Поведенческие характеристики взаимодействия с сенсорным экраном для идентификации пользователей мобильных устройств

А.В. Осин, Ю.В. Мурашко, В.И. Суворов

Московский технический университет связи и информатики, Москва

Аннотация: В работе на основе анализа поведенческих характеристик выявлены основные индикаторы, которые дают наибольшую точность при идентификации пользователей мобильных устройств. В рамках исследования написано ПО для сбора данных сенсорного экрана при выполнении типовых действий пользователя. На основе алгоритмов машинного обучения реализованы алгоритмы идентификации и показана точность. Полученные в исследовании результаты могут быть исследованы для построения систем непрерывной идентификации.
Ключевые слова: Поведение пользователей, сенсорный экран, непрерывная идентификация, биометрия, набор данных, классификация, глубокое обучение, рекуррентная нейронная сеть, мобильное устройство.

Введение

Идентификация пользователей мобильных устройств по ПИН-кодам и паролям на сегодняшний день не предоставляет достаточный уровень безопасности и удобства [1-3]. Эти методы подвержены таким атакам, как угадывание и перехват данных при вводе [4].

Ограничения методов идентификации, основанных на знании, подчеркивают необходимость разработки более безопасных и удобных для пользователя решений. Поэтому в настоящее время активно применяются методы, которые используют физические характеристики человека (т.е. физиологическую биометрию), такие, как отпечатки пальцев, характеристики речи, радужная оболочка, изображение лица, геометрия ладоней рук [5], или непроизвольные действия (т.е. поведенческую биометрию), такие как динамику нажатий клавиш клавиатуры и динамику движения курсора мыши или пальца [6].

Несмотря на то, что системы, основанные на поведенческих характеристиках, могут быть менее эффективны для идентификации по сравнению с физиологическими аналогами, их применение в непрерывной

идентификации является перспективным [7]. Например, в контексте двухфакторной аутентификации непрерывная поведенческая идентификация может служить дополнительным слоем безопасности поверх существующих методов [8].

Цель данной работы — сбор данных сенсорного экрана пользователей мобильных устройств и определение поведенческих характеристик взаимодействия с сенсорным экраном, значимых для их идентификации.

Сбор данных

В рамках исследования был сформирован набор данных, собранный с использованием специально разработанного программного обеспечения для операционной системы Android, зарегистрированного как «Программа для измерения поведенческих характеристик пользователя мобильного устройства» [9]. Программное обеспечение спроектировано таким образом, чтобы максимально точно имитировать обычное поведение пользователей мобильных устройств. Набор данных включает данные с сенсорного экрана, полученные при выполнении восьми заданий, отражающих типичные действия пользователя: ввод текста через виртуальную клавиатуру, чтение текста вертикальной прокруткой, просмотр изображений горизонтальной прокруткой, поиск объектов на изображении масштабированием двумя пальцами, нажатие на случайные квадраты на экране, перемотка рекламы в видеоролике, длительные нажатия на кнопки и рисование цифр, соответствующих текущей сессии выполнения заданий (см. рисунок 1). Такой подход обеспечивает разнообразие собранных данных, что позволяет учитывать широкий спектр поведенческих характеристик пользователя при взаимодействии с сенсорным экраном.

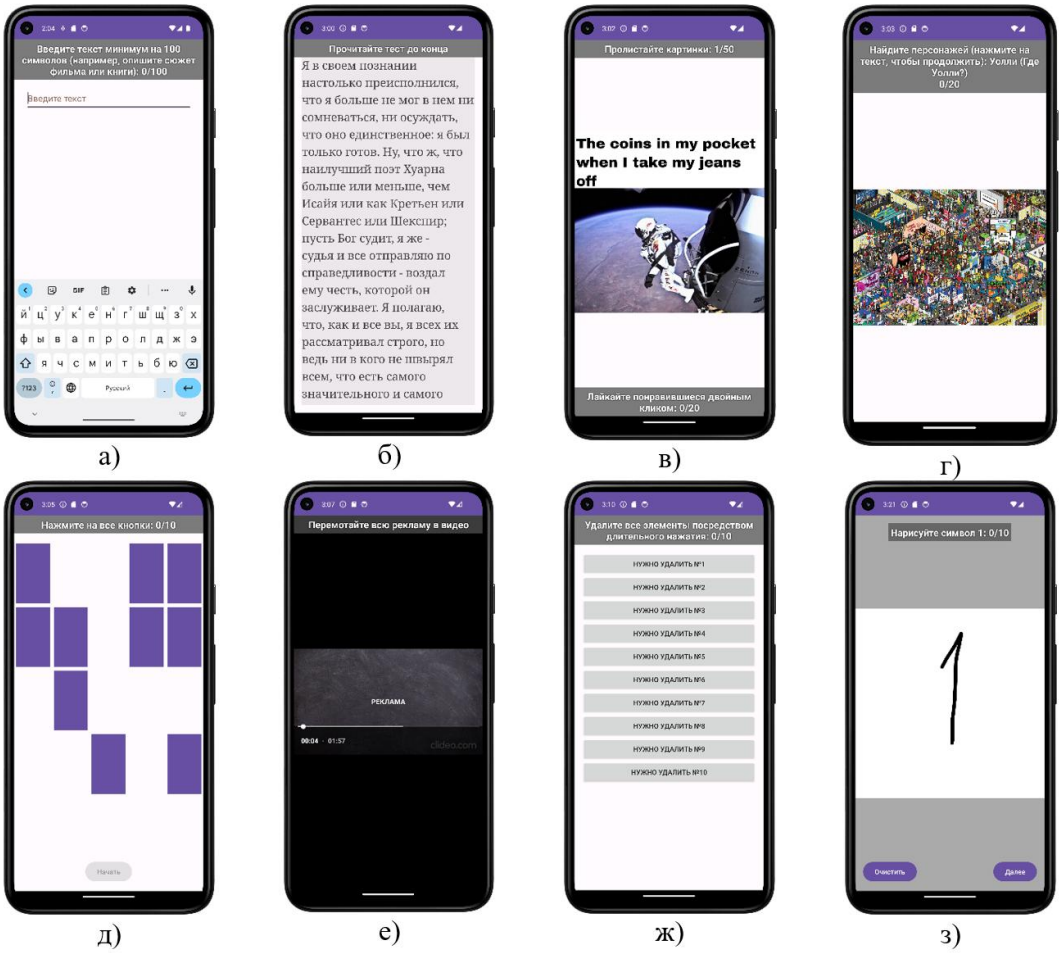

Рис. 1. – Графическое представление каждого из 8 различных заданий, включенных в приложение для сбора данных

В сформированный набор данных включаются координаты точек касания пальцев к сенсорному экрану мобильного устройства. Для унификации данных значения координат нормализуются относительно размеров экрана по ширине и высоте, что позволяет исключить влияние различий в физических размерах устройств. В случае касания экрана одним пальцем координаты сохраняются в формате $[x,y]$, где x и y — нормализованные значения горизонтальной и вертикальной позиции касания соответственно. При одновременном касании экрана двумя пальцами данные записываются в формате $[x_1,y_1,x_2,y_2]$, где индексы *1* и *2* соответствуют координатам первого и второго пальцев (см. рисунок 2).

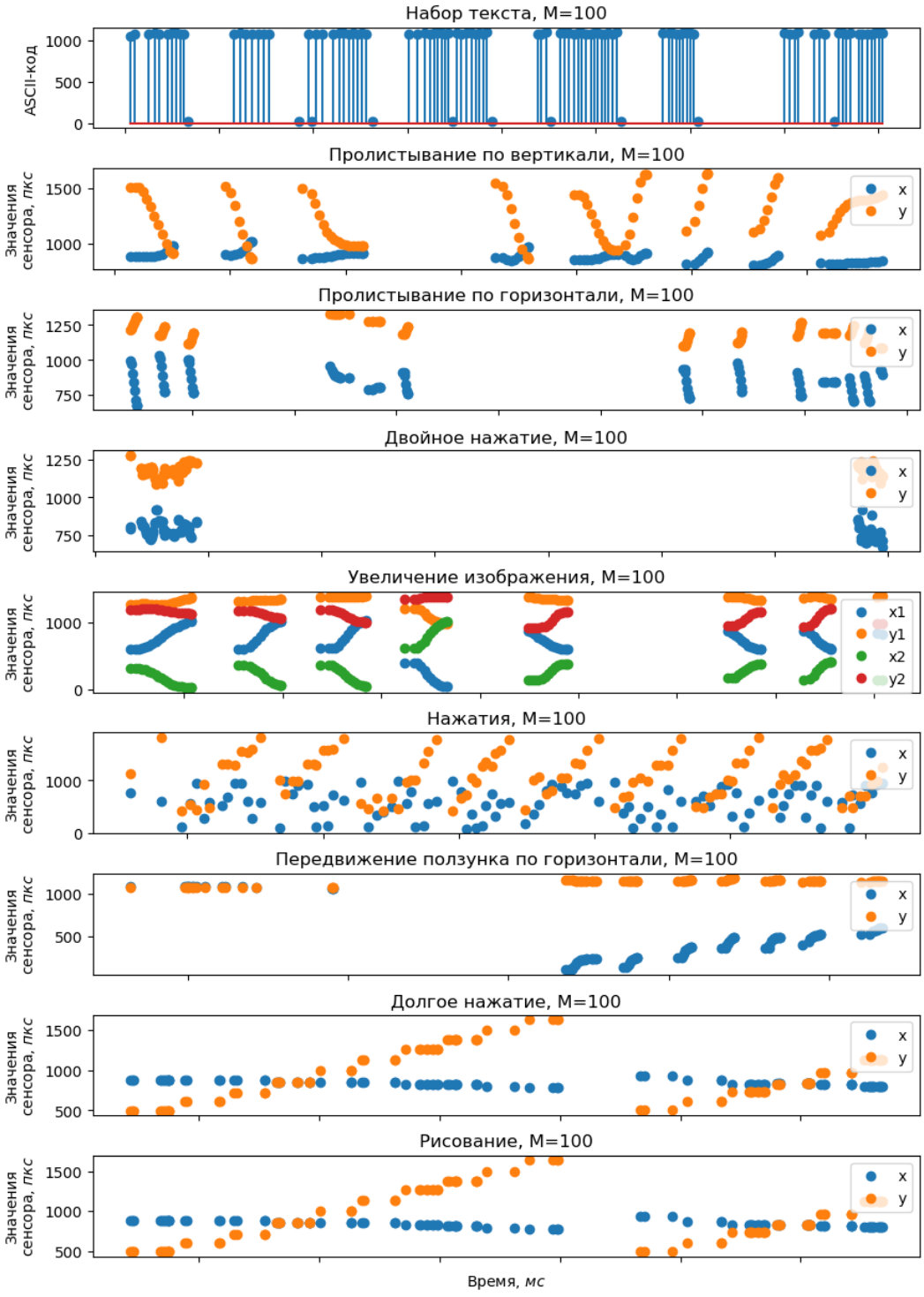

Рис. 2. – Данные с сенсорного экрана

Эксперимент

В ходе экспериментального исследования по идентификации пользователей мобильных устройств были собраны данные от 103 участников.

Сбор информации осуществлялся среди студентов в возрасте от 20 до 25 лет. По половому составу, 75% испытуемых были мужчинами, а 25% — женщинами. Каждый участник использовал свое собственное мобильное устройство, однако некоторые устройства были задействованы повторно; в результате общее число уникальных устройств составило 70, а максимальное количество пользователей с одинаковым устройством достигало 7. Характеристики собранных данных приведены в таблице №1.

Таблица №1

Характеристики набора данных

Задание	Количество пользователей, шт	Среднее количество строк на пользователя, шт	Процентиль 75%, шт	Процентиль 100%, шт	Всего строк, шт
Набор текста	103	778	916	1953	75499
Пролистывание по горизонтали	103	3745	4525	10852	363316
Двойное нажатие	103	262	282	510	25428
Пролистывание по вертикали	103	5433	4896	55650	527014
Увеличение изображения	103	16027	19709	88015	1554682
Нажатия	103	604	603	956	58664
Пролистывание по горизонтали	103	688	760	4400	66745
Рисование	103	2974	3379	9435	288572
Долгое нажатие	103	6843	8514	35768	663856

Для идентификации пользователей мобильных устройств в данном исследовании использовалась нейронная сеть, включающая два слоя долгой

краткосрочной памяти, два слоя пакетной нормализации и два слоя исключения (см. рисунок 3). Такая архитектура позволяет эффективно обрабатывать временные последовательности данных, сохраняя контекстную информацию и минимизируя риск переобучения [10]. Размер окна данных для входных последовательностей был установлен равным 80, что обеспечивает достаточную длину для анализа поведенческих паттернов. Обучение модели проводилось в течение 100 эпох с использованием пакетов размером 512, что способствовало стабильной сходимости и оптимизации параметров нейросети. Такой подход обеспечил высокую производительность модели и её способность точно классифицировать пользователей на основе их поведенческих данных.

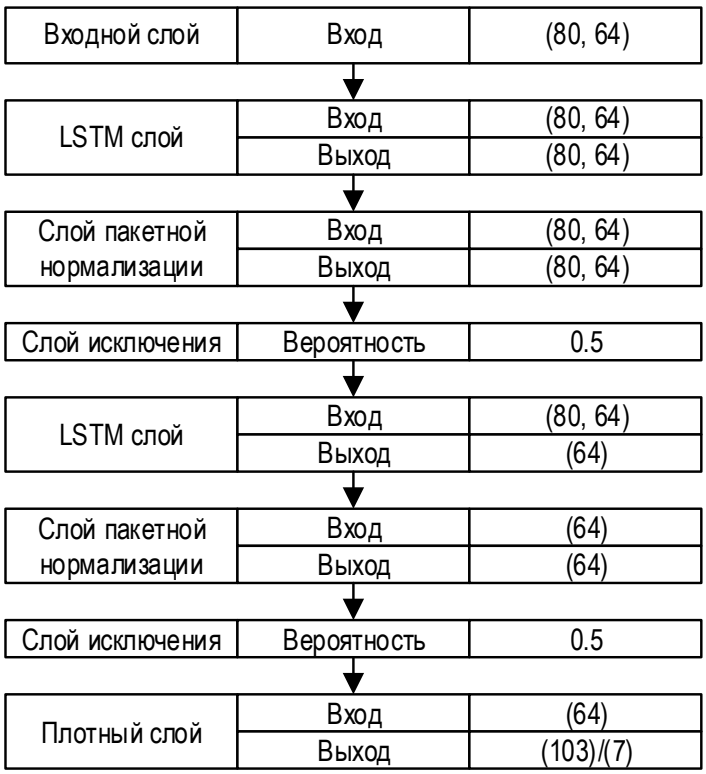

Рис. 3. – Архитектура модели

В таблице №2 представлены результаты точности классификации для каждого задания.

Таблица №2

Результаты точности идентификации для каждого задания

Задание	Точность
Ввод текста	0.75
Чтение текста	0.81
Просмотр изображений	0.86
Поиск объектов	0.84
Нажатие	0.73
Перемотка рекламы	0.81
Длительные нажатия	0.80
Рисование цифр	0.69

Задание по просмотру изображений продемонстрировало наивысшую точность в 0.86, тогда как задание по рисованию цифр показало наименьшую точность — 0.69.

Заключение

В данной работе представлено специализированное программное обеспечение для сбора данных пользователей мобильных устройств, с помощью которого был сформирован набор данных поведенческих характеристик взаимодействия с сенсорным экраном.

Исследование показало, что для идентификации пользователей наиболее значимые поведенческие характеристики взаимодействия с сенсорным экраном получены при выполнении заданий по пролистыванию изображений и поиску объектов.

На основе полученных результатов авторы продолжают исследования, направленные на дальнейшее повышение точности идентификации пользователей мобильных устройств. В следующем этапе работы

планируется создание модели пользователя, основанной на концепции динамического цифрового отпечатка. Включение дополнительных данных позволит более полно учитывать индивидуальные особенности пользователей, что повысит надёжность и точность идентификации.

Литература

1. Liang C. et al. Auth+ track: Enabling authentication free interaction on smartphone by continuous user tracking // Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems. – 2021. – pp. 1-16.

2. Sucasas V. et al. Attribute-based pseudonymity for privacy-preserving authentication in cloud services // IEEE Transactions on Cloud Computing. – 2021. – Т. 11. – №. 1. –pp. 168-184.

3. Papaioannou M. et al. A survey on security threats and countermeasures in internet of medical things (IoMT) // Transactions on Emerging Telecommunications Technologies. – 2022. – Т. 33. – №6. – С. e4049.

4. Фатхи Д. В., Галушка В. В. Повышение сложности пароля пользователя на основе комплексирования символов пароля и временных интервалов между ними // Инженерный вестник Дона. 2019. №1. URL: ivdon.ru/ru/magazine/archive/n1y2019/5594.

5. Остроух Е. Н. и др. Разработка методов и алгоритмов проверки работы предприятия с точки зрения информационной безопасности его функционирования // Инженерный вестник Дона. 2016. №2. URL: ivdon.ru/ru/magazine/archive/n2y2016/3575.

6. Осин А. В., Мурашко Ю. В. Обзор методов идентификации пользователя на основе цифровых отпечатков // Труды учебных заведений связи. – 2023. – Т. 9. – №5. – С. 91-111. URL: tuzs.sut.ru/jour/issue/view/35.

7. Кыясова Г. Ч., Батырова А. Разработка методов аутентификации и авторизации пользователей в информационных системах // Всемирный

ученый. 2024. Т. 1. №18. С. 104-109 URL: wsemiruch.online/archive/211570b5-791a-4011-a30a-b8eaa4149624

8. Wahab A. A., Hou D., Schuckers S. A user study of keystroke dynamics as second factor in web MFA // Proceedings of the Thirteenth ACM Conference on Data and Application Security and Privacy. 2023. pp. 61-72.

9. Мурашко Ю. В. Программа для измерения поведенческих характеристик пользователя мобильного устройства. Свидетельство о регистрации №2024660069. 2024. Бюллетень №5. URL: elibrary.ru/item.asp?id=67263726.

10. Stragapede G. et al. BehavePassDB: public database for mobile behavioral biometrics and benchmark evaluation // Pattern Recognition. 2023. Т. 134. С. 109089.

References

1. Liang C. et al. Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems. 2021. pp. 1-16.

2. Sucasas V. et al. IEEE Transactions on Cloud Computing. 2021. V. 11. №1. pp. 168-184.

3. Papaioannou M. et al. Transactions on Emerging Telecommunications Technologies. 2022. V. 33. №6. P. e4049.

4. Fathi D.V., Galushka V.V. Inzhenernyj vestnik Dona, 2019, №1. URL: ivdon.ru/ru/magazine/archive/n1y2019/5594.

5. Ostroukh E. N. et al. Inzhenernyj vestnik Dona, 2016, №2. URL: ivdon.ru/ru/magazine/archive/n2y2016/3575.

6. Osin A.V., Murashko Yu.V. Trudy uchebnyh zavedenij svyazi. V. 9, №5, 2023, pp. 91-111 URL: tuzs.sut.ru/jour/issue/view/35.

7. Kyyasova G. Ch., Batyrova A. Vsemirnyj uchenyj, 2024, V. 1. №18. pp. 104-109. URL: wsemiruch.online/archive/211570b5-791a-4011-a30a-b8eaa4149624.

8. Wahab A. A., Hou D., Schuckers S. Proceedings of the Thirteenth ACM Conference on Data and Application Security and Privacy, 2023, pp. 61-72.

9. Murashko Yu. V. Programma dlya izmereniya povedencheskih harakteristik pol'zovatelya mobil'nogo ustrojstva [Program for measuring the behavioral characteristics of a user of a mobile device], Svidetel'stvo o registracii №2024660069, 2024. Byulleten' №5. URL: elibrary.ru/item.asp?id=67263726.

10. Stragapede G. et al. Pattern Recognition, 2023, V. 134, P. 109089.

Дата поступления: 25.10.2024

Дата публикации: 9.12.2024