УДК 612.087.1:004.032.26 DOI: 10.18698/2541-8009-2018-05-313

НЕЙРОСЕТЕВОЙ ПОДХОД К ВЕРИФИКАЦИИ РУКОПИСНОЙ ПОДПИСИ

Н.А. Глущенко gluschenkona@sudent.bmstu.ru
SPIN-код: 3659-3840

Н.С. Коннова nkonnova@bmstu.ru
SPIN-код: 3672-6670

МГТУ им. Н.Э. Баумана, Москва, Российская Федерация

Аннотация

Рукописная подпись широко используется в повседневной жизни. Существуют несколько различных подходов к ее распознаванию. Данная статья посвящена методу статической (офлайн) верификации рукописной подписи. Выполнено сравнение различных подходов к верификации относительно ошибок первого и второго рода. Проведен обзор публикаций в данной предметной области и описан общий алгоритм верификации с применением искусственных нейронных сетей. Подробно рассмотрен предложенный авторами алгоритм верификации с применением многослойной нейронной сети, дано описание его стадий, приведены результаты его реализации на языке Python и сделан вывод относительно перспектив развития данного направления.

Ключевые слова

Нейронная сеть, персептрон, искусственный интеллект, биометрия, компьютерное зрение, обработка изображений, верификация, рукописная подпись

Поступила в редакцию 24.04.2018

Введение. Одно из самых распространенных направлений в развитии нейросетевых технологий связано с биометрией — технологией, посвященной измерению и анализу различных физических характеристик человека. Здесь предусмотрены автоматизированные меры верификации (сравнение образца с биометрическим шаблоном) и идентификации (сравнение образца со многими из базы данных) личности, основанные на физиологических (например, отпечатки пальцев, радужная оболочка глаза, сетчатка глаза, форма лица) и поведенческих (например, речь, почерк, походка человека и т. д.) принципах.

Верификация рукописной подписи является одним из наиболее часто используемых методов, например, при проведении финансовых и коммерческих транзакций, проверке документов и контроле физического доступа.

Существует два подхода к верификации подписи, различающихся по способу получения данных:

– статический (офлайн) метод, заключающийся в обработке и анализе изображения подписи;

– динамический (онлайн) метод, основанный на считывании подписи в режиме реального времени и выделении таких характеристик, как скорость письма, угол наклона пера, его давления и т. п.

Онлайн-подход является более точным, потому что здесь при верификации используются и динамические характеристики подписи, но офлайн-подход также широко распространен, например, в областях, где человек физически отсутствует во время процесса верификации или же когда нет подключения к сети или графического планшета (проверка банковского чека может быть выполнена лишь офлайн). Сущность обоих методов одинакова. Она включает в себя сбор данных, их предварительную обработку, извлечение признаков, принятие решения и оценку эффективности. В данной статье рассмотрен второй подход, наиболее универсальный и доступный в применении.

Сравнение используемых подходов. Основной целью при реализации процедуры верификации является сведение к минимуму ошибок при распознавании образца рукописной подписи. Данные ошибки можно подразделить на два вида:

– 1-го рода — ложный отказ в принятии подписи, когда система отказывает в доступе зарегистрированному лицу (далее — FRR, False Rejection Rate);

– 2-го рода — ложное принятие подписи (далее — FAR, False Acceptance Rate — система принимает поддельную подпись).

Оба типа ошибок связаны между собой и зависят от принятого порогового значения для определения подлинности подписи. Таким образом, при увеличении этого значения FRR уменьшается, а FAR увеличивается, и наоборот.

Для реализации статического метода верификации используют различные подходы, например, искусственные нейронные сети, скрытые марковские модели (далее — СММ), различные виды метрик, метод опорных векторов (далее — SVM, support vector machine), вычисление локальных экстремумов или вычисление матрицы расстояния [1]. В настоящее время предпочтение все чаще отдается нейросетевому подходу, и это можно объяснить рядом причин [2]. Во-первых, за последние полвека развитие нейросетевых технологий сделало большой скачок. Во-вторых, применение данного все более развивающегося подхода помогает верифицировать подпись более точно, нежели при использовании других. Это обусловлено тем, что нейронные сети эффективно строят нелинейные зависимости, которые точнее описывают данные, они более устойчивы к шумам во входных данных и более адаптированы к их изменениям. Как видно из приведенного в таблице сравнения, применение искусственных нейронных сетей (5-я и 6-я строки) позволяет достичь меньшего количества ошибок первого и второго рода, чем при использовании других подходов.

Сравнение FRR и FAR различных подходов

№ п/п	Подход к реализации верификации	FRR, %	FAR, %
1	СММ [3]	0,20	32,60
2	SVM [4]	20,06	18,53
3	Евклидова метрика [5]	21,70	19,20
4	Вейвлет-преобразование [6]	16,20	16,10
5	Сеть радиальных базисных функций [7]	7,00	5,00
6	Многослойный персептрон [8]	2,90	7,40

Описание нейросетевого подхода. При верификации с помощью нейронных сетей можно условно выделить две стадии (рис. 1):

– обучение;

– тестирование.

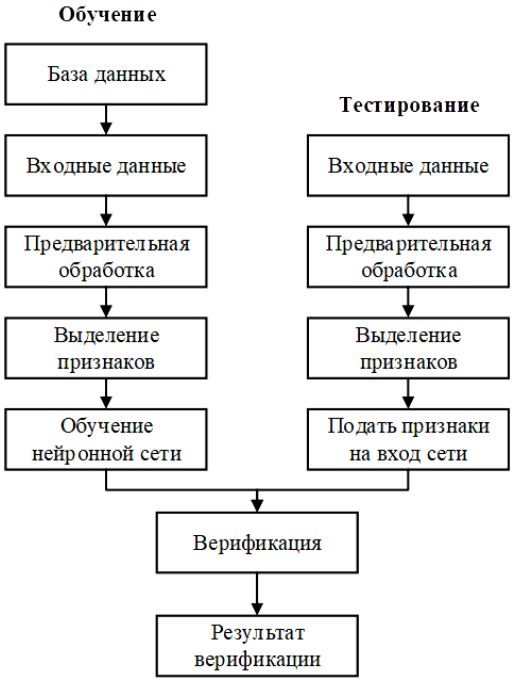


Рис. 1. Алгоритм офлайн-верификации подписи с применением нейронной сети

Обучение включает в себя:

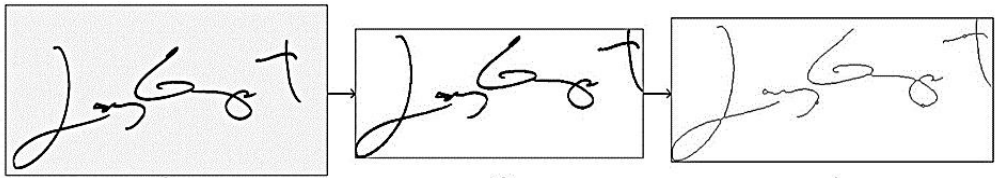
– извлечение изображения подписи из обучающей выборки;

– первичную обработку изображения, которая состоит из конвертации изображения в бинарное, его обрезки, нормализации размера и скелетизации;

– извлечение признаков, которые подбираются автором;

– обучение сети на обработанных изображениях.

На рис. 2 представлен пример обработки изображения подписи.



а *б* *в*

Рис. 2. Исходное (*а*), бинаризованное (*б*) и скелетезированное (*в*) изображения

Тестирование включает в себя такие шаги, как:

– извлечение подписи, подлинность которой необходимо определить;

– обработку изображения (аналогично обучению);

– извлечение признаков (аналогично обучению);

– подачу на вход обученной нейронной сети признаков;

– получение результата.

На эффективность распознавания влияет выбор типа нейронной сети. В данной области используются в основном многослойные искусственные нейронные сети прямого распространения с обратным распространением ошибки и сети радиальных базисных функций [9].

Отметим, что выбор признаков также является фактором, который влияет на процент ошибок 1-го и 2-го рода. Следовательно, важной задачей, помимо выбора архитектуры нейронной сети, является выбор признаков, извлекаемых из изображения. Их можно разделить на две основные группы:

– глобальные;

– локальные.

Глобальные признаки отражают всю структуру подписи и извлекаются из всего изображения (например, центр масс, вертикальная и горизонтальная проекции, отношение ширины к высоте подписи, область изображения). Локальные признаки извлекаются из каждой части изображения путем его сегментирования, поэтому они сильно различаются даже для одного и того же человека. Высокий процент ошибок обусловлен тем, что даже для одного человека образцы подписи значительно отличаются. Также со временем подпись может измениться. Поэтому необходимо как можно более эффективно подбирать глобальные и локальные признаки.

Выбор нейронной сети и набора признаков. В качестве прототипа нейронной сети был выбран многослойный персептрон (рис. 3) с гиперболическим тангенсом в качестве функции активации и пороговой функцией активации для выходного слоя. Таким образом, значение на выходе персептрона соответствует нулю в случае, если подпись признается поддельной, и единице, если подпись признается подлинной. Гиперболический тангенс принимает на вход любое вещественное число, а на выходе дает вещественное число в интервале от –1 до 1 и, подобно сигмоиде, может насыщаться. Но, как показывает практика, для решения поставленной задачи предпочтительнее использовать гиперболический тангенс, потому что выходное значение функции, в отличие от сигмоиды, центрировано относительно нуля [10].

В качестве глобальных признаков были выбраны:

– центр масс;

– высота подписи в пикселях после нормализации;

– отношение высоты к ширине;

– область изображения (количество черных пикселей на изображении);

– вертикальное разделение;

– горизонтальное разделение;

– максимум вертикальной проекции;

– максимум горизонтальной проекции;

– количество краевых точек;

– количество точек пересечений.

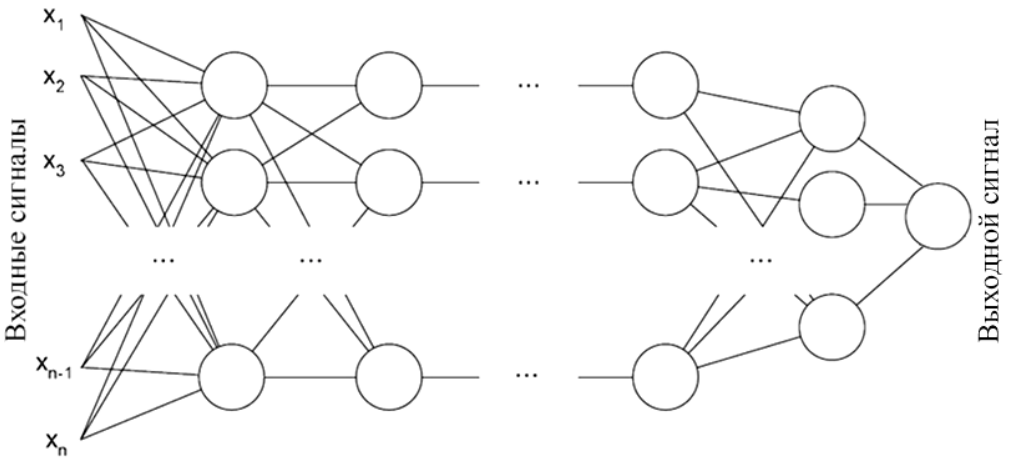


Рис. 3. Структура многослойного персептрона

Локальные признаки извлекаются путем разделения изображения на 96 частей и вычисления плотности пикселей для каждой из них. При обработке изображения на основе глобальных и локальных признаков формируется входной вектор длиной 164.

Программная реализация. Для реализации задачи были использованы такие библиотеки для языка Python, как Skimage, OpenCV для обработки изображений, NumPy и SciPy для расчетов, Keras и TensorFlow для реализации нейронной сети.

Также для проверки была выбрана база данных подписей для ICFHR (International Conference on Frontiers in Handwriting Recognition) 2010 Signature Verification Competition*, из которой были сформированы обучающая (19 подлинных и 15 поддельных подписей) и тестовая (60 подлинных и 70 поддельных подписей) выборки.

На рис. 4 представлен граф спроектированной нейронной сети, сгенерированный при помощи TensorBoard (набор инструментов визуализации, включенный в TensorFlow), где dense_1 — dense_3 — 1–3-й слои сети соответственно, a loss — функция потерь.

В результате работы алгоритма были достигнуты значения FRR = 3,3 %, FAR = 5 %.

Заключение. На данный момент опубликовано довольно много статей по данной тематике, однако ошибки первого и второго рода редко составляют хотя бы 3…4 % всех исследованных данных. В этом статическая верификация подписи уступает многим другим технологиям, например, сканированию отпечатков пальцев или радужной оболочки глаза. Однако, с учетом сложности данных методов и стоимости оборудования для их обеспечения, нейросетевой подход к верификации рукописной подписи является перспективным направлением, нуждающимся в оптимизации отрицательных качеств и повышении точности

* http://www.iapr-tc11.org/mediawiki/index.php/Datasets_List

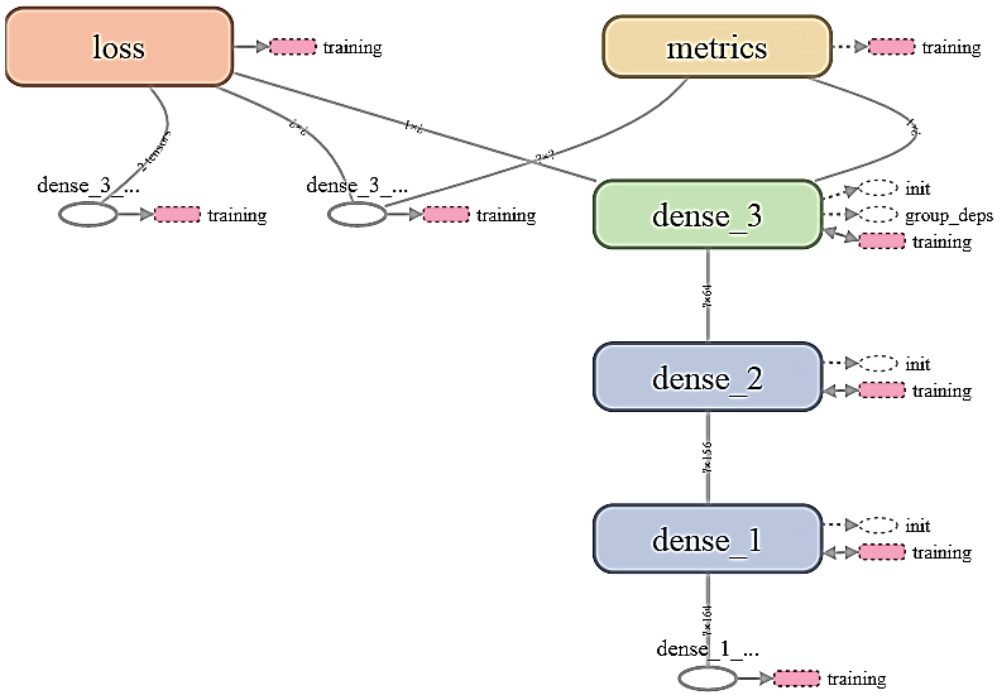


Рис. 4. Граф нейронной сети в TensorBoard

распознавания. Результатом проведенной работы является оценка ошибок распознавания образов из базы данных подписей. В дальнейшем планируется усовершенствовать алгоритм и улучшить статистику по ошибкам 1-го и 2-го рода, а также сформировать выборку большего объема. Предполагается, что точность распознавания нейронной сети можно повысить посредством увеличения количества и информативности признаков, извлекаемых из изображения. Главным направлением последующих исследований будет являться выделение новых глобальных и локальных признаков, позволяющих этого достичь.

Литература

[1] Dash T., Nayak T., Chattopadhyay S. Handwritten signature verification (offline) using neural network approaches: a comparative study. *International Journal of Computer Applications*, 2012, vol. 57, no. 7, pp. 33–41.

[2] McCabe A., Trevathan J., Read W. Neural network-based handwritten signature verification. *Journal of computers*, 2008, vol. 3, no. 8, pp. 9–22.

[3] Coetzer J., Herbst B.M., du Preez J.A. Offline signature verification using the discrete radon transform and a hidden Markov model. *EURASIP Journal on Advances in Signal Processing*, 2004, vol. 4, pp. 559–571.

[4] Deshmukh A., Desai S., Chaure T., Chothe A., Wankhade S. Automatic signature verification with chain code using weighted distance and Euclidean distance — a review. *International Journal of Research in Engineering and Technology*, 2016, vol. 5, no. 3, pp. 228–230.

[5] Moolla Y., Viriri S., Nelwamondo F., Tapamo J.S. Offline signature verification using locally optimized distance-based classification. *South African Computer Journal*, 2013, vol. 50, pp. 15–28.

[6] Daqrouq K., Sweidan H., Balamesh A., Ajour M. Off-line handwritten signature recognition by wavelet entropy and neural network. *Entropy*, 2017, vol. 19, no. 6, art. 252.

[7] Khan S., Dhole A. An offline signature recognition and verification system based on neural network. *International Journal of Research in Engineering and Technology*, 2014, vol. 3, no. 11, pp. 443–448.

[8] Ложников П.С., Сулавко А.Е., Еременко А.В., Волков Д.А. Экспериментальная оценка надежности верификации подписи сетями квадратичных форм, нечеткими экстракторами и персептронами. *Информационно-управляющие системы*, 2016, № 5, с. 73–85.

[9] Azzopardi G. How effective are radial basis function neural networks for offline handwritten signature verification? Thesis, B. Sc. University of London, 2006. 123 p.

[10] Петренко С. Это нужно знать: ключевые рекомендации по глубокому обучению (Часть 2). URL: http://datareview.info/article/eto-nuzhno-znat-klyuchevyie-rekomendatsii-po-glubokomu-obucheniyu-chast-2/ (дата обращения 03.11.2017).

Глущенко Наталья Александровна — студентка кафедры «Информационная безопасность», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

Коннова Наталья Сергеевна — кандидат технических наук, доцент кафедры «Информационная безопасность», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

NEURAL NETWORK APPROACH TO VERIFYING MANUAL SIGNATURE

N.A. Glushchenko gluschenkona@sudent.bmstu.ru
SPIN-code: 3659-3840

N.S. Konnova nkonnova@bmstu.ru
SPIN-code: 3672-6670

Bauman Moscow State Technical University, Moscow, Russian Federation

Abstract

Manual signature is widely used in daily life. There are several different approaches to its recognition. This article deals with the method of static (offline) verification of manual signature. We compare various approaches to verification with regard to the errors of the first and second kinds. The article reviews publications in this topical area and describes general verification algorithm with the use of artificial neutral networks. We consider the suggested verification algorithm using multi-layer neural network, describe its stages, present the results of its implementation in the Python language and make a conclusion concerning the prospects for further development of this field.

Keywords

Neutral network, perceptron, artificial intelligence, biometrics, computer vision, image processing, verification, manual signature

References

[1] Dash T., Nayak T., Chattopadhyay S. Handwritten signature verification (offline) using neural network approaches: a comparative study. *International Journal of Computer Applications*, 2012, vol. 57, no. 7, pp. 33–41.

[2] McCabe A., Trevathan J., Read W. Neural network-based handwritten signature verification. *Journal of computers*, 2008, vol. 3, no. 8, pp. 9–22.

[3] Coetzer J., Herbst B.M., du Preez J.A. Offline signature verification using the discrete radon transform and a hidden Markov model. *EURASIP Journal on Advances in Signal Processing*, 2004, vol. 4, pp. 559–571.

[4] Deshmukh A., Desai S., Chaure T., Chothe A., Wankhade S. Automatic signature verification with chain code using weighted distance and Euclidean distance — a review. *International Journal of Research in Engineering and Technology*, 2016, vol. 5, no. 3, pp. 228–230.

[5] Moolla Y., Viriri S., Nelwamondo F., Tapamo J.S. Offline signature verification using locally optimized distance-based classification. *South African Computer Journal*, 2013, vol. 50, pp. 15–28.

[6] Daqrouq K., Sweidan H., Balamesh A., Ajour M. Off-line handwritten signature recognition by wavelet entropy and neural network. *Entropy*, 2017, vol. 19, no. 6, art. 252.

[7] Khan S., Dhole A. An offline signature recognition and verification system based on neural network. *International Journal of Research in Engineering and Technology*, 2014, vol. 3, no. 11, pp. 443–448.

[8] Lozhnikov P.S., Sulavko A.E., Eremenko A.V., Volkov D.A. Experimental evaluation of reliability of signature verification by quadratic form networks, fuzzy extractors and perceptrons. *Informatsionno-upravlyayushchie sistemy* [Information and Control Systems], 2016, no. 5, pp. 73–85.

[9] Azzopardi G. How effective are radial basis function neural networks for offline handwritten signature verification? Thesis, B. Sc. University of London, 2006. 123 p.
[10] Petrenko S. Eto nuzhno znat': Klyuchevye rekomendatsii po glubokomu obucheniyu (Chast' 2) [What you need to know: key recommendations for deep learning (Part 2)]. Available at: http://datareview.info/article/eto-nuzhno-znat-klyuchevyie-rekomendatsii-po-glubokomu-obucheniyu-chast-2/ (accessed 03.11.2017).

Glushchenko N.A. — student, Department of Information Security, Bauman Moscow State Technical University, Moscow, Russian Federation.

Konnova N.S. — Cand. Sc. (Eng.), Assoc. Professor, Department of Information Security, Bauman Moscow State Technical University, Moscow, Russian Federation.