The Ministry of Education and Science of the Russian Federation
Far Eastern Federal University
School of Natural Sciences

3RD FEFU SNS STUDENTS, MASTER'S DEGREE STUDENTS AND POSTGRADUATE STUDENTS SCIENTIFIC-PRACTICAL CONFERENCE IN ENGLISH

Vladivostok

25 April – 08 May 2016

CONFERENCE PROCEEDINGS

AND THE CONTEST OF SCIENTIFIC REPORTS

Scientific electronic publication

Vladivostok
Far Eastern Federal University
2016

ISBN 978-5-7444-3816-6

UDC 082
LBC 94.3
F45

F45 **3rd Fefu SNS Students, Master's Degree Students and Postgraduate Students Scientific-Practical Conference in English,** Vladivostok, 25 April – 08 May 2016 [Electronic resource] : conference proceedings and the contest of scientific reports / chief editor S.G. Krasitskaya. – Electr. dat. – Vladivostok : Far Eastern Federal University, 2016. Uniform Resource Locator: https://www.dvfu.ru/schools/school_of_natural_sciences/sciences/. – Title screen.

ISBN 978-5-7444-3816-6.

The collected volume contains proceedings of the contest of scientific reports in English language and the results of scientific researches made by students, Master's Degree students and postgraduates students of the School of Natural Sciences FEFU, 25 April –08 May 2016.

UDC 082
LBC 94.3

Text electronic edition
Minimum System Requirements:
Минимальные системные требования:
Web browser Internet Explorer 6.0 or higher,
Opera version 7.0 or higher,
Google Chrome version 3.0 or higher).

A computer with Internet access.

Posted on the website of 06.28.2016

Volume 2.93 MB

Far Eastern Federal University
690950, Vladivostok, Sukhanova st., 8
Tel./Fax: (423) 226-54-43, 265-22-35 (*2383)
E-mail: dvfutip@yandex.ru, editor_dvfu@mail.ru

CONTENTS

THE CONTEST OF SCIENTIFIC REPORTS

Section II

MATHEMATICS AND INFORMATION TECHNOLOGY

Borshevnikov A.

A BIOMETRIC AUTHENTICATION SYSTEM BASED ON ELECTROENCEPHALOGRAM METHOD OF CONSTRUCTION

Far Eastern Federal University, School of Natural Sciences
LAdG91@mail.ru

The necessity in information security grows with the amount of information processeding. Information security tools are based on different mechanisms of protection. One of well-known mechanisms used in the protection system is biometric authentication. For example, hundred of millions people have biometric passports and the question of biometric data secure storage is quite urgent. Data recorded in the passport is used for the authentication of citizens when crossing the border of a state.

One of the most perspective types of biometric data is the human electroencephalogram (EEG). It should be noted that these parameters are practically impossible to capture.

The purpose of the paper was to propose a method of construction a biometric authentication system based on electroencephalogram. The tasks of the work were:

1. To describe the model of biometric authentication systems based on EEG;
2. To test the model and to obtain characteristics of the model.

The literature review let us make the following conclusions.

At present time the researches on the development of human identification methods based on EEG are actively conducted in the world. Researchers use different experimental techniques, as well as different methods of EEG signal processing [1]. The effectiveness of these best technologies is low. False Acceptance Rate (FAR, Type II error) for such technologies is in the range from 10% to 0.1%. One solution of this problem is changing the classical method of construction of an authentication system based on the EEG. We propose to use construction of a highly reliable biometric authentication system in accordance with a series of standards GOST R 52633 [2, 3]. Such neural networks are called neural network transformers "Biometry - access code". This approach has allowed us to significantly improve efficiency of the identification based on the EEG and reach values FAR = 10^{-12}.

In general, the approach described in the standard GOST R 52633 proposes to use for processing the biometric data neural network learned on a special algorithm. It was proposed to use a two-layer neural network learned on algorithm GOST R 52633.5-2011 with sigmoid transfer functions [3].

Earlier experiments in spite of the good results have a short coming. It requires an external stimulation to extract the EEG signal. Described disadvantage can be corrected through the use of other electrical brain potential. For example, its potential can be potential eye muscles movement [4].

It was decided to capture the potential of eye muscles movement by the following experiment. Metronome sound stimulation every 2 seconds was used to simplify the experiment. Data recording was carried out for 8 seconds. On each shot of the metronome, potential of eyes

movement in a certain direction (left - right - up - down) was recorded. Eyes movements were performed with closed lids. Eyes movements with closed lids make it impossible to determine the visual input a password by an intruder. The sequence of movements is "thought password".

For learning the neural network transformer it is necessary to create EEG database which is exposed to stimulation of image "Alien", i.e. to create intruder for which the neural network will generate a random secret key. We can use this database for subsequent processes the transformer learning. We also need to create EEG database of images "Our", i.e. a user who will be considered legitimate in the authentication system. This database must be removed immediately after learning the transformer, to prevent database stealing and using compromise the secret key.

One problem, which was solved while constructing the model was the choice of EEG parameters. To solve this problem it was suggested to choose the coefficients of the Fourier transform, and then normalize them. As an algorithm for processing EEG Fast Fourier Transform was taken. Transformation of coefficient Fourier transform can be described by the following formula:

$$v_i = \bar{a}_i \cdot \bar{w}_i, 1 \le i \le I,$$

where i - number of electrode from which the EEG is captured; $\bar{a}_i$ - the vector of biometric data, which the neural network is used in the converter; I - total number of electroencephalograph electrodes; $\bar{w}_i$ - the weight vector of the neural network first layer corresponding to the vector.

This is normalized value, which is fed to the inputs of neurons adders. We form the vector of values:

$$\bar{v} = \{v_i\}, 1 \le i \le I.$$

These values are input to the adders of the neural network first layer. Neurons of the first and second layer are similar in structure, but different in the processed data and obtained results. After data processing of the neural network first layer, the given values are supplied to the second layer. The output of each neuron of the second layer is a recovered bit secret key.

In this experiment the following parameters are used. The number of electrodes is I=14. Experimentally it has been found that for correct operation of the transformer selection of 10 Fourier coefficients is required. The number of neurons of the first layer is equal to 320. Size of the restored key has been selected to 256, which means 256 neuron used in the second layer of the neural network. The number of inputs to the neurons was 4.

To conduct the study the transformer database from 10 different biometric images each containing 20 EEG patterns was created. One image was selected as the image "Our". The other nine images were taken as the basis of image "Alien". We conducted an experiment which establishes the possibility of obtaining the secret key by an intruder in case of knowing the "thought password" (Table).

Users number	Hamming distance
1	18
2	37
3	118
4	87
5	8
6	125
7	119
8	125
9	125

Table. Hamming distance to the secret key of the user in case of an intruder knowledge "thought password"

The following results are the most interesting:

1. In case when an intruder guesses "thought password", Hamming distance of the intruder obtained key to the user's secret key equals 8.
2. In all experiments the user restores the key and the transformer correctly restores the secret key.

The results show that it is possible to construct a biometric authentication system based on EEG, but it requires further development, as the results do not meet the requirements of highly reliable biometric authentication system. Earlier it was shown that the obtained results can be used in different cryptographic applications, in particular, in procedure of the encryption key storing or digital signature key storing [5].

References:

1. Yang S. The Use of EEG Signals For Biometric Person Recognition. Doctor of Philosophy (PhD) thesis // Kent Academic Repository. University of Kent. URL: https://kar.kent.ac.uk/53681/1/235Thesis%20(Su%20Yang).pdf
2. Protection of the Information. Information Protection Technique. Requirements for Highly Reliable Means of Biometric Authentication: GOST R 52633.0-2006. - Introduced for the First Time; Introduced. 27.12.2006. - M .: Standartinform, 2007. - 25 P.
3. Protection of the Information. Information Protection Technique. Automatic Learning Neural Network Transformers "Biometry - Access Code": GOST R 52633.5-2011. - Introduced for the First Time; Introduced. 01.12.2011. - M .: Standartinform, 2012. - 20 P.
4. Gnezditsky, V.V. Inverse Problem of EEG and Clinical Electroencephalography (Mapping and Localization of Sources of Electrical Activity of the Brain). - M .: MEDpressinform, 2004. - 624 P.
5. Goncharov, S.M., Borshevnikov, A.E. Neural Network Transformer "Biometry - Access Code" Based on Electroencephalogram in Modern Cryptographic Applications. // Vestnik SibSUTI - Novosibirsk: Publishing House of SibSUTI, 2016. - № 1. - PP. 17-22.