

Классификация и теоретический анализ методов верификации динамики подписи

Э.С. Анисимова

Елабужский институт (филиал) КФУ, Елабуга

Аннотация: Данная работа посвящена теоретическому анализу методов, применяемых в задачах верификации динамики подписи, полученной с графического планшета. Проведена классификация трёх фундаментальных подходов к решению данной задачи: сопоставление с эталоном; стохастическое моделирование и дискриминативная классификация. Каждый подход в данной работе рассмотрен на примере конкретного метода: динамическая трансформация временной шкалы; скрытые Марковские модели; метод опорных векторов. Для каждого метода раскрыты теоретические основы, представлен математический аппарат, выявлены основные преимущества и недостатки. Результаты проведённого сравнительного анализа могут быть использованы в качестве необходимой теоретической базы при разработке современных систем верификации динамики подписи.

Ключевые слова: верификация, биометрическая аутентификация, динамика подписи, графический планшет, классификация методов, сопоставление с эталоном, стохастическое моделирование, дискриминативная классификация, скрытые Марковские модели, динамическая трансформация временной шкалы, метод опорных векторов, анализ временных рядов.

Введение

Сегодня проблема обеспечения надёжной биометрической аутентификации весьма актуальна [1]. Несмотря на наличие большого числа методов, использование для этой цели подписи находит достаточно широкое применение [2]. Ранее подпись рассматривалась исключительно как графический объект, но благодаря возникновению новых устройств ввода (графических планшетов (дигитайзеров), смартфонов) возникла задача анализа её динамики [3, 4]. Многообразие подходов к верификации личности по динамике подписи, основанных на разных теоретических концепциях, а также отсутствие их единой классификации и сравнительного анализа, затрудняет их объективную оценку, а также выбор модели для разработки практических приложений.

Динамика подписи

Динамика подписи описывается посредством динамических характеристик, считанных во время ввода подписи на экране планшета. Наиболее распространённый набор динамических характеристик включает в себя:

- координаты;
- давление;
- угловые характеристики (азимут, угол возвышения).

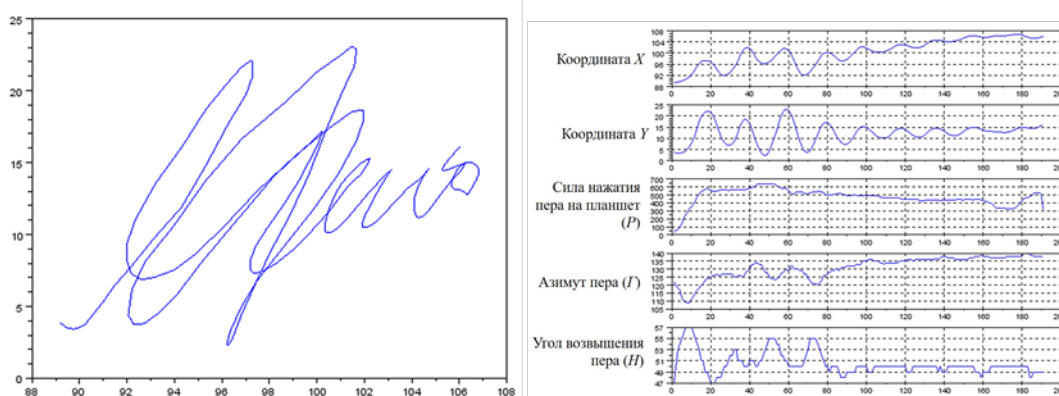


Рис. 1. – Подпись и её динамические характеристики

Подход на основе сопоставления с эталоном

Первым и наиболее наглядным подходом к задаче верификации динамики подписи является прямое сопоставление предъявленной подписи с одним (или несколькими) эталонными образцами пользователя. Суть этого подхода заключается в определении, насколько сильно новая подпись отличается от эталона.

Основная проблема здесь заключается в вариативности скорости написания, ведь один и тот же человек в разные моменты может воспроизводить подпись с разной скоростью. И тогда подписи, несмотря на схожую форму, будут иметь разную длину во времени. Для решения этой

проблемы был разработан метод динамической трансформации временной шкалы (Dynamic Time Warping, DTW) [5, 6].

Суть метода DTW заключается в нахождении оптимального выравнивания двух временных рядов, при котором бы достигался минимум суммарного расстояния между соответствующими элементами рядов. DTW ищет такую траекторию выравнивания, которая «растягивает» и «сжимает» временные оси обоих рядов, при которой будет достигнуто наилучшее совпадение их форм.

Пусть $A = (a_1, a_2, \dots, a_n)$ и $B = (b_1, b_2, \dots, b_m)$ - временные ряды, представляющие подписи (n и m – их длины).

Алгоритм DTW выполняется следующим образом:

1. Выполняется построение матрицы C локальных стоимостей размера $n \times m$, каждый элемент c_{ij} которой есть расстояние между i -ым элементом ряда A и j -ым элементом ряда B . Как правило, метрикой является евклидово расстояние.
2. Выполняется построение матрицы D аккумулярованных стоимостей размера $n \times m$, каждый элемент d_{ij} которой есть минимальная суммарная стоимость выравнивания подпоследовательностей $A' = (a_1, a_2, \dots, a_i)$ и $B' = (b_1, b_2, \dots, b_j)$. Причём $d_{ij} = c_{ij} + \min\{d_{i-1,j}, d_{i,j-1}, d_{i-1,j-1}\}$.
3. Осуществляется вычисление оптимального пути. Для этого выполняется заполнение матриц C и D , учитывая, что $d_{11} = c_{11}$. После заполнения матрицы D элемент d_{nm} будет содержать итоговую стоимость наилучшего выравнивания временных рядов, т.е. DTW-расстояние между рядами A и B . Чем меньше значение d_{nm} , тем более похожи подписи.

К преимуществам подхода относятся:

- инвариантность к скорости написания;
- интерпретируемость полученного результата;

- низкие требования к данным.

К недостаткам подхода относятся:

- высокая вычислительная сложность;
- зависимость от эталона (т.е. если в качестве эталона выбрана необычная подпись, то построенная система будет выдавать большое количество ложных отказов);
- возможность сопоставления одной точке очень длинного сегмента другого ряда;
- неспособность улавливать общие закономерности подписи.

Стохастическое моделирование

Цель данного подхода – построить математическую модель подписи и в дальнейшем в процессе верификации оценить вероятность порождения проверяемой подписи построенной моделью. Рассмотрим скрытые Марковские модели (Hidden Markov Models, HMM) [7, 8], относящиеся к рассматриваемому подходу.

Скрытая Марковская модель представляет собой статистическую модель, предполагающую, что векторы признаков подписи (в данном случае) порождаются некоторой цепью Маркова, состояния которой «скрытые», или ненаблюдаемые. В качестве скрытых состояний выступают определённые фазы написания: начало штриха, прямой горизонтальный сегмент, завершающий росчерк и т.п. Наблюдаемыми являются лишь динамические характеристики подписи.

Пусть λ - скрытая Марковская модель, $\lambda = (A, B, \pi)$. Здесь $A = \{a_{ij}\}$ - матрица вероятностей перехода; $a_{ij} = P(q_{t+1} = S_j | q_t = S_i)$ - вероятность перехода системы в скрытое состояние S_j в момент времени $t + 1$, если в момент времени t система находилась в скрытом состоянии S_i . Матрица A определяет порядок следования элементов подписи. $B = \{b_j(k)\}$ есть матрица

распределения вероятностей наблюдения; $b_j(k) = P(Q_k | q_t = S_j)$ есть вероятность генерации наблюдаемого вектора признаков Q_k в скрытом состоянии S_j . $\pi = \{\pi_i\}$ есть вектор начальных вероятностей, причём $\pi_i = P(q_1 = S_i)$ - вероятность того, что подпись начнётся со скрытого состояния S_i .

Применение НММ в задаче верификации подписи включает два этапа:

1. На основе подписей пользователя создаётся его индивидуальная λ , т.е. НММ. Выполняется поиск параметров A , B , π с помощью алгоритма Баума-Велша, который осуществляет подстраивание параметров модели для соответствия их обучающим данным. В итоге, для каждого пользователя сохраняется индивидуальная генеративная модель λ .
2. При поступлении верифицируемой подписи O , с помощью алгоритма прямого прохода вычисляется вероятность $P(O | \lambda)$ генерации моделью λ подпись O . Вычисленная вероятность сравнивается с порогом T : если $P > T$, подпись считается подлинной, иначе – поддельной.

Преимущества стохастического подхода:

- моделирование вариативности;
- основой подхода являются теория вероятностей и стохастических процессов, что обеспечивает предсказуемость;
- временная динамика в ядре модели.

К недостаткам относятся:

1. высокие требования к данным для обучения;
2. сложность выбора топологии и гиперпараметров;
3. предположение, что следующее состояние зависит только от текущего состояния;

4. сложность интерпретации.

Дискриминативная классификация

Цель данного подхода заключается в том, чтобы построить «решающую границу», которая бы наилучшим разделяла подлинные подписи от остальных. Отличительной чертой данного подхода является требование наличия не только положительных примеров (т.е. подлинных подписей), но и отрицательных (т.е. фальшивых).

Фундаментальной идеей метода опорных векторов (Support Vector Machine, SVM) [9, 10] (относящегося к данному подходу) является поиск в признаковом пространстве оптимальной гиперплоскости, т.е. гиперплоскости, которая находится на максимальном расстоянии (зазор) от ближайших объектов обоих классов. Объекты, находящиеся на границах зазора, называются опорными векторами.

В отличие от DTW и HMM, работающими с временными рядами, метод SVM требует вектор признаков фиксированной длины, т.е. преобразования подписи в набор признаков.

Применение метода SVM в задаче верификации подписи осуществляется следующим образом:

1. На основе положительных и отрицательных примеров для каждого человека создается индивидуальный SVM-классификатор.
2. При получении новой подписи выполняется её преобразование в набор признаков. Этот набор поступает на вход SVM-классификатор, который определяет, в какую область попадает набор (в область подлинных или фальшивых подписей).

Преимущества подхода:

1. высокая точность классификации.
2. низкий риск переобучения.
3. возможность находить сложные зависимости между признаками.

Среди недостатков подхода можно выделить:

1. потеря временной информации.
2. зависимость от выбора признаков.
3. необходимость наличия отрицательных примеров.
4. сложность интерпретации.

Сравнительный анализ подходов

Представим результаты сравнительного анализа подходов в виде Таблицы №1.

Таблица № 1

Сводная сравнительная таблица подходов

Критерий	DTW	НММ	SVM
Представление данных	Временные ряды	Временные ряды	Вектор фиксированной длины
Моделирование динамики	Высокое	Высокое	Отсутствует
Требования к данным	Низкие (от 1 до 5 подлинных подписей)	Средние (от 5 до 10 подлинных подписей)	Высокие (требуется также фальшивые подписи)
Интерпретируемость	Высокая	Низкая	Очень низкая
Вычислительная сложность	Обучение: отсутствует Верификация: $O(nxm)$	Обучение: затратное Верификация: быстрая	Обучение: затратное Верификация: очень быстрая
Робастность	Чувствителен к выбору эталона	Чувствителен к количеству состояний и качеству обучающей выборки	Высокая

Таким образом, выбор оптимального подхода к верификации подписи зависит от требований к системе: доступного объёма данных, требований к скорости, важности интерпретации и от того, какая информация используется для описания подписи (временные ряды или набор признаков).

Заключение

В данной работе был проведён систематический анализ и сравнение фундаментальных подходов к задаче верификации динамики подписи: DTW, НММ и SVM. Исследование показало, что не существует универсального «лучшего» метода. Выбор используемого подхода зависит специфики задачи. Для задач с минимальными требованиями к регистрации (1-5 подписей) и необходимостью интерпретации наиболее подходящим вариантом является DTW. Для задач, в которых имеется достаточное количество данных для обучения (5-10 подписей) и важна способность моделировать внутриличностную вариативность, наиболее подходящим является НММ. Для задач, в которых критически важна точность и приемлем сбор базы фальшивых подписей, SVM может демонстрировать превосходные результаты.

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. Исмагилова А.С., Н.Д. Лушников Комплексная биометрическая аутентификация пользователей информационной системы с применением нейронных сетей // Инженерный вестник Дона, 2024, №1. URL: ivdon.ru/ru/magazine/archive/n1y2024/8961.

2. Баянов Б.И. Методы обработки биометрических данных рукописного почерка // Инженерный вестник Дона, 2022, №12. URL: ivdon.ru/ru/magazine/archive/n12y2022/8100.
 3. Дорошенко Т.Ю., Костюченко Е.Ю. Система аутентификации на основе динамики рукописной подписи // Доклады ТУСУРа. 2014. №2 (32). С. 219-223.
 4. Chandra, S., 2020. Verification of dynamic signature using machine learning approach. Neural Comput & Applic, 32: 11875-11895.
 5. Kim, J.W., H.G. Cho and E.Y. Cha, 2006. A Study on Modified DTW for the Dynamic Signature Verification. Journal of Korean institute of intelligent systems, 16(6). URL: researchgate.net/publication/264152145_A_Study_on_Modified_DTW_for_the_Dynamic_Signature_Verification. Дата обращения 27.07.2025.
 6. Gwetu, M.V., 2021. A Dynamic Time Warping and Deep Neural Network Ensemble for Online Signature Verification. Lecture Notes in Computer Science, 12629. URL: doi.org/10.1007/978-3-030-70866-5_9. Дата обращения 27.07.2025.
 7. Pascual-Gaspar, J.M. and V. Cardeñoso-Payo, 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.
 8. Martinez-Diaz, M., J.R. Fierrez, M. Freire and J. Ortega-Garcia, 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.
 9. Meena, L., V.K. Chaurasiya, N. Purohit and D. Singh, 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.

10. Rohilla, S. and A. Sharma, 2017. SVM Based Online Signature Verification Technique Using Reference Feature Vector. Proc. Natl. Acad. Sci., 87: 125-136.

References

1. Ismagilova A.S., Lushnikov N.D. Inzhenernyj vestnik Dona, 2024, №1. URL: ivdon.ru/ru/magazine/archive/n1y2024/8961.
2. Bayanov B.I. Inzhenernyj vestnik Dona, 2022, №12. URL: ivdon.ru/ru/magazine/archive/n12y2022/8100.
3. Doroshenko T.YU., Kostyuchenko E.YU. Doklady TUSURa. 2014. №2. (32). pp. 219-223.
4. Chandra, S., 2020. Neural Comput & Applic, 32: 11875-11895.
5. Kim, J.W., H.G. Cho and E.Y. Cha, 2006. Journal of Korean institute of intelligent systems, 16(6). URL: researchgate.net/publication/264152145_A_Study_on_Modified_DTW_for_the_Dynamic_Signature_Verification. Date accessed 27.07.2025.
6. Gwetu, M.V., 2021. Lecture Notes in Computer Science, 12629. URL: doi.org/10.1007/978-3-030-70866-5_9. Date accessed 27.07.2025.
7. Pascual-Gaspar, J.M. and V. Cardenoso-Payo, 2007. Lecture Notes in Computer Science, 4642. URL: doi.org/10.1007/978-3-540-74549-5_110. Date accessed 27.07.2025.
8. 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.



9. 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.
10. Rohilla, S. and A. Sharma, 2017. Proc. Natl. Acad. Sci., 87: 125-136.

Дата поступления: 9.07.2025

Дата публикации: 25.08.2025