International Transaction Journal of Engineering, Management, & Applied Sciences & Technologies

http://TuEngr.com

PAPER ID: 10A13C

DATA AUGMENTATION AND NEURAL NETWORK MODELS CONSTRUCTION FOR HAND-WRITTEN CHARACTER RECOGNITION IN BIOMETRIC AUTHENTICATION SYSTEMS

Anastasia Gennadevna Isaeva [a*], Alexey Sergeevich Katasev [b], Amir Muratovich Akhmetvaleev [b], Dina Vladimirovna Kataseva [b]

[a] *Kazan Federal University, RUSSIA.*

[b] *Information Security Systems Department, Kazan National Research Technical University named after A.N. Tupolev, RUSSIA.*

ARTICLEINFO

Article history:
Received 14 May 2019
Received in revised form 25 July 2019
Accepted 06 August 2019
Available online 09 August 2019

Keywords:
biometric identification;
Augmented ANN;
Distorted handwriting;
Numeric handwriting;
Training ANN.

ABSTRACT

This paper solves the problem of neural network model construction for hand-written character recognition. The preparation of data for training neural networks was carried out using the augmentation method by including distortions of two types in the data: resizing and rotation of the characters. To build the models, two training sets were used: initial data and augmented data. The training accuracy of neural network models was 100%. To assess the generalization ability of the constructed models, a test sample with a volume of 1000 records (100 records for each digit) was formed, consisting of ordinary and distorted images of decimal digits missing in the training samples. The accuracy of the initial neural network model during testing was 84.7%, and the accuracy of the augmented model was 95 %. For each neural network model, errors of types I and II were calculated, having a value of 6.2% and 9.1% for the original neural network model and 1.8% and 3.2% for the augmented one. Consequently, the enrichment of the initial data allowed us to reduce the level of errors of the first type by 4.4%, and the number of errors of the second type by 5.9%. In addition, the total error of each model is calculated based on the three-block cross-validation method. The error of the original model was 0.21, and the augmented one - 0.07. Consequently, the total error of the augmented model decreased by 0.14 compared with the original model. Thus, the augmented neural network model is an effective hand-written character recognition tool and can be used in biometric authentication systems.

1. INTRODUCTION

Currently, in the biometric identification and authentication systems, the actual challenge is to

*Corresponding author (Anastasia Gennadevna Isaeva). E-mail: nastyaadema@mail.ru Volume 10 No.13 ISSN 2228-9860 eISSN 1906-9642 CODEN: ITJEA8 Paper ID:10A13C http://TUENGR.COM/V10A/10A13C.pdf DOI: 10.14456/ITJEMAST.2019.167

effectively recognize the characters handwritten by users [1,2]. On the one hand, it should be convenient for a person to use an authentication procedure, and on the other hand, the recognition accuracy must be high to prevent an attacker from gaining access to computer resources. At the same time, in order to increase the efficiency of information protection, corporate information systems increasingly use biometric authentication procedures, based, in particular, on the recognition of handwritten characters of registered users. At the same time, it is important to build fault-tolerant recognition systems that would solve the task with a high degree of accuracy both with use of the users' reference data and upon the noise pollution of biometric references in real-time.

In the paper, the problem is solved by developing an effective neural network model for recognizing the handwritten characters of users, which should be highly accurate due to the application of a special technique with augmentation (enrichment) of the training data set [3,4].

2. METHOD

Today, information systems use authentication methods based on checking the entered password using technical devices such as e-tokens, as well as using biometric authentication procedures [5]. The latter are the most reliable from the point of view of information security since a biometric reference cannot be lost, forgotten or replaced. For the task of recognizing handwritten characters of users, the choice of the most preferred method of biometric authentication becomes relevant. The most widely used are the following classes of methods [6-8]: template, feature, structural, and neural network.

In the first group of methods, hand-written character recognition is performed by comparing a scanned copy of the signature image with a biometric reference. For recognition, the input image is converted into a raster, and then it is compared with all known elements. Sample methods quickly and accurately perform recognition of images of handwritten signatures. However, their effectiveness is reduced if a noisy character is presented for recognition.

In the second group of methods, recognizable and reference images of handwritten characters are considered as *n*-dimensional feature vectors. When recognizing the next character, its vector is compared with the reference one. The similarity of the vectors by the selected distance measure corresponds to the successful completion of an authentication procedure by the user. Despite their simplicity and high efficiency of practical use, the feature methods, as well as the template ones, do not allow defective images to recognize with a high degree of accuracy.

In structural methods, the input vector image is described by a special graph that ensures the sustainability of recognition when the character form or the style are changed, which is important when recognizing handwritten characters. But just like the previous methods, they lose their advantage in the presence of noise and defects in the image.

The fourth group of recognition methods is based on the use of neural network models and algorithms [9]. In this case, the image being recognized is converted into a bitmask of a certain dimension; the brightness of each bit is encoded and written into a string. Thus, the number of input neurons in the model corresponds to the number of mask elements, and the number of output ones

corresponds to the number of different recognizable images. The advantage of neural networks is their universal approximating ability and the possibility of effective practical use for solving a wide range of tasks [10,11], including biometric authentication problems. In addition, if there is good training sample, neural networks are capable of detecting any objects with high accuracy under noisy conditions. Thus, when constructing neural network models of handwritten character recognition, special attention should be paid to the formation of initial data for their learning [12].

The analysis of the considered methods led to the conclusion about the preference of using neural networks in the task of biometric user authentication based on hand-written character recognition. However, when preparing data for training and testing the network, it is necessary to enrich them using different augmentation procedures (increase, decrease, rotation, and other character distortions). This will allow the training sample to diversify, and to improve the accuracy of the neural network model when recognizing actual characters.

In this paper a special augmentation method based on the initial enrichment of the training sample data with further examples obtained by using various kinds of distortions. To test the proposed technology, all numbers from “0” to “9” were chosen as basic handwritten characters.

For effective recognition of hand-written characters, a user preliminarily forms a set of reference records of all digits represented as 16-by-16- bit bitmasks. Figure 1 shows an example of such bitmasks for each digit.

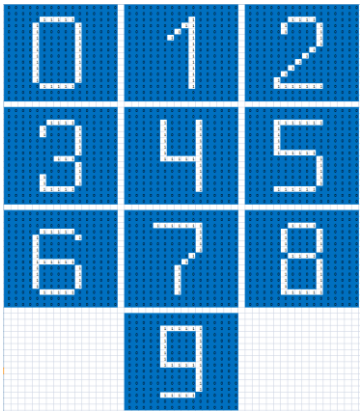

Figure 1: Example of decimal handwritten numbers.

Next, the initial data are formed for training and testing the neural network model. In this case, each bitmask is stretched to a row of 256 points in length corresponding to the dimension of the bitmask. A data sample is formed from a set of rows represented by 256 input values (0 or 1) and 10 output values (from 0 to 10).

After that, the prepared source data is enriched using the augmentation procedure. In this case, the neural network trained with the use of the initial data will be considered as the initial one, and the network trained on the enriched data will be considered as the augmented. In the latter case, the neural network has the best generalizing ability which makes it possible to recognize unfamiliar characters on the basis of such a network in the future.

There are several ways to enrich the source data. In this study, an augmentation method by adding distorted characters to the sample was used. In general, we can use various types of

distortions [13] from shift and rotation of individual parts of an image to placing over the image of additional lines, shadows, introducing blurriness, as well as the use of compression and stretching.

It is believed that the accuracy of image recognition is most influenced by such typical distortions as various rotations, as well as changes in the size of characters. Figure 2 shows an example of distorting the handwritten digits by changing their original dimensions.

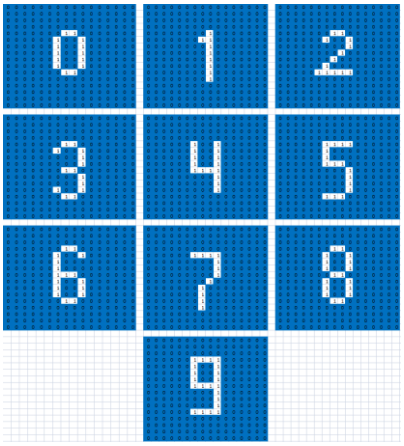

Figure 2: Example of distortion in the form of resizing characters

Figure 3 shows an example of distorting handwritten digits based on their rotation.

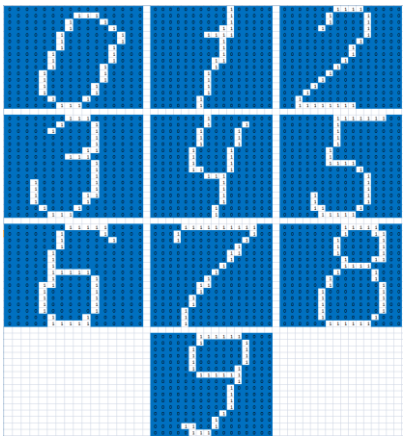

Figure 3: Example of distortion in the form of rotation of characters.

Thus, the original and augmented training sets will be used, respectively, to build two neural network models. In this case, the original training sample includes only reference records of digits and the augmented one complements them with distorted images.

A model in the form of a multilayer perceptron was chosen as the basis for the construction of neural network models. The constructed neural network models were successfully trained with 100% accuracy.

3. RESULT AND DISCUSSION

High accuracy results in training neural network models do not yet indicate their adequacy and the possibility of effective use in practice. Corresponding data samples consisting of 1000 records were formed for testing neural network models constructed and evaluating their generalizing ability. Moreover, in the test data, each image of the decimal digit was represented by 100 different variants, including the usual, distorted and noisy images. Table 1 presents the results of assessing

the generalizing ability of both the original and augmented neural network models.

Table 1: Test data recognition results based on the source and augmented neural networks

Digit	The number of cases of correct recognition		The number of cases of incorrect recognition	
	based on the original neural network	based on augmented neural network	based on the original neural network	based on augmented neural network
"0"	72	92	28	8
"1"	61	83	39	17
"2"	91	99	9	1
"3"	78	90	22	10
"4"	95	96	5	4
"5"	100	100	0	0
"6"	95	100	5	0
"7"	90	100	10	0
"8"	97	100	3	0
"9"	68	90	32	10

As can be seen from the table, when assessing the generalizing ability of the original neural network with 1000 test examples, 153 were recognized incorrectly. At the same time, the generalizing ability of this neural network model was 84.7%. When evaluating the generalizing ability of an augmented neural network of 1000 test cases, only 50 were recognized incorrectly. In this case, the generalizing ability of this model was 95 %. Consequently, based on the results of this experiment, we can conclude that the neural network trained on augmented data was 10.3% more accurate than the network trained on baseline data.

For each of the constructed neural network models, errors of types I and II were calculated. In biometric authentication systems, an error of type I is understood as the outcome of recognition when an unregistered user tries to enter the system and his/her handwritten character is perceived by the neural network model as correct. In this case, the attacker is given full access to the resources of the computer system. A type II error occurs when the presented biometric feature of a legal user is not recognized correctly. In this case, access for the registered user will be denied.

Each of the errors of types I and II was calculated when the initial and augmented neural networks were operating with test data samples.

The formula for calculating a type I error is as follows:

$$E_1 = \frac{n_1}{N} \times 100\% \quad (1),$$

Where n_1 is the number of cases when the sample of the hand-written character of an illegal user was perceived as correct, and N is the volume of the test data sample.

The formula for calculating a type II error is as follows:

$$E_2 = \frac{n_2}{N} \times 100\% \quad (2),$$

Where n_2 is the number of cases when a legal user's sample of a hand-written character was perceived as incorrect.

When testing the original neural network, as mentioned above, 153 examples were recognized incorrectly. Of these, 62 examples corresponded to the occurrence of a type I error, and the remaining 91 to the occurrence of a type II error.

The numerical value of the type I error is calculated as $E_1 = \frac{62}{1000} \times 100\% = 6{,}2\%.$

The value of the type II error $E_2 = \frac{91}{1000} \times 100\% = 9{,}1\%.$

When testing the augmented neural network having 50 recognition errors, 18 of them corresponded to errors of the first type, and 32 to the errors of the second type.

The numerical value for the type I error: $E_1 = \frac{18}{1000} \times 100\% = 1{,}8\%.$

The value for the type II error: $E_2 = \frac{32}{1000} \times 100\% = 3{,}2\%.$

The calculations made showed that the value of the type I error for the original neural network model was 6.2%, and the value of the type II error for this model was 9.1%. The corresponding type I and type II errors for the augmented neural network were 1.8% and 3.2%. Consequently, the augmentation of the neural network has reduced the number of errors of the first type by 4.4%, and the number of errors of the second type by 5.9%.

We calculate the total error of the original and augmented neural network models. To do this, we use the three-block cross-validation procedure [20]. This procedure involves splitting all available data into three equal parts, two of which are used to train the neural network, and the third is to test it. The cross-validation procedure is repeated three times by using different combinations of blocks for training and testing. The result of averaging the three test error values acts as a general model error.

Table 2 contains the results of a three-block cross-validation procedure and the total error determination of the original neural network model. As can be seen from Table 2, the total error of the original neural network model turned out to be 0.21.

Table 2: Total error calculation results for the original neural network model

Item No.	Error at 1 stage	Error at stage 2	Error at stage 3	Mean error
1	0.36	0.16	0.1	0.21
2	0.25	0.19	0.12	0.19
3	0.38	0.11	0.22	0.24
General model error				0.21

Table 3: Results of total error calculations for the augmented neural network model

Item No.	Error at 1 stage	Error at stage 2	Error at stage 3	Mean error
1	0.11	0.07	0.12	0.1
2	0.13	0	0.07	0.07
3	0	0.07	0.07	0.05
General model error				0.07

Table 3 contains the result of three-block cross-validation and the determination of the total

augmented model error. Table 3, the total error of the augmented neural network model was 0.07.

Consequently, the total error of the augmented neural network is 0.14 less than the corresponding error of the original neural network model.

4. SUMMARY

According to the results of the conducted research, it can be concluded that data augmentation has high efficiency and positively affects the accuracy of neural network models in recognizing handwritten characters. In all the experiments carried out related to the testing neural network models, calculating errors of types I and II, and calculating the total error, the augmented neural network showed significantly better results than the original neural network model.

5. CONCLUSION

Thus, augmentation is an effective method of enriching raw data for building neural network models that can be used as an effective tool for recognizing handwritten characters in biometric authentication systems.

6. AVAILABILITY OF DATA AND MATERIAL

Used or generated data already present in this study.

7. ACKNOWLEDGEMENT

The work is performed according to the Russian Government Program of Competitive Growth of Kazan Federal University. This work was supported by the Russian Federation Ministry of Education and Science, project № 8.6141.2017/8.9.

8. REFERENCES

[1] Chaudhari, K., & Thakkar, A. (2019). Survey on handwriting-based personality trait identification. Expert Systems with Applications, 124: 282-308.

[2] Choudhury, H., & Prasanna, S. (2019). Handwriting recognition using sinusoidal model parameters. Pattern Recognition Letters, 121: 87-96.

[3] Kamimura, R. (2019). SOM-based information maximization to improve and interpret multi-layered neural networks: From information reduction to information augmentation approach to create new information. Expert Systems with Applications, 125: 397-411.

[4] Shao, S., Wang, P., & Yan, R. (2019). Generative adversarial networks for data augmentation in machine fault diagnosis. Computers in Industry, 106: 85-93.

[5] Revathi, A., Jeyalakshmi, C., & Thenmozhi, K. (2019). Person authentication using speech as a biometric against playback attacks. Multimedia Tools and Applications, 78(2): 1569-1582.

[6] Liu, Q., Li, H., Zhang, Y., & Zhao, Z. (2019). Pattern recognition of messily grown nanowire morphologies applying multi-layer connected self-organized feature maps. Journal of Materials Science and Technology, 35(5): 946-956.

[7] Wang, T., Shu, K.-C., Chang, C.-H., & Chen, Y.-F. (2018). On the Effect of Data Imbalance for Multi-Label Pedestrian Attribute Recognition. Proceedings - 2018 Conference on Technologies and Applications of Artificial Intelligence, TAAI: 74-77.

*Corresponding author (Anastasia Gennadevna Isaeva). E-mail: nastyaadema@mail.ru Volume 10 No.13 ISSN 2228-9860 eISSN 1906-9642 CODEN: ITJEA8 Paper ID:10A13C http://TUENGR.COM/V10A/10A13C.pdf DOI: 10.14456/ITJEMAST.2019.167

[8] Katasev, A.S., Kataseva, D.V., & Emaletdinova, L.Yu. (2016). Neuro-fuzzy model of complex objects approximation with discrete output. Proceedings of 2nd International Conference on Industrial Engineering, Applications and Manufacturing, ICIEAM.

[9] Katasev, A.S., & Kataseva, D.V. (2016). Neural network diagnosis of anomalous network activity in telecommunication systems. Proceedings of IEEE Conference Dynamics of Systems, Mechanisms, and Machines, Dynamics.

[10] Ismagilov, I.I., Khasanova, S.F., Katasev, A.S., & Kataseva, D.V. (2018). Neural network method of dynamic biometrics for detecting the substitution of computer. Journal of Advanced Research in Dynamical and Control Systems, 10(10): 1723-1728.

[11] Anikin, I.V., Makhmutova, A.Z., & Gadelshin, O.E. (2016). Symmetric encryption with key distribution based on neural networks. Proceedings of 2nd International Conference on Industrial Engineering, Applications and Manufacturing, ICIEAM.

[12] Emaletdinova, L.Y., Matveev, I.V., & Kabirova, A.N. (2017). Method of designing a neural controller for the automatic lateral control of unmanned aerial vehicles. Russian Aeronautics, 60(3): 365-373.

[13] Wang, Y., Tang, Y.Y., Li, L., & Zheng, X. (2019). Block sparse representation for pattern classification: Theory, extensions, and applications. Pattern Recognition, 88: 198-209.

Anastasia Gennadevna Isaeva is a Junior Researcher, Kazan Federal University. She is affiliated with the research laboratory "Microwave Design and Radio Telecommunications" where she engages in the creation of an automated complex for end-to-end 3D design of microwave and high-frequency systems and the construction of measuring systems for high-frequency ranges.

Dr.Alexey Sergeevich Katasev is an Associate Professor of Information Security Systems Department of the Tupolev Kazan National Research Technical University named after A.N. Tupolev (KNITU-KAI). He is a Candidate of Technical Sciences. He graduated from the Physics and Mathematics Department of the Elabuga State Pedagogical Institute.

Amir Muratovich Akhmetvaleev is a Post-graduate student of Information Security Systems Department, Kazan National Research Technical University named after A.Tupolev (Kazan, Russia). He has a degree in Computer Science and Computer Engineering from Kazan National Research Technical University A.N. Tupoleva-KAI.

Dina Vladimirovna Kataseva is a Senior Lecturer at Department of Information Security Systems, Kazan National Research Technical University named after A.N. Tupolev. She is a graduate student at the same institute. She graduated in Accounting, Analysis, and Audit from Kazan State Institute of Finance and Economics. She also has studied in Informatics and Computer Engineering at Kazan National Research Technical University. A.N. Tupolev-KAI.