SNSIM

Procedia
Environmental Science, Engineering and Management
http://www.procedia-esem.eu

Procedia Environmental Science, Engineering and Management **7** (2020) (4) 591-598

International Conference on Agriculture, Environment and Allied Sciences (AEAS), December 24th-25th, 2020, Istanbul, Turkey

ADAPTIVE NEURAL NETWORK SYSTEM TO BUILD ENVIRONMENTAL PREDICTION AND CONTROL BY THEIR TYPING BIOMETRICS*

Oleg Yuryevich Panischev[1], Ekaterina Nikolaevna Ahmedshina[1], Nafis Gishkullovich Talipov[2], Alexey Sergeevich Katasev[2], Dina Vladimirovna Kataseva[2], Amir Muratovich Akhmetvaleev[2], Irina Vladislavovna Akhmetvaleeva[2]**

[1]Kazan Federal University, 18 Kremlyovskaya Street, Kazan, Republic of Tatarstan, Russia
[2]Kazan National Research Technical University named after A.N. Tupolev, Ulitsa Karla Marksa, 10, Kazan, Republic of Tatarstan, Russia

Abstract

Energy conservation, environmental protection, and intelligence are topics of interest in intelligent buildings. However, the energy requirement of various electrical equipment in smart buildings increases energy consumption. This paper presents a neural network-based prediction and control system for the regulation of building environmental parameters and discusses the problem of recognizing users by their typing biometrics. The expediency of its solution based on the training of a neural network is noted. The biometric authentication algorithm is described; the principles of this algorithm functioning, as well as the developed technology of biometric users authentication, are considered. This problem solution automating required the collection and preparation of initial data for analysis, neural network model constructing, as well as the research conducting and the accuracy of biometric user authentication based on the constructed models assessing. To prepare the initial data and form the training sample for the neural network training, a dataset consisting of 500 users typing biometrics templates, containing a username and a passphrase was created. A neural network model was constructed on the basis of the prepared data. The result of the calculated values ("Legal user" or "Illegal user") was used as an output feature. The research has shown, that the amount of the 1st type errors (the number of illegal users classified as legal) was 0%, and the value of the 2nd type errors (the number of legal users classified as illegal) was 3.3%. The percentage of correctly classified users based on the trained neural network was 96.7. Thus, the developed neural network system can be effectively applied for biometric user's authentication by using typing biometrics.

*Selection and peer-review under responsibility of the AEAS Conference
**Author to whom all correspondence should be addressed: opanischev@mail.ru

Keywords: biometric identification and authentication, environmental prediction, environmental prediction and control, neural network, typing biometrics.

1. Introduction

Currently, issues of environmental prediction, information security, in particular, computer systems user's biometric authentication (Kumar et al., 2017), are relevant for many subject areas (Das, 2017; Eom, 2014; Ismagilov et al., 2018). Recognizing users of a computer system, the identification and authentication subsystem should access (authorize) a legal user, and deny to access an illegal user. There are static (for example, fingerprint, hand geometry, iris) and dynamic (for example, handwritten signature, voice tone, typing biometrics) biometric authentication methods (Om and Banerjee, 2017). All of them have both obvious advantages (associated with the uniqueness of users biometric characteristics) and certain disadvantages (related to high cost, insufficient convenience of presenting a biometric standard, as well as with the presence of errors of the 1st and 2nd kind during recognition).

For the developers and researchers, the user's typing biometrics is the most attractive among the listed methods from the point of view of their low cost and recognition efficiency (Nelasa and Krischuk, 2001). Like handwriting, typing biometrics is developed over a certain (fairly short) time and then remains stable and unique for each user for a sufficiently long period of time. That is why typing biometrics can be viewed as an analogue of handwriting, and a passphrase typed on the keyboard can be viewed as an analogue of a genetically generated handwritten signature (Epishkina and Beresneva, 2020). Since a handwritten signature in most cases allows a person to be uniquely recognized and authenticated, using typing biometrics when typing a passphrase on the keyboard has the same capabilities. At the same time, such characteristics of typing biometrics as time delays (intervals) between pressing and releasing keys on the keyboard are often used for users recognition (Rosenberg-Adler and Weintraub, 2020).

After statistical processing of a set of such characteristics, a reference sample of a legal user is formed, as well as a vector of biometric elements of the typing biometrics of the current user trying to access system resources. The comparison by some criterion of a reference handwriting sample with a vector of biometric characteristics of the current user allows conducting authentication with a high degree of accuracy (Yellamma et al., 2020).

Thus, typing biometrics has a number of advantages over other methods of biometric authentication (Stefanova et al., 2012). The main of these advantages are the following: simplicity, low cost, no need to purchase additional equipment, the possibility of hidden user authentication. All this actualizes the necessity and practical usefulness of the development and use of biometric user authentication systems based on typing biometrics (Chantaf et al., 2020; Katasev, 2019).

2. Methods

It is known that biometric users authentication based on typing biometrics can be used in conjunction with password identification and authentication systems (Zhang et al., 2011). In this approach, the user enters a passphrase (presents it to the biometric authentication system) to confirm the identity of the identifier; the typing dynamics of the passphrase is the user's typing biometrics. In this case, an error in several characters of the passphrase will not lead to a denial of authentication. The decision to pass or not pass the authentication procedure will be made based on the analysis of the dynamics of entering a passphrase (user's typing biometrics).

It is important to take into account the following circumstance (Bhana and Flowerday, 2020): on the one hand, the length of the passphrase should not be short (it should allow a biometric sample of the user's typing biometrics to form from the point of view of the statistical processing method), and on the other hand, it should not be very long, so as not to be inconvenient for the user during his authorization. In this case, the passphrase must be memorized by the user, which also imposes a restriction on its length. Based on the above, the optimal length of a passphrase should be within the range from 21 to 42 characters, which is confirmed by the results of research conducted by a number of authors (Eremenko and Oliunina, 2019; Keith et al., 2009).

In addition, it is necessary to determine the characteristics of a user's typing biometrics in order to form a biometric standard. It is convenient from the point of view of practical implementation to record the time intervals for pressing and releasing keys while typing a passphrase. In this case, there is formed a time series of data (Dagaeva et al., 2019; Ismagilov and Khasanova, 2016; Last et al., 2018; Perfilieva et al., 2016) containing the values of the following characteristics (Eremenko and Oliunina, 2019):

- time between pressing the current key and releasing it;
- time between releasing the current key and pressing the next.

All values in the time series undergo statistical processing through calculating such characteristics of the initial data as mathematical expectation and dispersion (Khitsenko and Krutokhvostov, 2018). A biometric standard of the user's typing biometrics, as well as a vector of its input parameters, is subsequently formed from the values of these characteristics.

The formulas used to calculate the statistical characteristics of users' typing biometrics are as follows (Khitsenko and Krutokhvostov, 2018): the mathematical expectation of the time between pressing and releasing the current key (Eq. 1):

$$M_{PR} = \sum_{i=1}^{n} \frac{X_i}{n} \tag{1}$$

where X_i is the time interval between pressing and releasing the i-th key, and n is the number of characters pressed when typing a password phrase on the keyboard;

- the mathematical expectation of the time between releasing the current key and pressing the next (Eq. 2):

$$M_{RP} = \sum_{k=1}^{n} \frac{H_k}{n} \tag{2}$$

where H_k is the time interval between releasing and pressing the k-th key; - time variance between pressing and releasing the current key (Eq. 3):

$$D_{PR} = \sum_{i=1}^{n} \frac{(X_i - M_{PR})^2}{n} \tag{3}$$

- time variance between releasing the current key and pressing the next (Eq. 4):

$$D_{RP} = \sum_{k=1}^{n} \frac{(H_k - M_{RP})^2}{n} \tag{4}$$

The assessment of the information content of these features is carried out experimentally using the methods of mathematical statistics (Khitsenko and Krutokhvostov, 2018). Unlike password and technical authentication systems, it is always necessary for a biometric system not only to form a standard of a legal user but to train the system and configure it for a legal user. For effective recognition of users based on their typing biometrics, it is advisable to use adaptive self-learning neural network systems (Iryna et al., 2019; Ismagilov et al., 2019; Katasev et al., 2018a, 2018b), which allow performing efficient users biometric identification and authentication. The neural network authentication use allows to effectively adapt to the specific user's passphrase's biometric characteristics.

Thus, for neural network training, it is necessary to collect data of the user's typing biometrics, to prepare the collected data, to form training and testing samples, to construct a neural network model and to test it for the classifying ability assessing. As a result of the neural network training, a neural network model will be obtained that can effectively recognize users by their typing biometrics in biometric authentication systems. It provides adaptability of the biometric authentication system as a whole. The developed user recognition technology consists of the following stages:

1) data preparation and preliminary processing;
2) neural network training;
3) neural network model testing and evaluating.

The obtained initial data were presented in the form of a table, where each row represented users, and each column represented their parameters. To carry out this stage, we used our own database consisting of 500 user templates. Further, the process of data pre-processing and the formation of the training and testing samples took place. For this, a clear set of numerical parameters was selected that characterized users, the values of which were then included in the training and testing samples. The size of the training sample was 380 lines, and the size of the testing sample was 120 lines. When forming the samples, the requirement to balance the classes of solutions (legal/illegal user) in both samples was taken into account (Emaletdinova and Kabirova, 2019).

To solve the problem of constructing an adaptive biometric system for user recognition, a software package "Biometric Authentication System" has been developed. Its advantage is the ability to authenticate a user based on a trained neural network, which makes it possible to increase the efficiency of the biometric user authentication system using typing biometrics. Let's consider the processes of the neural network functioning. Let there be a training sample obtained by registering and entering a password phrase by users. It is necessary to train a neural network on this data and construct a neural network model (Katasev et al., 2018). For this, there are initial input and output characteristics:

1) input characteristics: username and user passphrase;
2) output characteristics: the result of authentication.

After the training sample formation, the neural network will be trained. Next, the user is authenticated to obtain the desired results. This operating mode of the software package is intended for user authentication using typing biometrics and obtaining authentication results. When training a neural network, its output error is minimized.

In accordance with the previously described characteristics of users' typing biometrics, the input parameters for the neural network model are as follows:

- x_1 - mathematical expectation of the time between pressing and releasing the current key;
- x_2 - mathematical expectation of the time between releasing the current key and pressing the next one;
- x_3 - dispersion of time between pressing and releasing the current key;
- x_4 - dispersion of time between releasing the current key and pressing the next one.

Thus, the vector of input parameters in the neural network model can be represented as X = { x_1, x_2, x_3, x_4}. The values of the output parameter of the neural network are "1" - legal user and "0" - illegal user. Fig. 1 shows a block diagram of the developed neural network.

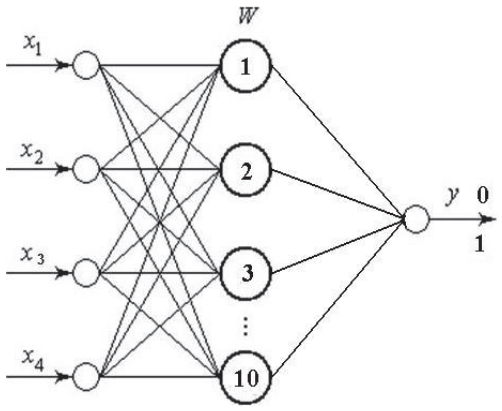

Fig. 1. Block diagram of the developed neural network

As it can be seen from the figure, the neural network is a single-layer perceptron (Ng et al., 2008) with four neurons in the input layer, ten neurons in the hidden layer, and one neuron in the output layer. Let's consider the results of the conducted experiments of user recognition by typing biometrics.

3. Results and discussion

A trained neural network must be tested to assess its classifying ability for correct recognition of data sets that were not involved in its training (Bruel et al., 2020). To solve this problem, a testing data set of 120 lines was used. In addition, errors of the 1st and 2nd kind were calculated according to the results of neural network classification (Zhang et al., 2017). In the context of solving the set problem, an error of the 1st kind should be understood as a situation when an attacker is recognized by a neural network model as a legal user. An error of the 2nd kind should be understood as a situation when a legal user is recognized by the neural network model as an attacker, accordingly. The following formula was used in this work to calculate errors of the 1st kind:

$$E_1 = \frac{n_1}{N_1} \times 100\%$$

where n_1 is the number of lines in the test sample characterizing illegal users, but classified by the neural network model as legal users; N_1 is the total number of lines in the test sample characterizing illegal users.

Accordingly, the following formula was used to calculate the errors of the 2nd kind:

$$E_2 = \frac{n_2}{N_2} \times 100\%$$

where n_2 is the number of lines in the testing sample characterizing legal users, but classified by the neural network model as illegal users; N_2 is the total number of lines in the testing sample that characterize legal users.

Assessment of the classifying ability of the neural network model showed the following classification results (calculation of errors of the 1st and 2nd kind):

- 1st kind errors value:

$$E_1 = \frac{n_1}{N_1} \times 100\% = \frac{0}{60} \times 100\% = 0\%$$

- 2nd kind errors value:

$$E_2 = \frac{n_2}{N_2} \times 100\% = \frac{2}{60} \times 100\% = 3{,}3\%$$

Thus, 0% of illegal users are recognized as legal, and 3.3% of legal users are recognized as illegal. It can be seen that the values for the indicated errors are insignificant (do not exceed the 5% error rate). Fig. 2 shows the percentage of the results obtained during testing of the software package.

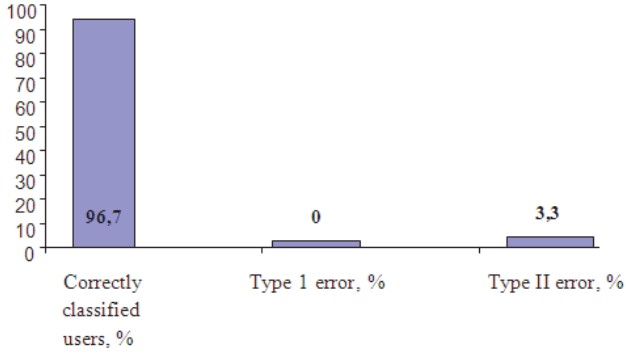

Fig. 2. Results of calculating errors of the first and second kind

As you can see from the diagram above, the biometric user authentication algorithm based on the neural network has shown good results.

4. Conclusions

As the study has shown, it is advisable to use modern methods of machine learning, i.e. neural networks for biometric authentication of users by typing biometrics. Training on the initial data, they are able to reproduce the laws hidden in them quite accurately, and solving the assigned problem with high accuracy. The results of the studies and experiments conducted allow us to conclude that the constructed neural network model is an effective tool for biometric user recognition. It allows us to minimize the number of errors of the 1st and 2nd kind. In addition, the overall accuracy of the model was 96.7%, which is a fairly high result.

Thus, the work has solved the problem of mathematical modelling for environmental prediction and control by typing biometrics based on the construction and study of a neural network model. The results of the experiments showed the effectiveness of the proposed approach to solving the problem. The constructed neural network model showed high recognition accuracy in terms of minimizing errors of the 1st and 2nd kind, as well as the general error of the model. This indicates its effectiveness and the possibility of practical use for users recognition in biometric identification and authentication systems.

Acknowledgements
The work is performed according to the Russian Government Program of Competitive Growth of Kazan Federal University.

References

Bhana B., Flowerday S., (2020), Passphrase and keystroke dynamics authentication: Usable security, *Computers and Security*, **96**, 101925.

Bruel J.-M., Combemale B., Guerra E., Syriani E., Vangheluwe H., (2020), Comparing and classifying model transformation reuse approaches across metamodels, *Software and Systems Modeling*, **19**, 441-465.

Chantaf S., Hilal A., Elsaleh R., (2020), *Palm Vein Biometric Authentication Using Convolutional Neural Networks*, In: *Smart Innovation, Systems and Technologies*, Howlett R., Jain L.C (Eds.), Springer, Cham, vol. 146, 352-363.

Dagaeva M., Garaeva A., Anikin I., Makhmutova A., Minnikhanov R., (2019), Big spatiotemporal data mining for emergency management information systems, *IET Intelligent Transport Systems*, **13**, 1649-1657.

Das A.K., (2017), A secure and effective biometric-based user authentication scheme for wireless sensor networks using smart card and fuzzy extractor, *International Journal of Communication Systems*, **30**, 2933-2939.

Emaletdinova L.Y., Kabirova A.N., (2019), Methods of constructing the neural network models of regulators for controlling a dynamic object with smooth monotonous behavior, *Russian Aeronautics*, **62**, 213-221.

Eom J.H., (2014), The design of robust authentication mechanism using user's biometrics signals, *International Journal of Security and its Applications*, **8**, 71-80.

Epishkina A.V., Beresneva A., (2020), *Online Handwritten Signature Verification: The State of the Art,* In: *Mechanisms and Machine Science*, Zhang X., Wang N., Huang Y. (Eds.), Springer, Cham, vol. 80, 329-334.

Eremenko I.I., Oliunina I.S., (2019), *The Optimal Time Typing to Identifying Users at the Typing biometrics*, Proc. 1st Int. Conf. on Control Systems, Mathematical Modelling, Automation and Energy Efficiency, SUMMA2019, November 20-22, Lipetsk, Russia, 515-517, http://summa2019.stu.lipetsk.ru/.

Eremenko I.I., Oliunina I.S., (2019), *Use of Machine Learning Methods for Solving Problem of User Identifying by Typing biometrics*, Proc. 2019 Int. Russian Automation Conf., RusAutoCon, 8-14 September, Sochi, Russia, http://doi.org/10.1109/RUSAUTOCON.2019.8867767.

Iryna D., Anton K., Hanna K., Bohdan Y., (2019), Corporate system users identification by the typing biometrics based on neural networks, *International Journal of Innovative Technology and Exploring Engineering*, **9**, 4156-4161.

Ismagilov I.I., Khasanova S.F., (2016), Algorithms of parametric estimation of polynomial trend models of time series on discrete transforms, *Academy of Strategic Management Journal*, **15**, 21-28.

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**, 1723-1728.

Ismagilov I.I., Molotov L.A., Katasev A.S., Kataseva D.V., (2019), Construction and efficiency analysis of neural network models for assessing the financial condition of enterprises, *Journal of Advanced Research in Dynamical and Control Systems*, **11**, 1842-1847.

Katasev A.S., (2019), Neuro-fuzzy model of fuzzy rules formation for objects state evaluation in conditions of uncertainty, *Computer Research and Modeling*, **11**, 477-492.

Katasev A.S., Emaletdinova L.Y., Kataseva D.V., (2018a), *Neural Network Spam Filtering Technology*, Proc. Int. Conf. on Industrial Engineering, Applications and Manufacturing, ICIEAM 2018, 15-18 May, Moscow, Russia, http://doi.org/10.1109/ICIEAM.2018.8728862.

Katasev A.S., Emaletdinova L.Y., Kataseva D.V., (2018b), *Neural Network Model for Information Security Incident Forecasting*, Proc. Int. Conf. on Industrial Engineering, Applications and Manufacturing, ICIEAM 2018, 15-18 May, Moscow, Russia, http://doi.org/10.1109/ICIEAM.2018.8728734.

Keith M., Shao B., Steinbart P., (2009), A behavioral analysis of passphrase design and effectiveness, *Journal of the Association for Information Systems*, **10**, 63-90.

Khitsenko V.E., Krutokhvostov D.S., (2018), *Statistical Monitoring of Typing biometrics for Continuous Authentication*, 14th International Scientific-Technical Conference on Actual Problems of Electronic Instrument Engineering, APEIE– Proceedings, 8546288, 171-174.

Kumar S., Paul S., Shaw D.K., (2017), Real-time multimodal biometric user authentication for web application access in wireless LAN, *Journal of Computer Science*, **13**, 680-693.

Last M., Bunke H., Kandel A., (2018), *Data Mining in Time Series and Streaming Databases*, World Scientific Publishing Co. Pte. Ltd., 171, https://doi.org/10.1142/10655.

Nelasa A.V., Krischuk V.M., (2001), *Using of the User Identification Methods on Typing Biometrics at Digital Signature Shaping*, The Experience of Designing and Application of CAD Systems in Microelectronics, Proc. of the 6th Int. Conf., CADSM 975824. 239-240, http://doi.org/10.1109/CADSM.2001.975824.

Ng W.W.Y., Yeung D.S., Tsang E.C.C., (2008), The localized generalization error model for single layer perceptron neural network and sigmoid support vector machine, *International Journal of Pattern Recognition and Artificial Intelligence,* **22**, 121-135.

Om H., Banerjee S. (2017), A password authentication method for remote users based on smart card and biometrics, *Journal of Discrete Mathematical Sciences and Cryptography*, **20**, 595-610.

Perfilieva I.G., Yarushkina N.G., Afanasieva T.V., Romanov A.A., (2016), *Web-Based System for Enterprise Performance Analysis on the Basis of Time Series Data Mining*, In: *Advances in Intelligent Systems and Computing*, Kacprzyk J. (Ed.), Springer, vol. 450, 75-86.

Rosenberg-Adler T., Weintraub N., (2020), Keyboarding difficulties: frequency and characteristics among higher education students with handwriting difficulties, *Learning Disabilities Research and Practice*, **35**, 82-88.

Stefanova M., Stefanov S., Asenov O. (2012), *Identity Protection Accessing E-Government through the Biometric Authentication Methods*, IS'2012 - 2012 6th IEEE Int. Conf. Intelligent Systems, Proc., 6335250, 6-8 September, Sofia, Bulgaria, 403-408.

Yellamma P., Rajesh P.S.S., Pradeep V.V.S.M., Manishankar Y.B., (2020), Privacy preserving biometric authentication and identification in cloud computing, *International Journal of Advanced Science and Technology*, **29**, 3087-3096.

Zhang Q., Xia D., Wang G., (2017), Three-way decision model with two types of classification errors, *Information Sciences*, **420**, 431-453.

Zhang R., Liu E., Pang L., (2011), A hybrid mutual authentication method based on biometric and password, *Journal of Computational Information Systems*, **7**, 5972-5979.