Access Control System with the Authentication Mechanism Implementation using Artificial Neural Network

Ye P Belova and I V Mashkina
Ufa State Aviation Technical University (UGATU), 450008, Ufa, Russian Federation

E-mail: super.yelenar@yandex.ru

Abstract. Biometric access control system is presently one of the innovative Information Security (IS) technologies. The article shows a possibility to use this technology to control logical access as well as the technologies provided to administrator-users of Information Systems (IS). A method to compare biometric data of users who have administrator rights is proposed. Individuals' unique voice parameters and Artificial Neural Networks (ANN) lay behind this method. The paper considers the specific ANN learning issues to solve the challenge over storing biometric patterns of users and authenticating them by values of the fourth formant characteristics as regard to the selected vowel phonemes as well as by additional voice qualities. The first and second type recognition errors are estimated. The architecture of the user authentication and authorization system that implements the method to monitor administrator-users of information systems has been designed.

1. Introduction

Authentication through user voice recognition is one of the most promising methods of biometric identity verification [1, 2]. It is implemented by reading qualities of a human voice recorded using a microphone. These qualities should be unique for each authenticated user, and a Biometric Authentication System (BAS) should contain a set of biometric data samples of legal users. For the voice authentication, no expensive equipment is required. It is a highly efficient and easy to use method, which does not cause discomfort, unlike, for example, iris recognition [3-5].

The proposed BAS operates is based on the method of authentication through user voice recognition, when user-pronounced sounds taken as biometric data are converted into specific numerical values to be extracted from the sound spectrograms using a developed algorithm and software. The obtained numerical values are fed into the Artificial Neural Network (ANN) through certain inputs, provided that the ANN was pre-configured to identify a particular user, whose biometric data were entered, or to identify an illegal user. Today the problems of Neural Netoworks implementation are extensively studied. Many papers have been published in the scientific literature, for example [6-9].

The article presents a system for authentication/authorization of users who have administrator rights. The method of hardened authentication and authority delegation that allows excluding the superuser by creating such single roles as network administrator, security administrator, virtual infrastructure administrator, administrator of ICS (Industrial Control System), is proposed in the paper.

The proposed variant of the ANN allows comparing the entered biometric data with the reference values belonging to four legitimate persons that are eligible for access to the server or host using the

rights assigned for each of them. Thus, the ANN is a specific database of the user biometrics, and it is configured to recognize such users. The numerical values corresponding to the biometric characteristic of a user are the analogue of the user password, which, however, is inseparable from the person to be authenticated.

This paper focuses on the development of the BAS based on the neural database of biometric patterns and such BAS should be able to prevent unauthorized access attempted both by any of legitimate users (including those who are not administrators) and an "alien".

2. **Formulation of the problem**

The objectives of this study are the creation of a biometric-pattern neural-database (BP-NDB) to harden the authentication and authorization of users who have the administrator's right as well as the design of the BAS. Attacks on authentication and authorization systems can come from both internal users and users who are external to the information system [10]. It is critically important for the authentication and authorization system to have the capability to prevent all attempts made by an "alien" to pass under the identifier belonging to one of the legitimate administrator users. Therefore, the paper analyses whether there is a capability to detect attempts taken by an "alien" to intrude the system that authenticates users who have administrator privileges.

3. **Description of the subject of research**

The characteristics of the fourth formant and frequency of a strong formant of a vowel produced by a user are responsible for creation of the biometric pattern of this person.

The following terms and definitions are used in the paper:

- A formant is a concentration of acoustic energy around a particular frequency domain [11, 12];
- The fourth vowel formant is the fourth burst of energy in a particular frequency domain, which is recorded on the spectrogram of the vowel;
- Frequency $f_{4\max}$ corresponds to the maximum amplitude of the energy burst in the fourth frequency domain on the spectrogram;
- Frequency f_{4s} determines the origin of the fourth particular frequency domain on the spectrogram;
- Frequency f_{4f} determines the end of the fourth particular frequency domain on the spectrogram;
- f_l is a frequency of a strong formant corresponding to the peak spike amplitude of any formant recorded on the spectrogram.

The article [13] proves the feasibility of using the frequency of the fourth vowel formant to authenticate users. Further experiments have revealed that the characteristics of the fourth formant used as components of an individual's voice pattern also shows high effect. It is advisable to use several formant characteristics as a speech parameter to increase the trustworthiness of recognition. The effectiveness of the characteristics of the fourth formant used in combination with such a biometric parameter as the frequency of the strong vowel formant has been confirmed experimentally.

Since the sound spectrograms of three Russian vowels "A", "O" and "E" have strongly-pronounced ranges of high intensity in the fourth particular frequency domain [14], then the characteristics of the fourth formant as well as the frequency of the strong formant of these sounds will be used for user authentication and authorization in the BAS.

Two software modules developed by the authors of this article differentiate the characteristics of the fourth vowel formant [15]. The first module is designed to obtain a spectrogram of a vowel pronounced by a user as the phonemes selected for the experiment. The second module implements the algorithm that extracts the characteristics of the fourth vowel formant.

The module for selecting the frequency of the strong formant (f_l) has not implemented by the authors, it has still being designed. Therefore, the frequency of the strong formant was allocated through the Bard software in a semi-automatic mode [16].

To conduct research, four people were invited as legal administrator-users (3 men and 1 woman) and 6 participants who played the role of so-called “aliens”: 3 people were involved in configuring the ANN based on their biometric patterns and 3 people participated in testing.

The whole ANN design process consists of the following steps: select input and output ANN variables, select an ANN architecture, design a learning sample, receive and process learn and test results.

Vector X is used as input variables. It includes the following metrics: number of user x_1 who presented their identifier, 12 inputs $(x_2,...,x_{13})$ for user-submitted biometric data that were pre-processed to differentiate the characteristics of the fourth formant and the strong formant frequencies. Values of characteristic $x_2,...,x_{13}$ were obtained after processing the spectrograms of sounds pronounced by a user in accordance with 3 selected vowel phonemes. Vector Y with dimension equal to four in terms of the administrator number was considered output variables of the ANN.

The network architecture described in the paper as a two-layer feedforward perceptron allows solving the set tasks in full. The number of neurons in the inner layer was selected taking into account the size of the learning sample, and the number of inputs and outputs [17]:

$$N = \left[\frac{Q*n}{m+n} \right], \text{ where}$$

- N is a number of neurons in the hidden layer;
- m is a number of inputs equal to 13;
- n is a number of outputs equal to 4;
- Q is a size of a learning sample;
- [ ] is rounding to the nearest integer.

4. Achieved results of research

As a part of this research, the ANN was created based on the characteristics of the fourth formant and frequencies of strong formants of vowels “A”, “O” and “E”. The network was set to recognize an “alien”. Figure 1 shows its architecture.

Input neuron 1 is a user identifier (from 1 to 4); input neurons 2-4 are values of characteristics of the fourth formant for vowel "A"; input neurons 5-7 are values of characteristics of the fourth formant for vowel "O"; input neurons 8-10 are values of characteristics of the fourth formant for vowel “E”, input neuron 11 is a frequency of the strong formant for vowel “A”; input neuron 12 is a frequency of the strong formant for vowel "O"; input neuron 13 is a frequency of the strong formant for vowel "E". Output neurons U1, U2, U3 and U4 are data of users 1–4. An active output neuron shows biometric data of a specific user that were fed to the input of the neural network. The active output neuron is defined with a value greater than the threshold at its output. If biometric characteristics corresponding to the first user’s identifier are fed to the ANN inputs, the output neuron U1 will be active, and so on. If biometric characteristics corresponding to the fourth user’s identifier are applied to the ANN inputs, then the output neuron U4 will be active.

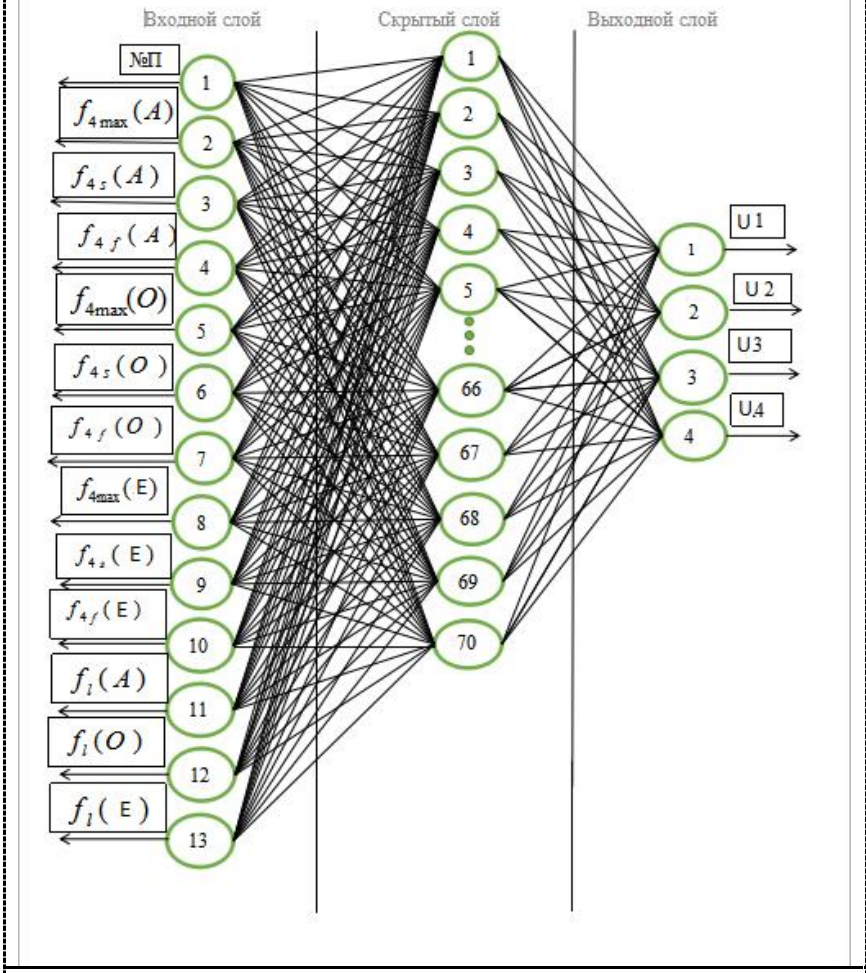

Figure 1. ANN architecture based on the characteristics of the fourth formant and frequencies of strong formants of vowels “A”, “O” and “E”

The learning sample contains 280 rows (learning examples). It includes four sets of rows (one set per person). In addition, each set consists of 3 parts: data intended for learning the ANN to recognize a legal user who provided their identifier; data intended for learning how to detect unauthorized actions taken by administrators in order to bypass authentication using an identifier of another administrator for the purpose of obtaining the privileges; data intended for learning how to detect attempts taken by an “alien” to bypass authentication using an identifier of any of the administrators.

The ANN was created and trained using the Matlab R2015b software. The developed ANN was trained, tested or verified based on 280 examples. The network was configured in 21th era. The value of the best root-mean-square network error was 0.0027267.

The 1st and 2nd type errors were calculated using the nntool GUI of the Matlab R2015b software.

The average value of the 1st type errors was 7.50%, since a legal user successfully passed the authentication procedure in 92.50% of cases (Table 1).

The average value of the 2nd type errors calculated when detecting the attempts taken by a legal admin user to bypass authentication by use of their colleague login was 5.83% (Table 1).

The average value of the 2nd type errors calculated when detecting attempts taken by an “alien” to bypass authentication by use of a login of another administrator was 1.67% (Table 1). This is the best

result compared with the corresponding results obtained by other researchers in their study dedicated to authentication based on various speech parameters and methods [3, 18, 19].

Table 1. Results of computing errors of the 1st type and 2nd type

Pass rates of legal admin users in percent					
User No.	1	2	3	4	Average value
Total	90%	100%	80%	100%	92.50%
The results of the 2nd type errors calculated when the admin user attempts to bypass authentication under another admin user login					
User No.	1	2	3	4	Average value
Total	10%	13.33%	0.00%	0.00%	5.83%
The results of the 2nd type errors calculated when the “alien” attempts to bypass authentication under another admin user login					
“Alien” No.	1	2	3	Average value:	
Total	0%	5%	0%	1.67%	

The total average value of the 2nd type errors was 3.75%, which is significantly less than the result given in [3, 18, 19].

Figure 2 shows the developed system for authentication and authorization based on the characteristics of the fourth formant and the frequency of the strong vowel formant.

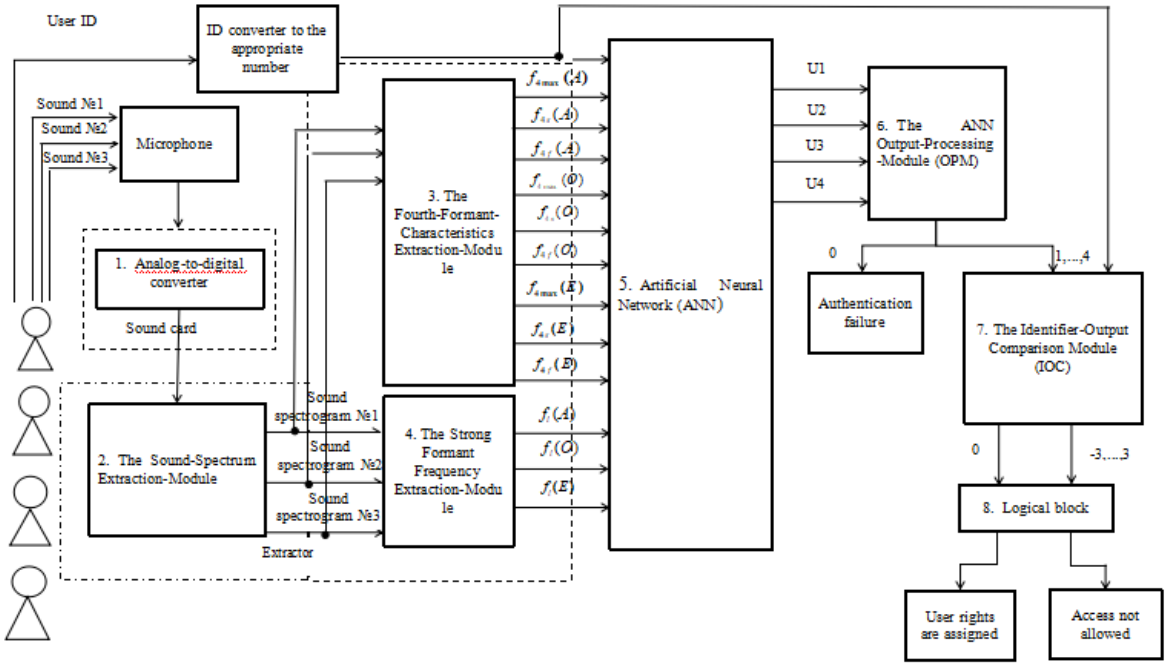

Figure 2. The architecture of the authentication and authorization system based on the characteristics of the fourth formant and the frequency of the strong vowel formant

The operation algorithm of the proposed authentication and authorization system is as follows:

- A user alternately pronouns vowels “A”, “O”, and “E”.
- 1 converts these sounds into digital signals.
- 2 processes digital signals and creates their spectrograms.
- The spectrograms are fed into 3 and 4.
- The processed biometric data arrives at 5.
- The user identifier is converted to the appropriate number (from 1 to 4). The user login is also fed into 5.
- The corresponding output $(U_1,...,U_4)$ shows the probability that the biometric data belongs to the particular user whose login is entered.
- The numerical probability values are fed into the 6.
- The authentication of a user who presented an identifier and biometric data will be finished unsuccessfully if ANN’s output, corresponding to the presented identifier, shows a value below the set threshold. 6 will consider this value equal to zero.
- If a value obtained at any ANN output is above the set threshold, then 6 assigns a digit (from 1 to 4) equal to the number of the active ANN output.
- The value (from 1 to 4) equal to the number of the active ANN output is fed from 6 output to one of the inputs of 7. The second input receives the login number corresponding to the entered identifier (from 1 to 4). The difference between the two inputs is calculated. If these numbers are equal, then 7 output will be 0. Biometric image of the user coincides with his ID.
- The value (from 1 to 4) equal to the number of the active ANN output is fed from 6 output to one of the inputs of 7. The second input receives the login number corresponding to the

entered identifier (from 1 to 4). The difference between the two inputs is calculated. If these numbers are equal, then 7 output will be 0.

- The calculation results are fed from 7 to 8.
- If the input of 8 receives the resulting value 0 from 7, then the administrator rights will be assigned in accordance with the access control policy.
- If the input of 8 receives a value from -3 to -1 range or a value from 1 to 3 range from the 7, then the corresponding administrator access will be denied.

5. Conclusion

Many researches in the information security field focus on the authentication through user voice recognition and identification of an "alien". The Artificial Neural Network (ANN) based on the fourth formant characteristics and frequencies of strong formants of vowels "A", "O" и "E" is considered a one of the effective solutions of this task. The average values of the 1st and 2nd type errors obtained during operation testing of the developed ANN show the high result of the concept and the possibility to continue research in this focus area. It is planned to further improve the recognition accuracy of "aliens" without increasing the 1st and 2nd type errors in identification of attempts taken by each of the administrators to access the information system under a login of another colleague. Conduction of studies to identify "aliens" in another group of users, whose spectrograms are similar to each other with an even greater percentage, is also outlined.

References

[1] Biometric Technology Market is Estimated to Generate $10.72 Billion by 2022 access mode: https://www.alliedmarketresearch.com/press-release/biometric-technology-market.html free
[2] Sorokin V N 2010 Speaker verification using spectral-temporal parameters of a speech signal *Information processes* **10 2** 87-104
[3] Sorokin V N and Tananykin A A 2012 Voice recognition: an analytical review *Information processes* **12 1** 1-30
[4] Imam S A, Bansal P and Singh V 2017 Review: speaker recognition using automated systems *AGU International Journal of Engineering & Technology* **5** 31-39
[5] Shah H N M, Abdollah M F, Lin C K, Ab Rashid M. Z, Kamarudin M N and Kamis Z 2014 Biometric Voice Recognition in Security System *Indian Journal of Science and Technology* **7**
[6] Pang Y, Sun M, Jiang X and Li X 2018 Convolution in Convolution for Network in Network *IEEE Trans. Neural Netw. Learn. Syst.* **29 5** 1587–97
[7] Zhang H, Wang Z and Liu D 2014 A Comprehensive Review of Stability Analysis oContinuous-Time Recurrent Neural Networks *IEEE Trans. Neural Netw. Learn. Syst* **25 7** 1229–62
[8] Yang C, Chen C, He W , Cui R and Li Z 2019 Robot Learning System Based on Adaptive NeuControl and Dynamic Movement Primitives *IEEE Trans. Neural Netw. Learn. Syst*. **30 3** 777–787
[9] Emary E, Zawbaa H M and Grosan C 2018 Experienced Gray Wolf Optimization Through Reinforcement Learning and Neural Networks *IEEE Trans. Neural Netw. Learn. Syst.* **29 3** 681–694
[10] Makarevich O B 2011 *Actual aspects of open security* (Taganrog: Publishing House TTI SFU) p 448
[11] Rabiner L R and Schafer R V 1981 *Digital processing of speech signals* (Moscow: Radio and communication) p 496
[12] Sydorenko I A and Kuskova P A 2013 About spectral analysis of phonemes using sound editors *Scientific statements of BelSU, History series. Political science. Economy. Computer science* **22 165** 246-250

[13] Belova Ye P and Mashkina I V 2018 Research Results of Artificial Neural Network for User Authentication According to Frequency of Fourth Formant of Vowel Sound Phoneme *2018 International Russian Automatisation Conference (RusAutoCon) IEEE Institute* URL: https://ieeexplore.ieee.org/document/8501680
[14] Mashkina I V and Belova Ye P 2019 Development of a neural network database of biometric images for voice authentication system *Problems of information security. Computer systems* **2** 86-93
[15] Gerasimov V V, Belova Ye P and Mashkina I V 2019 Isolation of the characteristics of the fourth formant of vowel sound *Certificate of state registration of the computer program of April 3,* 2019614367
[16] Bard 0.1.7, http://psi-logic.narod.ru/bard/bard.htm, free.
[17] Kafarov V V Gordeev L S, Glebov M B and Jingbao G 1995 *On the issue of modeling and control of continuous technological processes using neural networks* (TOXT) **2**
[18] Kulibaba O V and Privalov M V 2010 *The Selection of Characteristics for Voice Authentication in a Computerized Access Control System* (Information System Control System and Computer Monitoring (IYS KM-2010) Materials I all-Ukrainian science technical conference students, graduate students and young people, 19-21 May, 2010, Donetsk, DonNTU) 33-37
[19] Matveev Yu N 2013 Investigation of the informativeness of speech signs for systems of automatic speaker identification *Izvestiya Vuzov. Instrument making* **56 2** 47-51