УДК 004; 004.932
DOI: 10.37661/1816-0301-2024-21-4-72-84

Оригинальная статья
Original Article

Верификация нормализованных онлайн-подписей без вычисления динамических признаков

В. В. Старовойтов

Объединенный институт проблем информатики
Национальной академии наук Беларуси,
ул. Сурганова, 6, Минск, 220012, Беларусь
E-mail: valerys@newman.bas-net.by

Аннотация

Цели. Целью работы является исследование метода проверки подлинности подписи человека, выполненной на планшете стилусом и заданной тремя параметрами: координатами *X*, *Y* и давлением на планшет *P*.

Методы. Даны *N* подлинных динамических подписей человека. Данные, описывающие разные подписи, сделанные одним человеком, всегда имеют разное число точек. Исследованы основные варианты нормализации исходных данных подписей. По заданным подписям, которые называются модельными, строится индивидуальный образ подписей человека без вычисления динамических признаков. Для сравнения однотипных данных разных подписей используется метод динамической трансформации временно́й шкалы (Dynamic Time Warping, DTW). Результатами этого преобразования являются расстояния DTW между параметрами пар подписей. Данные расстояния служат координатами точки в трехмерном признаковом пространстве, описывающей сходство пары подписей. Множество таких точек формирует образ подлинной подписи человека. Параметры верифицируемой подписи в паре с каждой из *N* подлинных, использованных для построения образа, сравниваются на предмет близости к этому образу. Если более *N*/2 таких пар отстоит от образа подписи дальше определенного порога *T*, подпись считает фальшивой, иначе – подлинной.

Результаты. По итогам сравнительных экспериментов найден вариант нормализации исходных данных динамических подписей человека, позволяющий выполнять верификации таких подписей без использования дополнительных признаков, обычно вычисляемых по исходным данным *X*, *Y*, *P*.

Заключение. Эксперименты по формированию индивидуальных образов подписей каждого из 230 человек из общедоступной базы динамических подписей MCYT (подмножество базы DeepSignDB) и проверке подлинности 11 500 подписей, выполненных от имени этих людей, показали точность верификации 99,82 %. Из них половина подписей были подлинными, половина поддельными.

Ключевые слова: верификация, динамическая подпись, преобразование DTW, нормализация параметров, признаковое пространство

Для цитирования. Старовойтов, В. В. Верификация нормализованных онлайн-подписей без вычисления динамических признаков / В. В. Старовойтов // Информатика. – 2024. – Т. 21, № 4. – С. 72–84. – DOI: 10.37661/1816-0301-2024-21-4-72-84.

Конфликт интересов. Автор заявляет об отсутствии конфликта интересов.

Поступила в редакцию | Received 09.10.2024
Подписана в печать | Accepted 18.11.2024
Опубликована | Published 30.12.2024

Verification of normalized online signatures without calculating dynamic features

Valery V. Starovoitov

The United Institute of Informatics Problems
of the National Academy of Sciences of Belarus,
st. Surganova, 6, Minsk, 220012, Belarus
E-mail: valerys@newman.bas-net.by

Abstract

Objectives. Study of the method of verification of the authenticity of a human signature made on a tablet with a stylus and given three parameters: coordinates *X*, *Y* and pressure on the tablet *P*.

Methods. *N* genuine dynamic human signatures are given. Data describing different signatures made by one person always have a different number of points. The main variants of normalization of the original signature data are investigated. A model of an individual image of human signatures is built without calculating dynamic features. The method of dynamic time transformation (DTW) is used to compare similar data of different signatures. The results of this transformation are DTW-distances between the data of pairs of signatures. These distances serve as coordinates of a point in the feature space describing the similarity of a pair of signatures. A set of such points represents a model describing the similarity of genuine human signatures. The parameters of the signature being verified are compared with each of the *N* authentic signatures used to build the model for their proximity to the model. If more than half of these pairs are further from the model than a certain threshold *T*, the signature is considered fake.

Results. As a result of comparative experiments, a variant of normalization of initial data of dynamic human signatures was found, which allows verification of such signatures without calculating additional features usually calculated from the initial data *X*, *Y*, *P*.

Conclusion. Experiments to generate individual signature models for each of 230 people from the publicly available MCYT dynamic signature database (a subset of the DeepSignDB database) and verify the authenticity of 11,500 signatures made on behalf of these people showed a verification accuracy of 99.82 %. Half of them were genuine, half were fake.

Keywords: verification, dynamic signature, transformation DTW, parameter normalization, feature space

For citation. Starovoitov V. V. *Verification of normalized online signatures without calculating dynamic features*. Informatika [*Informatics*], 2024, vol. 21, no. 4, pp. 72−84 (In Russ.). DOI: 10.37661/1816-0301-2024-21-4-72-84.

Conflict of interest. The author declares of no conflict of interest.

Введение. Задача проверки подлинности подписи, выполненной на планшете, очень актуальна в настоящее время [1]. Подпись часто является некой производной от фамилии и имени человека. Поэтому на представление человеком подписи оказывает влияние его родной язык. Только в Индии объявлены главными 18 языков, на каждом из которых говорит более 1 млн человек, а всего на ее территории существует более 3000 языков [2]. Многие исследователи разрабатывают универсальные системы верификации подписи, не анализирующие индивидуальные особенности ее написания человеком. Поэтому применение таких систем ограничено, они работают только на подписях, подобных образцам, на которых обучались, например на китайских или западноевропейских подписях.

В настоящей работе описаны результаты исследований, полученные после опубликования статьи [3], в которой сформулирована задача верификации динамической рукописной подписи конкретного человека независимо от языка и страны проживания. В [3] представлены результаты верификации подписи, выполненной на планшете, с использованием 18 массивов динамических признаков, вычисленных по исходным данным, которые представляют подпись S в виде трех массивов: координат местоположения стилуса и давления им на планшет, т. е. $S=[X, Y, P]$, где $X=\{x_i\}$, $Y=\{y_i\}$, $P=\{p_i\}$, а i изменяется от 1 до K. Параметры S обычно регистрируются через фиксированные промежутки времени. Первая точка касания стилусом планшета имеет индекс $i=1$, последняя – $i=K$.

В работе [4] было выполнено исследование вопроса нормализации исходных данных, указанных выше, перед вычислением дополнительных динамических признаков, таких как ско-

рость и ускорение нанесения подписи в горизонтальном направлении (в плоскости *X*), вертикальном (в плоскости *Y*) и в плоскости *XY*. Скорость описывается дискретной первой производной от исходных данных, а ускорение – второй. В итоге на примерах реальных подписей разных людей показано, что при верификации подписей с использованием вычисления расстояний между динамическими признаками подписей методом DTW после мин-макс-нормализации данных *X, Y, P* снижается точность верификации.

В настоящей работе описаны результаты исследований по верификации подписей, нормализованных разными способами без вычисления динамических признаков. Верификация базируется на вычислении расстояний DTW между нормализованными исходными данными подписей *S*=[*X, Y, P*]. Выполнено сравнение разных вариантов нормализации этих данных на самой большой из доступных баз динамических подписей DeepSignDB [5] с использованием простого порогового классификатора.

Нормализация исходных данных подписи. Ряд публикаций содержит описание методов нормализации исходных параметров динамических подписей с последующим вычислением по ним признаков разных типов [6–10]. В разных статьях одинаковые методы называют поразному. Например, нормализация подписи по длине, по времени или масштабирование – это одно и то же.

Согласно статье [6] наиболее распространенным этапом предварительной обработки динамической подписи является ее нормализация. Различают несколько ее видов: нормализация горизонтального и вертикального положения (выравнивание), минимальная и максимальная нормализация, нормализация длины (масштабирование), нормализация по времени и *z*-нормализация. Также может применяться нормализация с повышением и понижением частоты дискретизации.

В работе [7] показано, что использование точек, в которых стилус был поднят, не внесло существенного улучшения в результаты классификации подписей. Экспериментальные исследования доказали, что *z*-нормализация превосходит мин-макс-нормализацию. Авторы исследовали новую комбинацию, называемую центрированной мин-макс-нормализацией, которая показала конкурентоспособные результаты, сопоставимые с *z*-нормализацией. Нормализация поворота подписи ухудшила результаты классификации более чем в 80 % случаев и не смогла обеспечить никакого улучшения производительности на подписях из трех баз данных. Исследования показывают, что ее использование более контрпродуктивно в современных классификаторах. В работе [7] также отмечено, что индивидуальные дискриминационные способности признаков *X, Y* и *P* значительно различаются в пяти базах данных. Результаты авторов показывают, что преобразование DTW эффективно компенсирует эти различия без предварительного знания о данных, хранящихся в базе, и достигает лучшей точности при использовании всех трех параметров. Они же показали, что лучшая конфигурация верификатора подписи использует *z*-нормализацию для сравнения *X, Y* и *P*>0 с использованием преобразования DTW, но она не выигрывает ни у одного из других подходов предварительной обработки данных подписи.

Авторы работы [8] исследовали четыре типа нормализации исходных данных и вычисляемых по ним признаков: без нормализации; нормализацию по времени посредством интерполяции данных кубическим сплайном и выбора 500 точек (фактически это нормализация по длине); масштабирование амплитуды значений до 1,0 и нормализацию по времени с последующей нормализацией по амплитуде. Лучшей точности авторы достигли при нормализации амплитуды, нормализация как по времени (точнее, длине массива), так и по амплитуде иногда также была полезной.

В статье [9] авторы сравнили четыре варианта нормализации исходных данных подписей. Лучшие результаты по совмещению подписей показала комбинация методов нормализации посредством масштабирования, поворота и сдвига подписи. После нормализации было применено преобразование DTW. В работе [10] выполнялась нормализация путем вычитания центра тяжести подписи и поворота.

Методы нормализации исходных данных динамической подписи условно можно разделить на три группы:

– удаление точек (или обнуление в них значений *X, Y*), в которых поднят стилус (*P*=0);

– геометрические преобразования подписи в плоскости *XY* (сдвиг, масштабирование размеров и длины, поворот подписи);

– амплитудная нормализация сигналов *X*, *Y*, *P* (*z*-нормализация, мин-макс-нормализация, обнуление среднего).

Возможны комбинации указанных методов нормализации данных. В настоящей работе исследовалось влияние на точность верификации разных вариантов нормализации исходных данных подписи *X*, *Y* и *P* согласно описанию, представленному в табл. 1.

Таблица 1
Методы нормализации исходных данных подписи

Table 1
Initial signature data normalization methods

Индекс *Index*	Функция *Function*	Описание *Description*
0	Исходные данные без изменений	Не удаляются точки x_i, y_i при p_i=0, $i \in [1; M]$
1	Обнуление *X*, *Y*, когда стилус поднят	x_i=0, y_i =0 при p_i=0
2	Удаление точек с нулевым давлением (p_i =0)	Удаляются точки, в которых поднят стилус, $z_j = x_i(p_i > 0)$
3	Обнуление среднего	$z_i = x_i - mean(x_i)$
4	Мин-макс- или [0; 1]-нормализация	$z_i = (x_i - \min(x_i)/(\max(x_i) - \min(x_i))$
5	*z*-нормализация	$z_i = (x_i - mean(x_i))/\sigma$, где σ – среднеквадратичное отклонение
6	Нормализация по длине до *L* точек	z_i – множество из *L* точек, равномерно аппроксимирующее множество $\{x_i\}$, $L>M$ или $L<M$
7	Поворот координат подписи $\{x_i,y_i\}$	Вычисляется главная компонента множества $\{x_i,y_i\}$ и угол между ней и горизонтальной осью, выполняется поворот множества точек $\{x_i, y_i\}$ на плоскости

Образ пар подлинных подписей человека. После нормализации данных, представляющих *N* подлинных подписей человека, следует сформировать образ его подписи, образованный парами подлинных подписей, и определить критерий, позволяющий отличать подлинные подписи этого человека от поддельных. Для этого строится область в признаковом пространстве, которая охватывает подписи конкретного человека. Для сравнения близости подписей, описанных нормализованными параметрами *X*, *Y*, *P*, в настоящей работе использовано преобразование DTW, на базе которого строятся наиболее точные классификаторы для анализа подлинности динамических подписей. Оно позволяет вычислять расстояния между двумя дискретными массивами, которые могут иметь разное число элементов.

Самый простой вариант образа подписей одного человека – это сфера, охватывающая множество расстояний DTW между парами *X*, *Y*, *P* подлинных подписей этого человека. Сфера представляет собой простейшую выпуклую фигуру, которая описывается координатами ее центра и радиусом. В данном случае центр совпадает с началом координат признакового пространства, поскольку расстояния не могут быть отрицательными. Остается один параметр, радиус *R*, описывающий $N(N–1)$ точек. Он равен максимальной длине векторов, соединяющих начало координат признакового пространства с точками, соответствующими образцам пар подлинных подписей. Радиус *R* может служить порогом при верификации:

$$T_1 = R = max\{\ \mathrm{dtw}(X_k,X_m),\ \mathrm{dtw}(Y_k,Y_m),\ \mathrm{dtw}(P_k,P_m)\ \},$$

где *k*, *m* означают номера двух подписей из *N* подлинных. Такой сферический образ строится для пар подписей каждого человека индивидуально. Преимущества образа заключаются в том, что он не зависит от родного языка подписанта и строится на базе *N* подлинных подписей всего одного человека, при этом поддельные не используются. Поскольку подпись человека достаточно вариативна, то при построении ее образа по разным подлинным наборам подписей человека значение радиуса сферы будет немного изменяться. В связи с этим можно использовать формулы вычисления порога *T*, адаптивно изменяющие радиус *R* в зависимости от числа используемых подлинных подписей *N* или других параметров:

$$T_2 = \alpha \times D(S_k,S_m) + f(N) = \alpha \times \sqrt{\mathrm{dtw}(X_k,X_m)^2 + \mathrm{dtw}(Y_k,Y_m)^2 + \mathrm{dtw}(P_k,P_m)} + f(N),$$

где $f(N)$ – линейная функция от N, $2 < \alpha < 3{,}5$ – константа;

$$T_3 = \mathrm{median}\{D(S_k,S_m)\} + \alpha \times \mathrm{std}\{D(S_k,S_m)\} + c,$$

где $2 < \alpha < 3{,}5$; c – экспериментально подбираемые константы.

Можно использовать и более сложные формулы вычисления T, которые разделяли бы поддельные и подлинные подписи, учитывая распределение DTW-расстояний, вычисленных для подлинных и поддельных подписей на достаточно большой базе. В настоящей работе экспериментально был выбран порог типа T_3.

Когда формула вычисления порога T определена, верификация выполняется следующим образом. Вычисляются расстояния DTW между парами нормализованных данных X, Y, P верифицируемой и каждой из N модельных подлинных подписей человека. Эти расстояния задают координаты N точек в трехмерном признаковом пространстве. Если более половины из них отстоит от центра дальше порога T, подпись считается фальшивой, иначе – подлинной.

Значения порогов будут разными не только для подписей разных людей, но и для разных наборов подлинных подписей одного человека при вычислении порога T.

Выбор метода нормализации исходных данных подписей. В табл. 2 собраны результаты точности распознавания подлинности подписей (accuracy, или ACC) при разных комбинациях нормализации исходных данных. Индексы нормализации определяют номера последовательно примененных методов нормализации, указанных в табл. 1. Всего сравнивались 24 варианта нормализации данных динамических подписей. Например, индекс 6274 означает, что сначала выполнена нормализация по длине подписи (данные всех подписей – одинаковое число точек), затем удалены точки, в которых стилус был поднят, после этого подпись была ориентирована горизонтально в плоскости XY и, наконец, к ее параметрам применена мин-макс-нормализация. После нормализации к этим данным применялось преобразование DTW. В табл. 2–5 лучшие показатели выделены жирным шрифтом.

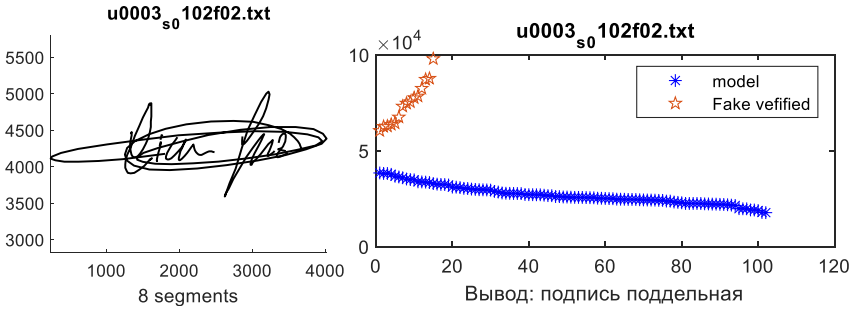
Таблица 2
Точность распознавания подписей первых 20 человек из базы MCYT при N=15

Table 2
Recognition accuracy of signatures of the first 20 people from the MCYT database for N=15

Индекс нормализации *Normalization index*	07	073	**074**	075	607	6073	**6074**	6075
Точность подлинных *Accuracy of genuine*	0,9800	0,9780	**0,9940**	0,9920	0,9800	0,9760	**0,9990**	0,9840
Точность поддельных *Accuracy of fake*	0,9640	0,8860	**0,9960**	0,8860	0,9500	0,8200	**0,9980**	0,8600
Точность *Accuracy*	0,9720	0,9320	**0,9950**	0,9390	0,9650	0,8980	**0,9940**	0,9220
Индекс нормализации *Normalization index*	17	173	**174**	175	617	6173	**6174**	6175
Точность подлинных *Accuracy of genuine*	0,9940	0,9960	**0,9960**	0,996	0,9920	0,9940	**0,9920**	0,9940
Точность поддельных *Accuracy of fake*	0,1860	0,4740	**1,0**	0,4740	0,1420	0,4400	**1,0**	0,4400
Точность *Accuracy*	0,5900	0,7350	**0,9980**	0,7350	0,5670	0,7170	**0,9960**	0,7170
Индекс нормализации *Normalization index*	27	273	**274**	275	627	6273	**6274**	6275
Точность подлинных *Accuracy of genuine*	0,9780	0,9740	**0,9940**	0,9920	0,9740	0,9740	**0,9940**	0,9920
Точность поддельных *Accuracy of fake*	0,8680	0,8740	**0,9940**	0,8580	0,9860	0,8060	**1,0**	0,9660
Точность *Accuracy*	0,9230	0,9240	**0,9940**	0,9250	0,9800	0,8900	**0,9970**	0,9790

Для выполнения сравнительных экспериментов были взяты 25 подлинных и 25 поддельных подписей 20 человек из базы MCYT, которая включена в базу DeepSignDB как одна из составляющих. Выполнялась нормализация данных X, Y, P каждой подписи 24 вариантами и вычислялись расстояния DTW между парами параметров, т. е. dtw(X_k,X_m), dtw(Y_k,Y_m), dtw(P_k,P_m), где k, m означают номер подписи из N подлинных одного человека. Эти расстояния задают точку в трехмерном признаковом пространстве. Для построения образа подписи каждого человека использовались N=15 его подлинных подписей. Множество из $N(N–1)$ таких точек формирует образ подлинной подписи конкретного человека в трехмерном признаковом пространстве.

На рис. 1 слева показана поддельная подпись человека u0003, справа – синими звездочками – расстояния от пар подлинных подписей, использованных для построения образа подписи до начала координат, красными – расстояния до пар (поддельная, подлинная). Все пары с поддельной подписью не попадают в образ пар подлинных подписей.



a) *b)*

Рис. 1. Визуализация поддельной динамической подписи человека u0003 (*a*); результат ее верификации на базе N=15 подлинных подписей (*b*)

Fig. 1. The visualization of a fake dynamic signature of a person with u0003 (a); the result of its verification based on N=15 authentic signatures (b)

Оценки точности верификации подписей (ACC_u и $BACC_u$) вычислялись для подлинных и поддельных подписей каждого человека u (у некоторых людей было разное число подписей) по формулам

$$ACC_u=(TN_u+TP_u)/(TN_u+FP_u+TP_u+FN_u),$$

$$BACC_u=(TP_u/(TP_u+FN_u) + TN_u/(TN_u+FP_u))/2,$$

где TN_u – число верно распознанных поддельных подписей, TP_u – число верно распознанных подлинных подписей, FN_u – число неверно распознанных поддельных подписей, FP_u – число неверно распознанных подлинных подписей. Если число подлинных подписей человека u равно числу его поддельных подписей, то $TP_u+FN_u = TN_u+FP_u$ и $ACC_u = BACC_u$, т. е. общая и сбалансированная точности верификации подписей этого человека равны. У разных людей может быть разное число подписей, поэтому общая оценка верификации подписей множества n людей определяется равенством

$$ACC=(\sum_{u=1}^{n}(TP_u+TN_u)) / \sum_{u=1}^{n}(TN_u+FP_u+TP_u+FN_u),$$

а сбалансированная оценка точности верификации всех подписей этих же людей – равенством

$$BACC= 0{,}5 \sum_{u=1}^{n}(TP_u/(TP_u + FN_u) + (TN_u/(TN_u+FP_u)),$$

т. е. они вычисляются как средние по множеству оценок для каждого человека ACC_u и $BACC_u$. Можно вычислить отдельно точность верификации подлинных подписей и отдельно – поддельных:

$$ACC_{real} = (\sum_{u=1}^{n} TP_u)/ \sum_{u=1}^{n}(TP_u+FP_u),$$

$$ACC_{fake} = (\sum_{u=1}^{n} TN_u)/ \sum_{u=1}^{n}(TN_u+FN_u).$$

Значение уровня равной ошибки (EER) в данной статье EER = 1 – BACC. При ACC ≠ BACC он дает более объективный уровень равной ошибки.

В табл. 2 приведены значения оценок точности подписей верификации 20 человек при N=15. В данном случае у каждого человека было по 25 подлинных и поддельных подписей, поэтому

$$ACC_{real} = TP/(TP+FN),$$

$$ACC_{fake} = TN/(TN+FP),$$

$$ACC = (ACC_{real} + ACC_{fake})/2.$$

Из анализа данных, представленных в табл. 2, следует, что лучшие результаты верификации получаются при использовании поворота подписи и мин-макс-нормализации независимо от применения методов нормализации первой группы. Обнуление среднего и z-нормализация существенно ухудшают точность распознавания поддельных подписей, а нормализация подписей по длине практически не влияет на результат. Экспериментально оценивалось преобразование всех подписей в массивы равной длины в 500, 1000, 1500 точек.

В табл. 3 собраны результаты верификации всех 21 745 подписей 574 человек из базы DeepSignDB, точнее, из ее размеченного на подлинные и поддельные подписи подмножества Development\stylus. Оно состоит из подписей, ранее собранных в четырех базах данных и выполненных на планшетах разных типов. Число подлинных и поддельных подписей человека в них различно. В табл. 3 приведены результаты верификации подписей после их нормализации, соответствующей индексу 174 согласно табл. 1. Показано, сколько подлинных и поддельных подписей ошибочно распознано в каждой базе и их общее число. Поскольку базы являются несбалансированными, в нижних строках приведены точность классификации по каждому классу (подлинные и поддельные), а также сбалансированная и общая точность. Сбалансированная точность объективнее показывает результат классификации в случае дисбаланса классов, а если размеры классов равны, она совпадает с общей точностью. Все значения точности в табл. 3 превосходят 0,99, т. е. уровень равной ошибки EER составляет менее 1 %.

Таблица 3
Сводная таблица верификации всех подписей из базы DeepSignDB

Table 3
Summary table of verification of all signatures from the database DeepSignDB

Номер базы *Base number*	1	2	3	4	Итого *Total*
ID человека *Person ID*	1-230	231-498	1009-1038	1039-1084	
Число N для построения образа *Number N for constructing the image*	15	14	15	6	
Всего человек *Total number of people*	230	268	30	46	574
Число подлинных подписей / ошибок *Number of genuine signatures / errors*	5747 / 9	4288 / 17	1200 / 18	368 / 5	11603 / 49
Число поддельных подписей / ошибок *Number of fake signatures / errors*	5750 / 0	3216 / 0	900 / 0	276 / 0	10142 / 0
Всего подписей *Total signatures*	11497	7504	2100	864	21745
Точность подлинных *Accuracy of genuine*	0,9968	0,9960	0,9850	0,9918	0,9910
Точность поддельных *Accuracy of fake*	1,0	1,0	1,0	1,0	1,0
Точность сбалансированная / EER, % *Balanced accuracy / EER, %*	0,9982 / 0,18	0,9980 / 0,20	0,9925 / 0,75	0,9932 / 0,68	**0,9955 / 0,45**
Точность общая *Overall accuracy*	0,9982	0,9977	0,9914	0,9922	**0,9949**

Экспериментально установлено, что для построения надежного образа подписи человека необходимы N=15 образцов его подлинных подписей. Увеличение N не дает существенного прироста точности. Их табл. 3 видно, что точность верификации поддельных подписей равна 100 % при достаточном числе предъявленных подлинных подписей каждого человека. Она зависит от N, от вариативности исполнения подписи человеком, но даже при N =5 общая точность верификации составляет около 99 % при практически 100 %-м распознавании фальшивых подписей (табл. 4). В табл. 4 собраны результаты верификации всех подписей из базы DeepSignDB при N=5. Такое число образцов подлинных подписей часто используется в литературе для сравнения результатов разных исследователей. Так же, как и в табл. 3, приведены общая и сбалансированная по двум классам точности классификации. В табл. 4 указаны значения EER. Они несколько хуже, чем в табл. 3, поскольку образы подписей строились по 10 парам подлинных подписей и не смогли в достаточной степени учесть вариативность исполнения подписей разными людьми. Тем не менее показатель EER в среднем равен 0,45 % при верификации подписей 574 человек.

Таблица 4
Сводная таблица верификации всех подписей из базы DeepSignDB при N=5

Table 4
Summary table of verification of all signatures from the DeepSignDB database for N=5

Номер базы *Base number*	MCYT-100	1	2	3	4	Итого *Total*
ID человека *Person ID*	1-100	1-230	231-498	1009-1038	1039-1084	1-1084
Всего человек *Total number of people*	100	230	268	30	46	**574**
Число подлинных подписей / ошибок *Number of genuine signatures / errors*	2498	5747 / 84	4288 / 49	1200 / 25	368 / 6	11603 / 164
Число поддельных подписей / ошибок *Number of fake signatures / errors*	2500 / 0	5750 / 0	3216 / 1	900 / 0	276 / 0	10142 / **1**
Всего подписей *Total signatures*	5000	11497	7504	2100	644	**21745**
Точность подлинных *Accuracy of genuine*	0,9852	0,9854	0,9886	0,9792	0,9837	0,9859
Точность поддельных *Accuracy of fake*	1,0	1,0	0,9997	1,0	1,0	0,9999
Точность сбалансированная / EER, % *Balanced accuracy / EER, %*	0,9926 / **0,74**	0,9927 / 0,76	0,9933 / **0,67**	0,9881 / 1,09	0,9907 / 0,93	0,9929 / 0,71
Точность общая *Overall accuracy*	0,9926	0,9927	0,9941	0,9896	0,9918	0,9924

Анализ результатов верификации предложенным методом. Некоторые подлинные подписи отдельных людей в данном исследовании были ошибочно распознаны как поддельные. На рис. 2 показаны подлинные подписи человека с идентификатором u0077, по 15 из них строился образ подписи этого человека согласно описанному выше методу. Все подписи немного отличаются друг от друга. При верификации каждой из 25 подлинных подписей этого же человека одна была определена как поддельная (левая верхняя на рис. 2). Она имеет видимые отличия от других подписей, по которым строился образ подписей данного человека. Вариативность динамических подписей – естественное явление, поэтому эксперту, отбирающему подписи для построения обобщенного образа, следует это учитывать.

Для сравнения на рис. 3 приведены подлинная (слева вверху) и 15 поддельных подписей человека u0077. Все они распознаны верно посредством описанного выше метода. Видны их визуальные отличия от подлинных подписей, но для обоснованного заключения эксперту необходимы количественные признаки, а не субъективные ощущения. Предложенный в статье метод позволяет объективно оценивать подлинность динамических подписей в сравнении с предоставленными подлинными образцами.

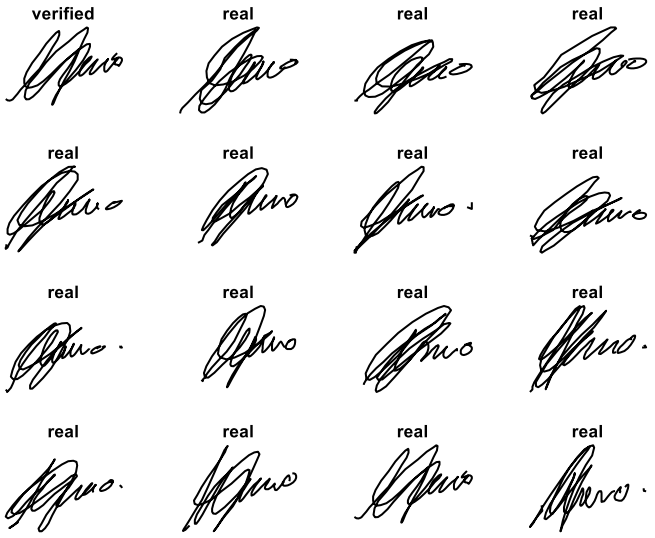


Рис. 2. Подлинные подписи человека u0077
Fig. 2. Genuine signatures of person u0077

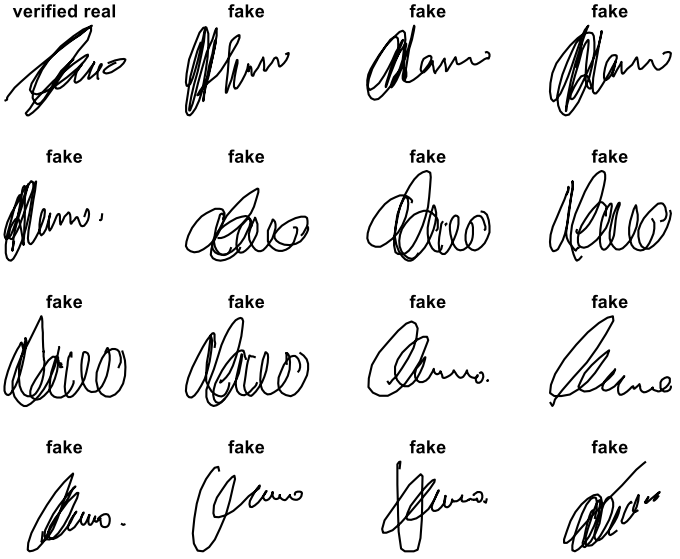


Рис. 3. Слева вверху подлинная подпись человека u0077.
Остальные подписи поддельные, распознанные верно
Fig. 3. On the top left is the genuine signature of person u0077.
The other signatures are fake, recognized correctly

На рис. 4 графически показаны результаты верификации всех 50 подписей, сделанных человеком u0077. При построении образа его подписей использованы N=15 подлинных подписей. Множество синих звездочек показывает расстояния от 105 пар модельных подписей до начала координат признакового пространства. Расстояния от пар верифицированных подписей до начала координат показаны крестиками для поддельных и звездочками для подлинных подписей. Множества расстояний, вычисленных при верификации каждой подписи, отсортированы и соединены линиями для удобства восприятия. Красная горизонтальная линия показывает порог, разделяющий цепочки расстояний, которые образованы подлинными и фальшивыми подписями, вычисленными по подписям этого человека. Каждая верифицируемая подпись оценивается на предмет близости к 15 модельным подписям и порождает 15 точек, соединенных ломаной на рисунке. Если верифицировалась подлинная подпись, она не использовалась для

построения образа подписей этого человека. Фактически для каждой подлинной подписи строился новый образ, а для поддельных использовался один. На рис. 4 слева вверху приведены результаты оценки близости 25 поддельных подписей к парам подлинных модельных подписей, в центре внизу – аналогично для 25 верифицируемых подлинных подписей. В центре рисунка одна цепочка точек, порожденная подлинной подписью, в основном превышает вычисленный порог, и эта подпись распознается как поддельная. Однако, если увеличить значение порога, чтобы эта подпись была корректно распознана, неверно могут быть определены поддельные подписи. На практике для разрешения конфликтной ситуации можно попросить пользователя расписаться еще один или несколько раз и выполнить повторную верификацию его подписи.

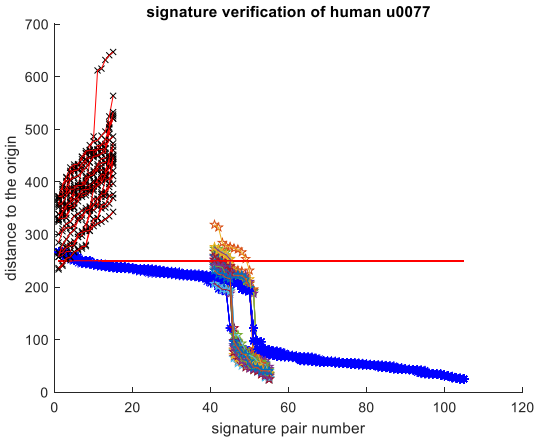
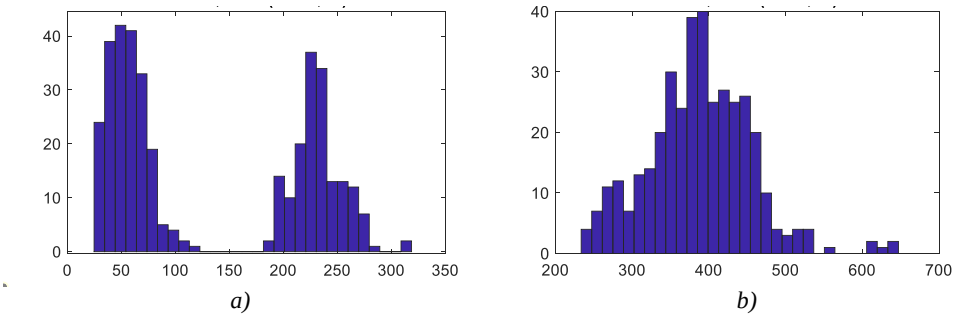


Рис. 4. Результаты верификации всех 50 подписей человека u0077

Fig. 4. Results of verification of all 50 signatures of the person u0077

На рис. 5 показаны гистограммы расстояний от начала координат признакового пространства до точек, образованных парами верифицируемых и модельных подписей человека u0077. Множества расстояний для подлинных и поддельных подписей пересекаются, что осложняет задачу распознавания поддельных. Расстояния до подлинных подписей можно разделить на две группы (рис. 5). Это говорит о том, что и подписи по степени сходства также можно разделить на две отличающиеся группы. От выбора подлинных подписей, используемых для построения их образа, зависит точность автоматической верификации других подписей, предъявляемых от имени этого человека. Тем не менее в табл. 3 показано, что все поддельные подписи, выполненные от имени 574 человек, были распознаны верно описанным методом.



a) *b)*

Рис. 5. Гистограммы расстояний от начала координат до пар верифицируемых подлинных (*a*) и поддельных (*b*) подписей человека u0077

Fig. 5. Histograms of distances from the origin to pairs of verified genuine (a) and fake (b) human signatures u0077

На рис. 6 и 7 показаны примеры верно распознанных подлинных и фальшивых подписей других людей. Следует отметить, что на всех рисунках приведены визуальные представления динамических подписей, сформированные ломаными, аппроксимирующими координаты X,Y в точках, где давление $P>0$.

a) *b)*

Рис. 6. Подписи человека ID0190: подлинная (*a*); фальшивая (*b*)
Fig. 6. Signatures of person ID0190: genuine (a); fake (b)

a) *b)*

Рис. 7. Подписи человека ID0191: подлинная (*a*); фальшивая (*b*)
Fig. 7. Signatures of person ID0191: genuine (a); fake (b)

В литературе для сравнительного анализа результатов верификации динамических подписей часто приводится показатель EER для базы MCYT-100 при использовании для обучения классификатора пяти подлинных подписей каждого из 100 человек. Следует отметить, что в основном исследователи делят подписи из данной базы на тренировочное и тестовое множества, при этом формируемые классификаторы являются человеконезависимыми (их надо обучать при изменении национального состава базы или ее расширении). Показатель EER вычисляется для тестового множества, которое в несколько раз меньше всей базы данных. В настоящей статье EER вычисляется для всех подписей этой базы, а классификатор строится персонально для каждого человека. Он является человекозависимым, для его построения требуются только подписи одного человека, он не зависит от национальности и языка этого человека.

Из табл. 5 следует, что показатель EER=0,74, достигнутый в настоящей статье, один из самых низких при верификации всех подписей 100 человек из базы MCYT-100. В настоящем исследовании классификатор строился персонально для каждого человека на базе его пяти подлинных подписей, затем выполнялась нормализация исходных параметров без вычисления других признаков. К параметрам *X*, *Y*, *P* применялось преобразование DTW, и для каждого человека адаптивно вычислялся порог, отделяющий фальшивые подписи от подлинных.

Таблица 5
Лучшие известные результаты на базе MCYT-100 при *N*=5
Table 5
Best known results based on MCYT-100 for N=5

Автор, год, ссылка *Author, year, link*	Метод *Method*	Число подписей для обучения *Number of signatures for training*	Число подлинных подписей тестируемых *Number of genuine signatures tested*	Число поддельных подписей тестируемых *Number of forged signatures tested*	EER, %
Jiang, 2022, [11]	Deep soft-DTW, convolutional recurrent adaptive network	Нет данных	Нет данных	Нет данных	1,01
Xia, 2017, [12]	Индекс нормализации 147, DTW	Нет данных	Нет данных	Нет данных	2,15
Fierrez, 2005, [10]	HMM+Parzen Windows	5×330=1650 подлинных	20×330=6600	25×330=8250	2,12
Sharma, 2016, [13]	DTW, VQ	Нет данных	Нет данных	Нет данных	1,81
Wu, 2019, [14]	Siamese network, DTW	80 %	5×100=500	5×100=500	1,75
Данная статья	Нормализация без вычисления признаков, DTW, порог	Пять подлинных одного	25×100=2500	25×100=2500	**0,74**

Примечание: в работе [10] использовалась база MCYT-330 с подписями 330 человек.
Note: in the paper [10] the MCYT-330 database with signatures of 330 people was used.

Заключение. В работе были экспериментально исследованы разные методы нормализации исходных данных динамической подписи. Показано, что верификацию динамических подписей для выявления фальшивых с высокой точностью можно выполнять без вычисления дополнительных динамических признаков, используя ограниченный набор (от 5 до 15) подлинных подписей одного человека. В работе строились индивидуальные образы подписей каждого из 574 человек из базы DeepSignDB (подмножество размеченных подписей множества Development\stylus). Общее число верифицируемых подписей составило 21 745. Если при построении индивидуальных образов подписей человека использовались всего пять его подлинных подписей, то из 10 142 поддельных подписей только одна была неверно классифицирована. Точность верификации поддельных подписей составила 0,9999. Из 11 603 подлинных подписей неверно классифицированы 164. Точность верификации подлинных подписей составила 0,9859. Сбалансированная точность верификации всех подписей базы MCYT-100 составила 0,9929, а уровень равной ошибки EER =0,74 %, что является лучшим из известных показателей. При увеличении числа подлинных подписей, используемых для построения образа подписей человека, повышается точность верификации его подписей.

Список использованных источников

1. Kaur, H. Signature identification and verification techniques: state-of-the-art work / H. Kaur, M. Kumar // Journal of Ambient Intelligence and Humanized Computing. – 2023. – Vol. 14, no. 2. – P. 1027–1045.

2. Чуприна М. В. Языковая политика в Республике Индия / М. В. Чуприна // Знание. Понимание. Умение. – 2012. – № 2. – С. 293–297.

3. Старовойтов, В. В. Верификация динамической подписи человека по ограниченному числу образцов / В. В. Старовойтов // Информатика. – 2024. − Т. 21, № 2. – С. 94–106.

4. Старовойтов, В. В. Следует ли нормализовать данные динамических подписей перед верификацией методом DTW? / В. В. Старовойтов // BIG DATA и анализ высокого уровня : сб. науч. ст. X Междунар. науч.-практ. конф., Минск, 13 марта 2024 г. : в 2 ч. – Минск, 2024. – Ч. 2. – С. 391–400.

5. DeepSign: Deep on-line signature verification / R. Tolosana, R. Vera-Rodriguez, J. Fierrez, J. Ortega-Garcia // IEEE Transactions on Biometrics, Behavior, and Identity Science. – 2021. – Vol. 3, iss. 2. – P. 229–239.

6. Saleem, M. Survey of preprocessing techniques and classification approaches in online signature verification / M. Saleem, B. Kovari // Image Analysis and Recognition. ICIAR 2020. Lecture Notes in Computer Science. – 2020. – Vol. 12131. – P. 253–266. – DOI: 10.1007/978-3-030-50347-5_23.

7. Saleem, M. Systematic evaluation of pre-processing approaches in online signature verification / M. Saleem, C. Lia Szucs, B. Kovari // Intelligent Decision Technologies. – 2023. – Vol. 17, no. 3. – P. 655–672.

8. Fenton, D. Evaluation of features and normalization techniques for signature verification using dynamic timewarping / D. Fenton, M. Bouchard, T. H. Yeap // IEEE Intern. Conf. on Acoustics Speed and Signal Processing Proceedings, Toulouse, France, 14–19 May 2006. – Toulouse, 2006. – Vol. 3. – URL: https://ieeexplore.ieee.org/document/1660860/keywords#keywords (date of access: 17.08.2024).

9. Signature alignment based on GMM for on-line signature verification / X. Xia, Z. Chen, F. Luan, X. Song // Pattern Recognition. – 2017. – Vol. 65. – P. 188–196.

10. An on-line signature verification system based on fusion of local and global information / J. Fierrez-Aguilar, L. Nanni, J. Lopez-Peñalba [et al.] // 5th Intern. Conf. Audio- and Video-Based Biometric Person Authentication, Hilton Rye Town, N. Y., USA, 20–22 July 2005. – Springer, 2005. – P. 523–532.

11. Discriminative feature selection for on-line signature verification / X. Xia, X. Song, F. Luan [et al.] // Pattern Recognition. – 2018. – Vol. 74. – P. 422–433.

12. BioSecure signature evaluation campaign (BSEC'2009): Evaluating online signature algorithms depending on the quality of signatures / N. Houmani, A. Mayoue, S. Garcia-Salicetti [et al.] // Pattern Recognition. – 2012. – Vol. 45, no. 3. – P. 993–1003.

13. Sharma, A. An enhanced contextual DTW based system for online signature verification using vector quantization / A. Sharma, S. Sundaram // Pattern Recognition Letters. – 2016. – Vol. 84. – P. 22–28.

14. Dsdtw: Local representation learning with deep soft-dtw for dynamic signature verification / J. Jiang, S. Lai, L. Jin, Y. Zhu // IEEE Transactions on Information Forensics and Security. – 2022. – Vol. 17. – P. 2198–2212.

15. Prewarping Siamese network: Learning local representations for online signature verification / X. Wu, A. Kimura, S. Uchida, K. Kashino // IEEE Intern. Conf. on Acoustics, Speech and Signal Processing, Brighton, UK, 2–17 May 2019. – Brighton, 2019. – P. 2467–2471.

References

1. Kaur H., Kumar M. Signature identification and verification techniques: state-of-the-art work. *Journal of Ambient Intelligence and Humanized Computing*, 2023, vol. 14, no. 2, pp. 1027–1045.

2. Chuprina M. V. *Language policy in the Republic of India*. Znanie. Ponimanie. Umenie [*Knowledge. Understanding. Skill*], 2012, no. 2, pp. 293–297 (In Russ.).

3. Starovoitov V. V. *Verification of the person's dynamic signature on a limited number of samples*. Informatika [*Informatics*], 2024, vol. 21, no. 2, pp. 94−106 (In Russ.).

4. Starovoitov V. V. *Should we normalize dynamic signatures data before DTW-based verification?* BIG DATA i analiz vysokogo urovnja : sbornik nauchnyh statej X Mezhdunarodnoj nauchno-prakticheskoj konferencii, Minsk, 13 marta 2024 goda : v 2 chastjah [*BIG DATA and Advanced Analytics : Collection of Scientific Articles of the X International Scientific and Practical Conference, Minsk, 13 March 2024 : in 2 Parts*]. Минск, 2024, part 2, pp. 391–400 (In Russ.).

5. 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, vol. 3, iss. 2, pp. 229–239.

6. Saleem M., Kovari B. Survey of preprocessing techniques and classification approaches in online signature verification. *Image Analysis and Recognition. ICIAR 2020. Lecture Notes in Computer Science*, 2020, vol. 12131, pp. 253–266. DOI: 10.1007/978-3-030-50347-5_23.

7. Saleem M., Lia Szucs C., Kovari B. Systematic evaluation of pre-processing approaches in online signature verification. *Intelligent Decision Technologies*, 2023, vol. 17, no. 3, pp. 655–672.

8. Fenton D., Bouchard M., Yeap T. H. Evaluation of features and normalization techniques for signature verification using dynamic timewarping. *IEEE International Conference on Acoustics Speed and Signal Processing Proceedings, Toulouse, France, 14–19 May 2006*. Toulouse, 2006, vol. 3. Available at: https://ieeexplore.ieee.org/document/1660860/keywords#keywords (accessed 17.08.2024).

9. Xia X., Chen Z., Luan F., Song X. Signature alignment based on GMM for on-line signature verification // Pattern Recognition, 2017, vol. 65, pp. 188–196.

10. Fierrez-Aguilar J., Nanni L., Lopez-Peñalba J., Ortega-Garcia J., Maltoni D. An on-line signature verification system based on fusion of local and global information. *5th International Conference Audio- and Video-Based Biometric Person Authentication, Hilton Rye Town, N. Y., USA, 20–22 July 2005*. Springer, 2005, pp. 523–532.

11. Xia X., Song X., Luan F., Zheng J., Chen Z., Ma X. Discriminative feature selection for on-line signature verification. *Pattern Recognition*, 2018, vol. 74, pp. 422–433.

12. Houmani N., Mayoue A., Garcia-Salicetti S., Dorizzi B., Khalil M. I., …, Vivaracho-Pascual C. BioSecure signature evaluation campaign (BSEC'2009): Evaluating online signature algorithms depending on the quality of signatures. *Pattern Recognition*, 2012, vol. 45, no. 3, pp. 993–1003.

13. Sharma A., Sundaram S. An enhanced contextual DTW based system for online signature verification using vector quantization. *Pattern Recognition Letters*, 2016, vol. 84, pp. 22–28.

14. Jiang J., Lai S., Jin L., Zhu Y. Dsdtw: Local representation learning with deep soft-dtw for dynamic signature verification. *IEEE Transactions on Information Forensics and Security*, 2022, vol. 17, pp. 2198–2212.

15. Wu X., Kimura A., Uchida S., Kashino K. Prewarping Siamese network: Learning local representations for online signature verification. *IEEE International Conference on Acoustics, Speech and Signal Processing, Brighton, UK, 2–17 May 2019*. Brighton, 2019, pp. 2467–2471.

Информация об авторе

Старовойтов Валерий Васильевич, доктор технических наук, профессор, Объединенный институт проблем информатики Национальной академии наук Беларуси.
E-mail: valerys@newman.bas-net.by

Information about the author

Valery V. Starovoitov, D. Sc. (Eng.), Prof., The United Institute of Informatics Problems of the National Academy of Sciences of Belarus.
E-mail: valerys@newman.bas-net.by