Impact Factor: 9.9 ISSN-L: 2544-980X

Handwritten Signature Verification Based on Convolutional Neural Network

U. Y. Axundjanov [1]

Abstract: This paper describes the results of recognizing handwritten signatures. For the experiments, the database of handwritten signatures BHSig260-Bengali, BHSig260-Hindi, CEDAR and TUIT was used. For classification, four options were used to reduce the signatures to sizes: 200×120, 250×150, 300×150 and 400×200 pixels. These images served as input for the proposed network architecture. As a result of testing the proposed approach, the average accuracy of correct classification of signatures on images of size 250×150 was achieved: for the CEDAR database it was 94.38%, for the BHSig260-Hindi database it was 95.63%, for the BHSig260-Bengali database it was 97.50% and for TUIT base is 90.04%.

Introduction

Biometric systems are used to identify a person based on physiological, psychological and behavioral characteristics [1, 3, 5]. Biometrics is used to verify and identify people [6]. A person's signature is one of his biometric images. Biometric systems can be divided into two groups depending on the type of characteristics being measured. The main groups of biometric systems include: Physiological biometric systems: This group includes systems that measure the unique physical characteristics of an individual. Examples include fingerprint recognition, facial recognition, iris recognition, hand recognition, and other systems that analyze anatomical features of the body. Behavioral biometric systems: In this group, systems measure characteristics associated with a person's behavior or manner of acting. Examples include voice recognition, gait recognition, signature analysis, and dynamic fingerprint recognition. These systems analyze unique patterns of behavior or actions that can be individually identified. Each group of biometric systems has its own advantages and limitations, and the choice of a particular system depends on the context of application and the requirements for security and usability.

One of the main advantages that handwritten signature verification technology has over other types of biometric technologies is that signatures are already accepted as a common method of personal identification. Handwritten signatures are a widely used behavioral biometrics. Even with the introduction of new technologies, handwritten signatures are constantly used in formal agreements, financial documents, identity documents, etc. The main difficulty observed in signature verification is inconsistencies between signatures of the same person: differences may arise due to the location and orientation of the signature, pen width, pen quality, stress, mood of the person and others. [2, 6].

Handwritten signature identification can be performed statically online and dynamically off-line. Static or off-line signature recognition is performed after its image on paper has been digitized. The digital images are then transformed and analyzed [2, 7]. In dynamic or online recognition systems, the analysis starts during the process of its creation. Additionally, information about the sequence of x and y coordinates of the signature points, information about the pressure force, writing speed, etc. is collected. The static mode of signature verification has fewer informative features, which makes its process more complex [2, 8, 10,11].

[1] Ferghana branch of Tashkent university of information technologies named after Muhammad al-Kwarizmi., Ferghana, Uzbekistan

Many different approaches have been proposed to solve this problem. Their recognition accuracy has been tested on publicly available datasets such as GPDS960, MCYT, BHSig260 and CEDAR and others. All these datasets contain three groups of signatures, genuine, random and qualified forgeries.

The application of neural network techniques helps to verify signatures more accurately. This is because neural networks efficiently construct nonlinear dependencies that describe the data more accurately, they are more robust to noise in the input data and are adaptive to changes in the data. Reviews of these works are given in [2, 5, 8, 9].

The authors of [5] proposed a method for static signature verification based on a convolutional neural network. They investigated that in the signature verification process, manually generated features have no or very little similarity to the signature. The authors reported that convolutional neural networks produced more relevant features than manually generated features. To evaluate the effectiveness of the method in this work, publicly available GPDS and PUC-PR data sets were used. They stated that their approach achieved the lowest EER (the ratio of the number of falsely accepted counterfeits to the total number of counterfeits), but there was an imbalance between the false positive rate (FPR) and false negative rate (FNR). Later, the authors extended their work [14] and analyzed the deeply learned features that were extracted in [12-14]. They explored different architectures and reported the lowest EER in the literature on the GPDS dataset.

The authors of the article [13] used the Siamese convolutional network architecture in their work to verify the signature. The 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 is two identical networks with common weights, the same parameters and configuration, which accept 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 two images is calculated using the Euclidean distance, during backpropagation, the parameters are updated in the same way in both networks. The network was trained to reduce the distance between a genuine-genuine pair and increase the distance between a genuine-fake pair. The authors evaluated their method on completely different datasets, for example, BHSig260, GPDS, CEDAR. But this method requires a lot of time and high computing power, since two networks are trained simultaneously.

Methods

To assess the effectiveness of recognition and verification, indicators such as the error of the first type FRR (the ratio of the number of incorrectly rejected genuine signatures to the total number of genuine signatures), the error of the second type FAR (the ratio of the number of incorrectly accepted counterfeits to the total number of counterfeits) and the EER measure - level equal to error probability, at which FAR and FRR are equal [14].

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;

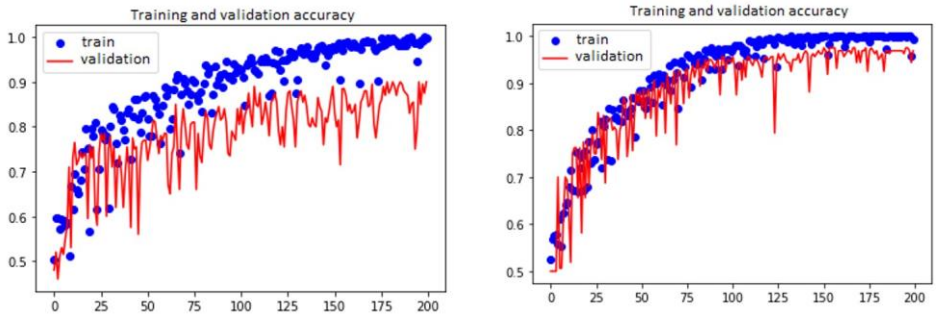
TN (True negative) - a true negative solution. The model predicted a negative result, the prediction matched reality;

The TUIT and BHSig260-Bengali databases of handwritten signatures were used as experimental data for training the system. 800 images of handwritten signatures of 40 people were taken from the TUIT database, 10 genuine and 10 forged signatures for each. This database of handwritten signatures was collected with the help of students from the Fergana branch of Tashkent University named after Muhammad al-Khorezmi. Sample signatures were scanned at 800 dpi (dots per inch) resolution, and

each signature was cropped at 850 × 550 pixels. From the Bengali database of handwritten signatures, 1080 handwritten signatures of 20 people were randomly selected.

800 handwritten signature images from TUIT database were used for training, validation and testing of the model, 1080 handwritten signature images were used from BHSig260Bengali database. In both databases, genuine and forged signatures were in equal amount. The computational experiment was conducted on https://colab.research.google.com/ platform.

Figure 1 shows the training and validation plots at 250×150 image resolution.



a) **b)**

Fig. 1 - Training and validation plots at 250×150 image resolution for bases: a) TUIT; b) BHSig260Bengali

Results and Discussions

For the next experiment, 800 handwritten signatures from 40 people were used from the TUIT database (this is approximately 22.2% of the total number of signatures presented in it), as well as the public databases of handwritten signatures BHSig260-Bengali, BHSig260Hindi and CEDAR [12-14]. For classification, four options were used to reduce the signatures to sizes: 200×120, 250×150, 300×150 and 400×200 pixels. From the Bengali database of handwritten signatures, 1080 handwritten signatures of 20 people were randomly selected, this is 20% of the total number of signatures represented in it; 1080 handwritten signatures of 20 people were randomly selected from the Hindi database, this is 12.5% of the total number of signatures presented in it; 960 handwritten signatures of 20 people were also randomly selected from the CEDAR database, which is approximately 36.3% of the total number of signatures presented in it.

Table 1 summarizes the results of the experiments. The trained neural network model showed the best result on both bases at the resolution of handwritten signatures of 250×150 pixels.

Table 1 - Results of verification of signatures from two databases

Handwritten signarure databases	200×120	250×120	300×120	400×120
TUIT	88,30	90,05	89,89	88,76
BHSig260-Bengali	94,88	97,54	96,40	95,66

To create a handwritten signature recognition system, several Python programs have been developed using deep learning models. The work of this software can be divided into several stages: preparing a data set, collecting images with simultaneous preprocessing, training on the collected data using a prepared learning model. The results of this experiment can be found on GitHub.com [12-14].

Conclusion

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

The average accuracy of correct classification of signatures was achieved on 250×150 images, for CEDAR base is 94.38%, for BHSig260-Hindi base is 95.63%, for BHSig260Bengali base is 97.50% and for TUIT base is 90.04%. In the future, it is planned to improve the algorithm and increase the recognition accuracy and generate a larger sample size. The main direction of further research will be the selection of informative features to achieve high recognition.

References

1. S. A.Chaudhry, H. Naqvi, M. K. Khan, An enhanced lightweight anonymous biometric based authentication scheme for TMIS (Multimedia Tools and Applications - 2017)
2. Hafemann, L.G. et.al., *Offline handwritten signature verification — Literature review* / Seventh International Conference on Image Processing Theory, Tools and Applications (IPTA) – 2017. 8p. DOI:10.1109/ipta.2017.8310112.
3. Hadeel J.Jriash. International Journal of Computer Science and Mobile Computing **4**, 10, 403-412 (2015)
4. Foroozandeh, A. et.al., *Offline Handwritten Signature Verification and Recognition Based on Deep Transfer Learning* International Conference on Machine Vision and Image Processing. – (2020). DOI:10.1109/mvip49855.2020.918748.
5. Hafemann L. G. et.al., *Writer-independent feature learning for Offline Signature Verification using Deep Convolutional Neural Networks* / International Joint Conference on Neural Networks (IJCNN) – P. 2576–2994 (2016). DOI:10.1109/ijcnn.2016.7727521.
6. Akhundjanov U.Y., Starovoitov V.V., System Analysis and Applied Information Science **1,** 12-18 (2022)
7. A. B. Jagtap, D. D. Sawat, R. S. Hegadi, *Siamese Network for Learning Genuine and Forged Offline Signature Verification* / // Recent Trends in Image Processing and Pattern Recognition, P. 131–139 (2019). DOI:10.1007/978-981-13-9187-3_12.
8. Impedovo S., et.al., *Verification of Handwritten Signatures: an Overview* /14th International Conference on Image Analysis and Processing. p.191-196 (2007). DOI:10.1109/iciap.2007.4362778.
9. Akhundjanov U.Y., Starovoitov V.V., System Analysis and Applied Information Science. **1**, 4-9 (2022)
10. Akhundjanov U.Yu. My_signature_verifiction / U.Yu. Akhundjanov // https://github.com [Electronic resource]. – 2022. Mode of access: https://github.com/MrUmidjan90/Mysignature verification/blob/main/Bingali.ipynb– Date of access: 27 February 2022.
11. Akhundjanov U. at al. Distribution of local curvature values as a sign for static signature verification. //BIO Web of Conferences. – EDP Sciences, 2024.
12. Akhundjanov U. at al. Handwritten signature preprocessing for off-line recognition systems. // BIO Web of Conferences. – EDP Sciences, 2024.
13. Kizi, T. S. G., & Murodiljanovich, I. K. (2024). Adaptive text recognition algorithms. *Miasto Przyszłości*, *47*, 269-273.
14. Kizi, T. S. G. (2024). Recursion and Him in Programming to Use. *Miasto Przyszłości*, *53*, 801-803.
15. Kizi, T. S. G., & Yuldoshaliyevich, S. M. (2024). CHOOSING TOOLS FOR IMPLEMENTING TEXT RECOGNITION SOFTWARE. *Miasto Przyszłości*, *47*, 261-264.