Оригинальная статья / Original article

https://doi.org/10.21869/2223-1536-2025-15-4-150-161

УДК 004.93, 004.896

Исследования алгоритмов нейросетевого распознавания динамической подписи пользователя в пространстве отсчетов многомерных кривых в сравнении с оптимальными алгоритмами обнаружения-различений многомерных сигналов

А. Х. Танцеров[1], Е. А. Данилов[1] ✉

[1] Пензенский государственный технологический университет
пр. Байдукова / ул. Гагарина, д. 1а / 11, г. Пенза 440039, Российская Федерация

✉ e-mail: danilov@penzgtu.ru

Резюме

Цель исследования. *Высокая степень распространения динамической подписи в различных областях, связанных с биометрическими технологиями (во многих странах четко сформулированы правовые процедуры для их использования), обусловливает значительное внимание к достоверности соответствующих алгоритмов биометрической аутентификации. Динамическая подпись частично свободна от недостатков, свойственных статической подписи, однако и для нее остро стоит проблема достоверности аутентификации пользователя информационными сервисами, обусловленная совокупностью разнородных факторов, поэтому целью проведенного исследования является повышение достоверности аутентификации пользователя по реализации его динамической подписи на основе экспериментально-структурного и параметрического синтеза проблемно ориентированных нейронных сетей и сравнения достоверности с классическими алгоритмами обнаружения-различений многомерных сигналов.*

Методы. *Алгоритм комплексной идентификации динамической сигнатуры подписи пользователя в пространстве отсчетов многомерных кривых в форме параллельного распознавания многомерного фрагмента кривой различными обнаружителями / классификаторами с последующим комплексированием и анализом результатов.*

Результаты. *Экспериментально исследованы алгоритмы нейросетевой идентификации динамической сигнатуры подписи пользователя в пространстве отсчетов многомерных кривых в сравнении с оптимальными алгоритмами обнаружения-различений многомерных сигналов. Эксперименты показали, что 3–5 основных параметров: две координаты пера в плоскости реализации планшета, давление на экран в совокупности с векторами скорости пера – обеспечивают приемлемую достоверность идентификации в интервале 0,8…0,95 в условиях малого числа пользователей и сохраняются на уровне 0,7 при их неограниченном увеличении. Средний выигрыш от применения разработанных моделей и алгоритмов идентификации подписи по сравнению со статистическими методами составил 25–35%, по сравнению с метрическими – от 5 до 15%.*

Заключение. *Для обеспечения заданных показателей надежности аутентификации пользователя необходимо декомпозировать аппаратно-программные модели идентификации динамической подписи по группам небольшого числа пользователей. Существуют оптимальное число и набор алгоритмов, которые доставляют максимум достоверности результата комплексирования: метрический в евклидовой метрике, корреляционный и нейросетевой.*

Ключевые слова: *динамическая подпись; идентификация; многослойная нейронная сеть; алгоритм Кульбака-Лейблера; кросс-корреляция; многомерная кривая.*

Конфликт интересов: *Авторы декларируют отсутствие явных и потенциальных конфликтов интересов, связанных с публикацией настоящей статьи.*

Для цитирования: Танцеров А. Х., Данилов Е. А. Исследования алгоритмов нейросетевого распознавания динамической подписи пользователя в пространстве отсчетов многомерных кривых в сравнении с оптимальными алгоритмами обнаружения-различений многомерных сигналов // Известия Юго-Западного государственного университета. Серия: Управление, вычислительная техника, информатика. Медицинское приборостроение. 2025. Т. 15, № 4. С. 150–161. https://doi.org/10.21869/2223-1536-2025-15-4-150-161

Поступила в редакцию 08.10.2025 *Подписана в печать 06.11.2025* *Опубликована 26.12.2025*

Research on neural network algorithms for user dynamic signature recognition in the space of multidimensional curve samples, in comparison with optimal detection–discrimination algorithms for multidimensional signals

Alexander K. Tantserov[1], Evgeny A. Danilov[1] ✉

[1] Penza State Technological University
1a / 11 Baydukov pass. / Gagarin Str., Penza 440039, Russian Federation

✉ e-mail: danilov@penzgtu.ru

Abstract

Purpose of research. *The widespread adoption of dynamic signatures in various biometric technology applications-supported by clearly defined legal procedures in many countries-drives significant attention toward the reliability of corresponding biometric authentication algorithms. While dynamic signatures are partially free from the drawbacks inherent in static signatures, the problem of authentication reliability remains critical due to the complex interplay of heterogeneous factors. Therefore, the aim of this study is to improve the reliability of user authentication based on the dynamic signature using experimental structural and parametric synthesis of problem-oriented neural networks and comparison with classical detection-discrimination algorithms for multidimensional signals.*

Methods. *The proposed method involves comprehensive identification of the user's dynamic signature in the sample space of multidimensional curves by means of parallel recognition of curve fragments using multiple detectors/classifiers, followed by integration and analysis of the results.*

Results. *Neural network algorithms for identifying the user's dynamic signature in the sample space of multidimensional curves were experimentally studied and compared with optimal detection-discrimination algorithms for multidimensional signals. The experiments demonstrated that 3–5 key parameters-including two stylus coordinates on the tablet plane, screen pressure, and stylus velocity vectors-ensure acceptable identification reliability in the range of 0,8 to 0,95 for a small number of users, and maintain a reliability level of about 0,7 with unlimited user scaling. The average gain in accuracy from using the developed models and algorithms, compared to statistical methods, amounted to 25–35%, and compared to metric methods, 5–15%.*

Conclusion. *To achieve the required reliability of user authentication, hardware-software identification models for dynamic signatures should be decomposed into groups with a limited number of users. There exists an optimal combination of algorithms that delivers maximum accuracy in result integration: Euclidean metric, correlation-based, and neural network classifiers.*

Keywords: *dynamic signature; identification; multilayer neural network; Kullback-Leibler algorithm; cross-correlation; multidimensional curve.*

Conflict of interest: *The Authors declare the absence of obvious and potential conflicts of interest related to the publication of this article.*

For citation: Tantserov A.K., Danilov E.A. Research on neural network algorithms for user dynamic signature recognition in the space of multidimensional curve samples, in comparison with optimal detection–discrimination algorithms for multidimensional signals. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta. Serija: Upravlenie, vychislitel'naja tekhnika, informatika. Meditsinskoe priborostroenie = Proceedings of the Southwest State University. Series: Control, Computer Engineering, Information Science. Medical Instruments Engineering.* 2025;15(4):150–161. (In Russ.) https://doi.org/10.21869/2223-1536-2025-15-4-150-161

Received 08.10.2025 *Accepted 06.11.2025* *Published 26.12.2025*

***

Введение

Динамические биометрические методы аутентификации приобретают массовое распространение в большинстве персональных [1] и корпоративных электронных устройств и систем [2]. Однако для динамической подписи остро стоит проблема достоверности аутентификации, обусловленная зависимостью ее реализации от параметров датчико-преобразующей аппаратуры, вариабельностью постановки для одного и того же носителя [3], обусловленной эмоциями, стрессом, усталостью, влиянием алкоголя или психотропных веществ, нейромоторными изменениями после приема лекарств, эффектами биологического старения, когнитивно-моторными нарушениями, настроением человека, временем, доступным для постановки подписи [4], или, собственно, готовностью к взаимодействию с системой аутентификации личности [5]. При этом актуальной является проблема, характеризующаяся непредсказуемостью, межличностной изменчивостью, позволяющая реализовать не обнаруживаемую со 100% вероятность подделки [6]. Одним из направлений разрешения данной проблемы является расширение пространства признаков идентификации [7] и регуляризация решения задачи распознавания, обусловленной ненаблюдаемыми состояниями пользователя и аппаратуры регистрации, на основе методологии решения некорректных задач [8]. Для многомерных кривых динамической подписи задача заключается в инвариантном представлении комбинаторного множества идентифицируемых математических объектов и поиске оптимального классификационного решения для ограниченного объема внутриклассовых выборок [9]. Современное направление, активно развивающееся для работы с большими объемами и подобным характером идентифицируемых данных, представлено методологией и средствами машинного обучения [9].

Материалы и методы

Исходными данными для решения задачи идентификации пользователя являются шаблоны его динамической сигнатуры подписи, представленные в виде многомерной кривой [10]. В качестве фактуры исходных данных для синтеза таких шаблонов используются открытые базы данных, содержащие до десятка параметров, динамической реализации подлинной и поддельной подписи пользователя [11]. Шаблон (или эталон) представляет собой математическую кривую, вложенную в многомерное (по числу параметров) пространство (рис. 1), как результат таксономии множества реализаций динамической подписи одного и того же пользователя [12].

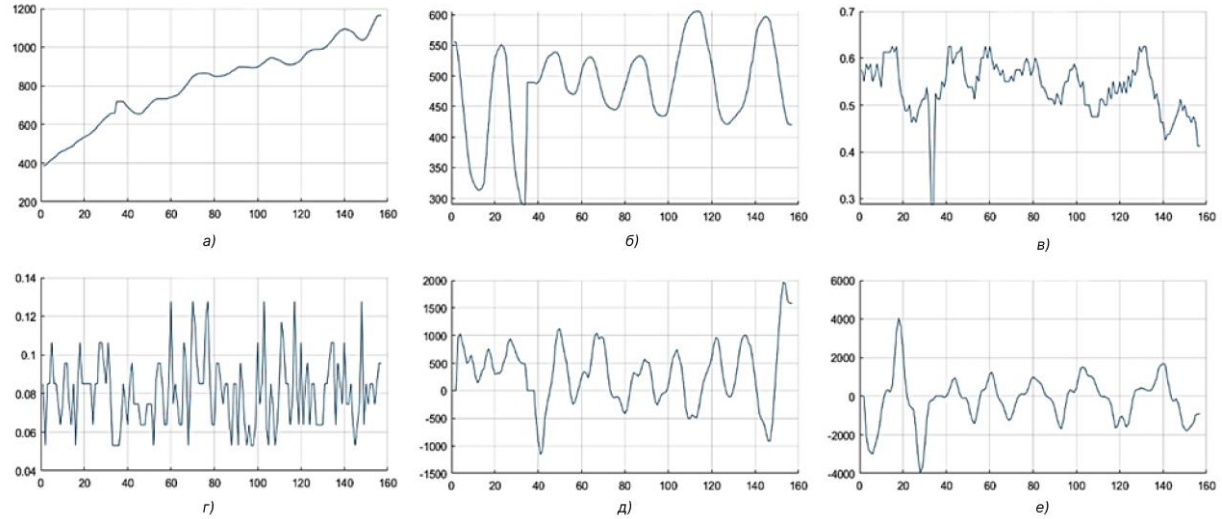
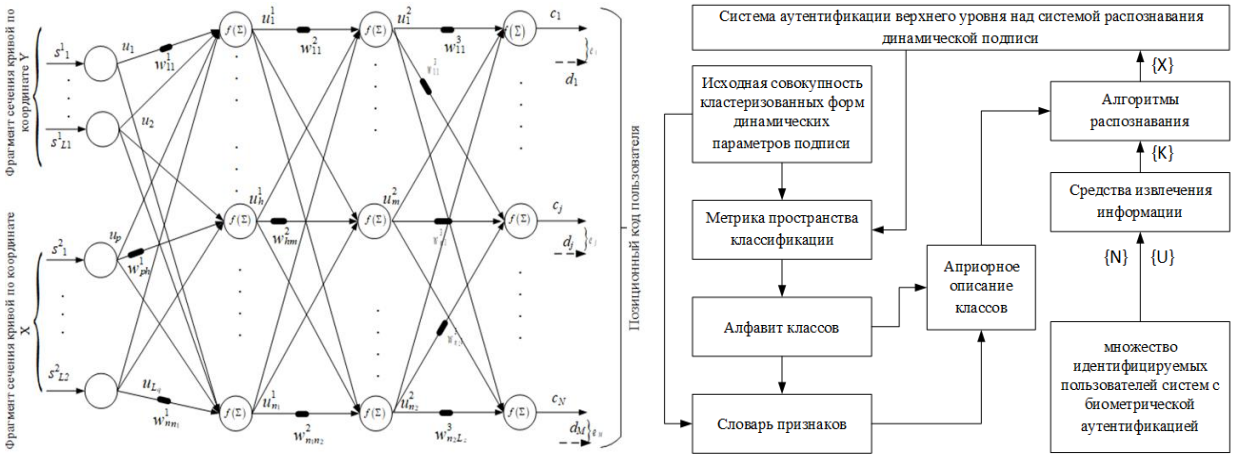


Рис. 1. Пример реализации девятимерной кривой – образца динамической подписи на интервале 180 отсчетов (2,5 с): *а* – координата пера *x*; *б* – координата пера *y*; *в* – давление пера; *г* – площадь контакта; *д* – скорость пера по оси *x*; *е* – скорость пера по оси *y*

Fig. 1. Example of the implementation of a nine-dimensional curve, representing a dynamic signature sample over an interval of 180 samples (2,5 s): *а* – pen x-coordinate; *б* – pen y-coordinate; *в* – pen pressure; *г* – contact area; *д* – pen velocity along the x-axis; *е* – pen velocity along the y-axis

Основным инструментом для распознавания фрагментов многомерной кривой подписи является многослойная нейронная сеть (НС) BProp [13], архитектура которой представлена ниже (рис. 2, *а*).



а *б*

Рис. 2. Применение алгоритмов распознавания динамической подписи: *а* – архитектура многослойной нейронной сети; *б* – общая схема взаимодействия модулей распознавания

Fig. 2. Application of dynamic signature recognition algorithms: *а* – architecture of a multilayer neural network; *б* – general scheme of interaction of recognition modules

Описание процесса постановки динамической подписи [14] и процесса распознавания (для повышения достоверности и надежности) несколькими алгоритмами [15] с последующим мажоритарным голосованием организуется в

соответствии со схемой взаимодействия модулей (рис. 2, *б*).

В основе исследовательской базы данных и доказательной фактуры настоящих исследований лежит база данных MOBLSIG [16], представляющая собой набор динамических подписей 83 пользователей (49 мужчин, 34 женщины), полученных с помощью мобильного устройства с емкостным сенсорным экраном (планшет Nexus 9, Android 6.0) [17]. Данные каждого пользователя содержат 45 истинных и 20 поддельных реализаций его подписи, каждая из которых представлена в формате файла «*.csv» (рис. 3).

Рис. 3. Исходное файловое представление динамической подписи

Fig. 3. Original file representation of a dynamic signature

Файл содержит от 120 до 160 отсчетов по одиннадцати параметрам динамической подписи, из которых в силу зашумленности и слабой информативности используются восемь:

1) *x* – проекция текущего положения пера на ось *x*;

2) *y* – проекция текущего положения пера на ось *y*;

3) *pressure* – текущая сила давления пера на экран;

4) *velocityx* – проекция вектора скорости пера на ось *x*;

5) *velocityy* – проекция вектора скорости пера на ось *y*;

6) *accelx* – проекция ускорения пера на ось *x*;

7) *accely* – проекция ускорения пера на ось *y*.

8) *accelz* – проекция ускорения пера на ось *z*.

Рассмотрим общую структуру макета программного комплекса моделирования процессов эталонирования и распознавания реализаций динамической подписи пользователя (рис. 4).

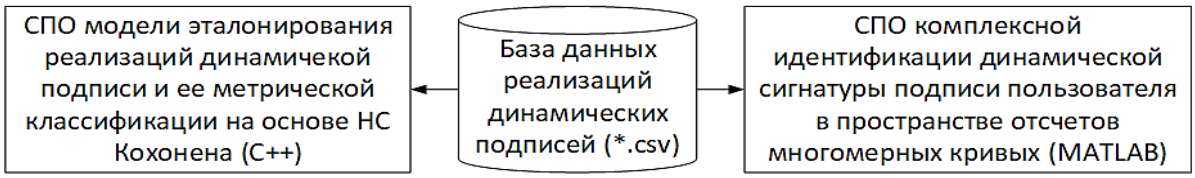


Рис. 4. Общая структура макета программного комплекса

Fig. 4. General structure of the software system prototype

В результате реализации сценария образования обучающих и проверочных выборок формируются параллелепипеды размерностью $n = 3$ с размерами $[l_1, l_2, l_3]$, где l_1 – число реализаций динамической подписи; l_2 – максимальная длительность подписи (отсчётов); l_3 – число кривых каждой подписи.

Нейросетевые алгоритмы распознавания используют два типа архитектуры сетей – со скалярной и векторной функцией выхода (вида [–1, –1, … –1, 1, –1,…, –1], где позиция единицы как компонент вектора указывает на реализацию конкретного пользователя) (рис. 5). Корректировка весов осуществлялась на основании алгоритма Левенберга – Марквардта [7]:

$$w_j(k+1) = w_j(k) + (J_j(k)J_j^T(k) + \chi I)^{-1} \times \times J_j(k)(d_j(k) - f(w_j^T(k)x(k))), \quad (1)$$

где χ – скалярный параметр; I – единичная матрица; $d_j(k)$ – выход j-го нейрона выходного слоя; $J_j(k) = \nabla_{Wj} f\left(w_j^T x(k)\right)$ – якобиан, матрица частных производных по весам w_j на k-й итерации обучения.

По результатам обучения формируются графики сходимости НС и визуализируются кривые подписей, использованные как входные векторы (рис. 6).

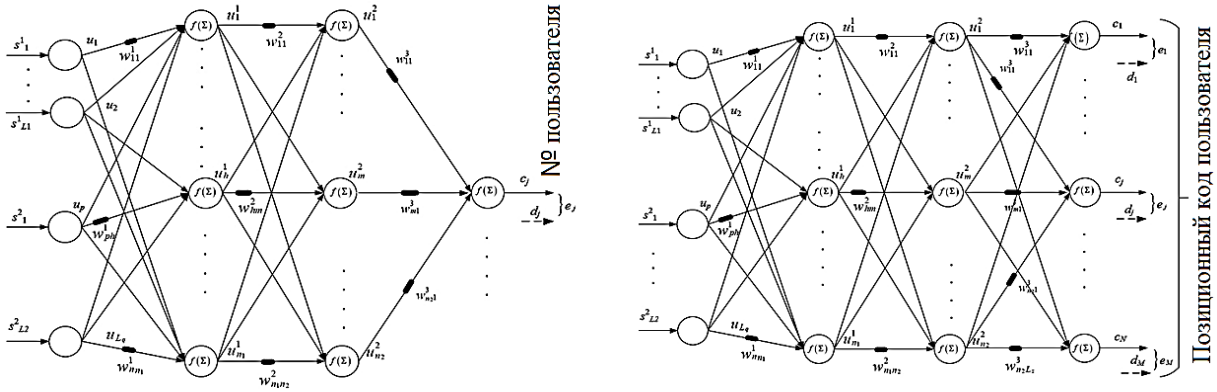


Рис. 5. Архитектуры НС вида BProp для идентификации многомерной реализации динамической подписи

Fig. 5. BProp-type neural network architectures for multidimensional dynamic signature identification

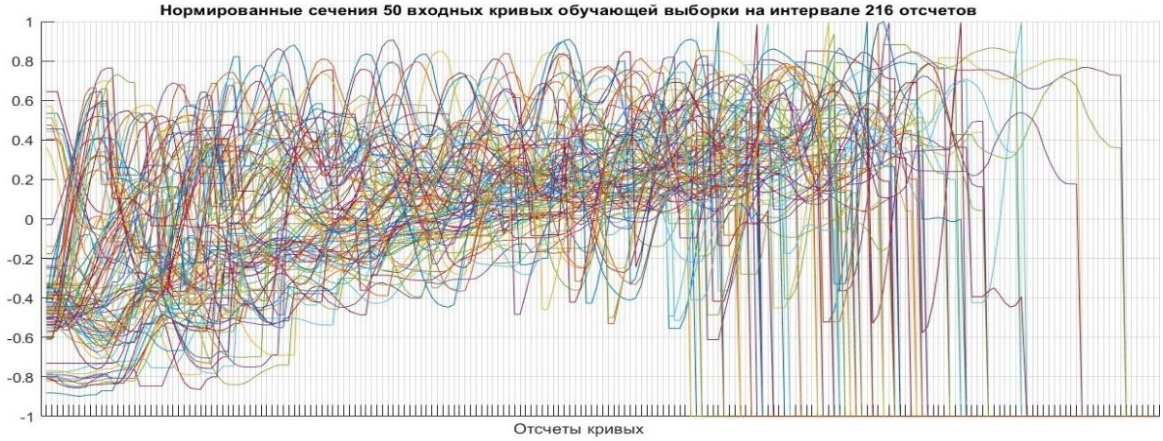


Рис. 6. Кривые подписей, использованные как входные векторы НС

Fig. 6. Signature curves used as input vectors of the neural network

Графический анализ такого рода данных позволяет экспертным способом оптимизировать процесс параметрического синтеза сети.

Результаты и их обсуждение

Число скрытых слоев НС в экспериментах варьировалось от одного до четырех при максимальной длине одной реализации подписи в 260 отсчетах. На рисунке 7 представлены усредненные по 30-ти точкам, 6-ти алгоритмам зависимости достоверности идентификации пользователя от числа кривых его динамической сигнатуры, участвующих в распознавании.

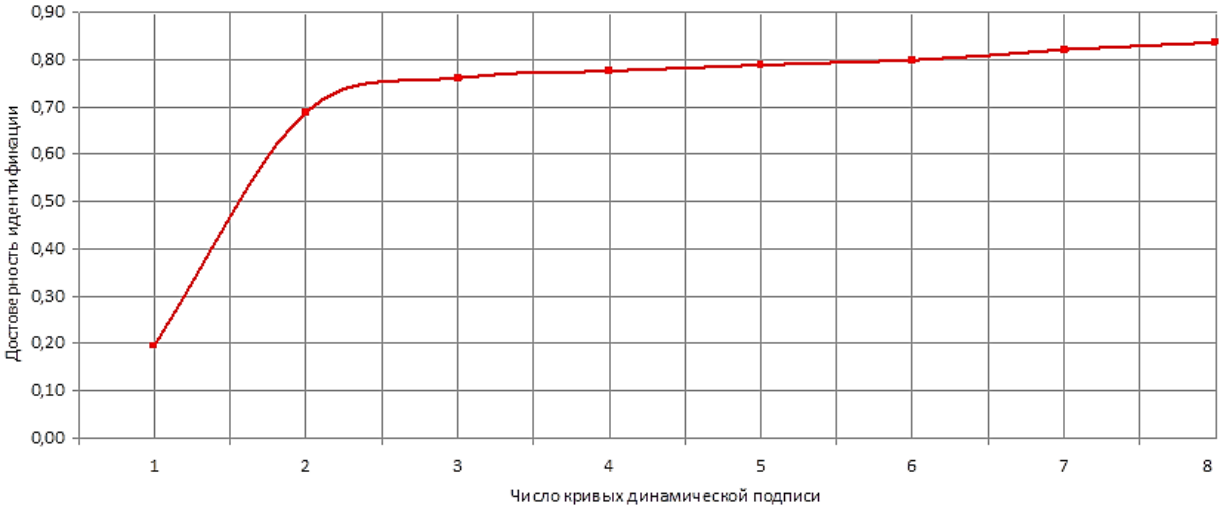


Рис. 7. Усредненная зависимость достоверности идентификации от числа кривых по выборке из 50-ти пользователей (в каждой точке графика усредненные результаты распознавания 10-ти пользователей из протокола испытаний (проверочной выборки), по 20 реализаций подписина каждого)

Fig. 7. Average dependence of identification reliability on the number of curves for a sample of 50 users (each point of the graph shows the averaged recognition results for 10 users from the test protocol (validation set), with 20 signature realizations per user)

Зависимость свидетельствует о том, что 3-5 основных параметров: две координаты x и y в плоскости реализации планшета, давление на экран в совокупности с векторами скорости пера по x и y – обеспечивают приемлемую достоверность идентификации.

Дальнейший рост числа кривых позволяет незначительно повысить достоверность [18], при этом сильно увеличив ресурсоемкость вычислений, т. к. алгоритм Левенберга – Марквардта требует построения матрицы Якоби J [19]:

$$\left(H+\alpha I\right)\delta = J^{\mathrm{T}}Ea,$$

$$J=\begin{bmatrix} \dfrac{\partial F\left(x_1,w\right)}{\partial w_1} & \cdots & \dfrac{\partial F\left(x_1,w\right)}{\partial w_M} \\ \cdots & \cdots & \cdots \\ \dfrac{\partial F\left(x_N,w\right)}{\partial w_1} & \cdots & \dfrac{\partial F\left(x_N,w\right)}{\partial w_M} \end{bmatrix}, \quad (2)$$

где $F(x_i,w)$ – значение выхода НС на i-й входной вектор X.

На рисунке 8 приведена усреднённая зависимость достоверности идентификации кривой (а по ней и пользователя) в зависимости от числа примеров обучающей выборки и числа пользователей.

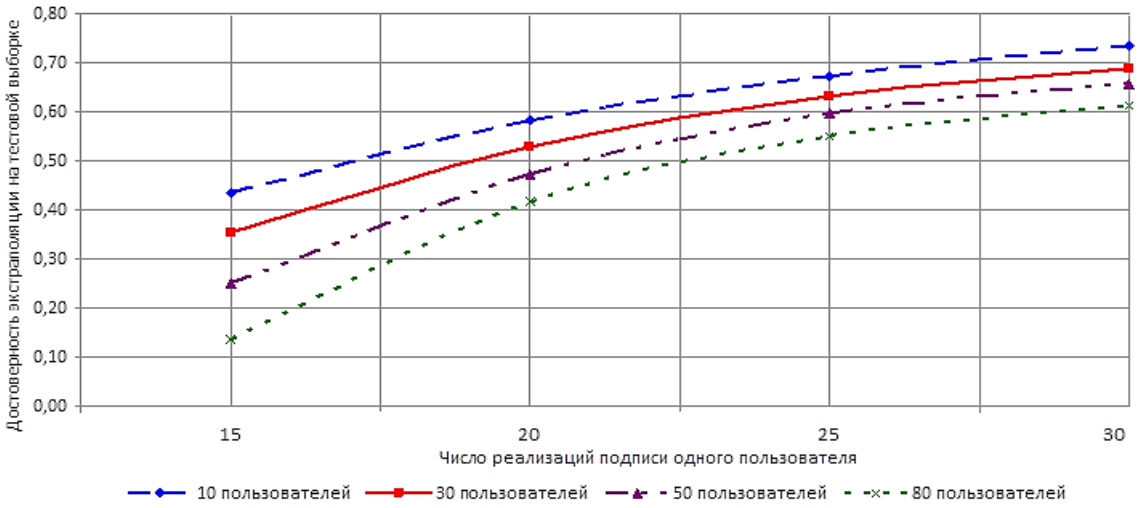


Рис. 8. Зависимость достоверности идентификации динамической подписи в зависимости от числа примеров обучающей выборки при фиксированном числе пользователей

Fig. 8. Dependence of dynamic signature identification reliability on the number of training samples for a fixed number of users

Анализ кривых (рис. 8) позволяет предположить, что для обеспечения заданных показателей надежности аутентификации пользователя необходимо декомпозировать аппаратно-программные модели идентификации динамической подписи по группам небольшого числа пользователей [20].

На рисунке 9 представлены зависимости идентификации динамической подписи пользователя от числа пользователей при фиксированных архитектурных параметрах НС, объемов обучающих – проверочных выборок.

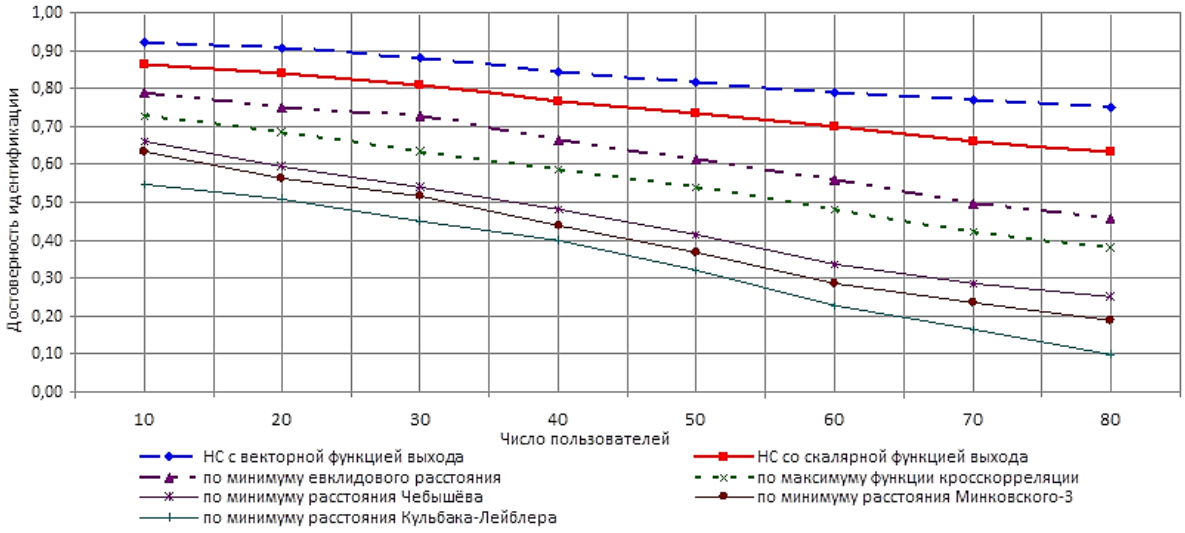


Рис. 9. Зависимость достоверности идентификации динамической подписи пользователя от числа пользователей (обучающих реализаций – 30, проверочных – 15 по каждому пользователю, кривых – 5 [x, y, p, v_x, v_y])

Fig. 9. Dependence of dynamic signature identification reliability on the number of users (30 training realizations and 15 test realizations per user, 5 curves per signature [x, y, p, v_x, v_y]))

Графический анализ зависимостей (рис. 9) свидетельствует о преимуществах НС с векторной функцией выхода над остальными алгоритмами. Статистический алгоритм Кульбака – Лейблера предсказуемо показал низкую достоверность в силу наличия шумов микротремора руки при постановке, что может быть компенсировано адаптивным сглаживанием в схеме аппаратно-программного комплекса биометрической аутентификации. Средний выигрыш от применения разработанных моделей и алгоритмов идентификации подписи по сравнению со статистическими методами составил 25–35%, по сравнению с метрическими – от 5 до 15%.

Выводы

Экспериментально исследованы алгоритмы нейросетевой идентификации динамической сигнатуры подписи пользователя в пространстве отсчетов многомерных кривых в сравнении с оптимальными алгоритмами обнаружения – различений многомерных сигналов. Эксперименты показали, что 3–5 основных параметров: две координаты пера в плоскости реализации планшета, давление на экран в совокупности с векторами скорости пера – обеспечивают приемлемую достоверность идентификации в интервале 0,8…0,95 в условиях малого числа пользователей и сохраняются на уровне 0,7 при их неограниченном увеличении.

Для обеспечения заданных показателей надежности аутентификации пользователя необходимо декомпозировать аппаратно-программные модели идентификации динамической подписи по группам небольшого числа пользователей. Существует оптимальное число и набор алгоритмов, доставляющих максимум достоверности результата комплексирования: метрический в евклидовой метрике, корреляционный и нейросетевой. Эксперименты показали преимущества НС с векторной функцией выхода над остальными алгоритмами. Статистический алгоритм Кульбака – Лейблера показал низкую достоверность в силу наличия шумов микротремора руки при постановке, что может быть компенсировано адаптивным сглаживанием в схеме аппаратно-программного комплекса биометрической аутентификации.

Список литературы

1. Биометрия в финансовой сфере 2020: выгоды для потребителя. Аналитическая записка. URL: https://www.fintechru.org/upload/iblock/659/g6k39ftq1hkehkn4b22znw1vsfa9lsrg.pdf?ysclid=mjlc9613ot802675625 (дата обращения: 04.09.2025).

2. Ломов Н., Петрова Д., Рязанцева Ю. Биометрия в финансовой сфере 2020: Выгоды для потребителя // Аналитическая записка. URL: https://www.fintechru.org/analytics/analiticheskaya-zapiska-po-biometrii/?ysclid=lvwb2x h8z610856013 (дата обращения: 06.09.2025).

3. Биометрия: что это и как она влияет на мир финансов // Frank Media. URL: https://frankmedia.ru/137504?ysclid=lvwb85nb3o106633262 (дата обращения: 05.05.2025).

4. Отчет об анализе размера, доли и тенденций мирового рынка биометрических систем – обзор отрасли и прогноз до 2032 года. URL:

https://www.databridgemarketresearch.com/ru/reports/global-biometric-system-market?ysclid=lvwg0cfco7989485412 (дата обращения: 05.09.2025).

5. Handbook of Biometric Anti-Spoofing. Presentation Attack Detection and Vulnerability Assessmen / S. Marcel, M. S. Nixon, J. Fierrez, N. Evans. Singapore: Springer, 2023. 595 p.

6. Jain A. K., Griess F. D., Connell S. D. Online signature verification // Pattern Recognition. 2022. N 35. P. 2963–2972.

7. Ростовцев В. С. Искусственные нейронные сети. 4-е изд. СПб.: Лань. 2024. 216 с.

8. Бишоп К. М. Распознавание образов и машинное обучение. СПб.: Диалектика, 2020. 960 с.

9 Carmona P. L., Salvador S. A., Fred L. N. Mathematical Methodologies in Pattern Recognition and Machine Learning: Contributions from the International Conference on Pattern Recognition Applications and Methods. Springer, 2020. 204 p.

10. Kevin P. Murphy. Probabilistic Machine Learning: Advanced Topics. MIT Press, 2023. 1175 p.

11. Rawlson K. Explainer: Signature Recognition. URL: https://www.biometricupdate.com/201601/explainer-signature-recognition (дата обращения: 26.09.2025).

12. Signature Verification System // Elsevier. Marketing. URL: https://www.elsevier.marketing/journal/Pattern-Recognition (дата обращения: 26.09.2025).

13. Танцеров А. Х., Данилов Е. А. Кинематическая модель формирования эталонных динамических параметров подписи пользователя // Вестник Рязанского государственного радиотехнического университета. 2025. № 92. С. 170–178. https://doi.org/10.21667/1995-4565-2025-92-170-178

14. Learning hierarchical features for scene labeling / C. Farabet, C. Couprie, L. Najman, Y. LeCun // IEEE Transactions on Pattern Analysis and Machine Intelligence. 2023. N 8 (35). P. 1915–1929.

15. Сюй А., Аминиан А. System Design. Машинное обучение. Подготовка к сложному интервью. СПб.: Питер, 2024. 320 с.

16. Танцеров А. Х., Данилов Е. А., Мартышкин А. И. Обзор и сравнение некоторых методов аутентификации подписи по динамическим параметрам // Вестник Рязанского государственного радиотехнического университета. 2025. № 92. С. 213–224. https://doi.org/10.21667/1995-4565-2025-92-213-224

17. Антал М., Сабо Л. Ж, Тордаи Т. Онлайн-проверка подписи на корпусе отпечатков пальцев MOBISIG, 2018. URL: http://www.ms.sapientia.ro/~manyi/mobisig/MOBISIG.ZIP, (дата обращения: 01.09.2025).

18. Suratgar A. A., Tavakoli M. B., Hoseinabadi A. Modified Levenberg-Marquardt method for neural networks training. 2022. P. 1745–1747.

19. Sousa, C. Neural network learning by the Levenberg-Marquardt algorithm with Bayesian regularization (part 1). URL: http://crsouza.blogspot.com/2009/11/neural-network-learning-by-levenberg_18.html (дата обращения: 05.09.2025).

20. Танцеров А. Х., Данилов Е. А. Современные подходы к распознаванию и аутентификации подписей: методы обработки изображений // XXI век: итоги прошлого и проблемы настоящего плюс. 2025. Т. 14, № 2 (70). С. 71–76. EDN SCSZTT

References

1. Biometrics in the financial sector 2020: benefits for the consumer. Analytical note. (In Russ.) Available at: https://www.fintechru.org/upload/iblock/659/g6k39ftq1hkehkn4b22znw1vsfa9lsrg.pdf?ysclid=mjlc9613ot802675625 (accessed: 04.09.2025).

2. Lomov N., Petrova D., Ryazantseva Y. Biometrics in the financial sector 2020: Benefits for consumers // Analytical note. URL: https://www.fintechru.org/analytics/analiticheskaya-zapiska-po-biometrii/?ysclid=lvwb2x h8z610856013 (accessed 06.06.2025).

3. Biometrics: what it is and how it affects the world of finance. Frank Media. (In Russ.) Available at: https://frankmedia.ru/137504?ysclid=lvwb85nb3o106633262 (accessed 05.09.2025).

4. Report on the analysis of the size, share and trends of the global biometric systems market – industry overview and forecast up to 2032. (In Russ.) Available at: https://www.databridgemarketresearch.com/ru/reports/global-biometric-system-market?ysclid=lvwg0cfco7989485412 (accessed 05.09.2025).

5. Marcel S., Nixon M. S., Fierrez J., Evans N. Handbook of Biometric Anti-Spoofing. Presentation Attack Detection and Vulnerability Assessmen. Singapore: Springer; 2023. 595 p.

6. Jain A.K., Griess F.D., Connell S.D. Online signature verification. *Pattern Recognition*. 2022;(35):2963–2972.

7. Rostovtsev V.S. Artificial neural networks. 4th ed. Saint Petersburg: Lan'; 2024. 216 p. (In Russ.)

8. Bishop K.M. Pattern recognition and machine learning. Saint Petersburg: Dialektika Publ., 2020. 960 p. (In Russ.)

9. Carmona P.L., Salvador S.A., Fred L.N. Mathematical Methodologies in Pattern Recognition and Machine Learning: Contributions from the International Conference on Pattern Recognition Applications and Methods. Springer, 2020. 204 p.

10. Kevin P. Murphy. Probabilistic Machine Learning: Advanced Topics. MIT Press; 2023. 1175 p.

11. Rawlson K. Explainer: Signature Recognition. Available at: https://www.biometricupdate.com/201601/explainer-signature-recognition (accessed 26.09.2025).

12. Signature Verification System. Elsevier. Marketing. Available at: https://www.elsevier.marketing/journal/Pattern-Recognition (accessed 26.09.2025).

13. Tantserov A.Kh., Danilov E.A. Kinematic model of the formation of the etalon dynamic parameters of the user's signature. *Vestnik Ryazanskogo gosudarstvennogo radiotekhnicheskogo universiteta = Bulletin of the Ryazan State Radio Engineering University*. 2025;(92):170–178. (In Russ.) https://doi.org/10.21667/1995-4565-2025-92-170-178

14. Farabet C., Couprie C., Najman L., LeCun Y. Learning hierarchical features for scene labeling. *IEEE Transactions on Pattern Analysis and Machine Intelligence*. 2023;(8):1915–1929.

15. Xu A., Aminian A. System Design. Machine learning. Preparation for a difficult interview. Saint Petersburg: Piter; 2024. 320 p. (In Russ.)

16. Tantserov A.Kh., Danilov E.A., Martyshkin A.I. Review and comparison of some methods of signature authentication by dynamic parameters. *Bulletin of the Russian State*

Radio Engineering University. 2025;(92):213–224. (In Russ.) https://doi.org/10.21667/1995-4565-2025-92-213-224

17. Antal M., Szabo L. J., Tordai T. Online verification of the signature on the fingerprint case MOBISIG, 2018. (In Russ.) Available at: http://www.ms.sapientia.ro/~manyi/mobisig/MOBISIG.ZIP, (accessed 01.09.2025).

18. Suratgar A.A., Tavakoli M.B., Hoseinabadi A. Modified Levenberg-Marquardt method for neural networks training. 2022. P. 1745–1747.

19. Sousa, C. Neural network learning by the Levenberg-Marquardt algorithm with Bayesian regulation (part 1). Available at: http://crsouza.blogspot.com/2009/11/neural-network-learning-by-levenberg_18.html (accessed 05.09.2025).

20. Tanzerov A.Kh., Danilov E.A. Modern approaches to signature recognition and authentication: image processing methods. *XXI vek: itogi proshlogo i problemy nastoyashchego plyus = XXI Century: the Results of the Past and the Problems of the Present Plus*. 2025;14(2):71–76. (In Russ.) EDN SCSZTT

Информация об авторах / Information about the Authors

Танцеров Александр Хабибуллоевич,
аспирант кафедры программирования,
Пензенский государственный технологический институт, г. Пенза, Российская Федерация,
e-mail: alex.tancerov@mail.ru,
Researcher ID: O-0537-2025,
ORCID: 0009-0006-7695-0514

Данилов Евгений Александрович,
кандидат технических наук, доцент кафедры программирования, Пензенский государственный технологический институт, г. Пенза, Российская Федерация,
e-mail: danilov@penzgtu.ru,
Researcher ID: OUI-0415-2025,
ORCID: 0000-0003-4114-7036

Alexander K. Tantserov, Postgraduate at the Department of Programming,
Penza State Technological Institute,
Penza, Russian Federation,
e-mail: alex.tancerov@mail.ru,
Researcher ID: O-0537-2025,
ORCID: 0000-0003-4114-7036

Evgeny A. Danilov, Candidate of Sciences (Engineering), Associate Professor at the Department of Programming,
Penza State Technological Institute,
Penza, Russian Federation,
e-mail: danilov@penzgtu.ru,
Researcher ID: OUI-0415-2025,
ORCID: 0000-0003-4114-7036