УДК 004.032.26

АХУНДЖАНОВ У. Ю., СТАРОВОЙТОВ В. В.

OFF-LINE ВЕРИФИКАЦИЯ РУКОПИСНОЙ ПОДПИСИ С ПРИМЕНЕНИЕМ СВЕРТОЧНОЙ НЕЙРОННОЙ СЕТИ

Государственное научное учреждение «Объединенный институт проблем информатики Национальной академии наук Беларуси»

Данная статья посвящена разработке метода обнаружения подделки рукописных подписей. Подпись до сих пор остается одним из самым распространенных методов идентификации личности. Подпись на финансовых и других документах может быть подделана, поэтому выявление подделки является актуальной задачей. Это задача бинарной классификации: определить является подпись подлинной или фальшивой.

В статье описываются результаты распознавания рукописных подписей, выполненных на бумажном носителе. Для экспериментов использовалась база рукописных подписей 10 человек. Для каждого человека было собрано 10 подлинных и 10 поддельных подписей, выполненных другими людьми. Подписи были оцифрованы в виде цветных изображений с разрешением 850×550 пикселей. Затем формировалось бинарное представление каждой подписи. Для классификации использовались три варианта уменьшения подписей до размеров: 128×128, 256×256 и 512×512 пикселей. Эти изображения служили исходными данными для сверточной нейронной сети.

В результате тестирования предлагаемого подхода средняя точность корректной классификации достигнута на изображениях среднего размера и равняется 93,33%.

Ключевые слова: *Распознавание, верификация, рукописная подпись, классификация, FRR, FAR.*

Введение

Распознавание образов широко применяется в таких областях, как цифровая обработка изображений, компьютерное зрение, биометрия создание интеллектуальных систем безопасности, контроля доступа и т. п. Одной из актуальных задач является распознавание рукописных текстов, подписей.

Термин «распознование» объединяет два понятия – «верификация» и «идентификаци». ***Верификация*** – это подтверждения соответствия представленной биометрической характеристики человека определенному идентификатору, который указывает пользователь. Процедура выполняется путем сравнивания кода (из представленной биометрической характеристики) с кодами, хранящимися в базе данных (БД) и соответствующими определенному идентификатору пользователя. ***Идентификация*** – это сравнение вычисленного по биометрической характеристике человека кода с кодами, хранящимися в БД, с целью авторизации пользователя [1].

Самый распространенный способ персональной аутентификации в биометрии является рукописная подпись. Он широко используется во многих банках, деловых операциях и документах, которые утверждаются с помощью подписей.

Идентификацию рукописной подписи можно выполнять статически в режиме online и динамически в режиме off-line.

Статическое или off-line распознавание подписи выполняется после того, как её образ на бумаге был оцифрован. Затем цифровые изображения преобразуются и анализируются [3]. В динамических или online системах распознавания анализ начинается в процессе её создания. Дополнительно собирается информация о последовательности координат x и y точек подписи, информация о силе нажатия, скорости написания и т.д.

Сложность задачи исследования подписи определяется следующими факторами [2]:

– подпись – это краткий и мало информативный набор данных;

– она может быть скопирована с применением технических средств;

– на проверяющего могут воздействовать сбивающие факторы;

– почерки разных людей естественным образом бывают схожи;

– подпись человека всегда вариативна.

Для решения данной проблемы было предложено множество различных подходов. Точность их распознавания проверялась на общедоступных наборах данных, таких как GPDS960, GPDS-4000, MCYT и CEDAR и др. Все эти наборы данных содержат три группы подписей, подлинные, случайные и квалифицированные поделки.

Распознавание рукописной подписи широко исследуются последние десятилетие, но остается открытой проблема создания технологии, которая могла бы показать высокую точность распознавания подписи.

Целью систем проверки подписи является в различение подлинных подписей от поддельных. Это сложная задача, особенно в статическом методе распознавания, использующем изображения полученных путем фотографирования или сканирования, где динамическая информация о процессе подписания недоступна.

Применение нейросетевых технологий помогает верифицировать подписи более точно. Это обусловлено тем, что нейронные сети эффективно строят нелинейные зависимости, которые точнее описывают данные, они более устойчивы к шумам во входных данных и адаптированы к их изменениям. Обзоры данных работ приведены в работах [3-6].

В статье [7] приведены формулы вычисления 76 функций, а в [8] описаны 44 функции оценки результатов бинарной классификации. В статье [9] даны формулы пяти наиболее распространенных функций оценки результатов бинарной классификации, представленных матрицей ошибок, и исследованы некоторые свойства этих функций.

В большинстве случаев результаты классификаторов оцениваются по матрицам ошибок (confusion matrix). В табл. 1 представлены объекты, верно, определенных классов (true) и ошибочно определенных классов (false) в виде такой матрицы [10].

Таблица 1 – Матрица ошибок бинарной классификации

Предсказанный класс	Истинная классификация	
	Класс 1	Класс 2
Класс1	True Positive (TP)	False Positive (FP)
Класс 2	False Negative (FN)	True Negative (TN)
Число объектов в классе	TP + FN = общее число объектов класса 1	FP + TN = общее число объектов класса 2

Для оценки эффективности распознавания и верификации используют такие показатели, как ошибка первого рода FRR (отношение числа ошибочно отклонённых подлинных подписей к общему числу подлинных подписей), ошибка второго рода FAR (отношение числа ошибочно принятых подделок к общему числу подделок) и мера EER - уровень равной вероятности ошибок, при котором FAR и FRR равны [1].

FAR и FRR определяются по формулам:

$$FAR = FPR = \frac{FP}{FP + TN}$$, где FPR = ложноположительный коэффициент;

$$FRR = FNR = \frac{FN}{FN + TP}$$, FNR = ложноотрицательный коэффициент;

FP (False positive) – ложноположительное решение, также называется ошибкой 1–го рода. Модель предсказала положительный результат, а на самом деле отрицательный;

TP (True positive) – истинноположительное решение. Модель предсказала положительный результат, прогноз совпал с реальностью;

FN (False negative) – ложноотрицательное решение, также называется ошибкой 2–го рода. Модель предсказала отрицательный результат, а на самом деле положительный;

TN (True negative) – истинноотрицательное решение. Модель предсказала отрицательный результат, прогноз совпал с реальностью;

Для оценки классификации нашей модели использовали функцию (Accuracy). Авторы статьи [10] считают, что функция Accuracy определяет долю правильных ответов и кратко можно перевести как правильность или точность. При равном число объектов обоих классов эту функцию можно использовать для оценки результатов классификации.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

В таблице 2 представлены результаты распознавания по метрике Accuracy.

Подготовка данных для распознования для цифровых изображений

В качестве экспериментальных данных для обучения системы распознавания рукописной подписи использовалась база, содержащая 200 изображений рукописных подписей 10 человек размером 850×550 пикселей. В базе было 10 подлинных и 10 поддельных подписей каждого человека. На (рис. 2 и рис.3) изображены примеры рукописных подписей 10 человек до и после предварительной обработки.

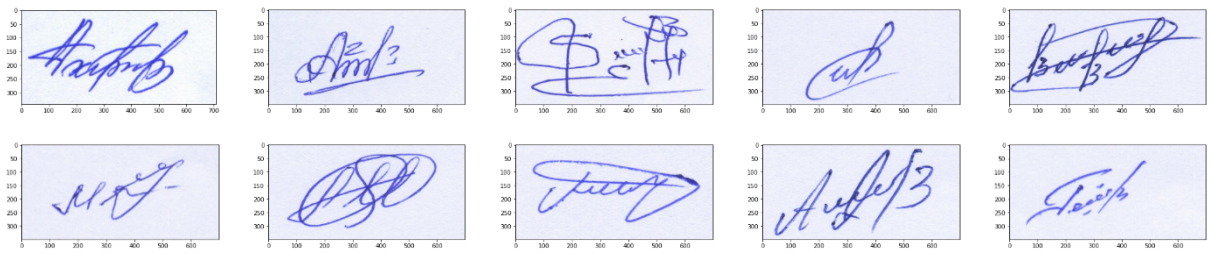


Рис.2 – Примеры образцов исходных подписей

Изображения рукописных подписей преобразовывалось в полутоновый вид, а затем в бинарный. Для этого использовался метод Отцу. С помощью данного метода вычисляется порог t, минимизирующий среднюю ошибку сегментации, т.е. среднюю ошибку от принятия решения о принадлежности пикселей изображения к объекту

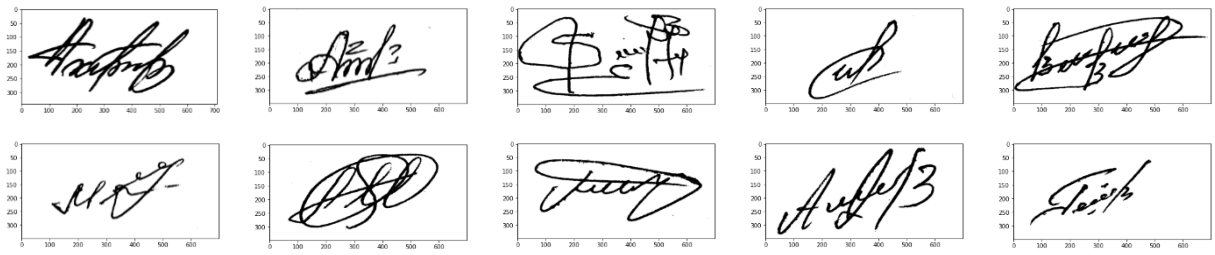


Рис.3 – Примеры образцов рукописных подписей после предварительной обработки

База данных была собрана с помощью студентов Ферганского филиала Ташкентского университета имени Мухаммада ал-Хорезми.

Применение сверторчной нейронной сети

Для распределения классов изображения создавали каталоги, в каждом каталоге создаются по два подкаталога, в соответствии с названиями классов: genuine (подлинные) и forced (поддельные).

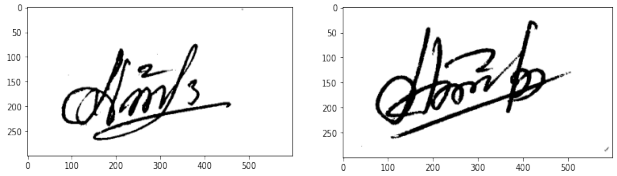
Эксперименты выполнялись с уменьшением подписей до размеров 128×128, 256×256, 512×512 пикселей.

Архитектура сверторчной нейронной сети

Модель глубокого обучения, использованная для получения результатов, описана ниже:

1. Слой свертки, размер ядра 3x3, количество карт признаков - 32 штуки, функция активации ReLU.
2. Слой подвыборки, выбор максимального значения из квадрата 2x2.
3. Слой свертки, размер ядра 3x3, количество карт признаков - 32 штуки, функция активации ReLU.
4. Слой подвыборки, выбор максимального значения из квадрата 2x2.
5. Слой свертки, размер ядра 3x3, количество карт признаков - 64 штуки, функция активации ReLU.
6. Слой подвыборки, выбор максимального значения из квадрата 2x2.
7. Слой преобразования из двумерного в одномерное представление.
8. Полносвязный слой, 64 нейрона, функция активации ReLU.
9. Слой Dropout. Это метод прореживания, который используется для усреднения получения результатов обучения.
10. Выходной слой, 1 нейрон, функция активации sigmoid.

Слои с 1 по 6 используются для выделения важных признаков на изображении, а слои с 7 по 10 - для оценки результата классификации.



а) б)

Рис. 5 – Примеры подписи

а) подлинная подпись б) поддельная подпись

На рис. 6. а) и б) приведены графики точности обучения и валидации, а также изменение точности и потерь во время обучения. На примере проверочных данных одного человека для изображений подписей с разрешением изображения подписи 256x256 пикселей.

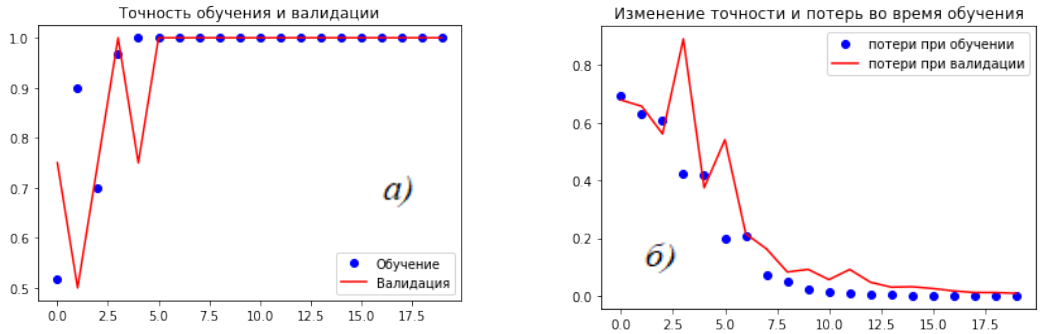


Рис.6 – Пример обучения нейросети (метрике accuracy) для одного человека:

а) - График обучения и валидации; б) - График функции потерь

На этапе обучения набор подписей 3-го человека показал наихудший результат валидации и тестирования. Вероятно подпись этого человека имеет нетипичные определяющие признаки.

На рис. 7. показаны образцы подлинной подписи для 3-го человека.

Рис. 7 – подлинные подписи

На рис 8. приведены графики точности обучения и валидации, а также изменение точности и потерь во время обучения. Обучение и точность на наборе проверочных данных для 3-го человека с разрешением изображения подписи 256x256.

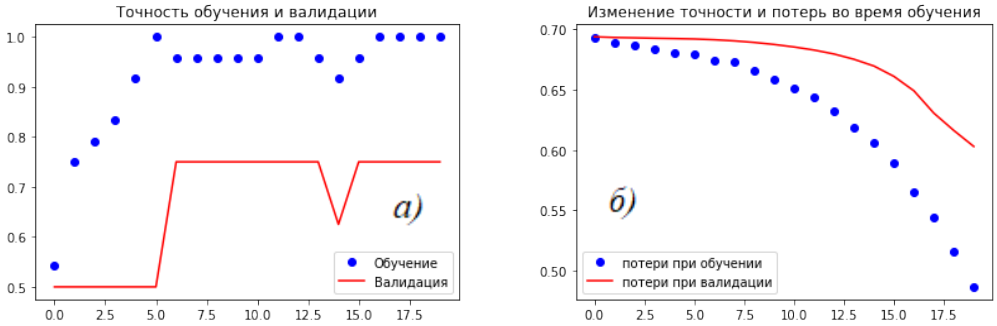


Рис.8 – Пример обучения нейросети по метрике accuracy для 2-го человека
а) *График обучения и валидации*; б) *График функции потерь подписей с разрешением*

Модель обучалась на рукописных подписях для всех 10 человек, а также индивидуально для каждого человека.
На рис.9. показаны графики обучения для всех 10 человек с размерами 128×128, 256×256, 512×512 пикселей. Из рис.9. видно, что точность обучения модели во всех случаях показала максимальный результат обучения

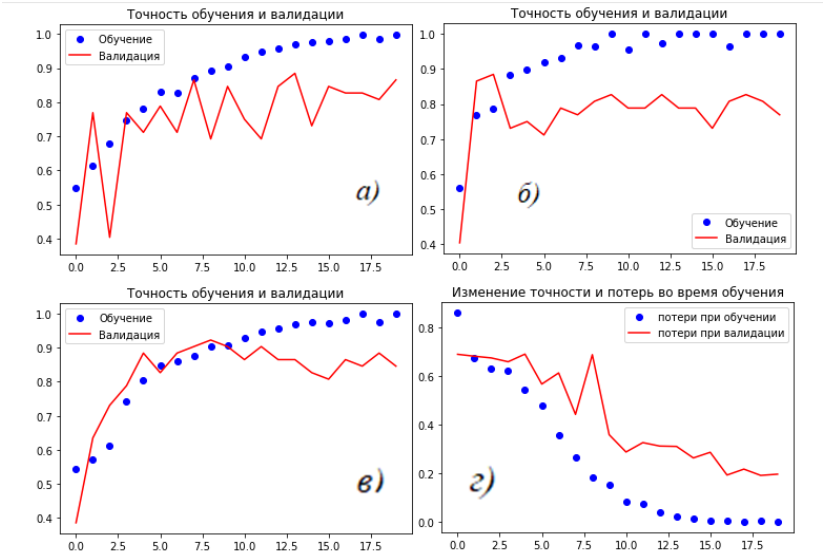


Рис.9 – Пример обучения нейросети для 10 человек:

а) График обучения и валидации сразрешением изображения 118x118;
б) График обучения и валидации сразрешением изображения 512x512;
в) График обучения и валидации сразрешением изображения 256x256;
г) График функции потерь подписей с разрешением 256x256.

Анализ результатов бинарной классификации данных

Для обучения, валидации и тестирования модели было использовано 200 изображений рукописных подписей в пропорции 8:1:1 соответственно. Половина из них была изображениями подлинными подписями, а вторая половина — подельными.

Вычислительный эксперимент проводился на компьютере, с дискретным видеокартой Intel (R) HD Graphics 5500 (1 ГБ видеопамяти).

Для создания системы распознавания рукописной подписи было разработано несколько программ на языке Python с использованием моделей глубокого обучения. Работу данного программного обеспечения можно разделить на несколько этапов: подготовка набора данных, сбор изображений с одновременной предобработкой, обучение на собранных данных посредством подготовленной модели обучения.

В результате тестирования модели TP = 85, TN = 83, FP = 7, FN = 5 и

$$Accuracy = \frac{85+83}{85+83+7+5} = 0,9333$$

Обученная модель нейронной сети лучший результат показала при разрешении рукописных подписей 256x256 пикселей (таблица № 2).

Таблица 2 – Результаты распознавания подписей отдельных людей

№ каждого человека	Правилность распознования с расширением 128x128	Правилность распознования с расширением 256x256	Правилность распознования с расширением 512x512
Человек №1	90,5	**95,2**	91,1
Человек №2	98	**100**	94,2
Человек №3	75,2	**76,2**	75,3
Человек №4	91,2	**96,4**	90,1
Человек №5	80,4	**93,5**	87,5
Человек №6	85,8	**92,1**	89,8
Человек №7	93,5	**94,6**	92,7
Человек №8	88,7	95	**96**
Человек №9	79,8	90,3	89,5
Человек №10	**100**	**100**	96
Среднее	**88,31**	**93,33**	**90,22**

Заключение

Off-line верификация подписи уступает в точности технологии on-line. Результаты экспериментов, описанных в статье, показали, что подход к верификации рукописной подписи является перспективным направлением.

Средняя точность корректной классификации подписей, достигнута на изображениях размера 256x256, и равняется 93,33%. В дальнейшем планируется усовершенствовать алгоритм и повысить точность распознавания, а также сформировать выборку большего объема с применением аугментации данных на этапе обучения сети. Основным направлением последующих исследований будет выделение информативных признаков, позволяющих достичь высокого точности распознавание.

ЛИТЕРАТУРА

1. **Старовойтов В.В., Голуб Ю.** Обработка изображений радужной оболочки глаза для систем распознавания. Минск: LAP LAMBERT Academic Publishing, 2018. – 188с.

2. **Бобовкин М.В.** Актуальные проблемы теории и практики судебно-почерковедческого исследования подписи // Вестник Московского университета МВД России. – 2017. – №.2. – С.109-115.

3. **Hafemann, L.G.** Offline handwritten signature verification — Literature review / **L.G. Hafemann, R. Sabourin, L.S. Oliveira** // Seventh International Conference on Image Processing Theory, Tools and Applications (IPTA) – 2017. 8p. DOI:10.1109/ipta.2017.8310112.

4. **Hadeel J.Jriash.** Offline handwritten signature verification system using neural network / **J.Jriash Hadeel, A. Z. Abdullah Nada** // International Journal of Computer Science and Mobile Computing. – 2015. Vol.4, Issue.10.– P. 403-412.

5. **Impedovo S.** Verification of Handwritten Signatures: an Overview / **S. Impedovo, G. Pirlo** // 14th International Conference on Image Analysis and Processing. – 2007. – P.191-196. DOI:10.1109/iciap.2007.4362778.

6. **Foroozandeh, A.** Offline Handwritten Signature Verification and Recognition Based on Deep Transfer Learning / **A. Foroozandeh, A.H. Ataollah, H. Rabbani** // International Conference on Machine Vision and Image Processing. – 2020, 7p. DOI:10.1109/mvip49855.2020.918748.

7. **Choi S.S.** A survey of binary similarity and distance measures / **S. S. Choi, S. H. Cha, C.C. Tappert** // Journal of Systemics, Cybernetics and Informatics. – 2010. – Vol. 8. – No.1. – P. 43–48.

8. **Canbek G.** Binary classification performance measures/metrics: A comprehensive visualized roadmap to gain new insights / **G. Canbek, S. Sagiroglu, T.T. Temizel, N. Baykal** // International Conference on Computer Science and Engineering. − 2017. – P. 821-826. DOI:10.1109/UBMK.2017.8093539.

9. **Sokolova M. Lapalme G.** A systematic analysis of performance measures for classification tasks / **M. Sokolova** // Information Processing & Management. – 2009. – Vol. 45. -№ 4. – P. 427–437.

10. **В. Старовойтов.** Сравнительный анализ оценок качества бинарной классификации / **В. Старовойтов, Ю. И. Голуб** // Информатика. – 2020. − Т. 17. − № 1. – С.87–101.

11. **Исрафилов, Х.С.** Исследование методов бинаризации изображений / **Х.С. Исрафилов** // Вестник науки и образования. – 2017. –Т.2.- № 6(30). − С. 43–50.

12. **Янковский, А.А.** Критерии выбора метода бинаризации при обработке изображений лабораторных анализов. АСУ и приборы автоматики [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/kriterii-vybora-metoda-binarizatsii-pri-obrabotke-izobrazheniy-laboratornyh-analizov/viewer. – Дата доступа: 25.12.2021.

REFERENCES

1. **Golub Yu., Starovoitov V.V.** Image processing of the iris for recognition systems. Minsk: LAPA LAMBERT Academic Publishing House, 2018. - 188 p.

2. **Bobovkin M.V.** Actual problems of the theory and practice of forensic handwriting analysis of the signature // Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia. - 2017. - No. 2. – P.109-115.

3. **Hafemann, L.G.** Offline handwritten signature verification — Literature review / **L.G. Hafemann, R. Sabourin, L.S. Oliveira** // Seventh International Conference on Image Processing Theory, Tools and Applications (IPTA) – 2017. 8p. DOI:10.1109/ipta.2017.8310112.

4. **Hadeel J.Jriash.** Offline handwritten signature verification system using neural network / **J.Jriash Hadeel, A. Z. Abdullah Nada** // International Journal of Computer Science and Mobile Computing. – 2015. Vol.4, Issue.10.– P. 403-412.

5. **Impedovo S.** Verification of Handwritten Signatures: an Overview / **S. Impedovo, G. Pirlo** // 14th International Conference on Image Analysis and Processing. – 2007. – P.191-196. DOI:10.1109/iciap.2007.4362778.

6. **Foroozandeh, A.** Offline Handwritten Signature Verification and Recognition Based on Deep Transfer Learning / **A. Foroozandeh, A.H. Ataollah, H. Rabbani** // International Conference on Machine Vision and Image Processing. – 2020, 7p. DOI:10.1109/mvip49855.2020.918748.

7. **Choi S.S.** A survey of binary similarity and distance measures / **S. S. Choi, S. H. Cha, C.C. Tappert** // Journal of Systemics, Cybernetics and Informatics. – 2010. – Vol. 8. – No.1. – P. 43–48.

8. **Canbek G.** Binary classification performance measures/metrics: A comprehensive visualized roadmap to gain new insights / **G. Canbek, S. Sagiroglu, T.T. Temizel, N. Baykal** // International Conference on Computer Science and Engineering. − 2017. – P. 821-826. DOI:10.1109/UBMK.2017.8093539.

9. **Sokolova M.** Lapalme G. A systematic analysis of performance measures for classification tasks / **M. Sokolova** // Information Processing & Management. – 2009. – Vol. 45. -№ 4. – P. 427–437.

10. **Starovoitov V. V., Golub Y. I.** Comparative study of quality estimation of binary classification. Informatics. – 2020. – Vol. 17, no. 1, P. 87−101 (in Russian).

11. **Israfilov, Kh.S.** Research of image binarization methods / **Kh.S. Israfilov** // Bulletin of science and education. - 2017. - No. 6(30). −P. 43–50.

12. **Yankovsky, A.A.** Criteria for choosing the binarization method for processing images of laboratory analyses. Automated control systems and automation devices [Электронный ресурс] - Режим доступа: https://cyberleninka.ru/article/n/kriterii-vybora-metoda-binarizatsii-pri-obrabotke-izobrazheniy-laboratornyh-analizov/viewer. – Дата доступа: 25.12.2021.

V.V. Starovoitov, U.Yu.Akhundjanov

VERIFICATION OF A STATIC (OFF-LINE) SIGNATURE USING A CONVOLUTIONAL NEURAL NETWORK

This article is devoted to the development of a method for detecting forgery of handwritten signatures. The signature still remains one of the most common methods of identification. The signature on financial and other documents can be forged, so detecting forgery is an urgent task. This is the task of binary classification: to determine whether the signature is genuine or fake.

The article describes the results of recognition of handwritten signatures made on paper. A database of handwritten signatures of 10 people was used for experiments. For each person, 10 genuine and 10 forgery signatures made by other people were collected. The signatures were digitized as color images with a resolution of 850×550 pixels. Then a binary representation of each signature was formed. Three variants of reducing signatures to sizes were used for classification: 128×128, 256×256 and 512×512 pixels. These images served as the source data for the convolutional neural network.

As a result of testing the proposed approach, the average accuracy of the correct classification was achieved on medium-sized images and is equal to 93.33%.

Keywords: *Recognition, verification, handwritten signature, classification, FRR, FAR.*

Старовойтов Валерий Васильевич, доктор технических наук, профессор. Главный научный сотрудник ОИПИ НАН Беларуси. Лауреат Государственной премии Республики Беларусь (2003г). Сфера научный интересов: обработка и анализ цифровых изображений, полученных в разных участках электромагнитного спектра. Опубликовал более 150 научных работ.
Starovoitov Valery, Doctor of Sciences and professor of computer science. He is a Principal research fellow at the United Institute of Informatics Problems, National Academy of Sciences of Belarus (UIIP NAN Belarus). Award: the State Prize of the Republic of Belarus in science. Research interests of professor Starovoitov are processing and analysis of digital images obtained in different parts of the electromagnetic spectrum. He has published over 150 papers.

E-mail: valerystar@mail.ru

Ахунджанов Умиджон Юнус угли, аспирант Объединенного института проблем информатики Национальной академии наук Беларуси.
Akhundjanov Umidjon Yunus ugli, PhD student at the United Institute of Informatics Problems, National Academy of Sciences of Belarus