UDC 004.032.26

STATIC SIGNATURE VERIFICATION BASED ON MACHINE LEARNING

U.Yu. Akhundjanov
phd student at the United Institute of Informatics Problems, National Academy of Sciences of Belarus

V.V. Starovoitov
doctor of engineering sciences, professor, chief researcher UIIP NAS of the Republic of Belarus

United Institute of Informatics Problems of the National Academy of Sciences of Belarus, Republic of Belarus E-mail: umidjan_90 @ mail.ru

U.Yu. Akhundjanov

Graduated from Tashkent University of Information Technologies named after Muhammad al-Kharazmiy Fergana branch. PhD student at the United Institute of Informatics Problems of the National Academy of Sciences of Belarus. Conducts research on off-line handwritten signature verification.

V. V. Starovoitov

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.

Abstract. This paper describes the results of handwritten signature recognition. A handwritten signature database of 40 people made on paper and a publicly available Bengali handwritten signature database of 100 people were used for the experiments. A handwritten signature database of 40 people was collected with 10 authentic and 10 fake signatures for each person made by other people. A Bengali handwritten signature database of 100 people was collected 24 authentic and 30 forged signatures for each person. For this experiment, 20 people were randomly selected from the Bengal Handwritten Signature Database. Four options were used to reduce the signatures to sizes: 200×120, 250×150, 300×150, and 400×200 pixels for classification. These images served as input data for the proposed network architecture.

As a result of testing the proposed approach, the average accuracy of correct classification for the first base of handwritten signatures reached 90.04%. For the base of Bengal handwritten signatures 97.50%.

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

Introduction.

Handwritten signatures are an undeniable and unique way of confirming a person's identity. Because of its simplicity and uniqueness, it occupies an important place in the field of behavioral biometrics. Signatures are the most widely used biometric attribute, they are widely used in many banks, business transactions and documents that are approved with signatures and therefore secure authentication becomes an imperative.

Biometrics by the type of biometric parameters used are divided into two types into physiological and behavioral, where physiological features include facial shape, fingerprint, iris, retina, DNA. [1, 2, 7, 8], behavioral biometrics include handwritten signature, gait, voice. [6, 9].

With the development of technology today, there are a large number of financial transactions that need to be verified for authenticity. Today, most institutions actively use traditional signature verification methods. For the most part, traditional methods are manual and require experienced

professionals for this purpose. Manual verification is time consuming and is a completely subjective process which depends greatly on the experience of the specialist verifying the signature in question. Biometrics plays an important role in development of a modern automatic identification and verification method [10].

Handwritten signature identification can be done statically in online mode and dynamically in off-line mode. Static or off-line signature recognition is performed after its image on paper has been digitized. The digital images are then transformed and analyzed [3]. In dynamic or online recognition systems the analysis begins during its creation. Additionally, information about the sequence of x- and y-coordinates of the signature points, information about the pressing force, writing speed etc. is collected. The static mode of signature verification has fewer informative features, which makes its process more complicated [11].

Many different approaches have been proposed to solve this problem. The accuracy of their recognition was tested on publicly available datasets, such as GPDS960, GPDS-4000, MCYT, BHSig260 and CEDAR, etc. All of these datasets contain three groups of signatures, genuine, random and qualified fakes.

The use of neural network technology helps to verify signatures more accurately. This is because neural networks effectively build non-linear dependencies, which describe the data more accurately, they are more robust to noise in the input data, and adapt to changes in the data. Reviews of these works are given in [3-6].

The authors of [12] proposed a method for static signature verification based on a convolutional neural network. They have investigated, that in the process of signature verification the manually created features have no or very little resemblance to the signature. The authors reported that convolutional neural networks produce more relevant features than manually created features. This paper used publicly available GPDS, PUC-PR datasets to evaluate the effectiveness of the method. They stated that their approach achieved the lowest EER (ratio of falsely accepted fakes to total fakes), but there was an imbalance between the false positive rate (FPR) and false negative rate (FNR). The authors later extended their work [11] and analyzed the deeply studied features that were extracted in [12]. They investigated different architectures and reported the lowest EER in the literature on the GPDS dataset.

The authors of [13] in their paper applied a Siamese convolutional network architecture for signature verification. A Siamese network has two identical networks with common weights, the same parameters and configuration, which accept different pairs of images as input. A Siamese network has two identical networks with common weights, identical parameters and configuration that take different pairs of images as input. These two networks are connected using a contrast loss function. According to the loss function, the similarity score between the two images is computed using the Euclidean distance, during back propagation the parameters are updated in the same way in both networks. The network was trained to reduce the distance between the "genuine - genuine" pair and increase the distance between the "genuine - fake" pair. The authors evaluated their method on completely different datasets, e.g., BHSig260, GPDS, CEDAR. But this method requires a large amount of time and high computational power, since two networks are trained simultaneously.

For estimation of efficiency of recognition and verification such indexes are used, as an error of the first kind FRR (ratio of the number of incorrectly rejected authentic signatures to the total number of authentic signatures), an error of the second kind FAR (ratio of the number of incorrectly accepted fakes to the total number of fakes) and measure EER - the level of equal probability of errors, at which FAR and FRR are equal [14].

FAR and FRR are determined by the formulas:

$$FAR = FPR = \frac{FP}{FP + TN},$$ FPR = False positive rate;

$$FRR = FNR = \frac{FN}{FN + TP}$$, FNR = False negative rate;

FP (***False positive***) - False positive solution, also called 1st kind error. The model predicted a positive result, but in fact it is negative;

TP (***True positive***) - a true positive solution. The model predicted a positive outcome, the prediction matched reality;

FN (***False negative***) - False negative decision, also called 2nd kind error. The model predicted a negative result and in fact it was positive;

TN (***True negative***) - a true negative solution. The model predicted a negative result, the prediction matched reality;

To evaluate the classification of our model, we used a function (Accuracy). The authors of the article [10] believe that the Accuracy function determines the share of correct answers and can be briefly translated as correctness or accuracy. When the number of objects of both classes is equal, this function can be used to estimate the classification results.

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

Preparation of data for handwritten signature recognition on images.

Two handwritten signature databases were used as experimental data for training the handwritten signature recognition system, one of which contained 800 handwritten signature images of 40 people. The database contained 10 authentic and 10 fake signatures of each person. Figure 1 shows examples of handwritten signatures for the first database.

This database of handwritten signatures was collected with the help of students at the Fergana branch of the Muhammad al-Khwarizmi Tashkent University. The signature samples were scanned at 800 dpi (dots per inch) and each signature was cut at 850×550 pixels. Figure 2 shows examples of Bengali handwritten signatures for the second base. A Bengali handwritten signature database of 100 people was collected with 24 authentic and 30 fake signatures for each person. For this experiment, 1,080 handwritten signatures of 20 people were randomly selected from the Bengal handwritten signature database.

The images of the handwritten signatures were converted to halftone and then to binary. For this purpose, a method of Otzu was used. This method is used to calculate a threshold t that minimizes the average segmentation error, i.e., the average error from deciding whether image pixels belong to an object or background [15-16].

Applications of a convolutional neural network.

A convolutional neural network is a very broad class of architectures, the main idea of which is to reuse the same parts of the neural network to handle different small local sections of inputs.

To distribute the image classes, directories were created, with two subdirectories created in each directory, according to the names of the classes: genuine and forced.

Experiments were performed with the reduction of captions to 200×120, 250×150, 300×150, and 400×200 pixels.

Figure 1. Examples of handwritten signatures for experiments

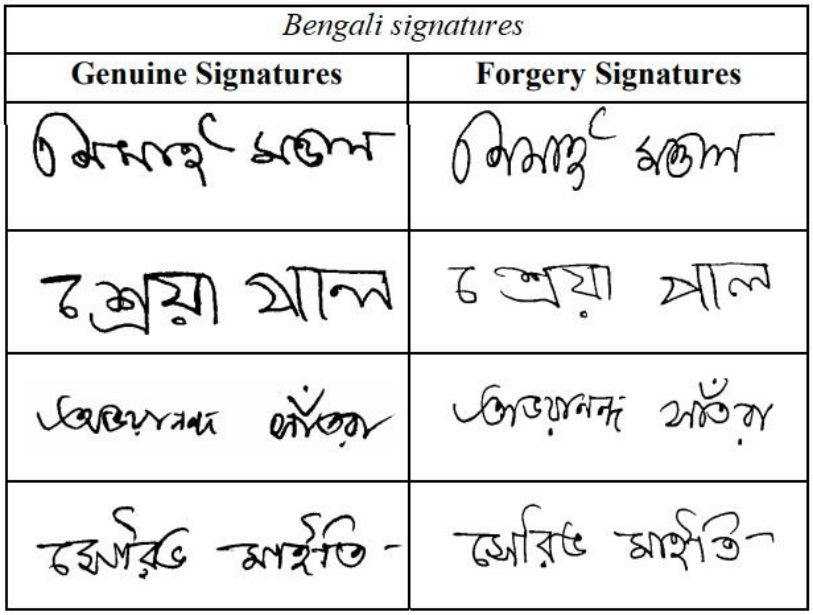

Figure 2. Examples of Bengali handwritten signatures for experiments

The architecture of the convolutional neural network.

The deep learning model used to produce the results is described below:

1. Convolution layer, kernel size 3x3, number of feature maps - 32 pieces, ReLU activation function.
2. Sub-sample layer, maximum value selection from 2x2 square.
3. The convolution layer, kernel size 3x3, number of feature cards - 32 pieces, ReLU activation function.
4. Layer of subsample, maximum value selection from 2x2 square.

5. The convolution layer, kernel size 3x3, number of feature cards - 64 pieces, ReLU activation function.
6. Layer of subsample, maximum value selection from 2x2 square.
7. Layer of conversion from two-dimensional to one-dimensional representation.
8. Full-link layer, 64 neurons, ReLU activation function.
9. Dropout layer. This is a thinning method which is used to average the training results.
10. Output layer, 1 neuron, sigmoid activation function.

Layers 1 to 6 are used to select important features in the image, and layers 7 to 10 are used to evaluate the classification result.

Results.

To train, validate and test the model, 800 handwritten signature images were used for the first base in an 8:1:1 proportion, respectively. Half of them were images of genuine signatures and the other half were images of fake signatures. For the second base, 1080 images of Bengali handwritten signatures in the proportion of 21:4:2, respectively. The computational experiment was performed on the https://colab.research.google.com/ platform.

Figure 3. Training and validation graph with 250x150 image resolution for first base

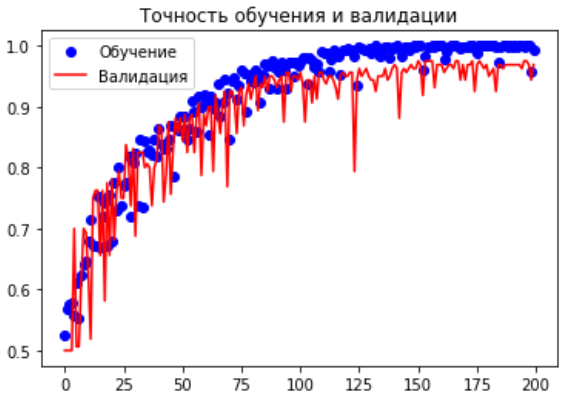

Figure 4. Training and validation graph with image resolution for the Bengali 250x150 base

Table 1. Results of signature recognition

Handwritten Signature Bases	The correctness of recognition with a 200x120 extension	The correctness of recognition with a 250x150 extension	The correctness of recognition with a 300x150 extension	The correctness of recognition with a 400x200 extension
Base 1	88,31	**90,04**	89,12	88,74
Base 2 (Bengali)	94,48	**97,50**	96,40	95,65

Table 1 shows the results of the experiments. The trained neural network model showed the best result in both bases at handwritten signature resolution of 250x150 pixels.

In order to create a handwritten signature recognition system, several programs were developed in Python using deep learning models. The work of this software can be divided into several stages: preparation of the dataset, image acquisition with simultaneous preprocessing, training on the collected data through the prepared learning model. The results of this experiment can be found on GitHub.com [17].

Conclusion.

Off-line signature verification is inferior to on-line technology in accuracy. The results of the experiments described in the article have shown that the approach to handwritten signature verification is promising.

The average accuracy of correct classification of signatures was achieved for the first base on images of size 250x150, and is equal to 90.04%, for the second base on images of size 250x150, and is equal to 97.50%. In the future, it is planned to improve the algorithm and increase the recognition accuracy, as well as to form a larger sample size. The main direction of further research will be the allocation of informative features that allow high recognition accuracy.

References

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

[2] Chaudhry, S. A. An enhanced lightweight anonymous biometric based authentication scheme for TMIS / S. A.Chaudhry, H. Naqvi, M. K. Khan // Multimedia Tools and Applications - 2017, 22 p. DOI:10.1007/s11042-017-4464-9.

[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] De Marsico, M. Iris recognition through machine learning techniques: A survey / M. De Marsico, A. Petrosino, S. Ricciardi // Pattern Recognition Letters – 2016, 14 p. DOI:org/10.1016/j.patrec.2016.02.001.

[8] Sharma S. Identity verification using shape and geometry of human hands / S. Sharma, S. R. Dubey, S. K. Singh, R. Saxena, R. K. Singh // Expert Systems with Applications – 2015. –P. 821–832. DOI: 10.1016/j.eswa.2014.08.052.

[9] Wan C. A Survey on Gait Recognition / C. Wan, L Wang, V. V. Phoha // ACM Computing Surveys. - 2018, 35p. DOI:10.1145/3230633.

[10] Ferrer, M. A. Robustness of Offline Signature Verification Based on Gray Level Features / M.A. Ferrer, J. F. Vargas, A. Morales, A.Ordonez // IEEE Transactions on Information Forensics and Security – 2012. – Vol.7, Issue.3.– P. 966–977. DOI:10.1109/tifs.2012.2190281.

[11] Hafemann L.G.Analyzing features learned for offline signature verification using deep cnns / L.G. Hafemann , R. Sabourin, L.S. Oliveira // 23rd international conference on Pattern recognition (ICPR). IEEE – 2016. – P. 2989–2994. DOI:10.1109/icpr.2016.7900092.

[12] Hafemann L. G. Writer-independent feature learning for Offline Signature Verification using Deep Convolutional Neural Networks / L.G. Hafemann, R. Sabourin, L.S. Oliveira // International Joint Conference on Neural Networks (IJCNN) – 2016. –P. 2576–2994. DOI:10.1109/ijcnn.2016.7727521.

[13] Jagtap, A. B. Siamese Network for Learning Genuine and Forged Offline Signature Verification / A. B. Jagtap, D. D. Sawat, R. S. Hegadi // Recent Trends in Image Processing and Pattern Recognition – 2019. – P. 131–139. DOI:10.1007/978-981-13-9187-3_12.

[14] 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).

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

[16] 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.

[17] Akhundjanov U.Yu. My_signature_verifiction / U.Yu. Akhundjanov // https://github.com [Electronic resource]. – 2022. Mode of access: https://github.com/MrUmidjan90/My-signature verification/blob/main/Bingali.ipynb– Date of access: 27 February 2022.

СТАТИЧЕСКАЯ ВЕРИФИКАЦИЯ ПОДПИСИ НА ОСНОВЕ МАШИННОГО ОБУЧЕНИЯ

У.Ю. АХУНДЖАНОВ
Аспирант Объединенного института проблем информатики НАН Беларуси

В.В. СТАРОВОЙТОВ
Главный научный сотрудник ОИПИ НАН Беларуси, доктор технических наук, профессор

Объединенный институт проблем информатики Национальной академии наук Беларуси, Республика Беларусь. E-mail: umidjan_90 @mail.ru

У.Ю. Ахунджанов

Окончил Ташкентский университет информационных технологий имени Мухаммада ал-Хоразмий Ферганского филиала. Аспирант Объединенного института проблем информатики НАН Беларуси. Проводит научные исследования о верификации рукописной подписи в режиме off-line.

В. В. Старовойтов

Главный научный сотрудник ОИПИ НАН Беларуси, доктор технических наук, профессор, 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.

Аннотация. В данной работе описываются результаты распознавания рукописных подписей. Для экспериментов использовалась база рукописных подписей из 40 человек, выполненных на бумажном носителе, а также общедоступный база Бенгальских рукописных подписей из 100 человек. База рукописных подписей из 40 человек было собрано 10 подлинных и 10 поддельных подписей для каждого человека, выполненных другими людьми. База Бенгальских рукописных подписей из 100 человек было собрано 24 подлинных и 30 поддельных подписей для каждого человека. Для данного эксперимента из Бенгальской базы рукописных подписей было рандомно выбрано 20 человек. Для классификации использовались четыре варианта уменьшения подписей до размеров: 200×120, 250×150, 300×150 и 400×200 пикселей. Эти изображения служили исходными данными для предложенной архитектуры сети.

В результате тестирования предлагаемого подхода достигнута средняя точность корректной классификации для первой базы рукописных подписей 90,04%. Для базы Бенгальских рукописных подписей 97,50%.

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