электронный журнал
МОЛОДЕЖНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК
Издатель Общероссийская общественная организация "Академия инженерных наук им. А.М. Прохорова"
ISSN 2307-0609

 # 01, март 2018

УДК 612.087.1; 004.032.26

Нейросетевой подход к верификации рукописной подписи

Глущенко Н. А., *студент*
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Информационная безопасность»
infinityddf@gmail.com

Научный руководитель: Коннова Н.С., старший преподаватель, к.т.н.
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Информационная безопасность»
nkonnova@bmstu.ru

Аннотация: В данной статье рассматривается метод 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. Приведен предложенный авторами алгоритм верификации с применением многослойной нейронной сети, описаны его стадии, приведены результаты его реализации на языке Python и сделан вывод относительно перспективы данного направления.

Ключевые слова: нейронная сеть (neural network), искусственный интеллект (artificial intelligence), биометрия (biometrics), верификация (verification), рукописная подпись (handwritten signature).

Введение

Одно из самых распространенных направлений в развитии нейросетевых технологий связано с биометрией – технологией, измеряющей и анализирующей различные физические характеристики человека. Она предлагает 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 находится среди 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 используются и динамические характеристики подписи, но офлайн метод также широко распространен, например, в областях, где человек не присутствует физически 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 внимание уделено второму подходу, как наиболее универсальному и доступному в применении.

1. Сравнение используемых подходов

Основной целью при реализации методов 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 его 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 по ряду 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 обусловливается 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 1 сравнения, применение искусственных нейронных сетей (5, 6 строки) позволяет достичь меньшего процента ошибок первого и второго рода, чем при использовании других подходов.

Таблица 1

Сравнение FRR и FAR различных подходов

№	Подход к реализации верификации	FRR	FAR
1	CMM [3]	0.2 %	32.6 %
2	SVM [4]	20.06 %	18.53 %
3	Евклидова метрика [5]	21.7 %	19.2 %
4	Вейвлет-преобразование [6]	16.2 %	16.1 %
5	Сеть радиальных базисных функций [7]	7 %	5 %
6	Многослойный персептрон [8]	2.9 %	7.4 %

2. Описание нейросетевого подхода

Верификацию при помощи нейронных сетей можно условно разделить на две стадии (см. 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 рисунке 2 представлен пример обработки изображения подписи.

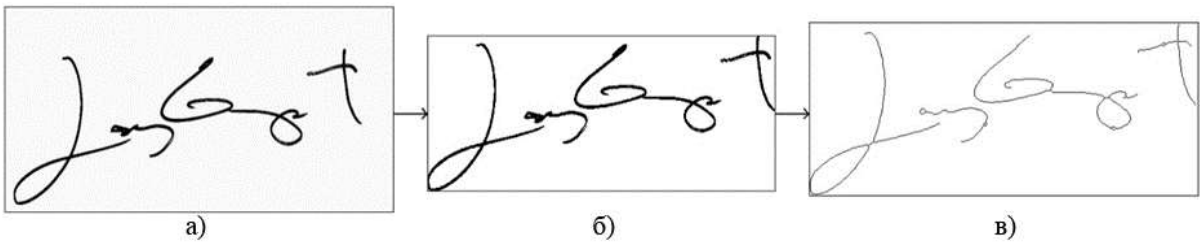

Рис. 2. Изображения: а) исходное, б) бинаризованное, в) скелетизированное

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].

Следует отметить, 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:

- локальные;
- глобальные.

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 человека. Высокий процент ошибок обусловливается тем, что даже для одного человека образцы подписи значительно отличаются. Также, со временем, подпись может измениться. Поэтому необходимо как можно более эффективно подбирать локальные и глобальные признаки.

3. Выбор нейронной сети и набора признаков

В качестве прототипа нейронной сети был выбран многослойный персептрон (рисунок 3) с гиперболическим тангенсом в качестве функции активации и пороговой функцией активации для выходного слоя. Таким образом, значение на выходе персептрона соответствует 0 в случае, если подпись признается поддельной, и 1, 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 отличии от сигмоиды, центрировано относительно нуля [10].

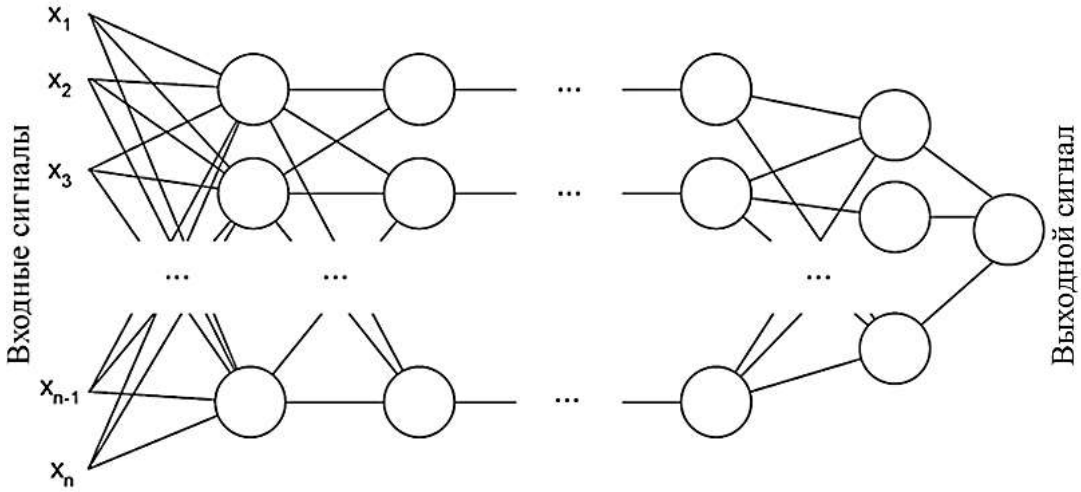

Рис. 3. Структура многослойного персептрона

В качестве глобальных признаков были выбраны:

- центр масс;
- высота подписи в пикселях после нормализации;
- отношение высоты к ширине;
- область изображения (это количество черных пикселей на изображении);
- вертикальное разделение;
- горизонтальное разделение;
- максимум вертикальной проекции;
- максимум горизонтальной проекции;
- количество краевых точек;
- количество точек пересечений.

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 размера длины 164.

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

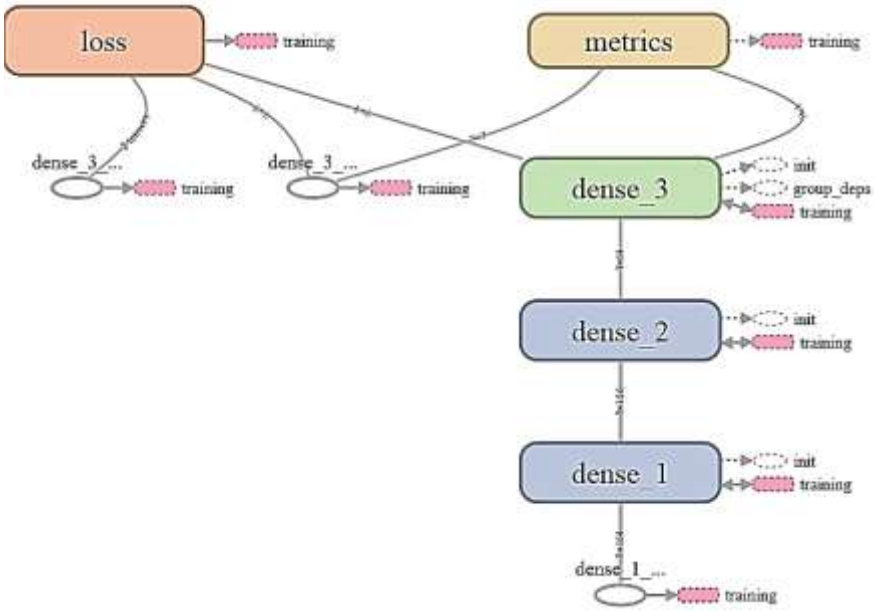

Рис. 4. Граф нейронной сети в TensorBoard

В результате работы алгоритма были достигнуты следующие показатели: FRR, равный 3.3 %, и FAR, равный 5 %.

Заключение

На данный момент написано довольно много статей по данной тематике, однако величина ошибок первого и второго рода редко достигает хотя бы 3-4 %. В этом статическая верификация подписи уступает многим другим технологиям, например, сканированию отпечатков пальцев или радужной оболочки глаза. Тем не менее, учитывая сложность данных методов и стоимость оборудования для их обеспечения, нейросетевой подход к верификации рукописной подписи является перспективным направлением, нуждающимся в оптимизации отрицательных качеств и повышении точности распознавания. Результатом проведенной работы является оценка ошибок распознавания образов из базы данных подписей. В дальнейшем планируется совершенствование алгоритма и улучшение статистики по ошибкам 1-го и 2-го рода, а также сбор большей по объему выборки. Предполагается, что точность распознавания нейронной сети может быть повышена посредством увеличения количества и информативности признаков, извлекаемых из изображения. Главным направлением последующих исследований будет являться выделение новых глобальных и локальных признаков, позволяющих этого достичь.

Список литературы

[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. P. 33-41.

[2]. McCabe A., Trevathan J., Read W. Neural Network-based Handwritten Signature Verification // Journal of computers. 2008. Vol. 3. No. 8. P. 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 // Journal on Applied Signal Processing. 2004. Vol. 4. P. 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. P. 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. P. 15-28.

[6]. Daqrouq K., Sweidan H., Balamesh A., Ajour M. Off-Line Handwritten Signature Recognition by Wavelet Entropy and Neural Network // Entropy. 2017. No. 19. DOI: 10.3390/e19060252.

[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. P. 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? // BSc Computing and Information Systems. London, 2006. 123 p.

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