АЛГОРИТМЫ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ ПО ЕГО ДИНАМИЧЕСКОЙ ПОДПИСИ

В.Н. Максименко, *к.т.н., доцент, Московский технический университет связи и информатики, vladmaks@yandex.ru;*
Р.Н. Дзямко-Гамулец, *Московский технический университет связи и информатики, roman.dzyamko-gamulets@outlook.com.*

УДК 621.391

Аннотация. В данной работе проанализированы основные проблемы аутентификации человека по его динамической рукописной подписи. Рассмотрены варианты решения этой проблемы. Дано описание динамической рукописной подписи и ее характеристик. Рассмотрены достоинства и недостатки каждого алгоритма, а также их особенности.

Ключевые слова: динамическая подпись; порог; тензоры; временные зависимости.

ALGORITHMS FOR AUTHENTICATING A USER BY HIS DYNAMIC SIGNATURE

Vladimir Maximenko, *Candidate of Technical Sciences, docent, Moscow Technical University of Communications and Informatics;*
Roman Dzyamko-Gamulets, *Moscow Technical University of Communications and Informatics.*

Annotation. In this paper, the main problems of authenticating a person by his dynamic handwritten signature are analyzed. Options for solving this problem are considered. A description of the dynamic handwritten signature and its characteristics is given. The advantages and disadvantages of each algorithm, as well as their features, are considered.

Keywords: dynamic signature; threshold; tensors; time dependencies.

Введение

Неоспоримое преимущество биометрических систем защиты информации заключается в их высоком уровне безопасности. На сегодняшний день биометрические методы аутентификации стараются внедрять в большинстве электронных устройств и систем.

Биометрические методы аутентификации делятся на две группы: статические и динамические. Статические основаны на физиологических характеристиках человека (геометрия руки, отпечаток пальца), в то время как динамические – на поведенческих характеристиках человека (голос, клавиатурный почерк).

Среди динамических можно выделить метод аутентификации человека по его динамической рукописной подписи. В отличие от большинства статических методов аутентификации, данный метод не требует установки дополнительного оборудования для его внедрения в существующие информационные системы. Известные алгоритмы аутентификации динамической рукописной подписи [1] обладают низкой точностью, поэтому представляют интерес для дальнейших исследований с целью программной реализации и автоматизации механизма динамической рукописной подписи.

Алгоритмы верификации подписи имеют важное значение, поскольку от их

выбора зависит точность работы метода. В данной статье подробно описаны эти алгоритмы, а также методы сравнения подписей и принятия решения об их подлинности.

Методы и подходы анализа подписи

В качестве устройства ввода предполагается использование сенсорного планшета, мобильного телефона или компьютерной мышки, с помощью которых человек может оставлять свою подпись в режиме реального времени. Подпись, в которой анализируется не только итоговое изображение подписи, но и сам процесс ее получения, называется динамической (онлайн) подписью – в противоположность статической (оффлайн), где анализируется только изображение [2].

В динамической подписи данные собираются в зависимости от времени. К таким данным относятся функции координат от времени, а также давление. Следует отметить, что часто при динамической подписи могут собираться и другие данные, например, угол наклона пера. Однако задача данного исследования состоит в том, чтобы проводить аутентификацию можно было почти на любом современном мобильном устройстве среди смартфонов, планшетов, компьютеров и не только.

Из этого следует, что, в действительности, возможно получить только зависимости координат пера от времени, однако на некоторых мобильных устройствах также можно извлечь и давление. В данной работе акцент делается именно на представлении подписи как двух функций: координат по оси абсцисс и ординат от времени, то есть:

$$x = x(t),$$
$$y = y(t).$$

Из этих функций можно получить представление подписи в виде кривой на плоскости:

$$F(x, y) = 0.$$

Для аутентификации человека по его подписи необходимо установить, что имеющаяся подпись достаточно близка к тем подписям, для которых достоверно известно, что они принадлежат этому же лицу [3]. Здесь возникает вопрос о том, что понимать под термином «близость» и как ее считать на основе уже имеющихся подписей. Проанализируем различные подходы к аутентификации человека по его подписи, а также необходимые элементы для этого.

Аутентификацию подписи можно рассматривать как задачу классификации в машинном обучении [4]. Для этого необходимо иметь большой набор подписей, принадлежащих как текущему идентифицируемому лицу, так и другим лицам. На основании этих данных необходимо составить модель, которая для новых подписей могла бы прогнозировать вероятность того, что они сделаны идентифицируемым лицом. Среди алгоритмов машинного обучения можно выделить нейронные сети, метод опорных векторов, наивный байесовский классификатор, метод случайного леса.

Главный минус подобного подхода – необходимость брать чужие подписи на этапе обучения. Если требуется защитить пользователя от подделок его собственной подписи, то для обучения алгоритмов необходимо получить подписи, схожие с подлинной подписью пользователя, что сильно усложняет задачу и

требует дополнительных действий от каждого нового пользователя, поэтому для широкого применения такой метод не подходит.

Другой способ – выделение из подписи определенных признаков и сравнение двух подписей по этим признакам [5]. В этом случае необходимо поставить три задачи:

- создание алгоритма получения признаков из подписи;
- выбор способа сравнения признаков из двух разных подписей на близость, ввод понятия расстояния между признаками;
- определение расстояния между признаками, при котором две подписи будут считаться сделанными одним и тем же лицом.

Под признаками понимаются наборы чисел, полученные из функций координат подписи при помощи определенного алгоритма. Признаки могут представлять собой числа, векторы, матрицы или объекты более сложной и многомерной структуры, называемые тензорами. Числа, векторы и матрицы также относятся к тензорам, поэтому в дальнейшем можно говорить только о тензорах, как наиболее общих структурах.

Выбор алгоритма – довольно сложная задача, потому что разные алгоритмы могут акцентироваться на разных аспектах подписи. Из этого следует, что имеет смысл применять различные алгоритмы выделения признаков, а потом их результат усреднять [6]. Математическая формулировка звучит следующим образом: пусть S множество всех подписей, каждая подпись представлена парой функций $(x(t), y(t))$. Необходимо найти такое отображение f:

$$f: S \rightarrow T,$$

где: T – пространство тензоров фиксированной размерности, соответствующей алгоритму, задаваемому отображением f.

После выделения признаков и получения тензоров необходимо иметь возможность их сравнения. Математически задачу можно сформулировать следующим образом: найти отображение r:

$$r: T \times T \rightarrow \mathbb{R},$$

которое будет удовлетворять трем аксиомам метрики. Таким образом, мы получим метрическое пространство, в котором можно сравнивать два тензора, определяя расстояние между ними. Чем ближе расстояние к нулю, тем ближе тензоры, и можно считать, тем более похожи две подписи по этому признаку. Строго говоря, можно рассмотреть случаи таких функций, которые не удовлетворяют всем трем аксиомам метрики [7], но они должны соответствовать ожидаемому поведению о том, что близость к нулю означает похожесть подписей [8].

Определение порога принятия гипотезы о подлинности подписи, ниже которого две подписи считаются сделанными одним и тем же лицом, является непростой задачей. Этот порог можно оценить на основании собранной статистики и желаемых ошибок I и II рода. Для этого нужно провести множество экспериментов с настоящими и поддельными подписями и на основании этих данных построить функцию плотности распределения по метрике близости для настоящих и поддельных подписей.

Далее, имея эти функции и выбирая различные значения порога, можно посчитать ошибки I и II рода – они численно равны площадям под кривыми соответствующих функций плотностей. Исходя из практического применения,

необходимо решить, что минимизировать сильнее – ошибку I рода или II. В задаче аутентификации по подписи обычно более критической ошибкой является принятие ложной подписи как истинной, то есть ошибка II рода [9].

Математически формулировка сводится к минимизации функционала:

$$\alpha \cdot E_I(x) + \beta \cdot E_{II}(x) \rightarrow min,$$

где: $E_I(x)$ – функция ошибки I рода в зависимости от порога;

$E_{II}(x)$ – функция ошибки II рода в зависимости от порога;

α – вес ошибки I рода;

β – вес ошибки II рода.

Сами функции ошибок в зависимости от порога определяются следующим образом:

$$E_I(\tau) = \int_{\tau}^{+\infty} p_1(x)dx\,,$$
$$E_{II}(\tau) = \int_{-\infty}^{\tau} p_2(x)dx\,,$$

где: τ – величина порога;

$p_1(x)$ – плотность вероятности распределения настоящих подписей;

$p_2(x)$ – плотность вероятности распределения поддельных подписей,

причем при $i = 1, 2$, $\int_{-\infty}^{+\infty} p_i(x)dx = 1$, что следует из того, что эти функции – плотности вероятности, а вероятность их всех возможных значений равна 1.

Функции плотности определяются на основании гистограмм, полученных опытным путем, с помощью аппроксимации данных плотностей кривой. Выбор кривой плотности – отдельный вопрос, но в простейшем случае можно ограничиться линейной интерполяцией при достаточно большом количестве испытаний [10].

Необходимо отметить, что такой способ позволяет оценить лишь порог для конкретной подписи у определенного человека, и нельзя утверждать, что такое же распределение ошибок будет для других людей. Для решения этой проблемы можно эту оценку провести не на одном пользователе, а на выборке людей, и для каждого из них найти функции распределения плотностей и вычислить порог, усреднив его. Также можно найти дисперсию, чтобы понять, насколько велико распределение этих порогов.

Все ранее приведенные рассуждения справедливы в том случае, когда у нас есть одна подпись человека и нам необходимо проверить другую на сходство с ней. Однако в большинстве случаев подпись у человека может изменяться под воздействием различных факторов, таких как усталость, настроение, эмоциональное состояние, положение написания и т.д. [11]. В связи с чем, сравнение на основании только одного экземпляра подписи может быть не очень хорошим вариантом.

Для этого необходимо иметь возможность сравнивать сразу с несколькими подписями. Но простое сравнение с каждой из подписей экземпляров тоже может иметь сложности, так как шансы на совпадение подписи из определенного набора, даже весьма большого, могут быть не очень велики. Есть смысл выделить некоторую среднюю подпись человека, поточечно усреднив функции координат для всех имеющихся экземпляров подписи, и уже с ней сравнивать [12].

Также можно оценить расстояние каждой подписи из имеющихся экземпляров по выбранным признакам до средней подписи, что определит

дисперсию и среднеквадратическое отклонение. И порог в данном случае можно задавать как долю от среднеквадратического отклонения, то есть:

$$\tau = \kappa \cdot \sigma,$$

где: τ – порог;

σ – среднеквадратическое отклонение;

κ – коэффициент, подлежащий определению в зависимости от требований к ошибкам I и II рода.

Анализ подходов выделения признаков.

В конечном итоге возникает один вопрос: какой выбрать алгоритм для выделения признаков и можно ли их комбинировать? Существуют разные способы выделения признаков. Среди простейших признаков можно отметить:

- длина подписи;
- затраченное время;
- угол подписи;
- отношение высоты к ширине;
- количество разрывов линии.

Среди более сложных можно отметить следующие:

- матрица расстояний между точками кривой подписи;
- набор моментов инерции кривой подписи относительно разных осей;
- коэффициенты разложения Фурье функций координат;
- функции координат, которые можно сравнивать по занимаемой площади под кривыми;
- производные координат подписи.

Признаки по способу выделения можно разделить на две категории: те, которые учитывают временную зависимость и работают с функциями координат подписи (динамическая подпись), и те, которые учитывают только конечную геометрическую линию подписи (статическая подпись).

Поскольку разные алгоритмы могут учитывать разные характеристики подписи, предлагается комбинировать и усреднять результат их предсказаний. При оценке расстояния новой подписи от усредненной по каждому признаку можно составить общую формулу вида:

$$r = \sum_{i=1}^{n} \alpha_i \cdot r_i,$$

где: n – количество признаков;

r – итоговое расстояние;

r_i – расстояние по i-ому признаку;

α_i – коэффициент важности i-го признака. Эти веса подбираются на основании опыта, где для каждого признака независимо оценивается его точность. Тогда более точные признаки должны иметь более высокие веса.

В простейшем случае, когда все признаки равноценны, получаем:

$$r = \frac{\sum_{i=1}^{n} r_i}{n}.$$

Заключение

В современном мире биометрические методы аутентификации стараются внедрять во все сферы жизни для обеспечения безопасности, поэтому разработка и улучшение результатов их работы всегда будет актуальной задачей.

В данной статье приведены основные понятия для решения задачи аутентификации пользователя по его динамической подписи. Рассмотрено математическое представление рукописной подписи, а также математическая формулировка поставленной задачи.

Введено понятие уникальных признаков, извлекающихся из подписи, и описан способ применения этих признаков для решения задач верификации. Указаны различные алгоритмы выделения уникальных признаков и рассмотрено понятие близости подписей (или расстояние между подписями), позволяющее сравнивать два экземпляра подписи и определять степень их схожести.

Также введено понятие усредненной подписи и указаны причины ее применения. Описан способ получения единого расстояния как взвешенной комбинации расстояний по каждому признаку.

Рассмотрен алгоритм принятия решения о подлинности подписи на основании выбора порога, пропорционального среднеквадратическому отклонению имеющихся экземпляров подлинных подписей конкретного пользователя, а также описан метод получения этого порога.

Литература

1. Аникин И.В. Распознавание динамической рукописной подписи на основе нечеткой логики // Вестник КГЭУ, 2016. – № 3 (31). – С. 48-64.
2. Ворона В. А. Биометрические технологии идентификации в системах контроля и управления доступом // Computational nanotechnology, 2016. – № 3. – С. 224-241.
3. Хомяков Э.Г. Метод фазового анализа письменных объектов при проведении почерковедческих исследований: дис. канд. юрид. наук. Ижевск, 2002. – 115 с.
4. Дикий Д.И. Исследование применимости искусственных нейронных сетей для верификации пользователей по динамике почерка // Научно-технический вестник информационных технологий, механики и оптики, 2017. – Т. 17. – № 4. – С. 677-684.
5. Ходашинский И.А. Аутентификация пользователя по динамике подписи на основе нечеткого классификатора // Компьютерная оптика, 2018. – Т. 42. – № 4. – С. 657-666.
6. Ложников П.С. Разработка метода идентификации личности по динамике написания слов: автореф. дис. ... канд. техн. наук: 05.13.01. – Омск, 2004. – 22 с.
7. Бондаренко В.А. Метрические пространства: учебное пособие; Яросл. гос. ун-т им. П. Г. Демидова. – Ярославль: ЯрГУ, 2017. – 108 с.
8. Архипов В.А. Технология поиска при решении задач прикладной математики / // Вычислительные технологии, 1995. – Т. 4. – № 10. – С. 51-62.
9. Леус А.В. Биометрическая аутентификация по динамическим характеристикам подписи [Электронный ресурс], 2009. Режим доступа: http://www.secuteck.ru/articles2/sys_ogr_dost/biometrich-autentifikac-po-dinamich-harakter-podpisi/ (дата обращения: 17.01.2018).
10. Аникин И.В. Распознавание динамической рукописной подписи на основе нечеткой логики // Вестник КГЭУ, 2016. – № 3 (31). – С. 48-64.
11. Винберг А.А., Шванкова М.В. Почерковедческая экспертиза. Учебник для вузов МВД СССР. – Высшая следственная школа МВД СССР, Волгоград, 1977. – 207 с.
12. Колядин Д.В. Алгоритм выделения экстремальных точек применительно к

задаче биометрической верификации рукописной подписи // Исследовано в России, 2005. – С. 532-540.