ORES
Научно-практический электронный журнал
Оригинальные исследования (ОРИС), *ISSN 2222-0402*
www.ores.su
original-research.ru

СОВРЕМЕННЫЕ ПРОБЛЕМЫ АЛГОРИТМОВ ВЕРИФИКАЦИИ ДИНАМИЧНЫХ РУКОПИСНЫХ ПОДПИСЕЙ

Дзямко-Гамулец Роман Николаевич,
Аспирант
Московский технический университет связи и информатики
Факультет кибернетики и информационной безопасности, кафедра экологии, безопасности жизнедеятельности и электропитания
roman.dzyamko-gamulets@outlook.com

Иевлев Олег Павлович,
Кандидат технических наук
Московский технический университет связи и информатики
Факультет кибернетики и информационной безопасности
ievlev@mtuci.ru

Аннотация

Алгоритмы верификации динамичных рукописных подписей человека становятся всё более актуальными в контексте обеспечения информационной безопасности и биометрической аутентификации. Однако, несмотря на активное развитие данной области, существует ряд нерешённых проблем, связанных с высокой вариативностью подписей, недостаточной устойчивостью к подделкам и ограниченностью используемых датасетов. В данной статье проводится обзор современных методов верификации, выделяются ключевые проблемы, а также предлагаются направления для будущих исследований.

Ключевые слова: динамическая рукописная подпись, биометрическая аутентификация, машинное обучение, верификация подписи.

MODERN PROBLEMS OF DYNAMIC HANDWRITTEN SIGNATURE VERIFICATION ALGORITHMS

Dzyamko-Gamulets Roman Nikolaevich,
Master
Moscow Technical University of Communications and Informatics
Faculty of cybernetics and information security, department of ecology, life safety and power supply

Ievlev Oleg Pavlovich,
Candidate of technical sciences
Moscow Technical University of Communications and Informatics
Faculty of cybernetics and information security

ABSTRACT

Algorithms for verifying dynamic handwritten signatures are becoming increasingly relevant in the context of information security and biometric authentication. Despite the active development of this field, there remain a number of unresolved issues related to high variability in signatures, limited resistance to forgery and restricted size and diversity of available datasets. This article provides an overview of current methods in signature verification, highlights key challenges, and suggests directions for future research.

Keywords: dynamic handwritten signature, biometric authentication, machine learning, signature verification.

Введение

С ростом цифровизации и удалённого взаимодействия всё более востребованными становятся надёжные методы аутентификации пользователей. Биометрическая аутентификация на основе рукописной подписи представляет собой удобный и привычный способ подтверждения личности. При этом динамические характеристики подписи, такие как скорость, ускорение, нажим, и координаты пера во времени, обеспечивают дополнительный уровень защиты по сравнению с традиционной (статической) подписью [1]. Тем не менее, алгоритмы верификации сталкиваются с рядом вызовов, обусловленных как техническими, так и человеческими факторами. Подпись человека подвержена изменчивости в зависимости от физиологического состояния, настроения, устройства ввода и внешних условий [2]. Это затрудняет построение универсальных и устойчивых моделей.

Актуальные проблемы

Современные подходы к верификации рукописных подписей можно условно разделить на две группы:

Классические методы машинного обучения [3]:

- Использование признаков, извлечённых вручную (например, средняя скорость, дисперсия давления, количество пиков ускорения);
- Классификаторы: k-ближайших соседей (k-NN), SVM, решающие деревья и ансамбли (Random Forest, AdaBoost).

Методы глубокого обучения [4]:

- Свёрточные нейронные сети (CNN), применяемые к представлению подписи в виде изображений или спектрограмм;
- Рекуррентные нейронные сети (RNN, LSTM, GRU), обрабатывающие временные ряды параметров подписи;
- Комбинированные архитектуры: CNN + RNN, Transformer.

Выше перечислены лишь часть методов верификации на сегодняшний день, каждый метод использует свои уникальные алгоритмы верификации и способы оценки эффективности. Однако, чтобы любой из методов мог найти активное применение в офлайн и онлайн системах, показатели ошибок I и II рода должны удовлетворять современным требованиям пользователей, как в лабораторных, так и в обыденных условиях.

Несмотря на успехи, достигнутые в области верификации, существуют многочисленные проблемы, ограничивающие точность и надёжность современных алгоритмов:

Высокая внутриклассовая вариативность

Подписи одного и того же человека могут значительно отличаться друг от друга, особенно в долгосрочной перспективе. Алгоритмы часто неспособны различать допустимые вариации от подделок, что приводит либо к ложным отклонениям, либо к ошибочному принятию.

Ограниченность и несбалансированность датасетов

Существующие публичные наборы данных (например, BioSecure, MCYT, SVC2004, SigWiComp) имеют ограниченное количество участников и сессий. Часто наблюдается перекос между числом подлинных подписей и имитаций, что усложняет обучение устойчивых моделей [5].

Сложность генерации реалистичных подделок

Большинство датасетов используют имитации, выполненные вручную (skill forgeries), что не отражает уровень угрозы от современных методов генерации (например, GAN, deepfake-подписи). Это снижает актуальность оценок устойчивости алгоритмов к подделкам [6].

Отсутствие стандартизации оценки

Разные исследования используют различные метрики (FAR, FRR, EER), способы препроцессинга и кросс-валидации. Это затрудняет объективное сравнение результатов и воспроизводимость экспериментов.

Адаптация к устройствам и условиям ввода

Модели часто оказываются чувствительными к типу планшета или стилуса, на которых была собрана обучающая выборка. Перенос модели на новые условия без деградации точности остаётся открытой задачей.

Перспективы решения проблем

Для преодоления перечисленных ранее ограничений необходимы инновационные подходы и более гибкие методы. В данном разделе описаны перспективные направления развития систем верификации, которые уже демонстрируют обнадёживающие результаты в научной литературе и прототипах систем:

Расширение и синтетическая генерация датасетов

Применение GAN и других генеративных моделей позволяет создавать синтетические подписи, увеличивая объём данных и покрытие сценариев. При этом важно сохранять реалистичность и разнообразие [7].

Мета-обучение и few-shot learning

Данные подходы позволяют обучать модели на ограниченном количестве данных, адаптируясь к новым пользователям с минимальными примерами.

Трансферное обучение

Перенос предварительно обученных моделей (например, на больших биометрических датасетах) позволяет улучшить обобщающую способность и уменьшить потребность в данных от каждого пользователя [8].

Адаптивные и персонализированные модели

Модели, обучающиеся в процессе эксплуатации, способны подстраиваться под индивидуальные особенности пользователя и изменения его подписи во времени.

Объединение биометрических признаков

Интеграция методов верификации с другими биометрическими характеристиками (например, распознаванием лица или речи) повышает общую надёжность системы [9].

Заключение

Верификация динамичных рукописных подписей остаётся сложной, но перспективной задачей в области биометрической аутентификации. Несмотря на достигнутые успехи, существующие алгоритмы сталкиваются с рядом фундаментальных проблем, связанных с изменчивостью подписи, ограниченностью данных и угрозами подделки. Для преодоления этих вызовов требуется развитие гибких, адаптивных и устойчивых моделей, способных эффективно работать в реальных условиях. Продолжение исследований в этом направлении критически важно для повышения безопасности цифровых систем и доверия к ним со стороны пользователей.

Список литературы:

1. Береснева А.В., Епишкина А.В. Подходы к онлайн верификации собственноручной подписи // Безопасность информационных технологий. 2020. Т. 27. №2. [Электронный ресурс] // BIT.MEPHI. 2020. Режим доступа: https://bit.mephi.ru/index.php/bit/article/view/1272
2. Боровик И.Г., Зубарева М.Г. Использование нейросетевого подхода для верификации рукописной подписи // Молодой ученый. 2016. № 11 (115). С. 150-154. [Электронный ресурс] // Молодой учёный. 2018. Режим доступа: https://moluch.ru/archive/115/30581
3. Moises D., Miguel A. Ferrer, Gennaro V. Explainable Offline Automatic Signature Verifier to Support Forensic Handwriting Examiners // Neural Computing and Applications. 2023. № 36. С. 2411-2427. [Электронный ресурс] // Springer Link. 2023. Режим доступа: https://link.springer.com/article/10.1007/s00521-023-09192-7
4. Özyurt F., Majidpour J.,Tarik A. Rashid, Koç C. Offline Handwriting Signature Verification-A Transfer Learning and Feature Selection Approach // Traitement du Signal. 2023. Т. 40. №. 6. С. 2613-2622. [Электронный ресурс] // ResearchGate. 2023. Режим доступа: https://www.researchgate.net/publication/376983486_Offline_Handwriting_Signature_Verification_A_Transfer_Learning_and_Feature_Selection_Approach
5. Parziale A., Diaz., Miguel A. Ferrer, Marcelli A. SM-DTW: Stability Modulated Dynamic Time Warping for signature verification // Pattern Recognition Letters. 2019. № 121. С. 113-122. [Электронный ресурс] // ResearchGate. 2019. Режим доступа: https://www.researchgate.net/publication/380730413_SM-DTW_Stability_Modulated_Dynamic_Time_Warping_for_signature_verification
6. Tolosana R., Vera-Rodriguez R., Fierrez J., Ortega-Garcia J. DeepSign: Deep On-Line Signature Verification // IEEE Transactions on Biometrics, Behavior, and Identity Science. 2021. [Электронный ресурс] // ResearchGate. 2021. Режим доступа: https://www.researchgate.net/publication/339471818_DeepSign_Deep_On-Line_Signature_Verification
7. Албасу Ф.Б., Аль Аккад М.А. Использование методов глубокого обучения для верификации подписей // Интеллектуальные системы в производстве. 2023. Т. 21. № 3. С. 27-39. [Электронный ресурс] // ИСТУ. 2023. Режим доступа: https://izdat.istu.ru/index.php/ISM/article/view/5666/3501

8. Пятаева А.В., Мерко М.А., Жуковская В.А., Пиньчук И.А., Елисеева М.С. Распознавание рукописной подписи с применением нейронных сетей // International Journal of Advanced Studies. 2023. Т. 13. № 3. С. 130-148. [Электронный ресурс] // Elibrary. 2023. Режим доступа: https://elibrary.ru/download/elibrary_55811841_54384438.pdf
9. Мискевич П.Л., Петровец В.Н. Использование сиамской нейронной сети для верификации рукописной подписи // 60-я юбилейная научная конференция аспирантов, магистрантов и студентов БГУИР. 2024. С. 564-565. [Электронный ресурс] // БГУИР. 2024. Режим доступа: https://libeldoc.bsuir.by/bitstream/123456789/57542/1/Miskevich_Ispol%27zovanie.pdf

References:

1. Beresneva A.V., Epishkina A.V. Approaches to online verification of a handwritten signature // Security of Information Technology. 2020. Vol. 27. No. 2. [Electronic resource] // BIT.MEPHI. 2020. Access mode: https://bit.mephi.ru/index.php/bit/article/view/1272
2. Borovik I.G., Zubareva M.G. Using a neural network approach to verify a handwritten signature // Young scientist. 2016. No. 11 (115). P. 150-154. [Electronic resource] // Young scientist. 2018. Access mode: https://moluch.ru/archive/115/30581
3. Moises D., Miguel A. Ferrer, Gennaro V. Explainable Offline Automatic Signature Verifier to Support Forensic Handwriting Examiners // Neural Computing and Applications. 2023. No. 36. P. 2411-2427. [Electronic resource] // Springer Link. 2023. Access mode: https://link.springer.com/article/10.1007/s00521-023-09192-7
4. Özyurt F., Majidpour J., Tarik A. Rashid, Koç C. Offline Handwriting Signature Verification- A Transfer Learning and Feature Selection Approach // Traitement du Signal. 2023. Vol. 40. No. 6. P. 2613-2622. [Electronic resource] // ResearchGate. 2023. Access mode: https://www.researchgate.net/publication/376983486_Offline_Handwriting_Signature_Verification_A_Transfer_Learning_and_Feature_Selection_Approach
5. Parziale A., Diaz., Miguel A. Ferrer, Marcelli A. SM-DTW: Stability Modulated Dynamic Time Warping for signature verification // Pattern Recognition Letters. 2019. No. 121. P. 113-122. [Electronic resource] // ResearchGate. 2019. Access mode: https://www.researchgate.net/publication/380730413_SM-DTW_Stability_Modulated_Dynamic_Time_Warping_for_signature_verification
6. Tolosana R., Vera-Rodriguez R., Fierrez J., Ortega-Garcia J. DeepSign: Deep On-Line Signature Verification // IEEE Transactions on Biometrics, Behavior, and Identity Science. 2021. [Electronic resource] // ResearchGate. 2021. Access mode: https://www.researchgate.net/publication/339471818_DeepSign_Deep_On-Line_Signature_Verification
7. Albasu F.B., Al Akkad M.A. Using deep learning methods for signature verification // Intelligent systems in production. 2023. Vol. 21. No. 3. P. 27-39. [Electronic resource] // ISTU. 2023. Access mode: https://izdat.istu.ru/index.php/ISM/article/view/5666/3501

8. Pyataeva A.V., Merko M.A., Zhukovskaya V.A., Pinchuk I.A., Eliseeva M.S. Handwritten signature recognition using neural networks // International Journal of Advanced Studies. 2023. Vol. 13. No. 3. P. 130-148. [Electronic resource] // Elibrary. 2023. Access mode: https://elibrary.ru/download/elibrary_55811841_54384438.pdf
9. Miskevich P.L., Petrovets V.N. Using Siamese Neural Network for Verification of Handwritten Signatures // 60th Anniversary Scientific Conference of Postgraduate, Master's and Undergraduate Students of BSUIR. 2024. P. 564-565. [Electronic resource] // BSUIR. 2024. Access mode: https://libeldoc.bsuir.by/bitstream/123456789/57542/1/Miskevich_Ispol%27zovanie.pdf