

Теоретический анализ методов верификации личности по динамическим характеристикам рукописной подписи

Э.С. Анисимова

*Елабужский институт (филиал)
Казанского (Приволжского) федерального университета*

Аннотация: Данная работа посвящена теоретическому анализу и сравнительной характеристике методов и алгоритмов автоматической верификации личности по динамическим характеристикам рукописной подписи. Рассмотрены процессы сбора и предобработки динамических характеристик. Проведён анализ классических методов, включая скрытые Марковские модели, метод опорных векторов, а также современных нейросетевых архитектур, среди которых рекуррентные, свёрточные и сиамские нейронные сети. Выделены преимущества использования сиамских нейронных сетей в задачах верификации при условии малого объёма обучающих данных. Определены ключевые метрики оценки качества биометрических систем. Обобщены преимущества и недостатки рассмотренных методов, а также обозначены перспективные направления исследований.

Ключевые слова: верификация, подпись, машинное обучение, динамическая характеристика, скрытые Марковские модели, метод опорных векторов, нейросетевой подход, рекуррентные нейронные сети, свёрточные нейронные сети, сиамские нейронные сети, ошибка первого рода, ошибка второго рода, равновероятная ошибка.

Введение

Автоматическая верификация подписи является весьма актуальной задачей биометрии [1]. Она востребована в сфере финансов, в системах электронного документооборота. В отличие от статического подхода, при котором анализируется общее изображение подписи, динамический подход анализирует процесс записи подписи на графическом планшете, тем самым повышая надёжность системы верификации. Технически подпись, введённая на графическом планшете, представляет собой совокупность временных рядов, раскрывающих изменение во времени значений динамических характеристик (координат, давления, углов наклона), что открывает широкие возможности для применения алгоритмов машинного обучения [2]. Актуальность данного исследования обусловлена растущим спросом надёжных и трудно фальсифицируемых систем верификации в финансовом

секторе, системах электронного документооборота, а также на мобильных устройствах.

Сбор и предобработка данных

Для осуществления процесса сбора данных рукописной подписи необходимы определённые технические устройства: графические планшеты, стилусы для смартфонов и планшетов или специальные пэды для подписи. Данные устройства позволяют с высокой частотой дискретизации фиксировать ряд параметров (динамических характеристик) в каждый момент времени, формируя временной ряд. Основными динамическими характеристиками являются: координаты, давление, углы наклона пера [3].

Предобработка данных, как правило, включает в себя: фильтрацию шума; интерполяцию и ресэмплинг для нормализации длин временных рядов; пространственную нормализацию (масштабирование, перенос координат для обеспечения инвариантности к размеру и положению) и нормализацию давления.

Методы анализа и верификации

Разделим существующие методы верификации подписи на две основные группы: классические и нейросетевые.

Рассмотрим классические методы.

- Скрытая Марковская модель (Hidden Markov Model – HMM) – это стохастическая модель, которая идеально подходит для моделирования временных рядов. Процесс создания подписи представляется как последовательность скрытых состояний (начало штриха, основная часть, петля...). Причём каждому состоянию соответствует определённое распределение вероятностей считываемых параметров. Преимуществом данного метода является способность моделировать временную структуру

подписи. Недостатком является чувствительность метода к возможным вариациям, а также сложность определения оптимальной топологии модели [4, 5].

- Метод опорных векторов (Support Vector Machine – SVM) является одним из основных классических алгоритмов для решения задач бинарной классификации. Для применения данного метода предварительно осуществляется представление подписи в виде вектора признаков фиксированной длины. Принцип работы метода заключается в построении в пространстве признаков оптимальной разделяющей гиперплоскости, которая отделяет классы подписей друг от друга. Эффективность метода зависит от качества вектора признаков и правильного подбора функции ядра [6, 7].

В настоящее время большую популярность получили нейросетевые методы [8].

- Рекуррентные нейронные сети предназначены для обработки последовательных данных. Они способны улавливать сложные, нелинейные и долговременные зависимости в данных. Среди них выделим сети долгой краткосрочной памяти (Long Short-Term Memory – LSTM) и управляемые рекуррентные блоки (Gated Recurrent Unit – GRU), решающие проблему затухания градиента. Они содержат специальные блоки, позволяющие нейросети запоминать нужную информацию на длительное время и забывать ненужную. Нейронная сеть последовательно проходит точки подписи шаг за шагом, обновляет внутреннее состояние и в результате выдаёт векторное представление (эмбеддинг) подписи, используемое в дальнейшем при проведении классификации [9].

- Свёрточные нейронные сети используются в следующих вариантах: одномерном и двумерном. Первый вариант предполагает применение свёртки к временным рядам динамических характеристик. В этом случае нейросеть выступает в роли детектора локальных паттернов движения пера. Двумерный вариант предполагает представление подписи в виде изображения с помощью значений координат. К изображению применяется свёрточная сеть, которая извлекает визуальные паттерны (формы петель, углы штрихов, ...).
- Сиамские нейронные сети успешно применяются для решения задачи верификации подписи в условиях, когда на каждого пользователя доступно малое количество эталонных подписей. В архитектуре сиамской сети выделяют следующие составляющие: две идентичные подсети, имеющие одинаковую архитектуру и общие веса; вход, причём на вход первой подсети подаётся векторное представление тестовой подписи, а на вход второй – векторное представление эталонной подписи того же участника; модуль сравнения, вычисляющий метрику схожести между векторами признаков обеих подписей. Обучение осуществляется с использованием специальной функции потерь, минимизирующей расстояние для пар подлинных подписей, и максимизирующей его для пар подписей, из которых одна – подлинная, а другая – фальшивая. Таким образом, система учится понимать, насколько подписи похожи [10].

Метрики оценки качества

В любой системе биометрической верификации возможны ошибки первого рода (False Rejection Rate – FRR) и ошибки второго рода (False

Acceptance Rate – FAR). Ошибка первого рода есть вероятность того, что подлинная подпись будет ошибочно отклонена. Ошибка второго рода есть вероятность того, что фальшивая подпись ошибочно будет принята за подлинную.

Основными метриками оценки качества являются равновероятная ошибка (Equal Error Rate – EER) и кривая рабочей характеристики приёмника (Receiver-Operating characteristic – ROC). Равновероятная ошибка есть основная интегральная метрика для оценки качества системы и соответствует точке на кривой ошибок, где значение FRR равно значению FAR. Чем ниже EER, тем выше точность, а также надёжность системы. ROC-кривая есть график, показывающий доли верных положительных срабатываний (True Positive Rate – TPR) от доли ложных положительных срабатываний (False Positive Rate – FPR) при различных значениях порога. Чем ROC-кривая ближе к верхнему углу, тем более качественно работает система. Кроме того, площадь под кривой (Area Under Curve – AUC) является важным показателем качества.

Заключение

В данной работе был проведён теоретический анализ основных методов верификации человека по динамическим характеристикам рукописной подписи. Классические методы (HMM, SVM) хорошо изучены и менее требовательны к вычислительным ресурсам. Однако их точность в случае высокой вариативности подписи может быть недостаточно высокой. Нейросетевые методы (LSTM, свёрточные, сиамские сети) способны автоматически извлекать сложные признаки из сырых данных, не требуя ручного подбора. Рекуррентные сети (LSTM) идеально подходят для улавливания зависимостей во времени, а свёрточные – для пространственных или временных паттернов. Кроме того, точность нейросетевых методов гораздо выше, чем у классических. Отличительной чертой сиамских сетей

является возможность обучения на выборках небольшого объёма, что является обычным сценарием в реальных приложениях. Однако в целом нейросетевые методы требуют больших объёмов данных для обучения (кроме сиамских сетей) и значительных вычислительных ресурсов. Перспективным направлением будущих исследований является разработка гибридных нейросетевых моделей, сочетающих сильные стороны различных архитектур, например, свёрточной и LSTM; оптимизация нейросетевых моделей в условиях ограниченных ресурсов; исследование проблемы старения шаблона, связанной с изменением подписи с течением времени.

Благодарность за финансовую поддержку работы

Работа выполнена за счет гранта Академии наук Республики Татарстан, предоставленного молодым кандидатам наук (постдокторантам) с целью защиты докторской диссертации, выполнения научно-исследовательских работ, а также выполнения трудовых функций в научных и образовательных организациях Республики Татарстан в рамках Государственной программы Республики Татарстан «Научно-технологическое развитие Республики Татарстан».

Литература

1. Лёнина К.Н., Анисимова Э.С. Разработка и анализ признаковой модели динамической рукописной подписи // Инженерный вестник Дона, 2025, №1. URL: ivdon.ru/ru/magazine/archive/n1y2025/9754.
2. Chandra, S., 2020. Verification of dynamic signature using machine learning approach. Neural Comput & Applic, 32: 11875-11895.
3. Баянов Б.И. Методы обработки биометрических данных рукописного почерка // Инженерный вестник Дона, 2022, №12. URL: ivdon.ru/ru/magazine/archive/n12y2022/8100.

4. Pascual-Gaspar, J.M. and Cardeñoso-Payo, V., 2007. Automatic Online Signature Verification Using HMMs with User-Dependent Structure. Lecture Notes in Computer Science, 4642. URL: doi.org/10.1007/978-3-540-74549-5_110. Дата обращения 27.07.2025.
5. Martinez-Diaz, M., Fierrez, J.R., Freire, M. and Ortega-Garcia, J., 2007. On The Effects of Sampling Rate and Interpolation in HMM-Based Dynamic Signature Verification. ICDAR, 2. URL: researchgate.net/publication/4288183_On_The_Effects_of_Sampling_Rate_and_Interpolation_in_HMM-Based_Dynamic_Signature_Verification. Дата обращения 27.07.2025.
6. Meena, L., Chaurasiya, V.K., Purohit, N., and Singh, D., 2021. Comparison of SVM and Random Forest Methods for Online Signature Verification. Lecture Notes in Computer Science, 12616. URL: doi.org/10.1007/978-3-030-68452-5_30. Дата обращения 27.07.2025.
7. Rohilla, S. and Sharma, A., 2017. SVM Based Online Signature Verification Technique Using Reference Feature Vector. Proc. Natl. Acad. Sci., 87: P. 125-136.
8. Yelmati, S. and Rao, J., 2021. Online Signature Verification Using Fully Connected Deep Neural Networks. International Journal of Engineering and Manufacturing, 11: P. 41-47.
9. Salturk, S. and Kahraman, N., 2024. Deep learning-powered multimodal biometric authentication: integrating dynamic signatures and facial data for enhanced online security. Neural Comput & Applic, 36: P. 11311-11322.
10. Shen, Q., Luan, F. and Yuan, S., 2022. Multi-scale residual based siamese neural network for writer-independent online signature verification. Appl Intell, 52: P. 14571-14589.

References

1. Lyonina K.N., Anisimova E.S. Inzhenernyj vestnik Dona, 2025, №1. URL: ivdon.ru/ru/magazine/archive/n1y2025/9754.

2. Chandra, S., 2020. Neural Comput & Applic, 32: 11875-11895.
3. Bayanov B.I. Inzhenernyj vestnik Dona, 2022, №12. URL: ivdon.ru/ru/magazine/archive/n12y2022/8100.
4. Pascual-Gaspar, J.M. and V. Cardeñoso-Payo, 2007. Lecture Notes in Computer Science, 4642. URL: doi.org/10.1007/978-3-540-74549-5_110. Date accessed 27.07.2025.
5. Martinez-Diaz, M., J.R. Fierrez, M. Freire and J. Ortega-Garcia, 2007. ICDAR, 2. URL: researchgate.net/publication/4288183_On_The_Effects_of_Sampling_Rate_and_Interpolation_in_HMM-Based_Dynamic_Signature_Verification. Date accessed 27.07.2025.
6. Meena, L., V.K. Chaurasiya, N. Purohit and D. Singh, 2021. Lecture Notes in Computer Science, 12616. URL: doi.org/10.1007/978-3-030-68452-5_30. Date accessed 27.07.2025.
7. Rohilla, S. and A. Sharma, 2017. Proc. Natl. Acad. Sci., 87: 125-136.
8. Yelmati, S. and J. Rao, 2021. International Journal of Engineering and Manufacturing, 11: 41-47.
9. Salturk, S. and N. Kahraman, 2024. Neural Comput & Applic, 36: 11311-11322.
10. Shen, Q., F. Luan and S. Yuan, 2022. Appl Intell, 52: 14571-14589.

Дата поступления: 6.08.2025

Дата публикации: 25.09.25