Biometric authentication on the basis of electroencephalograms parameters

A E Sulavko, A E Samotuga, D G Stadnikov, V A Pasenchuk, S S Zhumazhanova

Omsk State Technical University, 11 Mira ave., Omsk, 644050, Russia

Abstract. Static biometric patterns such as fingerprint, iris and face are difficult to keep secret. Since the open pattern has a little potential replacement options stealing a strange open biometrics provides great opportunities for compromising systems.Authentication on the basis of electroencephalogram pattern (EEG) is the most secure kind of biometric security. The present study aims to develop a method of biometric authentication by the EEG data with high accuracy. Several neural network EEG pattern verification algorithms have been tested. A method for verification of the human EEG pattern based on a modified Bayes hypothesis formula has been developed. The following error indicators FAR < $10^{-4}$ with FRR = 0.062 were achieved.

This work was supported by the Russian Foundation for Basic Research (RFBR) and the Government of the Omsk Region (grant 18-41-550002).

1. Introduction
Passwords, encryption keys and electronic signature can be separated from the owner. This fact makes remedies based on these authenticators vulnerable to social engineering methods and subject to a variety of abuses. It is possible to eliminate or at least reduce the influence of the “human factor” on the security of information systems using biometric protection. Static high-informative biometric patterns (fingerprint, iris, face, etc.) are difficult to keep secret (we cannot always be in gloves, masks and glasses, without compromising open biometric patterns). This means that they can be falsify. Theft of strange open biometrics for a qualified attacker is not a problem (data can be removed from the glass, door handles, photos, etc.). In this regard, there are great opportunities for compromising systems, since an open image has few possible replacement options (10 fingers, 2 eyes and one face). Manufacturing technologies of electronic and digital fake are constantly improving.

The secret contained in the biometric pattern, repeatedly enhances its protective properties. However, a simple combination of a password and a fingerprint complicates system hacking a few but does not change the situation drastically and does not eliminate the root of the problems. The biometric pattern is required to be secret (the secret must be inside the pattern) then the password compromise does not lead to system compromise since the password still needs to be correctly reproduced (said, wrote or printed). But the probability of "false acceptance" error for handwritten, voice patterns as well as keyboard handwriting patterns is much higher than for fingerprints. Furthermore, if the authentication is carried out not in a trusted environment, these patterns also can be stolen (e.g., using the recorder, a keyboard interceptor et al.).

Electroencephalogram (EEG) -based authentication is a combination of biometrics, a secret and method of data entry protected from third parties (to steal the “thought” you need to penetrate the brain-computer channel, which is still difficult and even more difficult to interpret the signal). Hidden remote interception and falsification of the EEG pattern in the near future is not feasible.
The particularity of EEG patterns is the presence of features (biometric parameters) which are not subject to conscious volitional control by the subject but to some extent depend on the psycho-emotional state [1]. It makes possible to implement protection against attempts to undergo an authentication procedure under pressure from third parties.

By present there is already an element base for creating compact multi-channel neuro-headsets, and dry electrodes that allow recording the signal through the hair cover have been developed. Thus, on the basis of EEG it is possible to create the most secure method of biometric authentication, but provided that high recognition accuracy will be achieved. The present study aims to develop a method of biometric authentication of the EEG data with high accuracy.

2. Requirements for biometric authentication systems based on EEG

At present time 256 bits can be considered a sufficient length of a cryptographic key. Such key length provides a strong protection and used to generate a digital signature in accordance with the recommendations of Russian standard GOST 34.10-2012. Probability of coincidence of 256 bit key by rough iterating its values is less than 10^-77. The length of modern hash functions reaches 512 bits (SHA-3) and higher. Brute force of password that protected such hash functions provided they are correct (totally random) generating is an impossible task for a modern computing hardware. Of course, this is only true when the entropy of possible passwords, as well as the output sequence of the hash function is equals (or close to) its length.

However, underestimated requirements are typically imposed to biometric systems. The probability of a “false acceptance” FAR = 10^-9 is considered an excellent indicator, but if we consider that the attacker has the opportunity to perform a brute force search of artificially generated biometric patterns in order to find a sufficiently close one to the pattern of the victim user (by analogy with the selection of a password) then this indicator is clearly reduced. There are various ways to generate competing examples [2], including some based on the synthesis of natural biometric humans patterns. In Russia there is a standardized method (GOST 52633.2) for generating synthetic including attackers.

This situation is partly due to the inability to verify the reliability of the biometric system with FAR = 10^-77 in an "authentic" experiment in accordance with ISO / IEC 19795-1. There is not enough planet population for this. In fact, to verify this possibility a comparable base of natural biometric patterns is not required. Missing patterns can be obtained artificially on the basis of crossings natural patterns and then their descendants (this testing ideology is reflected in another Russian standard GOST 52633.3).

When testing, it is necessary to ensure a sufficient level of diversity and statistical confidence of the test sample of natural biometric patterns nevertheless its volume can be increased by creating synthetic examples.

“False rejection” errors (FRR) of the pattern affect the availability, but are not safety critical if their frequency (probability) is within adequate limits. It can be considered an acceptable level FRR = 0.1 [3].

An important aspect for biometric authentication systems concerns the secure storage and transmission of biometric patterns via communication channels. Modern standards (family of GOST R 52633, ISO / IEC 24745: 2011, ISO / IEC 24761: 2009, ISO / IEC 19792: 2009) and actual practice require that the biometric template be protected from compromise. This is achieved using fuzzy extractors [4] (fuzzy vault, fuzzy complement - algorithms based on error correction codes applied to raw biometric data) or trained artificial neural networks (ANN) [3] (neuron links and weights tables do not compromise the user template). These security schemes are used in biometrics-code converters that generate encryption keys or passwords from the user's biometric pattern, which activate the cryptographic mechanism. After the security system has been trained, the biometric pattern is “associated” with the cryptographic key. Both components are stored together in such form that it is impossible to get one of them without knowing the other. At the present moment, hidden or remote interception of EEG is impossible. But it is temporary. EEG interception techniques may appear. Usually an attacker uses the weakest link. In present case, it may be a data transmission channel (a man-in-the-middle attack is possible after removing the potentials). Therefore in practice if the protection system is threatened (or compromised) by analogy with the password it should be possible to change the key visual stimulus.
3. Experiment by the collection of data of EEG patterns

In the experiment 75 subjects participated. Each subject before passing the tests rested on the preceding day and was in a calm state at the time of the experiments. The neurological status of all subjects before the start of the experiment was assessed as normal.

Two series of experiments was conducted. The first is focused on the development of persistent individual responses of the brain to a visual stimulus, occurring primarily in striatal and extrastriate cortex (fields 17, 18 and 19 according to Brodmann at Fig. 1). The second series of experiments is based on the Rorschach test and is also aimed at stimulating the frontal lobes of the brain (in addition to fields 17, 18, 19 according to Brodmann). For each type of experiments respective static (non-animated) visual stimuli were prepared. These stimuli were displayed in the virtual reality glasses (geometric shapes and "Rorshaha spots"). Subject watched stimuli being in the lying position (Fig. 2).

At the same time brain EEG was recorded using the Neuron-Spectrum-4 / P 21-channel electroencephalograph from Neurosoft Company (with a noise level of less than 0.3 µV and a quantization frequency of 5000 Hz per channel, which is subsequently converted to a frequency of 500 Hz).

![Figure 1. Electrode arrangement according to 10-20 system: A) the involved electrodes (Fpz, Fp1, Fp2, Fz, F3, F4, Cz, Oz, O1, O2) and referents (A1, A2) were highlighted; B) the correspondence of the electrodes to the lobes of the cerebral cortex; C) the relative position of the electrodes and the Brodmann fields.](image)

The connection of the electrodes to the surface of the subjects' head was carried out according to the 10–20 scheme (Fig. 1), which is the standard electrode location method used for collecting EEG data. Although the method was developed that was not based on any anatomical considerations (Brodmann areas, etc.), it is used in modern practice. R. Sutor defined and described the relationship between the system 10–20, Brodmann regions and brain functions in [5]. The lettering of the system 10-20 means the areas of the cerebral cortex, where the corresponding electrodes are located (F – frontal, T – temporal, C – central, P - parietal, O – occipital). In all experiments we used monopolar attachment of electrodes. The electrodes with even numbers (2, 4, 6, 8) are located on the right side of the head, with the odd (1,3,5,7) – on the left. Electrodes in the name of which have «z» literal are reference. Electrodes in the name of which have an «o», are reference. The sensitivity zone of the electrode, that is, the diameter of the area, the signals of which are summed at a particular electrode, varies from 20 to 50 mm and depends on the thickness of the bones of the skull and the distance from the cortex to the electrode. Moreover the increase in the density of the electrodes slightly improves the readings, since the signals of the neighboring areas are summed up (the closer the electrodes are the higher the correlation of the signals).
Figure 2. Monitoring of subjects EEG.

The choice of the involved electrodes (Fpz, Fp1, Fp2, Fz, F3, F4, Cz, Oz, O1, O2, Fig. 3) is determined by the nature of the study, which is based on the human perception of visual stimuli and analysis of the corresponding brain responses in it different parts (fields) depending on the level of processing of incoming information.

Figure 3. Recording signals in Neurosoft EEGViewer program.

All subjects underwent both series of experiments at least twice on different days. Subjects watched the patterns making short breaks. The minimum time of observation of visual patterns by the subjects was 10 minutes per day in each series of experiments (more than 20 minutes in two days in total). Thus EEG data was accumulated that can be used to conduct experiments on the recognition of subjects (including training and test samples).

4. EEG analysis and feature extraction

The authentication system based on EEG assumes learning, pattern recognition procedures. As well as the transformation of the original EEG signals into feature vectors to a fixed length which are processed by the specified procedures (Fig. 4).
Figure 4. Biometric authentication based on EEG.

Spectral and correlation analysis of EEG signals were used to extract the features. The EEG signal is usually described by the concept of rhythmic activity, which is usually classified by frequency [6], divided into alpha (8-13 Hz), beta (14-40 Hz), gamma (30-100 Hz), theta (4–8 Hz) and delta (1-4 Hz) rhythms (waves, ranges). Therefore the signals were previously passed through bandpass filters and information about frequencies below 0.5 Hz and above 100 Hz which was noise was deleted. A notch filter (45-55 Hz) was also used to eliminate interference caused by power supply lines (in Russia, their frequency is 50 Hz). Further EEG patterns was divided into fragments of equal length, each fragment was transformed into a vector of 1540 features:

- integral amplitude spectra of the EEG signals were received via Short-Time Furrier Transform (STFT) with finding the mean values of each harmonic for all windows (similar to the approach used in [7] for calculating the speech signal features). The width of the STFT window was 512, step was 32, only the average amplitudes of the first 100 harmonics of each signal (a total of 1000 features) were used as features;
- integral amplitude spectra of the autocorrelation functions of EEG signals, obtained in a similar way. The window width of the STFT was 64, step was 8 and average amplitudes of all 32 harmonics of the autocorrelation function of each signal (a total of 320 features) was used as features;
- relative frequencies of occurrence of extremes for all EEG signals (10 features at all);
- relative frequency of occurrence of the extrema of the autocorrelation function for all EEG signals (a total of 10 features);
- relative frequencies of transitions through the “zero” of autocorrelation functions for all EEG signals (10 features total);
- matrix of pairwise correlation coefficients between EEG signals and their derivatives (10 signals, 10 derivatives, a total of 190 features).

According to the results of the EEG analysis there are no significant differences between the records formed under the influence of various visual patterns (Rorschach tests and geometric figures).

5. Evaluation features informativeness

As is known the multidimensional probability density function contains all information about a random variable including information about the correlation relationships between measurements. To construct a 1540-dimensional probability density function it is necessary to accumulate a huge (not feasible in practice) number of examples of a multi-dimensional random variable (with an increase in the dimension of the feature space the required sample size grows exponentially). However a feature can be represented as a one-dimensional (independent) random variable and information about correlations can be obtained by calculating a matrix of paired correlation coefficients between features. Thereby the information will be saved (with some errors) while the sample size for assessing the informativeness of the features will remain at typical level for a one-dimensional random variable.

A scale and a method for evaluating the informativeness of a feature through the construction of probability density functions of its values and the determination of their intersection areas $S_q$ for the Own and strange patterns (Fig. 5) were proposed in [8]. The pattern “Own” means a biometric pattern belonging to a registered user who has trained the authentication system using his own EEG examples. The pattern of "Strange" – any patterns of the EEG that do not belong to the subject. Area $S_q$ is translated into its own information according to the formula:
\[ I_{\text{opt}}(a_i) = -\log_2 S(a_i). \]

Informativeness of a single feature can be considered analogous to its quality and uniqueness. But the total amount of information in the biometric pattern is influenced by the correlation of the features. A part of the pattern information is always “transferred” to the matrix of paired correlation coefficients between features which is almost unique in every biometric pattern.

Studies have shown that the distribution law of the majority of dynamic biometric features is close to normal, less often is lognormal and double exponential distribution [7]. However for many EEG features this statement is not true. The distribution law is complex and differs for different subjects (the test was carried out on the basis of the chi-squared test). The construction of empirical probability densities as histograms of the relative frequencies of the featured values that normalized over the length of the interval is more correct. The number of intervals must be large in order to reduce the effect of quantization noise of continuous data on the estimation accuracy. 25–30 intervals is sufficiently to obtain an average score for all subjects with a sample size of "Own" of the order of 125–300 examples.

![Figure 5. Distributions building of features values: a. informativeness definition of j feature for i subject through probability densities “Own” and “Strange” (if we accept the hypothesis of the normal distribution of the features), b. Empirical probability densities "Own" for 3 subjects has built on the values of the j feature.](image)

In accordance with the assessment more than 99% of the EEG features under consideration correspond to a very uninformative one by a scale from [8] (the average \( I_{\text{opt}} \approx 0.2 \) bit). For this reason fuzzy extractors can be considered a priori ineffective since they are efficient only if the features are highly informative [9]. The informativeness of EEG features formed under the influence of various visual patterns (Rorschach tests and geometric figures) is almost identical.

### 6. Verification of EEG patterns by using neural network algorithms

A computational experiment on the recognition of EEG images using neural network algorithms was carried out. All EEG recordings were divided into 10 second fragments (examples of EEG). Each classifier was trained on the 7 minutes of EEG recording data (42 examples). The “Strange” training sample for each test subject consisted of 7 minutes of recording the EEG of the other 37 (half of the total) randomly selected subjects (1554 examples). Examples of EEGs that were not used in training including those recorded on another day were used as test data.

For comparison three types of “wide” networks were taken [10]: a perceptron trained according to GOST R 52633.5, a network of quadratic functionals, and a network of multidimensional Bayes difference functionals. An increase in the number of layers is not relevant for neural network automatics of biometric authentication. It is much more efficient to increase the number of inputs and outputs of the network [3]. This leads to a slow increase in the quality of solutions – reducing the probabilities of errors and increasing the entropy of the "Strange" codes. Based on the above all networks in the experiment had only one hidden layer.

The perceptron artificial neuron is based on the functional (1) and the threshold activation function. The weights modules of the neurons of the first layer are calculated by the formula (2). Connections of neurons with features are determined randomly.
\[ y = \sum_{j=1}^{N} \mu_j a_j, \]  
\[ \mu_j = \frac{m_j(a_j) - m_j(a)}{\sigma_j(a) \sigma_j(a)}, \]  
where \( a_j \) – a value of the \( j \) feature, \( N \) – a number of neuron inputs, \( m_j(a_j) \) – an expected value of \( j \) feature of the "Own" pattern, \( \sigma_j(a) \) – a standard deviation of \( j \) feature of the "Own" pattern, \( m_j(a) \) and \( \sigma_j(a) \) – similar parameters for the image of "Alien". If a neuron is configured to issue "Own" pattern then the sign of the weighting factor is chosen based on rules: «+» while \( m_j(a_j)<m_j(a) \), or «-». If the neuron is set to zero then signs are inverted.

A quadratic neuron is built on the basis of the Pearson measure (3) \[9, 10\]. Only if the features are not correlated the Pearson measure is effective. Therefore the connections were set randomly but with the expectation that the features with a correlation coefficient more than 0.3 should not fall into one neuron. The network of Bayesian multidimensional functionals (4) \[10\] was formed on the basis of the opposite requirement: each neuron processed features with coefficients of pair correlation more than 0.7. The greater \( N \) and the higher the coefficient between the features the more efficient the Bayesian functional works \[11\].

\[ B = \frac{1}{\sqrt{\sum_{j=1}^{N} (m_j(a_j) - a_j)^2 / \sigma_j(a_j)^2}}, \]
\[ d_i = \sum_{j \neq i} \left| \frac{m_j(a_j) - a_j}{\sigma_j(a_j)} - \frac{m_i(a_i) - a_i}{\sigma_i(a_i)} \right| \]

As we can see from Table 1 the probability of errors turned out to be significant. This should be due to two main factors: 1. functionals (3), (4) and (1) with the setting (2) does not take into account the asymmetry and excess of distributions while calculations; 2. feature informativeness is extremely low. Consequently a stronger enrichment of the image input data taking into account all the features of the distribution of attributes is required. It is necessary to use large statistics of the values of the features when comparing EEG patterns with a biometric template to obtain reliable solutions at the output of the classifier.

| Network type                        | parameter                      | FRR  | FAR  | EER  |
|-------------------------------------|--------------------------------|------|------|------|
| perceptron                          | 1024 neuron, \(N=5\)           | 0.225| 0.015| 0.099|
| perceptron                          | 1024 neuron, \(N=10\)          | 0.42 | 0.015| 0.135|
| Network of quadratic forms          | 1024 neuron                     | 0.07 | 0.04 | 0.06 |
| Bayes Difference Functional Network | 1024 neuron, \(2<N<120\) (the number of inputs for all neurons is different) | 0.15 | 0.015| 0.065|

**7. Verification of EEG patterns by using a modified Bayesian formula**

In the course of the work it was revealed that dividing signals into fragments of greater length (5, 10 seconds each) is not rational since it does not increase the informativeness of the features.

It is much more profitable to divide the EEG into small segments with a duration of no more than 1.5 seconds while using as many as possible of these segments during the training and authentication stages. A large number of segments at the training stage allows you to collect more complete statistics and build empirical probability density functions of feature values with higher accuracy. The use of several EEG fragments at the stage of authentication allows us to construct a vector of signs of greater length (the vectors of each EEG fragment are combined into one long vector in which the features are cyclically repeated several times).

A similar computational experiment was carried out based on a statistical approach. The size of the EEG recordings for training was not changed – 7 minutes but the number of examples was increased (280 examples of “Own”, 10,360 examples of “Strange”). Two hypotheses were determined: “Own” and “Strange”. Two histograms of relative frequencies describing the hypotheses “Own” and
“Strange” ($H_0$ and $H_1$ respectively) with the number of intervals more than 25 were constructed for each subject by each feature. The test sample was similar to the previous experiment. However, each test sample consisted of 20 EEG fragments of 1.5 seconds. Thus the length of the feature vector was equal to N = 30800.

The classifier was based on the modified Bayes hypothesis formula (5). A posteriori probabilities for each subject of the “Own” and “Strange” hypotheses were calculated for N = 30,800 steps. At each step the a posteriori probabilities of hypotheses $H_0$ and $H_1$ are calculated using formula (5), taking into account the value of the next feature. At each step the posteriori probability calculated by the previous step was taken as the prior probability of the hypothesis. All hypotheses were initially considered to be equally probable $P(H_j|A_0) = 0.5$. FRR and FAR were calculated at each step (Fig. 6) depending on the threshold value $T$ for $P(H_0|A_j)$.

$$P(H_j|A_j) = P(H_j|A_{j-1}) + \left( \frac{P(H_j|A_{j-1})P(A_j|H_j)}{\sum_{i=1}^{N} P(H_i|A_{j-1})P(A_j|H_i)} - P(H_j|A_{j-1}) \right) \times (W_j)$$

(5)

where $P(H_j|A_j)$ – posterior probability of $i$ hypotheses by $j$ step, $P(A_j|H_j)$ – conditional probability of $i$ hypotheses is equal to relative frequency of $j$ feature for $i$ hypotheses, $W_j$ – weight of $j$ feature, $W_j \in [0; 1]$. When $W_j = 1$ we have the classical version of the Bayes formula. Since features are assumed to be statistically independent this version the Bayes classifier is often called “naive”. When $W_j = 1$ it becomes impossible to balance $T$ (when $j < N$ there is always a situation where $P(H_j|A_j) = 0$ when $P(H_j|A_j) = 1$ as a result the new information after this point is not taken into account and FAR tends to one). The described effect can be called a failure when the bitness of data types with a "floating point" (e.g. double in C #) is not enough because of the possibility of a significant change in a posteriori probabilities in one step. The mentioned effect arises the more often the more N, the lower the informativeness of the features and the smaller the number of hypotheses. In present case these parameters such that the effect of "failure" appears inevitable.

The increments of the posterior probabilities of hypotheses must be limited ($W_j < 1$) due to the negative impact of failures. We compared the effectiveness of two options – with a fixed (6) and variable weight (7) depending on the informativeness of the $j$ feature for the subject:

$W_j = 1/N$  \hspace{1cm} (6)

$W_j = (1/N) \cdot I_{inf}(a_j)$  \hspace{1cm} (7)

The second option was more effective (Fig. 6). When $W_j < 1$ (7) the Bayesian classifier may be called "cautious" because there is no longer "blind" trust to the input data.

It is possible to balance the probabilities of FRR and FAR as can be seen from Fig. 6 by changing $T$. The classifier is easily adjusted to a single threshold for all subjects at which errors of the second kind do not occurs while the FRR gradually decreases with an increase in the EEG monitoring time of the authenticated subject. Table 2 shows the most illustrative of the known earlier achieved results.

Table 2. A comparative data on the human EEG recognition reliability.

| A summary of the method | Result |
|------------------------|--------|
| Analysis of brain activity that occurs in brain fields that are responsible for reading and word recognition [12] | 3–18% errors, 45 subjects |
| Assessment of individual brain reactions to various stimuli: primary visual perception, recognition of familiar faces, taste [1] | 0% errors, 50 subjects |
| The key generation algorithm based on EEG using the evoked potential of the P300 and two-layer neural networks (GOST R 52633.5) [13] | $10^{-15}$% errors, 15 subjects |
| Conversion of subjects EEG who are at rest into a 400-bit key [14] | 0.024% errors, 42 subjects |
Figure 6. Probabilities of EEG Subject Verification Errors: a. excluding informativeness (T=0.5), b. c. taking into account the informativeness (T=0.5), c. taking into account the informativeness (T=0.54)

As you can see from the table in some works the zero level of errors is indicated which is incorrect in fact - there are no zero probabilities in biometrics. In this paper there were no errors of the 2nd kind. Therefore we assume that FAR<10^-4 with FRR = 0.062 based on the number of experiments.
8. Conclusion

A visual comparison of the amplitude spectra, auto- and cross-correlation functions, as well as wavelet sonograms constructed by means of EEGViewer (Neurosoft) did not allow us to reveal any features characterizing the differences or similarities of EEG belonging to different people. Differences become visible when building empirical probability densities of feature values on large statistics, as a result these statistical distributions can be used as biometric templates.

A method for verifying EEG patterns based on a modified Bayes hypothesis formula was proposed. It has been achieved low error rates: FAR < 10^{-4} with FRR = 0.062. However the developed method requires the use of mechanisms for additional protection of the templates when it is stored on the server (the parameters of the histograms of the relative frequencies of the feature values completely compromise the biometric pattern of the user unlike the parameters of the trained neural network).

The using of “wide” neural networks, networks of quadratic forms and multidimensional difference Bayesian functionals in combination with absolutely stable (non-iterative) learning algorithms did not give good results. A feature of the EEG pattern recognition problem is the presence of a large number of extremely uninformative features with asymmetric probability density functions which are difficult to approximate with known distribution laws as well as the possibility of forming a training sample of sufficiently large volume dividing the EEG record into many small fragments. This allows us to consider multilayer networks (including convolutional networks) and “deep learning” methods as an alternative basis for building a classifier which is planned for the near future. A variant of aggregation a “wide” neural network with the proposed method for building a secure neural network container based on them that stores the parameters of a hybrid neural network consisting of classical neurons and neurons of Bayes' highest likelihood is also possible.

9. Reference

[1] Ruiz–Blondet, M.V. et al. 2016 CEREBRE: A Novel Method for Very High Accuracy Event-Related Potential Biometric Identification IEEE Transactions on Information Forensics and Security, 11(7) pp 1618–1629.
[2] Hafemann L G, Sabourin R and Oliveira L S 2019 Characterizing and evaluating adversarial examples for Offline Handwritten Signature Verification IEEE Transactions on Information Forensics and Security 1 pp 1–27
[3] Malygin A, Seilova N, Boskebeev K and Alimseitova Z 2017 Application of artificial neural networks for handwritten biometric images recognition COMPUTER MODELLING & NEW TECHNOLOGIES 21 pp 31–8
[4] K. Jain A, Nandakumar K and Nagar A 2008 Biometric Template Security EURASIP Journal on Advances in Signal Processing 2008 1–17
[5] Soutar R 2014 Chapter Two – An Introductory Perspective on the Emerging Application of qEEG in Neurofeedback Clinical Neurotherapy ed D S Cantor and J R Evans (Boston: Academic Press) pp 19–54
[6] van Albada S J and Robinson P A 2013 Relationships between Electroencephalographic Spectral Peaks Across Frequency Bands Front Hum Neurosci 7 56
[7] Sulavko A, Volkov D, Zhumazhanova S S and Borisov R V 2018 Subjects Authentication Based on Secret Biometric Patterns Using Wavelet Analysis and Flexible Neural Networks 2018 XIV International Scientific-Technical Conference on Actual Problems of Electronics Instrument Engineering (APEIE) (Novosibirsk, Russia, 2–6 Oct. 2018) pp 218–27
[8] Sulavko A E, Zhumazhanova S S and Fofanov G A 2018 Perspective Neural Network Algorithms for Dynamic Biometric Pattern Recognition in the Space of Interdependent Features 2018 Dynamics of Systems, Mechanisms and Machines (Dynamics) (Omsk, Russia, 13–15 Nov. 2018) pp 1–12
[9] Ivanov A I, Kachajkin E I and Lozhnikov P S 2016 A complete statistical model of a handwritten signature as an object of biometric identification 2016 International Siberian Conference on Control and Communications (SIBCON) (Moscow, Russia, 12-14 May 2016) pp 1–5
[10] Ivanov A I, Lozhnikov P and Sulavko A 2017 Evaluation of signature verification reliability
based on artificial neural networks, bayesian multivariate functional and quadratic forms

[11] Ivanov A I, Vyatchanin S E and Lozhnikov P S 2017 Comparable estimation of network power for chisquared Pearson functional networks and Bayes hyperbolic functional networks while processing biometric data 2017 International Siberian Conference on Control and Communications (SIBCON) (Astana, Kazakhstan, 29–30 June 2017) pp 1–3

[12] Armstrong B C, Ruiz-Blondet M V, Khalifian N, Kurtz K J, Jin Z and Laszlo S 2015 Brainprint: Assessing the uniqueness, collectability, and permanence of a novel method for ERP biometrics Neurocomputing 166 pp 59–67

[13] Goncharov S, Borshevnikov A 2016 Nejrosetevoj preobrazovatel’ «Biometriya – kod dostupa» na osnove ehlektroehntsefalogrammy v sovremennykh kriptograficheskikh prilozheniyakh [Neural network transformer “Biometry - access code” based on the electroencephalogram in modern cryptographic application] (in Russian) Vestnik SibGUTI 1 pp 17–22

[14] Damasevicius R, Maskeliunas R, Kazanavičius E and Woźniak M 2018 Combining Cryptography with EEG Biometrics Computational Intelligence and Neuroscience 2018 1–11

Acknowledgments

This work was supported by the Russian Foundation for Basic Research (RFBR) and the Government of the Omsk Region (grant 18-41-550002).