количество опубликованных работ по исследованию режима верификации (74%) намного выше, чем режим идентификации (26%),

Основное внимание в этом документе уделяется аутентификации с использованием сенсорной динамической биометрии, поэтому в дальнейшем наш анализ находится в режиме проверки. Чтобы оценить пригодность метода биометрической аутентификации для реальных приложений, для оценки системы необходимо использовать три основных критерия. Это точность проверки, эффективность системы и удобство использования системы.

*2.5.1 Verification accuracy*

Метрики, которые обычно используются для оценки точности проверки метода биометрической аутентификации, представляют собой коэффициент ложного отказа (FRR), коэффициент ложного приема (FAR) и равную частоту ошибок (EER). Связь между этими метриками показана на рис. 5, и их определения приведены ниже

*2.5.1.1 False rejection rate FRR*

Это процентное отношение числа легитимных пользователей, которые ложно отвергаются от общего числа законных пользователей. Более низкое значение FRR означает, что меньше легитимных пользователей ложно отклонено. Это также означает, что уровень юзабилити системы выше. FRR также упоминается как частота ложных тревог, ложная отрицательная скорость, ложная частота несоответствий или ошибка типа II

*2.5.1.2 False acceptance rate FAR*

Это процентное отношение числа незаконных пользователей, которые ложно приняты против общего числа незаконных пользователей. Опять же, меньшее значение FAR указывает на ложно принятое количество нелегальных пользователей, а это также указывает на то, что система имеет более высокий уровень безопасности. FAR также упоминается как частота сбоя при промахе, ложноположительная скорость, частота ложных совпадений или ошибка типа I

*2.5.1.3 Equal error rate ERR*

EER - это показатель с одним числом показателей, который обычно используется для измерения и сравнения общего уровня точности различных методов проверки подлинности биометрических данных. Его иногда также называют коэффициентом ошибок при переходе (CER). EER может быть получен путем нахождения точки перехвата двух графиков, один для FRR, а другой для FAR. Как правило, чем ниже значения FRR и FAR, тем ниже значение EER, которое, в свою очередь, указывает на более высокую точность метода биометрической аутентификации. Однако FRR и FAR отрицательно коррелируют, поэтому невозможно одновременно снизить значения FRR и FAR. Поэтому в реальных приложениях FRR и FAR обычно корректируются и определяются на основе требований безопасности и удобства использования приложений. В некоторых публикациях термин «точность», а не EER, используется в качестве показателя точности точности. Стоит отметить, что «точность» и EER на самом деле одни и те же; «Точность» определяется как обратная величина EER. Другими словами, более высокое значение «точности» указывает на более высокую производительность точности метода биометрической аутентификации.

Характеристики точности также можно графически визуализировать, используя кривую рабочих характеристик приемника (ROC), как показано на рис. 6. Этот график получен путем построения подлинной скорости приема (GAR) против FAR при различных пороговых значениях согласования. GAR - это процентное соотношение между правильно принятыми законными пользователями и общим числом законных пользователей. Он также называется инверсией FRR (100- FRR), истинной положительной скоростью или истинной частотой совпадений. Большая область под кривой (ближе к кривой в верхнем левом углу графика) указывает на лучшую производительность

*2.5.2 System efficiency*

Эффективность системы относится к вычислительной стоимости или задержкам аутентификации, налагаемым методом биометрической аутентификации. Удовлетворение этого критерия особенно важно для вычислительных ограниченных ресурсов мобильных устройств. Сложный метод аутентификации может наложить более высокий уровень вычислительных издержек, увеличивая задержки аутентификации и уменьшая удобство использования системы. Поэтому важно разработать методы аутентификации, которые будут представлять как можно более низкие вычислительные накладные расходы

*2.5.3 System usability*

Юзабилити системы (или принятие пользователем) системы аутентификации также является важным фактором успешного развертывания нового метода аутентификации. Пользователи в конечном итоге откажутся или захотят использовать любую систему, которая утомительна или медленна в использовании, даже если она может предложить более высокий уровень защиты. Поэтому система аутентификации должна обеспечивать хороший уровень удобства использования системы, и это может быть достигнуто ( I) максимально снизить нагрузку на пользователя, (ii) как можно меньшее вмешательство пользователей и (iii) как можно более короткие задержки аутентификации

**3. Experimential design**

*3.1 Working mode*

Режим проверки может работать как в статическом, так и в динамическом режиме. Статический и динамический режимы работы дополняют друг друга, то есть они могут быть развернуты независимо или вместе друг с другом для повышения уровня защиты, предоставляемого развернутому мобильному устройству. Далее мы обсудим два режима работы. В дальнейшем мы используем термин Verification-in-Static-Mode (ViSM), чтобы ссылаться на режим проверки, используемый в статическом рабочем режиме и в режиме Verification-in-Dynamic-Mode (ViDM), чтобы ссылаться на режим проверки Которые используются в динамическом рабочем режиме.

*3.1.1 Verification-in-static-mode (ViSM)*

Одним из сценариев применения ViSM является статическая аутентификация, которая также известна как однократная аутентификация. При статической аутентификации пользователь пытается аутентифицировать себя в системе в начале сеанса входа в систему или в некоторые предопределенные интервалы во время сеанса. Например, метод аутентификации сенсорной динамики может быть интегрирован с существующим методом аутентификации кода доступа, образуя так называемую двухфакторную систему аутентификации, в которой метод аутентификации пароля служит первым фактором, а способ аутентификации сенсорной динамики служит дополнительным, т.е. Второй, коэффициент аутентификации. Эта двухфакторная система аутентификации обеспечивает более высокий уровень защиты, чем любой из двух методов аутентификации, когда они используются в одиночку. Кроме того, использование второго фактора аутентификации может также предотвратить совместное использование кода доступа.

*3.1.2 Verification-in-dynamic-mode (ViDM)*

Примером прикладного сценария ViDM является динамическая аутентификация, также известная как непрерывная аутентификация. Метод динамической аутентификации выполняет проверку подлинности пользователя в сеансе приложения или сеанса связи (то есть после выполнения начальной аутентификации). Функция динамики может быть отражена при использовании информации, которая генерируется в режиме реального времени во время сеанса, для аутентификации пользователя и / или использования нескольких экземпляров аутентификации в сеансе, но интервалы между несколькими экземплярами аутентификации не являются Предопределено, например Они могут определяться появлением некоторых событий касания. Система аутентификации касания особенно подходит для этого режима, поскольку данные о динамике касания могут быть получены прозрачно в течение определенного периода времени, чтобы повторно идентифицировать личность пользователя без вмешательства пользователя, и это может быть сделано в любой момент сеанса. Непрерывная проверка подлинности может снизить риски безопасности несколькими способами, такими как несанкционированное совместное использование устройств, потеря устройства / кража, захват сеанса и т. Д. Конечно, как и в случае любого метода биометрической аутентификации, важно добиться низкого значения FRR для Сделать систему более удобной, поскольку, в противном случае, законный пользователь может быть заблокирован из службы в середине сеанса. Согласно нашему обзору литературы, было опубликовано больше статей для статическо

й аутентификации (77%), чем динамическая аутентификация (23%)

*3.2 Acquisition devices*

Важным фактором является выбор устройства для сбора данных. Различные устройства могут быть оборудованы различными датчиками, которые могут обладать способностью приобретать различные типы функций. Например, обычное мобильное устройство с физической клавиатурой может только приобретать функцию синхронизации. Напротив, недавно выпущенное сенсорное мобильное устройство с большей вероятностью будет иметь несколько более мощных встроенных датчиков, которые могут приобретать больше функций (таких как давление, перемещение и ориентация). В центре внимания этой статьи - проверка подлинности сенсорной динамики, в дальнейшем мы сосредоточим наши обсуждения на мобильных устройствах с сенсорными экранами. Для существующих работ по динамике нажатий клавиш на мобильных устройствах с физическими клавиатурами читатели отсылаются к обзорным статьям, таким как (Crawford, 2010; Teh et al., 2013)

Большинство исследовательских работ, проводимых в области сенсорной динамики, используют смартфоны в качестве устройств сбора данных. Исключение составляют работы Антала и Сабо (2014 год), Бонд и Ахмед Авад (2015 год) и Сараванана и др. (2014 г.), и в этих случаях использовались цифровые таблетки. Это во многом связано с тем, что большая группа пользователей мобильных устройств фактически использует смартфоны, а не цифровые планшеты (Taylor, 2015). Исследователи использовали более современные и более мощные мобильные устройства для выполнения своих исследовательских работ. Современные устройства обычно поставляются с более высокими датчиками точности и разрешения, которые способны захватывать более качественные функции. Современные устройства также обладают большими вычислительными возможностями и ресурсами, которые могут лучше поддерживать использование более сложных алгоритмов и более эффективных датчиков. Другой критерий выбора устройства - это предполагаемая платформа разработки, связанная с мобильной операционной системой, и эта проблема обсуждается в следующем разделе

*3.3 Development platform*

Чтобы получить данные о динамике касания, нам необходимо использовать набор инструментов, и для разработки набора инструментальных средств нам необходимо выбрать платформу разработки. Основываясь на нашем исследовании литературы, Android является самой популярной платформой разработки для сбора данных о динамике касания, за которой следует iOS, а затем Windows. При выборе платформы разработки следует учитывать эти четыре фактора, а именно его настраиваемость, гибкость, стоимость и долю на рынке

*3.3.1 Customizability*

Для получения данных о динамике касания важно регистрировать различные события входа сенсорного экрана. Однако собственные методы ввода (такие как виртуальная клавиатура или виртуальная цифровая клавиатура), используемые мобильной операционной системой, не обеспечивают никаких вызовов функций для получения этих данных. Это, как правило, является частью мер безопасности, используемых для защиты от простой реализации программ-шпионов или приложений сенсорного журнала (Kambourakis et al., 2014). Поэтому для получения данных о динамике касания нам необходимо создать собственные методы ввода с необходимыми функциональными возможностями. В отличие от своих конкурентов (iOS и Windows), Android сделал это проще, предоставив функции библиотеки с открытым исходным кодом, которые позволяют разработчикам изменять структуру приложения (Meng et al., 2013), предоставляя им большую гибкость в разработке и настройке приложений.

*3.3.2 Flexibility*

Гибкость в плане кросс-платформенного развития, бокового скачивания и видимости файловой системы является одним из критериев, которые способствуют популярности выбранной мобильной платформы разработки. Android поддерживает кросс-платформенную разработку, а это означает, что разработчики могут гибко разрабатывать мобильные приложения с использованием любых операционных систем и использовать существующие ресурсы в своих разработках. Кроме того, как Android, так и Windows позволяют загружать, что означает, что приложение можно непосредственно установить на мобильное устройство, не предварительно опубликовав его в магазине мобильных приложений. Публикация приложений требует жестких процедур и может занять много времени. Таким образом, загрузка бокового канала может сократить время и усилия на тестировании и разработке приложений. Кроме того, прямые исследователи файлов были предоставлены как поставщиками Android, так и Windows. Это означает, что к данным и системным файлам можно обращаться напрямую без дополнительных настроек или установок каких-либо сторонних приложений. Это предоставляет удобный способ для исследователей передавать полученные файлы данных между различными устройствами для дальнейшего анализа.

*3.3.3 Cost*

Стоимость, необходимая для приобретения инструмента разработки и устройства, также должна учитываться при выборе. Официальные интегрированные среды разработки (IDE), необходимые для разработки приложений для устройств Android и Windows, - Android Studio и Visual Studio Express, соответственно. Они доступны для скачивания бесплатно. С другой стороны, Xcode IDE (устройства iOS) доступна только после того, как была оплачена годовая абонентская плата за публикацию приложений, а стоимость платы показана в Таблице 1. Кроме того, Android использовался широким Диапазон мобильных устройств. Среди крупнейших производителей мобильных устройств на базе Android - Samsung, HTC и LG. Этот широкий диапазон устройств может предоставить нам более дешевый вариант для проведения наших экспериментов

*3.4 Degree of control*

Степень контроля относится к ограничениям или ограничениям, налагаемым при проведении эксперимента. Он охватывает три различных аспекта, а именно: (i) выбор устройства сбора данных, (ii) управление настройкой эксперимента и (iii) выбор строки ввода. Как правило, количество экспериментов, которые налагают ограничения, превышает количество тех, которые этого не делают, и это имеет место для всех трех аспектов, как показано на рис. 8.

*3.4.1 Acquisition device selection*

Устройства, используемые в экспериментах, могут быть выбраны с использованием одного из двух подходов. Один из них заключается в использовании предопределенного устройства, а другой - в использовании конкретного объекта (в дальнейшем именуемого мобильным устройством, набранным для эксперимента). На основании нашего обзора литературы большинство экспериментов, опубликованных в литературе (94%), за исключением работы, опубликованной в Alotaibi et al. (2014 год), Йохансен (2012 год) и Самура и др. (2014 г.), были предприняты с использованием первого подхода. Основная причина использования предопределенного устройства состоит в том, чтобы предотвратить любые несоответствия в приобретенных функциях. Например, наличие аппаратных датчиков (Alotaibi et al., 2014) и вариации в разрешении или чувствительности сенсора (Seo et al., 2012) между различными устройствами может привести к несогласованности в полученных данных. Кроме того, поскольку субъекты, как правило, более знакомы со своими собственными устройствами, позволяя субъектам использовать свои собственные устройства для получения данных, могут вводить предвзятость в их экспериментальные результаты. Этого можно избежать, требуя от субъектов использования заранее определенного устройства для всей операции сбора данных (Serwadda et al., 2013).

В отличие от этого, некоторые эксперименты, описанные в литературе, проводились без каких-либо ограничений типов устройств, которые должны использоваться, поэтому субъекты могут использовать свои собственные устройства для получения данных. Таким образом, для участия в экспериментах может быть привлечено больше субъектов из разных групп населения. Например, Johansen (2012) позволил субъектам осуществлять сбор данных с помощью своих мобильных устройств через мобильное приложение, поэтому субъектам не нужно физически присутствовать или контролироваться на протяжении всей операции сбора данных. Другими словами, поскольку этот подход устраняет физические и географические барьеры в проведении экспериментов, сбор данных может проводиться в большем масштабе и может охватить более широкую аудиторию. Это также утверждалось Самурой и др. (2014), что, используя устройство, к которому привыкли испытуемые, полученные экспериментальные результаты могут лучше отражать их фактическое поведение при использовании. Это согласуется с нашим наблюдением, что эксперименты, которые не налагали никаких ограничений на устройства ввода, также эксплуатировались в неконтролируемой среде, так что сенсорная динамика субъекта может быть приобретена в естественном состоянии (дальнейшее обсуждение в следующем разделе).

*3.4.2 Experimental setting control*

Экспериментальное управление установкой относится к степени ограничений, налагаемых на эксперимент во время операции сбора данных. Сбор данных может проводиться в двух режимах: (i) наблюдение строгим протоколом или (ii) неконтролируемый без каких-либо ограничений. В статьях Alotaibi et al. (2014 год), Йохансен (2012 год), Колли и др. (2012) и Samura et al. (2014) сообщили об экспериментах, которые были проведены без каких-либо конкретных ограничений. Большинство экспериментов (89%), приведенных в литературе, фактически проводились в контролируемых и контролируемых средах. Основная причина для управления экспериментом заключается в том, чтобы уменьшить уровень вариаций в моделях сенсорной динамики, которые могут быть вызваны внешними факторами, такими как отвлекающие факторы, когнитивная нагрузка и болезнь и т. Д. Управление экспериментом с использованием строгого протокола может помешать этим внешним факторам (Trojahn et al., 2013), позволяя более точно оценивать первичные экспериментальные переменные (т.е. отличительные способности признаков или точность результатов классификаторов) (Cai et al., 2013). Кроме того, неконтролируемая и неконтролируемая экспериментальная установка может привести к тому, что полученные данные будут искажены или искажены, что приведет к снижению качества данных

*3.4.3 Input string selection*

Как выбрать входные строки или какие входные строки следует использовать во время экспериментов - еще один фактор, который следует учитывать при проведении экспериментов, связанных с динамикой касания. В большинстве экспериментов, описанных в литературе (72%), испытуемых просили предоставить предопределенный набор входных строк во время операции сбора данных. Другими словами, входные строки, используемые в этих экспериментах, одинаковы для всех субъектов. Это означает, что образцы, полученные от разных субъектов в одном наборе данных, могут быть повторно использованы для целей оценки (а не только для генерации шаблонов), и, как результат, можно получить большее количество пробных образцов, не приобретая их отдельно. Однако в некоторых ситуациях такой подход может оказаться непрактичным. Например, эксперименты по сбору данных, проведенные Draffin et al. (2014), Y. Meng et al. (2014) и Meng et al. (2013 г.) были нацелены на получение всех данных о динамике касания за весь сеанс взаимодействия с устройством. Из-за характера и цели этих экспериментов предопределение набора входных строк было бы непрактичным

**4. Data acquisition**

*4.1 Subject size*

Известно, что размер предмета, используемый в эксперименте, влияет на полученные результаты эксперимента (Maxion and Killourhy, 2010; Xu et al., 2014). Чем больше размер объекта, использованный в эксперименте, тем лучше результаты эксперимента Могут свидетельствовать о масштабируемости исследования (Bartlow and Cukic, 2006) и отражать истинную точность работы метода биометрической аутентификации при развертывании в реальном мире (Jagadeesan and Hsiao, 2009).

В большинстве экспериментов было задействовано менее 50 субъектов (Buschek et al., 2015; Kambourakis et al., 2014; Y. Meng и др., 2014), с некоторыми менее 5 субъектами (Nixon et al., 2014; Rao et al. , 2014). Мы смогли найти только три эксперимента (Gascon et al., 2014, Serwadda et al., 2013; Trojahn et al., 2013), которые использовали большое количество испытуемых (соответственно 315, 190 и 152 испытуемых). Размеры предметов, использованные в экспериментах, опубликованных в литературе, суммированы на рис. 9

В большинстве экспериментов (94%) субъекты набирались на добровольной основе, то есть без получения каких-либо денежных пособий. Только в нескольких экспериментах испытуемым были выданы денежные карточки (Buschek et al., 2015; Xu и др., 2014) или некоторые формы призов (Johansen, 2012). Награды или призы были использованы для мотивации субъектов к участию в экспериментах, увеличивая темпы участия. Операция сбора данных может быть ресурсоемким процессом, который требует некоторой самоотверженности и усилий со стороны субъектов. Чтобы увеличить долю участия или количество субъектов, участвующих в эксперименте, Kolly et al. (2012) предложил, чтобы инструменты сбора данных можно было распространять через магазин мобильных приложений. Это может быть возможным способом привлечения большего числа субъектов, но, таким образом, контроль за операцией сбора данных, безусловно, станет ограниченным, и риск подделывания или манипулирования данными станет выше.

*4.2 Subject demography*

Субъекты могут быть выбраны на основе трех переменных, а именно, их возраста, принадлежности и профессии. Эти три переменные совместно коррелируют с частотой использования устройства субъектом и знакомством. Поэтому, если субъекты не выбраны должным образом, могут быть непреднамеренные смещения в экспериментальных результатах.

В опубликованных экспериментах субъекты часто выбирались из конкретной группы населения, например, (I) с узким распределением по возрасту (т. Е. 19-26) (Antal and Szabó, 2014, Buschek et al., 2015; Kambourakis et al., 2014), (ii) в пределах одной организации (то есть в рамках исследования (Alotaibi et al., 2014, Giuffrida et al., 2014, Samura et al., 2014) или (iii) с конкретной профессией (т.е. учениками) (Draffin et al., 2014; Y. Meng et al. ., 2014; Meng et al., 2013). Это связано с тем, что определенная группа населения более доступна и дешевле для исследователей, которые часто имеют ограниченные ресурсы для проведения своих экспериментов. Тем не менее, можно утверждать, что данные, полученные из специальной группы населения, могут реально не представлять более широкое сообщество

Исследования, проведенные Coakley et al. (2015 год), Эль-Абед и др. (2014) и Kolly et al. (2012 г.) являются одними из немногих произведений, которые мы смогли найти в литературе, которые набирали предметы у населения с широкой демографией, например. Люди из разных возрастных групп и / или с разными профессиями. Их цель состоит в том, чтобы разнообразить тематическую демографию набора данных, чтобы полученные результаты экспериментов могли лучше соответствовать сценариям реального мира

*4.3 Input string type*

Тип входной строки является важной экспериментальной переменной в исследовании биометрии касания, поскольку функция, используемая для биометрии сенсорной динамики, берется из входной строки субъекта. Как правило, субъекты должны предоставлять символьный (то есть алфавитный, специальный символ или алфавитно-цифровой ввод), основанный на цифрах (то есть только цифровой ввод) и / или другие неспецифические сенсорные события. Большинство опубликованных экспериментов по динамике касания требовали либо введения символьного, либо цифрового ввода, как показано на рис. 10

Строка ввода, основанная на символах, может быть далее классифицирована на короткие и длинные строки символов. Короткая строка ввода обычно состоит из имени пользователя или пароля (Huang et al., 2012; Mahnoush Babaeizadeh et al., 2014), случайной комбинации символов (Antal and Szabó, 2014; Rao et al., 2014) или Набор словарных слов (Buschek et al., 2015; Giuffrida et al., 2014). Длинная строка ввода обычно представляет собой сегмент текстов (Gascon et al., 2014) или несколько абзацев текстов (Feng et al., 2013; Samura et al., 2014). Аналогично, входная строка, основанная на цифрах, также может быть разделена на короткие и длинные цифры. Строка с короткими цифрами обычно длиной от 4 до 6 цифр. Он обычно напоминает код разблокировки мобильного устройства (Zheng et al., 2014) или PIN-код ATM (Sen и Muralidharan, 2014). С другой стороны, длина строки с длинными цифрами обычно превышает 10 цифр, как, например, номер социального страхования (Johansen, 2012) или телефонный номер (Jain et al., 2014). Другие неспецифические типы ввода включают в себя случайное получение некоторых непрерывных событий касания (Draffin et al., 2014, Y. Meng и др., 2014), случайный ввод жестов с несколькими касаниями (Sae-Bae et al., 2012) , Или сенсорные входные взаимодействия с общим элементом пользовательского интерфейса (например, кнопки, флажки и слайдеры) (Kolly et al., 2012; Saravanan и др., 2014), сделанные в течение определенного периода времени. Поскольку большинство опубликованных экспериментов по сенсорной динамике были сфокусированы на входных данных, основанных на символах или цифрах, в дальнейшем мы сосредоточим наши обсуждения на этих двух типах ввода

*4.4 Input sample size*

Известно, что размер входной выборки набора данных оказывает влияние на точность, надежность и убедительность результатов эксперимента (Sen and Muralidharan, 2014, Wolff, 2013). Чем больше число образцов, которые мы используем, тем лучше представление о поведении сенсорной динамики субъекта и, как результат, тем выше точность, которую мы могли бы достичь (Tasia et al., 2014).

Существует два способа получения нескольких выборок в одном сеансе сбора данных: (i) многократное получение фиксированной входной строки (для ввода по символам или по цифре) или (ii) непрерывное получение событий касания в течение фиксированного периода времени ( Для неспецифического ввода). Согласно литературным данным, контрольное количество образцов на сеанс для каждого испытуемого составляет от 10 до 20 повторений для фиксированного типа входного сигнала (Buschek et al., 2015; Kambourakis et al., 2014; Sen and Muralidharan, 2014; Trojahn et al. , 2013) и 5-10 минут для неспецифического типа ввода (Meng et al., 2013; Xu et al., 2014).

Запрос большого количества образцов от субъекта в одной сессии сбора данных нецелесообразен. Это связано с тем, что предметы могут быть недоступными в течение длительного времени или могут испытывать дискомфорт при длительном сеансе приема (Tasia et al., 2014). Поэтому важно выбрать оптимальное количество выборок на сеанс сбора данных. В качестве альтернативы, вместо того, чтобы приобретать большое количество выборок за один длительный сеанс сбора данных, мы можем выполнять операцию сбора данных в несколько коротких сеансов, распределенных в течение определенного периода времени. Такой подход может снизить уровень дискомфорта, наложенного на объект, а также лучше отразить любые внутрисеансовые варианты (дальнейшее обсуждение в следующем разделе).

*4.5 Acquisition session and interval*

Как упомянуто выше, операция сбора данных для каждого субъекта может выполняться и завершаться либо в рамках одного сеанса, либо разворачиваться по нескольким сеансам, разделенным предопределенным временным интервалом. В большинстве описанных экспериментов (64%) данные по каждому субъекту были получены в течение одного сеанса

Хотя вышеописанный подход относительно дешевле, не всегда бывает целесообразно запрашивать большое количество выборок от каждого субъекта за один сеанс. Что более важно, биометрия сенсорной динамики, как и другая поведенческая биометрия (т.е. голос, походка и подпись), нестабильна со временем (Xu et al., 2014). Это означает, что внутрисессионные различия между разными входными выборками могут быть Сессии, даже если входные выборки предоставлены одним и тем же субъектом. Если выборки получены за один сеанс, внутрисессионные варианты могут не быть захвачены. Это очевидно в экспериментальной работе, описанной Buschek et al. (2015), где точность оценки, оцененная с использованием данных, полученных за один сеанс, в два раза выше, чем результаты, полученные в разных сеансах. Это означает, что экспериментальная оценка с использованием данных, полученных в отдельных сеансах, может быть чрезмерно оптимистичной и может не отражать истинную точность метода проверки подлинности биометрических данных при развертывании в реальном мире

В идеальном случае операция сбора данных должна быть разделена на несколько сеансов, разделенных несколькими интервалами. Таким образом, интрасессионные вариации могут быть лучше зафиксированы. Этот подход был применен в нескольких экспериментах, описанных в литературе, и в этих экспериментах выбранные интервалы, разделяющие различные сеансы сбора данных, варьировались от минут (Johansen, 2012), дней (El-Abed et al., 2014, Serwadda et al. , 2013; Xu et al., 2014) до недель (Buschek et al., 2015; Tasia et al., 2014). Стоит отметить, что при определении числа проб и длин интервалов, разделяющих разные сеансы, следует уделять внимание тщательным соображениям. Это объясняется тем, что эти два фактора могут влиять на долю участия испытуемого в эксперименте. Например, операция сбора данных, которая охватывает более длительный период времени, с большей вероятностью получит более низкую долю участия субъекта (из-за наличия предметов) или может привести к более высокому отсеваемому субъекту (из-за большей приверженности, требуемой от Предметы) (De Luca et al., 2012). Таким образом, существует баланс между лучшей фиксацией закономерностей динамического изменения сенсорной динамики субъектов и сохранением степени участия субъекта и приверженности операции сбора данных.

*4.6 Legitimate and illegitimate subject samples*

Степень точности системы проверки подлинности сенсорной динамики измеряется с использованием значений FAR и FRR (обсуждаемых в разделе 2.5). Чтобы вычислить эти значения, требуются две категории образцов, а именно, допустимые и нелегитимные выборки. Приобретение законных образцов - это простой процесс, описанный выше. Однако для получения незаконных образцов от субъекта существует три подхода: (i) разбиение образцов субъекта на два подмножества, одно из которых используется в качестве законных образцов, а другое используется для незаконных образцов; (Ii) получение дополнительных выборок из подмножества субъектов, участвующих в наборе данных, и использование этих дополнительных выборок в качестве незаконных образцов; Или (iii) набор дополнительных предметов для обеспечения незаконных образцов.

Основываясь на наших исследованиях литературы, первый подход чаще всего принимается (85%). Например, в этих экспериментах (Giuffrida et al., 2014, Y. Meng et al., 2014, Trojahn et al., 2013, Wolff, 2013), t из полученных образцов i были использованы в качестве незаконных образцов, Rest, (t - i), используемые как законные. Подмножество нелегитимных образцов может быть выбрано в рандомизированном (Trojahn et al., 2013; Wolff, 2013) или предопределенном порядке (Giuffrida et al., 2014; Y. Meng и др., 2014). При таком подходе Равное количество легитимных и нелегитимных образцов может быть получено с минимальными или никакими дополнительными ресурсами. Однако этот подход имеет ограничение, когда входная строка не является одинаковой для всех предметов, так как невозможно сравнить шаблоны сенсорной динамики двух входных строк, когда они разные.

В экспериментах, которые не используют одну и ту же входную строку для всех субъектов, может использоваться второй подход к получению незаконных образцов. Например, Tasia et al. (2014) набрали 100 субъектов для предоставления законных образцов. Затем 10 субъектов были случайным образом отобраны из 100 субъектов и получили PIN-коды всех других субъектов. Каждому из этих 10 испытуемых была предоставлена дополнительная задача: предоставить 5 олицетворенных образцов каждого из других 99 субъектов. При таком подходе 10 отобранных испытуемых должны уделять больше времени и усилий эксперименту, что может препятствовать добровольному участию. По этой причине количество незаконно полученных образцов обычно меньше, чем количество, полученное с использованием первого подхода (путем разделения уже полученных легитимных образцов)

Третий подход заключается в наборе отдельного пула предметов специально для обеспечения незаконных образцов. Возьмите Dhage et al. (2015), Gascon et al. (2014 год) и Сен и Муралидхаран (2014 год), вместо того чтобы запрашивать субъектов, набранных для предоставления законных образцов, исследовательская группа набрала дополнительные предметы для обеспечения незаконных образцов. Таким образом, более вероятно получить сбалансированное количество законных и незаконных образцов. Стоит отметить, что при таком подходе для каждого прироста размера объекта в наборе данных должны быть набраны два субъекта. Это означает, что ресурс и усилия, необходимые для получения набора данных, удвоены по сравнению с двумя другими подходами

*4.7 Public dataset*

Доступность общедоступного набора данных для исследований биометрии сенсорной динамики очень важна. Например, при таком наборе данных мы могли бы проводить сравнение различных алгоритмов в одном и том же наборе данных и / или различных экспериментальных установках. Доступность общедоступного набора данных также позволяет исследователям сосредоточиться на более сложных проблемах исследования, тратя меньше времени на приобретение данных. Однако доступность открытого набора данных в области биометрии сенсорной динамики по-прежнему ограничена. Это может быть связано с тем, что сенсорные устройства не были с нами в течение очень долгого времени, а создание или получение таких данных - это процесс времени и ресурсов. На момент написания этой статьи мы смогли найти только три общедоступных набора данных по отношению к динамике касания. Эти наборы данных представлены в таблице 2.

*4.7.1 Dataset 1*

Эксперимент по сбору данных, проведенный El-Abed et al. (2014 г.) участвовали 51 субъект, вводя фиксированную строку на основе символа «rhu.university» на смартфоне Nokia Lumia 920 Windows. Субъекты должны были присутствовать на трех разных сессиях со средним интервалом между сессиями 5 дней. Используется в качестве практического занятия, поэтому фактическое получение данных началось со второй сессии. В общей сложности 15 образцов были получены от каждого субъекта в течение второй и третьей сессий

*4.7.2 Dataset 2*

Другой набор данных, опубликованный Tasia et al. (2014), был основан на цифровых последовательностях. Устройство, используемое для получения данных, было смартфоном раннего поколения, работающим на уровне API 2.0.1 (Éclair) API 6, который был выпущен в декабре 2009 года. Субъекты должны были предоставить только 2 образца За сеанс и 5 сеансов использовались с межсессионным интервалом продолжительностью не менее 1 недели. Данные были получены в условиях ограниченного класса, в которых участвовали в основном студенты университетов. Строки ввода не были предопределены; Субъектам было разрешено свободно выбирать свои PIN-коды, большинство из которых имеют длину от 4 до 8 цифр.

*4.7.3 Dataset 3*

Antal и Szabó (2014) сделали еще одну попытку публиковать и публиковать данные. Число вовлеченных субъектов является наименьшим из трех публичных наборов данных. Сбор данных в этом эксперименте был выполнен с использованием планшета Nexus 7 и смартфона LG Optimus L7 P700. В документе не объясняется, почему были использованы два разных типа устройств, и будет ли использование различных типов устройств иметь какие-либо последствия для производительности. Входная строка, используемая для сбора данных, была предопределена как «.tie5Roanl». Кроме того, полученные события касания включают не только входную строку, но также клавишу переключения (переключение между нижним и верхним символами) и клавишу переключения клавиатуры (переключение между символами и цифровыми клавишами). Эти вторичные ключевые события могут захватывать ценную и отличительную информацию о шаблонах динамики касания. Кроме того, в этом эксперименте большинство испытуемых предоставляли свои пароли 30 раз каждый на 2 изолированных сеансах в течение 2 недель (продолжительность между двумя сеансами была неизвестна). Некоторые недопустимые исходные данные были удалены, поэтому набор данных был унифицирован только для 51 входных выборок на субъекта (вместо 60 из обоих сеансов)

**5. Feature extraction**

Шаблоны динамики сенсорного экрана содержат уникальные функции, которые можно использовать для отличия друг друга. На этапе извлечения признаков эти функции извлекаются путем обработки необработанных данных динамики касания, полученных от объекта. Общие признаки, обсуждаемые в литературе, можно разделить на три категории, а именно: (i) временные рамки, (ii) пространственные и (iii) движения. Исследования, проведенные по этим признакам, обобщены на рис. 11

*5.1. Timing feature*

Функция синхронизации - это наиболее широко используемая функция в сенсорной динамической биометрии. Сенсорное событие (касание пальцем вниз или поднятие вверх) на виртуальной клавиатуре генерирует цифровые прерывания, которые могут быть обнаружены при вызовах функций API ОС для мобильных телефонов (Kambourakis et al., 2014). Каждое из этих событий может быть связано со значением временной метки. Эти значения timestamp не имеют семантического значения и нуждаются в дальнейшем управлении. Основываясь на этих значениях временной отметки, можно выделить два различных типа синхронизации с различной длиной

*5.1.1 Timing feature types*

Выполняя математические операции с двумя значениями временной метки события прикосновения, можно получить два типа типов хронометража. Первый - это время ожидания (DT), и оно относится к продолжительности времени касания с той же клавишей. Он также известен как интервал, нажмите или удерживайте время в литературе. Это значение может быть получено путем вычитания значения временного штампа ключа из его значения времени нажатия клавиши. Второй - время полета (FT). Он относится к временному интервалу между сенсорными событиями двух последовательных клавиш. Он также известен как латентность. Как показано на фиг. 12, существует четыре варианта FT. Следует отметить, что, согласно Шенгу и др. (2005), FTA может иметь отрицательное значение. Этот сценарий происходит, когда объект нажимает следующую клавишу перед тем, как отпустить предыдущий. Однако этот сценарий более вероятен при приобретении функции хронирования с использованием компьютерной клавиатуры вместо использования виртуальной клавиатуры. Это связано с различием физического и геометрического размера виртуальных клавиш от физических клавиш; Очень редко для субъекта использовать несколько пальцев одновременно при предоставлении их ввода на виртуальных клавишах. В результате шансы на нажатие следующей клавиши перед освобождением предыдущей значительно сокращены или в некоторых случаях не существуют при использовании виртуальной клавиатуры

*5.1.2 Timing Feature length*

Функция хронометража может быть извлечена с различными характеристиками. Самая короткая длина функции называется uni-graph, которая является характеристикой времени, извлекаемой путем принятия значений времени нажатия сенсорного события для одной и той же клавиши. Функции синхронизации, извлеченные из двух или более ключей, называются di-graph и n-graph соответственно. Графическая иллюстрация различных длин n-графов показана на рис. 13. В большинстве экспериментов, описанных в литературе, используются униграфы и диграфы. Единственными двумя исключениями были эксперименты, проведенные Giuffrida et al. (2014 год); Trojahn et al. (2013 г.), где был извлечен n-граф размером 3 или больше. Причина, по которой большой размер n-графа обычно не используется, заключается в том, что больший n-граф содержит меньшую детализацию детализации (Trojahn et al., 2013). Это было экспериментально доказано Giuffrida et al. (2014 г.). В своем эксперименте авторы сравнили результаты точности различных размеров n-графа. Результат сравнения показал, что больший размер n-графа обеспечивает более низкую точность

*5.2 Spatial feature*

Пространственная функция - это характеристика, связанная с физическим взаимодействием между кончиком пальца и поверхностью сенсорного экрана устройства, и ее можно получить, когда выполняется касание. Три наиболее распространенных пространственных признака в литературе - размер, давление и положение касания. Визуальные примеры этих трех пространственных функций, извлеченных с помощью мобильного устройства Android, описаны в Y. Meng et al. (2014 г.).

*5.2.1 Touch size*

Размер касания представляет собой приближение области экрана, к которой прикасается сенсорное событие. Каждому событию касания соответствует значение размера касания. Значение обычно возвращается из функции API и масштабируется до значения в диапазоне от 0 до 1 (Zheng et al., 2014). Это значение обычно используется как данные об элементах без дополнительных манипуляций. Размер касания, полученный от объекта, определяется размером пальца объекта. Например, Никсон и соавт. (2014) отметил, что взрослый мужчина-субъект обычно производит большее значение размера касания, чем ребенок или взрослая женщина-субъект. Это означает, что людям с разными размерами пальцев трудно подражать друг другу.

*5.2.2 Touch pressure*

Давление прикосновения - еще одна особенность, которая часто используется вместе с сенсорным размером. Значение давления нажатия измеряет аппроксимированное усилие, указанное на экране при каждом касании. Он выражается в абстрактной единице со значением в диапазоне от 0 (мягкое прикосновение) до 1 (более жесткое прикосновение) (Zheng et al., 2014). Как и в случае с сенсорным размером, значение давления касания, извлеченное функцией API, можно использовать непосредственно без дополнительных манипуляций. Значение давления прикосновения связано с мышцей пальца субъекта, которая уникальна для каждого объекта. Таким образом, одному субъекту трудно подражать сенсорному давлению другого субъекта исключительно посредством наблюдений, делая систему аутентификации касания касания, которая использует особенность касания давления, очень устойчивую к атак с использованием плеча (Feng et al., 2013).

*5.2.3 Touch Position*

Позиция касания - это двумерная матричная функция, которая фиксирует местоположение приземления пальца на экране устройства (или клавише). Каждое касание может быть связано с координатами x и y, измеренными в пиксельных единицах (Kolly et al., 2012). Положение касания клавиши зависит от размера кончика пальца и когнитивного предпочтения. Это изменение позволяет использовать положение касания в качестве отличительного признака для идентификации объекта. Это подтверждается наблюдениями, описанными Johansen (2012), где позиции касания, предоставленные разными субъектами, сильно различаются между разными субъектами в их эксперименте. Позиция касания может быть выражена двумя различными способами: (i) в качестве абсолютных координат касания относительно всего экрана (Y.Meng et al., 2014) или (ii) как смещение центра центра (Draffin et al., 2014). Кроме того, с помощью некоторых математических манипуляций могут быть получены дополнительные функции. К ним относятся расстояние (Buschek et al., 2015; Kambourakis et al., 2014), скорость (Kambourakis et al., 2014) или угол (Serwadda et al., 2013) между двумя касаниями. Тем не менее, существует проблема с этим координатным представлением значений положения касания (Alotaibi et al., 2014); То есть система координат экрана зависит от устройства. Используя разные устройства, зафиксированные значения позиции касания не согласованы. Поэтому значения позиции касания должны быть нормализованы, если операция сбора данных не выполняется на устройстве с аналогичной моделью (Jain et al., 2014)

*5.3 Motion feature*

Современные мобильные устройства оснащены двумя аппаратными датчиками движения, акселерометром и гироскопом. Эти датчики широко используются в приложениях, таких как устройства сопряжения устройств и приложения контроля цикла сна, которые используют данные движения или зависят от движения (Owusu et al., 2012). Каждое касание обычно вызывает небольшое движение и / или вращение устройства. Эти функции движения могут быть захвачены и использованы для идентификации объекта

Датчик акселерометра измеряет линейную скорость движения, применяемую к устройству с течением времени. Он предназначен для обнаружения движения вдоль оси x, y и z как в положительном, так и в отрицательном направлениях. Эти три значения измеряются в единицах м / с2 (Aviv et al., 2012). С другой стороны, датчик гироскопа измеряет скорость вращения, приложенную к устройству по трем осям: (i) наклон вперед и назад (шаг), (ii) скручивание из стороны в сторону (рулон) и (iii) поворот от Портрет к пейзажу (рыскание). Эти значения измеряются в единице рад / с (Giuffrida et al., 2014). Инжир. 14 показано графическое представление различных движений, захваченных обоими датчиками.

Обычно необработанные данные движения, полученные этими двумя датчиками, не могут быть легко использованы в качестве данных характеристик. Это происходит потому, что каждое касание генерирует более одного значения движения и вращения. Чтобы сделать данные пригодными для использования в качестве функциональных данных, мы должны применить некоторые статистические вычисления, такие как min, max, mean и variance, для необработанных данных, и результаты этих вычислений могут быть использованы в качестве значимых данных о характеристиках (de Mendizabal-Vazquez et. Al., 2014, Ho, 2013). Кроме того, как Zheng et al. (2014) отметил, что оба датчика чувствительны к крошечным изменениям движения. Поэтому они решили объединить сенсорные значения x, y и z-оси в вектор признаков, вместо того, чтобы использовать их отдельно

Исследователи делятся на вопрос, действительно ли датчик акселерометра обеспечивает лучшее отличительное свойство, чем датчик гироскопа. Например, экспериментальные результаты Giuffrida et al. (2014) показывают, что данные акселерометра могут лучше фиксировать узоры сенсорной динамики объекта, чем данные гироскопа. Однако наблюдения, сделанные Кай и Ченом (Cai and Chen, 2012), показывают другой результат, то есть данные гироскопа обеспечивают лучшую точность, особенно если объект использует устройство во время движения. В литературе большинство характеристик характеристик движения сенсорной динамики относятся к обоим типам датчиков. Это хорошо, потому что данные обоих типов датчиков могут дополнять друг друга, что ведет к лучшей точности идентификации объекта