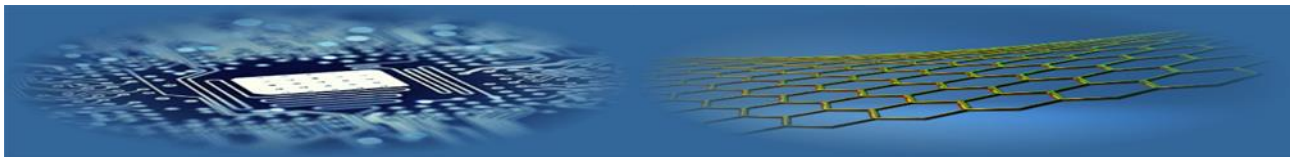

# Application of artificial neural networks forhandwritten biometric images recognition

**A Malygin[1], N Seilova[2], K Boskebeev[3], Zh Alimseitova[2]**

[1]*Penza State University, Penza, Russia*
[2]*Kazakh National Technical Research University named after K.I. Satpaev, Almaty, Kazakhstan*
[3]*Kyrgyz State Technical University named after I. Razzakov, Bishkek, Kyrgyzstan*

**Abstract**

The development of information technology leads to new requirements for the development of security systems, identity authentication and other protection mechanisms. The article is devoted to the use of artificial neural networks for handwritten biometric images recognition that are used in high-authentication systems. There is given a general structure of the biometric-neural network authentication system, the structural scheme of information processing in biometric-neural network authentication systems, the structural scheme for learning the neural network converter of the biometric parameters vectors in the key code (password). There is formed and trained a network of neurons, are formed neural network containers on the basis of structures. The choice of the length of the biocode of neural network converters is substantiated. After graduation, testing is conducted and the probabilities of errors of the first and second kind are determined. There is given an example of a software implementation, where are given a learning mode, checking the results of training, testing the results of training.

*Keywords:*

artificial neural networks,
authentication,
biometric image,
first-kind errors,
second-kind errors

## 1 Introduction

Nowadays, the processes of informatization of modern society are actively underway. Internet space and digital mobile telephony are widely used. Almost all states declare their desire to create an e-government to provide services to their citizens. All these processes pose a number of problems before biometrics and cryptography. What was created in the last century, in terms of biometric technologies, does not work in the Internet space. Unfortunately, until now the Internet remains anonymous, impersonal environment with low confidence to it. This, on the one hand, is a breeding ground for all sorts of fraudsters, and on the other hand it undermines the confidence of ordinary citizens to new information technologies.

In the ordinary world, a government representative checks the citizen's credentials by his identity card or passport. In a virtual world, everything turns out to be more complicated, you can not use your identity card scan, even if it's a biometric identification card with a radio-readable RFID chip. You can not read the contents of the chip. Personal data contained in a bio-ID chip can not be used in the Internet space. For the Internet and other open information spaces, it is necessary to create special Internet passports or Internet identity cards, which on the one hand are biometric, and on the other hand are some cryptographic constructions that protect the confidentiality of personal data of their owners.

This problem is currently being given considerable attention. Researchers of the United States and NATO create and promote the relatively weak biometrics of open biometric images. Biometric authentication tools are built using fuzzy logic. Researchers from Russia, Belorussia and Kazakhstan suggest using neural network converters as biometric-code, while biometric authentication tools are built using large-scale artificial neural networks.

Researchers conducted in Kazakhstan, Russia and Belorussia in recent years have shown that existing biometric technologies can be significantly enhanced through the use of artificial neural networks [1-18]. They enrich the data in a continuous form, and usually for all input errors correction duplicate redundancy is enough, that is, 512 input biometric parameters the neural network converts into 256 bits of the output code with virtually no errors.

From the point of view of obtaining biometric properties, the neural network biometric converters are always better than "fuzzy extractors". This can easily be demonstrated by the example of poor biometric data, giving errors of 50% and more of biocode digits. Classical self-correcting codes are not capable to correct more than 50% of the errors, neural networks cope with this problem if their redundancy becomes threefold (inputs three times more than outputs).

## 2 The use of large neural networks

The use of large neural networks allows considering "good" biometric data along with "bad" and "very bad" biometric data. Moreover, the "worse" the biometric data is used, the more the network of artificial neurons should be and the more difficult it is to train.

The general structure of the biometric neural network authentication system is shown in Figure 1.

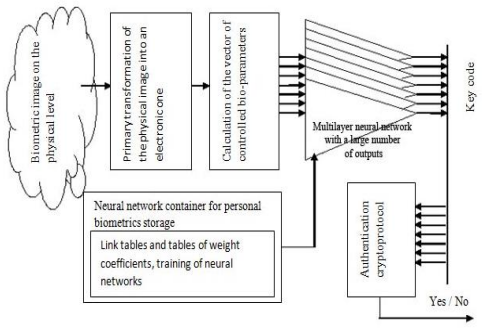


FIGURE 1 The general structure of the biometric neural network authentication system

It should be noted that for the solution of this problem artificial low-dimensional neural networks are unsuitable [12, 14, 17].

The process of input biometric image converting into an output long password (key) can be represented in the form of a diagram on Figure 2 [18].

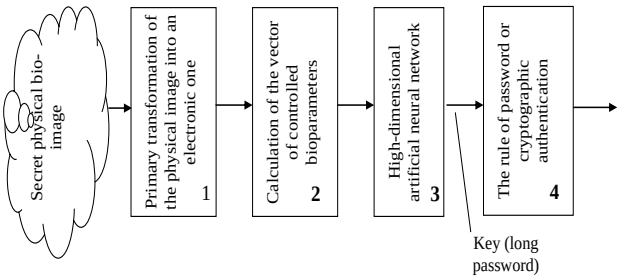


FIGURE 2 Structural diagram of information processing in biometric-neural network authentication systems

## 3 General training scheme of neural network converters biometry – code

The training scheme of the neural network biometric parameters vector converter into the key code (password) is represented by the scheme on Figure 3 [11]. For learning, you need $N_1$ of examples of the vectors "Own" and $N_2$ of examples of the vectors "Aliens".

Training of the artificial neural network should be carried out automatically (without human intervention in the process of artificial neural network parameters selection), the user must have a guarantee that his long password (key) involved in the training process will not be compromised.

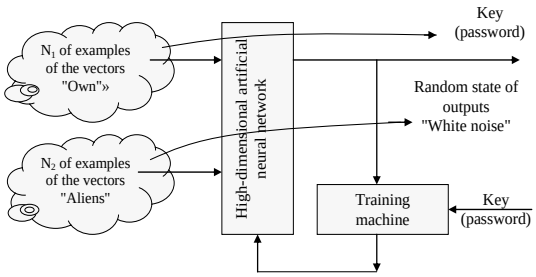


FIGURE 3 The structural scheme of training of the neural network biometric parameters vector converter into the key code (password)

During the training, the weight coefficients of the artificial neural network should be selected by the training machine in such a way that during the appearance of the elements of the vector "Own" on the inputs of the artificial neural network a long password (key) appears on the outputs of the artificial neural network. During the appearance on the inputs of the artificial neural network of the data vectors corresponding to the images "Alien", random states - "white noise" - should appear on the outputs of the artificial neural network. Training is carried out by alternately presenting of the images "Own" and "Aliens" with an intermediate selection of coefficients.

In order to use neural network bio-data enrichment it is necessary to be able to train single artificial neurons. [19-23].

## 4 Formation and training of the network of neurons. Neural Network Containers

In order to obtain the access biocode it is necessary to create a network of neurons with the number of outputs equal to the length of the key. The more inputs and outputs the neural network has the higher the quality of the decisions making. How strong this relationship is can be seen from the data in Table 1.

TABLE 1 The quality increase of solutions depending on the number of inputs and outputs of the artificial neural network

| Number of inputs of the neural network | Number of outputs of the neural network | The probability of rejecting to "Own" | The probability of missing the "Alien" |
|---|---|---|---|
| 5 inputs | 1 output, 2 classes | $P_1 = 0,1$ | $P_2 = 0,17$ |
| 48 inputs | 1 output, 2 classes | $P_1 = 0,1$ | $P_2 = 0,03$ |
| 480 inputs | 1 output, 2 classes | $P_1 = 0,1$ | $P_2 = 0,005$ |
| 480 inputs | 256 outputs, $2^{256}$ classes | $P_1 = 0,1$ | $P_2 = 0,000000001$ |
| Training of the neural network with 480 inputs and 256 outputs was conducted on 20 examples of the image "Own" and on 128 examples of images "Alien" by the algorithm GOST R 52633.5-2011 | | | |

It can be seen from the Table 1 that a simple increase of the number of inputs of the biometric parameters is not very effective. It is much more important to increase in parallel the number of its outputs in parallel with the number of inputs. With the same number of inputs (480 inputs) an increase in the number of outputs from 1 to 256 gives a gain of about a billion times as the decisions made by the neural network (six zeros additionally appear). At the same time, other costs of computing resources increase approximately up to 100 times, an exponential relationship between the sizes of artificial intelligence and the quality of decisions made by it is seen.

One of the most important task is the choice of the structure used by the neural network. Typically, in the literature on artificial neural networks, networks are divided into single, double and triple layers, as well as networks with more than three neurons. Such a wide variety of neural network structures for biometrics is not relevant. GOST R 52633.5-2011 provides either single-layer or two-layer neural networks. For two-layer neural networks, the functions of the first and second layers are separated. Neurons of the first layer fulfill the function of biometric data enrichment and enriched data quantizing. If the quality of enrichment was not large enough, then the second layer of neurons corrects the biocode errors of the neurons of the first layer.

It should be noted that the second layer of neurons can always be replaced by the usual classical code that detects and corrects errors, but neural network error correction is more advantageous. The advantage of using neural network correctors – during the training of the second layer on the

examples of "Own" biocodes, the real indicator of stability of each of the biocode digits of is estimated.

Practice shows that the vast majority of biocode digits has a high stability, only isolated bits of code with an exactly known position are unstable.

The second layer of neurons train to correct unstable digits and simultaneously to hash (mix) both stable and unstable ones. All classical codes with errors detection and correction are constructed in the context of the hypothesis of equiprobable error distribution between code digits. Only because of this, classical self-correcting codes lose to neural network error correctors, which during the training take into account the real distribution of the stability indicators of the "Own" biocodes.

In addition to the number of network neurons layers, it is necessary to choose the number of inputs of each neuron and to specify the connection of inputs with the numbers of the network inputs. So, if the entire neural network has 480 inputs and the average information of the inputs is about 0.3 bits, then it is needed to use neurons with the number of inputs from 1 to 18 (depending on the quality of the biometric parameters used by the neuron and the correlation between them). The required number of inputs can be found only during the training of the neuron. Initially, a small number of inputs are randomly selected, if the quality of the solution does not reach the specified value, then the number of inputs of the neuron is increased. Ultimately, there is produced a single layer network of neurons, where each neuron has its own number of inputs connected randomly to the inputs of the entire network. After training, in addition, we obtain a table of weight coefficients for the input connections of each of the neurons.

A formally trained network is described by the tables of neuron connections and weight coefficients tables. If the network is two-layer, the tables of connection numbers and weight coefficients tables must be created for each of the layers of neurons. The layers of neurons are trained sequentially. After training the first layer of neurons, the examples of images "Own" and "All Aliens" are broadcast from the input of the neural network to the outputs of the neurons, there are received examples of the biocodes and neurons of the second layer are trained on them.

Tables of neural network connections and weight coefficients tables of the trained neurons form the so-called neural network containers. In the neural network container there is enough information to reproduce at the appropriate moment a software-trained neural network and to convert the biometric data of the person to the code of his cryptographic access key. The authentication procedure built using a neural network container is shown on Figure 4.

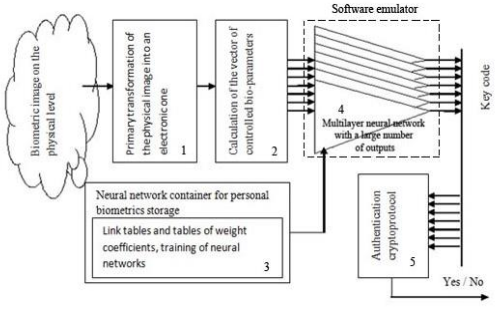


FIGURE 4 Block diagram of biometric authentication using a neural network container

Formation and the use of neural network containers for storage of human biometrics and interfaces of interaction with them are regulated by GOST R 52633.4-2012 [24].

The choice of GOST R 52633.5-2011 for a two-layer network of neurons (perceptrons) is conducted due to the fact that this neural network structure is universal and can solve any problems. M. Minsky and S. Papert [25] showed that a single perceptron is not universal.

In fact, the training of artificial neural networks in accordance with GOST R 52633.5-2011 at increasing the number of inputs for neurons is carried out more and more stable. Therefore, large neural networks after their training work more reliably than classical algorithms of multidimensional statistics and linear algebra. Constructing a quadratic decision rule in the form of a 480-dimensional hyperellipse is technically impossible, whereas it is quite possible to construct an approximation of this hyperellipse by 480-dimensional parallelepipeds (4 perceptrons with 480 inputs in the first layer of the network).

## 5 Rational choice of the biocode length of the neural network converters

If it is required 256 bits key code length for the subsequent cryptographic authentication, then from this condition it is unambiguous that the biometric-code neural network converter must have 256 outputs. If the neural network converter is single-layer, then the first layer must have 256 neurons.

As it was noted earlier, cryptographic protection is always much stronger than password and biometric protection. This fact is well observed when we change the number of neurons in the first layer of the network. In the first approximation, the probability of biometric errors $P_{2,Б}$ will decrease with the increasing of the number of used neurons, the corresponding decrease curves are shown in Fig. 5. However, the rapid growth of resistance (rapid decrease in the probability of $P_{2,Б}$) does not occur continuously. Usually a linear decrease in the probability $P_{2,Б}$ is observed only at the initial position of the growth of the number of neurons. Further, the growth indicator slows down and, starting from a certain moment, the probability of errors of the second kind generally ceases to decrease.

The moment of stop of the decrease in the probability of errors of the second kind depends on the informative nature of the biometric image of "Own". The Figure 5 presents two curves of the probability of errors reduce in the biometric component of authentication.

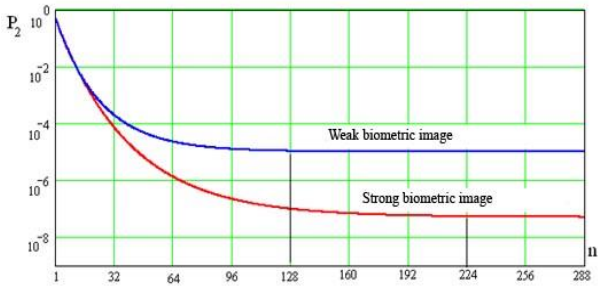


FIGURE 5 The influence of the number of outputs of a single-layer neural network on the probability of errors of the second kind

It can be seen from the Figure 5 that a "weak" small informative biometric image gives a higher error probability

($P_{2,Б} = 10^{-4,7}$), saturation for this image occurs with a key length of 128 bits, that is, with a 256-bit output length of 50% the redundancy of the code, which can be spent painlessly on detection and correction of errors.

A more "stronger" biometric image has a saturation area for codes longer than 224 bits ($P_{2,Б} = 10^{-7,1}$), that is, for this code the redundancy will be 12.5%. This redundancy can also be used to detect and correct errors by classical self-correcting codes. If this redundancy is not enough, then it is necessary to increase the output biocode length to the required.

In some cases (for example, using foreign cryptographic algorithms), the key length may be less than the length before the saturation start area of the biometric-neural network protection. This situation just corresponds to the second case of application of the relatively "strong" biometry (the lower curve of Figure 5) with the required key length of 128 bits. Formally, we can confine with 128 neurons in the first layer of a neural network, but this will lead to a certain losses of quality indicators.

In cases where it is technically advantageous to have a number of neurons greater than the length of the output cryptographic key (for example, 224 > 128), it is necessary to implement a hash of the biocode. After hashing, trim the hash function to the desired length and use it as a key.

In cases when keys are formed outside the biometric application, the value of the hash function can be brought to the specified one if it is added according to the module of two with the addition. If this is necessary, the hashing of the biocode "Own" is performed with "Salt". The “Salt” and the addition of the hash function are stored openly.

It should be noted that the above technique is suitable not only to shorten the length of the key, but also to increase it. This means that for a relatively "weak" biometric image of "Own" (the upper curve of Figure 5), we can dispense with a network of 128 artificial neurons, increasing the length of the biocode by hashing from 128 to 256 bits. This method is suitable for saving computing resources. Cryptographic hashing is usually performed about 1000 times faster than software emulation of an artificial neural network.

## 6 Neural network biocode correction by the second layer of neurons

In cases when the classic self-correcting codes give too much information loss (require too much redundancy) GOST R 52633.5-2011 recommends the use neurons of the second layer to correct the errors admitted by the neurons of the first layer. Before setting the neurons of the second layer, the standard recommends to estimate the stability of each of the digits of the biocode "Own". For this purpose, test examples of the image "Own" are submitted and the probabilities of errors of the first kind for each of the digits $P_{1,i}$ are calculated. Further, the stability indicators of each of the digits are calculated:

$$\gamma_i = 2 \cdot \left| P_{1,i} - 0.5 \right|, \quad (1)$$

where $\gamma_i$ – stability indicator of i digit, taking values of 1.0 for absolutely stable digits and a value of 0.0 for unstable digits with equiprobable states "0" and "1".

Adjusting the neuron of the second layer, it is necessary to set its weight coefficients in proportion to the stability index (1). The sign of the weight coefficients is chosen randomly. The inputs of the correction neuron are connected to the digits of the biocode randomly, while converting the values of the digits of the biocode: the state "0" is converted to the state -1, the state "1" is assigned the value +1. As a result of multiplication of random signs of weight coefficients and random states of digits of the biocode ±1, a state close to zero appears at the output of the neuron adder.

The neuron adjusting goes to random cyclic permutations of the sign in the pairs of inputs. Obviously, in a neuron with 64 inputs, the maximum possible output state will be close to +64, and the minimum possible value will be close to -64. If the adjustable neuron must correct 1 error and give the state "1", then it is necessary to achieve the maximum value of the response to the examples of "Own" close to +2. If the adjustable neuron should correct 1 error and give a state of "0", then it is necessary to achieve the maximum response value to the examples of "Own" close to -2. The number of errors corrected by the neuron should always be about one unit less than the module of the maximum response to the examples "Own".

It should be noted that the second layer of neurons performs two functions. First, it corrects the biocode errors of the previous layer of neurons, and secondly, the adder of the second layer of neurons (mix) hashes the data of the codes "Alien".

## 7 Hashing of "Alien" data performed by neurons of the second layer

The ideal biometric converter should completely eliminate the uncertainty of the codes "Own" and maximize the entropy of the codes "Alien". The input entropies of continuous data of the examples of the image "Own" and of the examples of the image "Alien" are comparable:

$$H_{480}(\bar{v}) \approx \mathrm{H}_{480}(\bar{\xi}), \quad (2)$$

where $H_{480}(\bar{v})$ - input entropy of continuous data of the examples of the image "Own"; $\mathrm{H}_{480}(\bar{\xi})$ - input entropy of continuous data of the examples of the image "Alien".

After implementing of the neural network transformation, the situation changes:

$$\begin{cases} H_{256}(c) \approx 0; \\ H_{256}(x) \approx 256. \end{cases} \quad (3)$$

In fact, small entropy of the codes "Own" and the closeness of the entropy of the codes "Alien" to the limit value of 256 bits determines the closeness of the real converter to the ideal one.

A two-layer neural network improves its properties from layer to layer, designating the codes of the first layer by the index 1, and the codes of the second one – by the index 2, we can write

$$\begin{cases} H_{256}(c_1) \rangle H_{256}(c_2) \approx 0; \\ H_{256}(x_1) \langle H_{256}(x_2) \approx 256. \end{cases} \quad (4)$$

This situation is seen on the corresponding Hamming distance distribution of the codes "Own" and "Alien".

Figure 6 shows that at the output of the neurons of the first layer, the biocode has resistance to picking attacks of approximately 56 bits (the distance between the edges of the Hamming distance distributions of "Own" and "Alien").

After correcting the errors by the neurons of the second layer, the visible distance between the sets is more than 100 bits, but this is an imaginary (overestimated) resistance, due to the fact that the neurons of the second layer not only control the biocode "Own", but also hash the codes "Alien". The hashing properties of the second layer of neurons can be estimated as the ratio of the entropy of the codes "Alien" at the output of the neural network to the entropy of the biocodes at the output of the neurons of the first layer.

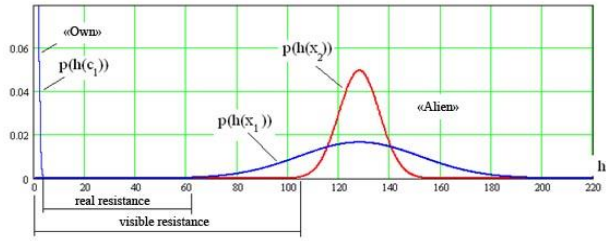


FIGURE 6 Compression of the Hamming distance distribution at the output of neurons of the second layer due to the hashing properties of neurons

The fact that the neurons of the second layer of the network have sufficiently strong hashing properties is explained by the random arrangement of weight coefficients and the rounding operation of the summation results performed by them. Any unidirectional operation leading to a decrease in the length of the code has some hashing properties, because the source data can not be restored from the short output codes. In our case, the summation results of the code correcting neuron can vary from -64 to +64, and its output code has only two values of "0" and "1". There is an operation of truncating the length of the 9-bit code to the 1st digit.

## 8 Probabilities of errors of the first and second kind

After training the system of biometric-neural network authentication it is necessary to evaluate the quality of training. The probability of an error of the first kind $P_1$ and the probability of an error of the second kind $P_2$ are estimated.

The user must know the real assessment of the resistance to the specific implementation selection attacks of biometric authentication after its training, built on the reproduction of a specific secret biometric image. Testing is carried out using $N_1$ - test examples of the vectors of the image "Own" and $N_2$-test examples of the vectors of the image "Aliens". The structural scheme of testing is shown on Figure 7.

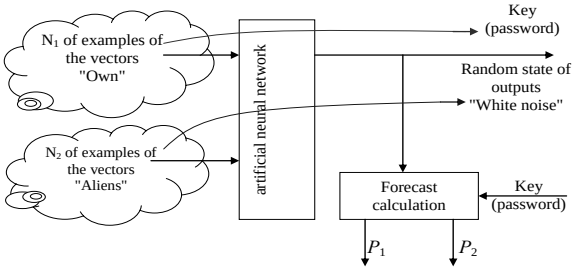


FIGURE 7 Structural scheme of testing the biometric-neural network authentication system after training

Any biometric protection is built on the fact that it is able to recognize the image "Own" and reliably to isolate many images "Alien" ("All Aliens"). Obviously, the means of biometric protection (biometric authentication) can be mistaken. The main task (task number 1) for biometrics is to provide the donor with a biometric image "Own". An error in the execution of this task is treated as an error of the first kind. The main characteristic of the efficiency of the biometric authentication tool is the probability of errors of the first kind $P_1$.

The second task of the biometric authentication tool is to prevent the donor from accessing the "Alien" image. The second most important characteristic of biometrics is the probability of errors of the second kind $P_2$ due to possible collisions of the images "Own" and "Alien" on the set of features (biometric parameters) under consideration.

Obviously, the probability of errors of the second kind $P_2$ will be less, if more biometric parameters take into account this or that biometric authentication tool. Only those biometric tools that analyze hundreds or even thousands of biometric parameters can be considered reliable. In this case, the attacker should not know the selected biometric image, only in this case the biometry can be considered as highly reliable.

## 9 Software implementation of handwriting image recognition

A necessary condition for training the skills of stable spelling of the recommended word and the correct formation of an impersonal base of biometric images is the familiarization by the donor with biometrics of the specialized software and hardware complex "Neuro-Test 1.2" [26].

The program uses an emulator of an artificial neural network, which has many outputs. The number of outputs of an artificial neural network is determined by the length of the biometric key generated by it. This excludes the hacking of the program through the detection and substitution of the last bit of the decisive rule. The program has a multi-bit decisive rule, the bit values combination of which is unique and unknown to the attacker. The program "NeuroTest 1.2" uses the algorithm of rapid automatic training of the artificial neural network with 256 outputs.

The main window of the program is shown on Figure 8.

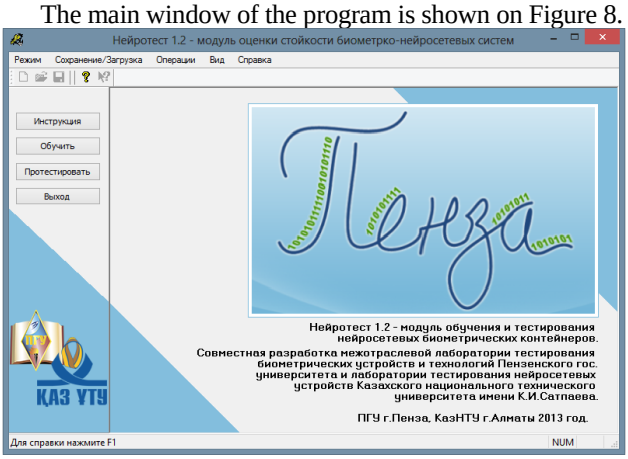


FIGURE 8 The main window of the program "NeuroTest 1.2"

***Training mode.*** Training begins with the initialization of the training mode (the "Train" button or the "System training" mode).

Next, you need to reproduce a pre-defined handwritten word by your hand on the field of the “Genius” graphic tablet.

After entering the handwritten word, click the "Add" button, the lined field is cleared, and the number of the next

entered example appears in the right part of the window. If a hand trembles during entering a handwritten word-password, or the image is not typical, click the "Clear" button. In this case, the word is deleted without entering into the database of examples. You need to reproduce the word for 20 times. The input of handwritten images is controlled by the instructor.

You can view saved examples by clicking on the number in the right part of the window (Figure 9).

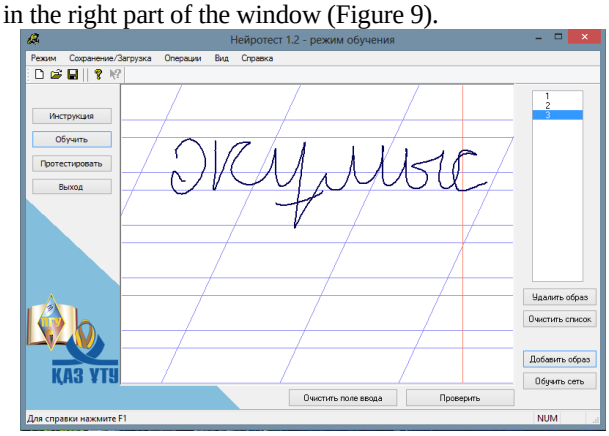


FIGURE 9 Handwritten images view

If any example does not match the handwriting, then it must be deleted by clicking on the "Delete image" button. If you do not like all the images or you need to change the word-password, then all the images in the list are deleted (the "Delete All" button).

Training of the system (neural network) is carried out by clicking the "Train" button. In this case, for a time up to 30 seconds a window appears with a forecast of the probabilities of system errors and with the number of the group to which you belong (Figure 10).

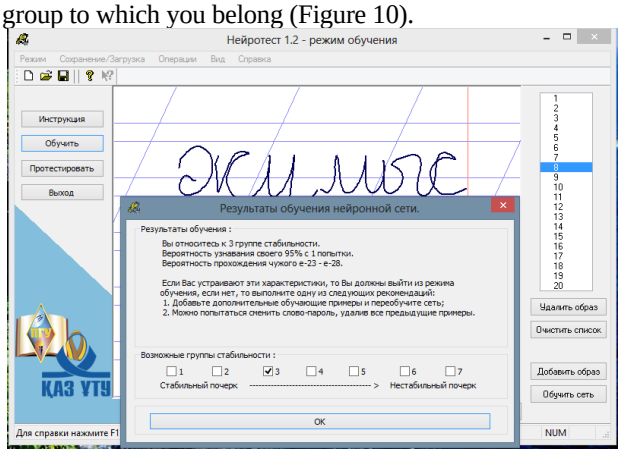


FIGURE 10 Completion of neural network training

If you do not like the group number and probabilistic characteristics, you can independently change the group number and retrain the neural network. It is important to remember that it is not recommended to change the group number by more than 1 to 2 positions, therefore, you can only switch to neighboring positions.

Perhaps the user was in the seventh group, for which the probabilistic characteristics of the system are too bad. You can change the training environment by deleting the most unlikely example. If there are difficulties with choosing the worst example, you can delete all the training examples and try to write them again, or add a few more training examples. After deleting the worst or after adding an additional example, click the "Train" button again. If you still can not get into the desired group, then the most unlikely example is deleted, or one more additional one is added and the network is trained again. If, after several attempts to re-train the network, you can not reach the desired strength group, you must try to change the word.

*Controlling the recognition of "Own"*. After training the neural network it is necessary to check the quality of recognition by the system of "Own". The training test is performed by reproducing a handwritten word and by pressing the "Check" button. In this case, a window appears (Fig. 11) showing the key generated by the neural network in binary and hexadecimal encodings (the unmatched bits of the source key and of the generated one are marked with asterisks). The total number of unmatched binary key symbols is also displayed.

These data can be used for independent statistical testing of the system.

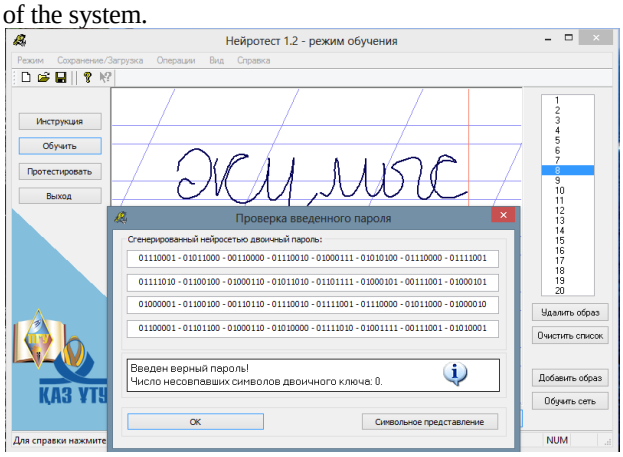


FIGURE 11 **Enter of an image** "Own"

If the system recognize the image "Own" badly, then it is necessary to add the unrecognized image to the base of the training examples and train the network again. After adding several new images, the network will be able to recognize the user inputting a handwriting image, but some characteristics of the system may deteriorate.

If the results of the training suit (GROUP 3 ... 4), then you need to save the data to disk. The folder number corresponds to the number of the biometric donor's personal identifier.

***Test mode.*** The testing of the system begins with the initialization of the testing mode (the button "Test" or "Mode >> Network Testing").

Before you start testing, you need to make sure that the neural network is trained. In the test mode, you can check the input of handwritten images on the trained network, and you can also add a "good" image to the base of the training examples.

The system is tested by reproducing the handwritten word-password and by pressing the button "Check the entered password". The traffic light in the upper right corner lights up. The red light of the traffic light corresponds to a very large discrepancy between the dynamics of the reproduction of the handwritten word-password and the newly entered verification word (Figure 12).

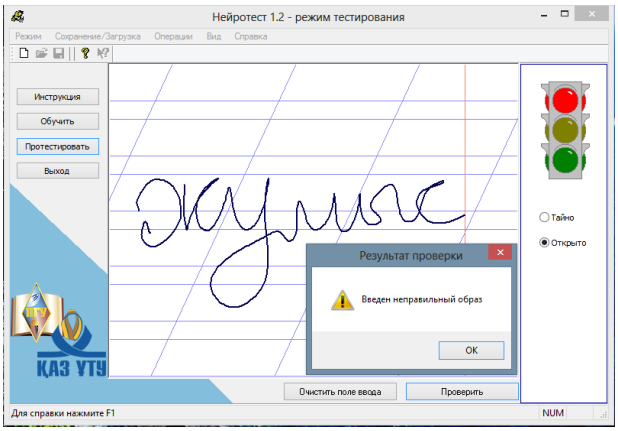


FIGURE 12 Example of entering an incorrect handwritten password

Frequent red light in the verification mode during the presentation of "Own" handwritten word indicates a poor recognition. The yellow light illuminates when several bits of the key do not match, the image is close to the reference one. The green light corresponds to the complete coincidence of the entered image with the reference one (the key is reproduced by the neural network without errors).

## 10 Conclusions

The two-layer network of neurons is universal in combination with the going next digital cryptographic authentication machine. This combination allows you to create any biometric information protection applications. An increase in the number of neurons in the layers of the network (in the first and in the second) is a very, very effective technique.

Nowadays, the best means of highly reliable biometric authentication provide the probability of errors of the second kind at a level of one billionth or less, that is, an attacker trying to overcome biometric protection must produce a billion different biometric images (for example, to reproduce with his hand a billion manuscript passwords). If the reproduction of one handwritten password takes 10 seconds, then the attacker will need 10 billion seconds, which is 321 years of continuous efforts. This is a lot more time for one person life. Alone, by the simply substituting of real biometric images it is impossible to overcome a highly reliable protection by the secret biometric image.

## References


[1] GOST R 52633.5-2011 2012 *Information protection. Information protection technology. Automatic training of neural network converters of biometry access code* Standartinform: Moskow

[2] Volchikhin V I, Ivanov A I, Funtikov V A 2005 *Fast algorithms of training neural network mechanisms of biometric-cryptographic information protection* Monograph Penza State University: Penza p. 273

[3] Akhmetov B S, Ivanov A I etc 2013 Connection between high-dimensional entropy and high-dimensional correlation with mathematical expectation of coefficients modules of pair correlation *Bulletin of KBTU* 240-4

[4] Akhmetov B S, Ivanov A I etc 2013 Estimation of the probability of the errors of the neural network converters biometry-code on the basis of small samples. High technology - the key to sustainable development *Mat. II Int. Sci. Conf.* **1** 234-4

[5] Akhmetov B S, Ivanov A I etc 2011Synchronization of procedures for neural network training of handwriting features by the points of change in the direction of movement of the pen *Proceedings of the II Int. Scientific-prac. conf. "Information and Innovation Technologies: Integration of Science, Education and Business"* **2** 118-6

[6] GOST R 52633.3-2011 2012 *Information protection. Information protection technology. Testing the resistance of means of highly reliable biometric protection to selection attacks* Standartinform: Moskow

[7] Akhmetov B S, Volchikhin V I etc 2013 Algorithms for testing of biometric neural network information protection mechanisms *Monograph* LEM: Almaty p.152

[8] Akhmetov B S, Zakharov O S etc 2013 A method for estimating the probabilities of errors in neural network converters biometry-code using very small test samples. *Bul. of KazNTU* **3**

[9] Akhmetov B S, Ivanov A I etc 2013 An entropy-correlation approach to the calculation of the probability of joint occurrence of a large number of dependent events *Bulletin of KBTU* **2**(25) 55-5

[10] Akhmetov B S, Ivanov A I etc 2013 Biometric authentication of citizens in open information spaces. *Proceedings of the 1 st international scientific and practical conference "Intellectual information and communication technologies - the means of implementing of the third industrial revolution in the light of the" Kazakhstan-2050 "strategy"* 458-2

[11] Malygin A Yu, Akhmetov B S etc. 2012 Accounting of the correlations influence on the results of testing of the biometry-code converters *Information and telecommunication technologies: education, science, practice: Col. pr. of Int . Scientific-practical. Conf.* 34-4

[12] Ball Rud etc 2007 *A guide to biometrics Technosphere* Moskow p. 368

[13] Larin P Z, Rever E I 2004 Circle around the finger? Deception of Biometric Access Systems Using Dactyloscopic Identification of Personality *Information Security* **3**

[14] Arakala A, Jeffers J, Horadam K J - 2007 Fuzzy Extractors for Minutiae-Based Fingerprint Authentication *Advances in Biometrics (LNCS 4642). Springer* 760-10

[15] Ratha N K, Chikkerur S 2007 *Generating cancelable fingerprint templates IEEE Trans. PAMI* **29**(4) 561-12

[16] ISO / IEC 19784-1: 2006 *BioAPI - Biometric Application Programming Interface - Part 1: BioAPI Specification* http: //www.bioapi.org/

[17] GOST R ISO / IEC 19784-1-2007 2007 *Automatic identification. Biometric Identification. Biometric program interface. - Part 1. Specification of biometric software interface* Standartinform: Moscow

[18] GOST R ISO / IEC 19784-2-2010 2011 *Automatic identification. Biometric Identification. Biometric program interface. - Part 2. The interface of the supplier of the biometric archive function* Standartinform: Moscow

[19] Kruglov V V, Long M I, Golunov R. Yu 2001 *Fuzzy logic and artificial neural networks* Fizmatlit:Moscow p. 221

[20] Rutkovskaya D, Pilinsky M, Rutkowski L 2004 Neural networks, genetic algorithms and fuzzy systems *Trans. from Polish by Rudinsky I.D.* Hot line - Telecom

[21] Simon Khaikin 2006 *Neural networks: Full course* Williams:Moscow p. 1104

[22] Wesserman F 1992 *Neurocomputer technology: theory and practice* Mir:Moscow p. 240

[23] Ivanov A I 2000 *Biometric identification of the personality according to the dynamics of subconscious movements* Monograph Publishing House of the PGU:Penza

[24] GOST R 52633.4-2012 2012 *Information security. Information protection technology. Interfaces of interaction with neuronet converters biometry-code* Standartinform: Moscow

[25] Minsky M, Peipert S 1971 *Perceptrons* Mir:Moscow

[26] Akhmetov B S, Alimseitova Zh K, Malygin A Yu, Yubuzova H I 2015

Formation of the biometric base of handwritten images in the Kazakh language for biometric authentication programs of the individual *Proceedings of the II International Scientific and Practical Conference "Information and Telecommunication Technologies: Education, Science, Practice"* **2** 32-4

## AUTHORS


**Malygin A**

**Current position, grades:** Professor of the military Department of the Penza state University
**University studies:** doctor of technical Sciences
**Scientific interest:** information security, neural networks, biometric systems
**Publications** (number or main)**:** More than 100 publications in the field of information security
**Experience:** teaches at Penza state University

**Nurgul Seilova**

**Current position, grades:** Head of department Information Security
**University studies:** candidate of technical Sciences
**Scientific interest:** network technologies, Information Security
**Publications** (number or main)**:** More than 30 publications
**Experience:** 15 years of teaching experience and 3 years in managerial positions

**Kylychbek Boskebeev**

**Current position, grades:** Professor of Kyrgyz State Technical University after I.Razzakov
**University studies:** Ph.D. (Engineering)
**Scientific interest:** The development of Intellectual information systems
**Publications** (number or main)**:** 7 Russian Scientific Citation Index
**Experience:** experience of service is 20 years

**Zhuldyz Alimseitova**

**Current position, grades:** lecturer of the Kazakh national research technical University named after K. I. Satpayev
**University studies:** Kazakh national technical University (1999)
**Scientific interest:** information security, neural networks, biometric systems, cryptography
**Publications** (number or main)**:** More than 30 publications in the field of information security
**Experience:** teaches at Kazakh national research technical University named after K. I. Satpayev discipline on information security and information protection