Generation of a biometrically activated digital signature based on hybrid neural network algorithms

P S Lozhnikov, A E Sulavko

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

Abstract. This paper suggests a model of a hybrid wide neural network based on perceptrons, quadratic form networks and multidimensional difference and hyperbolic Bayes functionals. It is experimentally proved that this model is highly efficient when used for biometric authentication and generation of a digital signature activated biometrically. The paper suggests methods of generating keys of a digital signature and personal authentication by handwritten patterns, a key stroke manner and facial parameters. Comparatively high rates of reliability for taken solutions were achieved that were estimated taking into account the variability of dynamic biometric patterns over time.

1. Introduction
In the 21st century a majority of documents is created using a special software: text editors, accounting systems, etc. Next, legally valid documents may be distributed in two ways: in analog (a paper document) or in digital (an electronic document). In the first case the document is printed and verified with a handwritten signature and a company’s stamp. In the second case the document stays in a digital form, and a digital signature ensures its authenticity and integrity. Nowadays we see the whole segments of document flow are migrated into the digital environment: public services, banking, e-procurement.

Consequently, a number of court proceedings that deal with unauthorized e-document creation increases. Users allow strangers to access secret keys of their digital signatures, give these keys to unauthorized people, allow a presence of malicious software. These violations mark the main security issue of the digital environment: in comparison with a handwritten signature a digital signature is detachable. If an intruder takes possession of a secret key of a non-owned digital signature and signed a document using it, this document will be legally valid according to the legislation. Today a majority of judicial acts is decided against the owners of such discredited digital signatures.

In an analog environment a paper document becomes legally valid with a handwritten signature, and the issue of its detachment does not exist. Another issue exists instead: an intruder’s simulation of a signature. In order to prove the fabrication in a court large time expenditure is required for a graphologic examination. In these circumstances, the owner of the simulated signature always has chances to prove a fact of forgery.

Thus, two issues connected with the usage of signatures for attesting documents in analog and digital environments are stated. The term “signature” has different natures in different environments: in an analog environment it is a dynamic biometric image fixed on a paper as a picture of a signature, in a digital environment it is a result of a cryptographic modification of a secret (private) key and a hash-function of a document. Therefore, a hybrid document flow management is suggested to move to that implies the mutual exclusion of issues stated above. A hybrid document may be stored in a digital form or as a paper, and contain a picture of a signature protected with a digital signature and private or...
open biometric patterns, that allow fast timely checking its integrity and authenticity irrespective of a data carrier type. A key feature of a hybrid document is a digital signature that is formed using a personal biometric pattern. In this case algorithms of translating biometric features into a secret key of a digital key are used.

In this paper we suggest to use a so called biometric handwritten signature (an autograph or a handwritten password) or a dynamic facial image and parameters of key stroking while typing a password phrase as biometric patterns.

Russia’s interest in the development of a market of biometric systems reflects in the structure of the National Technological Initiative (NTI). In a draft of the NTI there is a market called SafeNet with a segment “Applied systems for security” that is almost completely devoted to solving a task of biometrics: deployment the first ever national biometric authentication platform, a biometrically activated digital signature and so on.

2. Using “wide” hybrid neural network to generate a secret key of a digital signature

Currently scientists work on the development and research of the methods of building and training large neural networks with a small number of layers (wide neural networks) for biometric authentication [1, 2] and other [3]. Fast algorithms of training and testing wide neural networks appeared in Russia several years ago [4] and provided the basis of the series of the Russian State Standard GOST P 52633 standards that deal with the development of systems of highly-reliable biometric authentication. These algorithms are not unique and give rise to a class of potentially more efficient algorithms. This approach is being developed by Russian and Kazakhstani scientists mainly.

As opposed to deep artificial neural networks, wide networks have several benefits (in comparison with other approaches of image recognition, wide neural networks, in particular):
1. High performance speed that allows using these algorithms with low-end devices.
2. A possibility to use absolutely stable training procedures for a small number of instances (15-25) of an image to be recognized regardless the complexity of the artificial neural networks (they learn in layers with every neuron being trained independently from other network neurons).
3. Fast procedures of evaluating possibilities of image recognition errors (using comparatively small test sets on the analogy with the method described in the GOST P52633.3-2011 standard) may be applied.
4. Unsupervised learning.
5. High potential of increasing the reliability of decisions made due to different functionals used by neurons.

Wide neural networks may be configured to generate a fixed binary sequence when a pattern belonging to a specific class inputs and a random equally distributed bit sequence (white noise) when a pattern belonging to an unknown class inputs. Thus, network data may be used to generate encryption keys or a digital signature activated biometrically.

By modification of the functionality we mean that a basis of a neuron may form not only the functionals of weighted sum (1) that is a standard for a classic perceptron, but any other function of several arguments as well. Any proximity measure may be selected as such functional. Arguments of the functional are values of the features. Input data of a neuron is enriched and a calculated value of a functional enters an activation function. In a simple case the activation function is a threshold function. This case is considered in this paper. In theory, a neuron may have several functionals and several activation functions. Every activation function produces one neuron output. In this paper every neuron have one activation function and one output, consequently.

This class of neural network algorithms under consideration is flexible with regard to a feature space. Different segments of a wide network process features with a specific level of mutual correlative dependence. Every artificial neuron has inputs associated with values of features that are the most relevant to its functional.

The back propagation principle is not used for training wide neural networks. Every neuron is trained independent on others, its parameters are configured based on the law of distribution of the processed features. With regards to the biometric authentication the probability density function may be defined in accordance with a known law of distribution as a rule (normal in most cases, or close to it). A wide
neural network is trained layer by layer, that means every next layer is trained on the base of output values of neurons form the previous layer taking them as feature values. It may be said that every layer of a wide network consists of several subnets, the process of neuron configuration is specific for every subnet.

In the simplest case, only one layer of neurons can be configured. This is often enough for most image recognition tasks. The increase of the layers number requires justification. A reasonable explanation in this case may be the use of another principle of enriching the data entering the next layer of the network, to take into account additional information about the image.

There are functionals for processing conditionally independent and strongly dependent data. In this work we use a one-layer network of neurons based on classic functionals of perceptrons, quadratic forms and multidimensional Bayesian functionals (Fig.1). At the output of the network there is a neuron correcting erroneous bits of a binary code generated using the network. The neuron may be configured to correct a certain number of bits, changing the number it is possible to achieve the best proportion of probabilities (percentage) for False Rejection Rates (FRR) and False Acceptance Rates (FAR). This neuron is built using error correcting coding suggested in the work [5] and developed specially for biometrics. Intrinsically a task of recognition of a biometric pattern differs form a task of generating a digital signature key activated biometrically by the fact that in the first case Hamming measure acts as a neuron or other functional (Hamming weighted measure, for instance, the Bayesian formula [6] or others).

**Figure 1.** Work of the biometrics-code translator based on hybrid networks

Within such architecture of the neuron network an increase in a number of neurons does not lead to the complication of the learning process and to a growth in a size of a learning sampling. It leads to an almost linear increase of time required for learning and generating keys. A possibility of comparatively fast learning of wide neuron networks consisting of 20 samples of human biometric patterns is a significant feature and defines the viability of its application for biometric authentication and generating digital signatures with biometric activation.

When a biometrics-code translator is applied it is important to protect the biometric pattern and the key from being compromised. A network segment being a perceptron may be treated as rather protected from this threat [2]. It is impossible to extract the data of the learning sampling from the neuron weights and recreate a template of the biometric pattern in a timely manner (it is a computationally complex and poorly formalized task). However, quadratic forms and the Bayesian
functional deal with parameters of feature distribution laws directly, that leads to a necessity of storing parameters data. If a server keeping a table of neural network functionals is not trusted, there is a threat of restoring key fragments and a template of the user’s biometric pattern using the data from the table of neural network functionals. In this case a mechanism of a protected neural network container [1] may be applied to protect the biometric template at the stage of storage. This mechanism means the parameters of a neuron from a hybrid network are encrypted at the outputs of the perceptron’s neurons. If the perceptron’s neurons output the correct fragments of the key, the parameters of other neurons will be decrypted. Otherwise the network will generate noise as the decrypted values of the weight coefficients will not match the personal template.

Correcting codes from the work [5] allow secure storing error syndromes and do not allow restoring a key without presenting a biometric pattern that is rather close to the authentic one. In combination with the mechanism of a protected neural network container [1] these error correcting codes [5] solve the task of secure storage of the table of neural network functionals. However, the influence of the mechanism of protected neural network container on the probability of erroneous decisions made by the wide neural network is still open.

2.1. A subnet based on a perceptron

A perceptron, an artificial neuron of a subnet, is based on a functional (1) and a threshold activation function. Modules of weights of the neurons from the first layer are calculated using the formula (2). The Russian standard GOST P 52633.5-2011 and works [1, 2] describe the operations of network configuration in details.

\[
y = \sum_{j=1}^{N} \mu_j a_j,
\]

where \( m_j(a_j) \) are mathematical expectations of values of the \( j \)-th feature of an authentic pattern (“Own”), \( \sigma_j(a_j) \) is a root-mean-square deviation of values of the \( j \)-th feature of an pattern (“Own”), \( m_j(a_j) \) and \( \sigma_j(a_j) \) are analogical figures for an unknown pattern (“Non-Own”). If a neuron is configured to output “one” when the “Own” pattern inputs, then a sign of the weighting coefficient is selected following the rule: “+” if \( m_j(a_j) < m_j(a_j) \), otherwise “-“. If the neuron is configured to zero, the signs are inverted.

A single-layer perceptron with a threshold activation function is characterized by a decrease in efficiency if the neuron outputs are correlated. The stronger the relation between the features, the higher the correlation of the outputs. Researches show that the quality of perceptrons is accessible if the module of correlation coefficients between features is less that 0.7 (\( \phi < 0.7 \))

2.2. Subnet of quadratic forms

If the feature space is "plane" then the shortest path from the image to the center of the template can be found using the Euclidean measure. If the ranges of values of particular features vary significantly in scale, the space ceases to be "ideally plane", but it can be normalized by calculating distances with the help of the Pearson measure (3) [7]. Chi-module measure provides similar results while recognizing images (4). In the tasks of biometric authentication (identification) correlation between the features “bends” the space in the neighborhood of images templates. In order to take into account the heterogeneity of the curvature/bending of the feature space in the theory a quadratic form of (5), also called the Mahalonobis measure, can be used.

\[
\Pi = \sqrt{\sum_{j=1}^{N} \frac{(m_j - a_j)^2}{\sigma_j^2}},
\]

\[
\chi = \sum_{j=1}^{N} \frac{|m_j - a_j|}{\sigma_j},
\]
\[ y = (m - \bar{a})^T \cdot [R]^{-1} \cdot (m - \bar{a}), \]  

(5)

where \( a_j \) is the value of the \( j \)-th feature, \( N \) is the number of features processed by the functional (the dimension of the functional), \( m \) and \( \sigma \) are the mathematical expectation and the standard deviation of the \( j \)-th feature values calculated from the training sample data, \( \bar{a} \) is the vector of features values in the normalized coordinate system, \([R]\) is the matrix of pair correlation coefficients between the features. The use of this quadratic form is complicated by the fact that it is required to perform the inversion of the correlation matrix \([R]\), which is not possible in practice. The point is that this operation is ill-conditioned and performed with significant errors \([8]\). An attempt of such treatment leads to a problem called the "dimensional curse" \([9]\), at least in the problems of dynamic biometric images recognition on training samples in dozens of examples.

The work \([10]\) suggests an adaptable algorithm of learning a perceptron based on the GOST methodology R 52633.5-2011 to configure a quadratic form (5). However, this algorithm does not solve the task of processing strongly dependent features.

For these reasons, proximity measures, which are quadratic forms, are focused on processing only independent and weakly dependent data.

2.3. Subnet of Bayesian functional

The results of recent studies indicate that there are functionals (proximity measures) that can take fewer wrong decisions if the correlation between the features is high. The first group of such proximity measures was called multidimensional Bayesian functionals. They evaluate not only the proximity of the image to the standard, but also the dependence of a certain feature of the image on several other features. There are multidimensional correlation \([11]\), difference \((6) [8]\), Bayesian hyperbolic functionals \((7) \) and \((8) [12])\).

\[ d_t = \sum_{j=1}^{N} \left| \frac{m_j - a_j}{\sigma_j} - \frac{m_j - a_j}{\sigma_j} \right|, j \neq t \]  

(6)

\[ g_{t-} = \sum_{j=1}^{N} \left( \frac{(m_j - a_j)^2}{\sigma_j^2} - \frac{(m_j - a_j)^2}{\sigma_j^2} \right), j \neq t \]  

(7)

\[ g_{t+} = \sum_{j=1}^{N} \left( \frac{(m_j - a_j)^2}{\sigma_j^2} + \frac{(m_j - a_j)^2}{\sigma_j^2} \right), j \neq t \]  

(8)

The greater value of \( N \) and higher the coefficient of equal correlation of features, the more effectively the Bayesian functional works. Equal correlation in this case is meant that the coefficient of pair correlation between the \( t \)-th and \( j \)-th features is within certain limits (the interval of the \( \pm 0.1 \) order is admissible one) \([1]\). The work \([1]\) suggested a methodology of building a network of multidimensional Bayesian functionals possessing a moderate redundancy and high efficiency.

3. Dynamic biometric patterns

We suggests 2 variants of using a technology of generating secret keys of a digital signature based on biometric images:

1. The first variant presupposes a usage of a handwritten signature or a handwritten password as a biometric pattern. In this case the generation of a digital signature activated biometrically will not significantly influence current business-processes in an organization as a signature is a traditional method of verifying the authenticity of paper documents.

2. The second suggested method of generating a digital signature is the usage of data obtained from standard equipment like a keyboard and a web-camera to create a secret key. In this case facial parameters and a key stroke manner are used. We suggest an “advanced” technology of protecting electronic samples of documents based on this method that is as follows. Having generated a hybrid documents, its owner can restrict an access of other people to its selected parts,
and restrict certain actions (printing, editing, etc.). At this time the content of any of these parts of the document will be encrypted using an open key of a person who is granted an access. If more than one person have access to any part of the document, several copies of the document are created and each one is encrypted using the corresponding open key. While a user is working with an electronic hybrid document, a real-time continuous monitoring of facial parameters and a key stroke manner is performed. These parameters are used for generating a private key used further for decrypting the corresponding parts of the document (Fig. 2). While fixing changes of personal biometric characteristics recording in a process of work, the document temporarily “changes” or “hides” its content completely or totally, block some functions of editing it. A user cannot “bypass” the program as all confidential information is encrypted by corresponding cryptographic keys. Public information is not encrypted. Such technology of an active protection is called a technology of “an enlivened document”. In fact, documents will contain information about who created and edited it and what was the psychophysiological state of this person.

![Figure 2](image)

**Figure 2.** A picture of a process of accessing a fragment of an electronic hybrid document.

To increase the reliability of the process of key generation, a multi-factor method that combines both suggested variants is used.

### 3.1. Parameters of a handwritten password or a signature

In a computer representation a signature can consist of functions of a pen position on a tablet $x(t)$, $y(t)$ and pen pressure on a tablet $p(t)$, where $t$ is a time in a discrete form. Every handwritten pattern passes through spectral and correlative analyses to compute a fixed number of informative features. This vector includes both values characterizing the outer appearance (distances between certain points of a signature image, parameters of its slope, width, length) and the dynamics of its reproduction (amplitudes of harmonics for functions $x(t)$, $y(t)$, $p(t)$, that correspond a frequency of vibration of a signer’s hand (approximately 1-10 Hz), coefficients of correlation between these and derived functions, coefficients of the Daubechies D6 wavelet transform). The process of computing these features in detail is described in the work [13].

### 3.2. Parameters of a face and a key stroke manner

Several characteristics from the work [14] were used as facial parameters, in particular:
- Distances between eyes, a center of a face, a tip of a nose (in pixels, values are normalized by a diagonal of a face in a frame).
- Area of eyes, a nose, a mouth (values are normalized by a face area).
- Coefficients of correlation of intensity and color parts of pixels (according to RGB) between all pairs of the following area of a face: eyes, a nose, a mouth. These features describe facial asymmetry.
- Parameters describing a color of eyes and skin.
To isolate the face (skin), eyes, nose, mouth and the subsequent analysis of these areas, the Viola-Jones method was used. This detector has a low probability of false detection of the face and well recognizes facial features at an angle (up to 30 degrees) [15]. To determine the color components of the eye, the area of the iris and the pupil are initially separated using the algorithm for detecting circles on the basis of the Hough transformation.

Time of key retention and pauses between key strokes were used as features of a key stroke dynamics [16].

4. Reliability scoring of generating keys of a digital signature based on hybrid wide networks

An experiment to estimate the reliability of generating keys by a hybrid neural network was carried out (Fig. 1). The experiment involved 90 people, each of them entered the biometrical data during one month. The first day the person entered 40-45 samples of a certain handwritten pattern, and tried to type a password phrase with a keyboard (“система защиты должна постоянно совершенствоваться”, that means “the protection system must be constantly improving”). Next, once a week a person repeated entering biometric data (20-25 attempts). After each procedure of typing a phrase with a keyboard a test person looked in the direction of a web-camera to take a photo that fixed facial parameters. To collect data we used Wacom tablet, a standard mechanical keyboard and a web-camera with a resolution 640x480.

As a result every person gave 120-145 biometric images of each type (a face, a key stroke manner, a handwritten pattern). A total number of samples of each type exceeds 10000.

For each person three hybrid neural networks were formed to generate a personal key based on the following biometric patterns:
- Handwritten passwords/signatures (Fig. 3);
- Patterns of a face and a key stroke manner (Fig. 4);
- Patterns of a face, a key stroke manner and handwritten passwords/signatures (Fig. 5).

The authentication (or generation of cryptographic keys) by facial data only or a key stroke manner is not secure. A face is an open biometric pattern that may be forged (using a photo or other “replicas”). An open pattern may be used for identification purposes only or as additional information for personal verification. A key stroke manner recording with a standard keyboard is too unstable (more unstable than handwriting dynamics as multiple researches show). The reliability of biometric authentication via a key stroke manner is comparatively slow. However, this pattern may be secret therefore it may be compensated with a facial image.

There is no single method of configuring hybrid wide neural network in any specific case. However, to define limit conditions the following arguments may be used.

First of all, a wide network of different functionals must provide a large range of input information processing methods. As long as neurons make different mistakes, their number may be increased adding new computing elements into the network structure. Solutions made by these new elements do not repeat the solutions of the existing neurons. An estimation of the correlation between the work of all elements of a neural network is unreasonable as it is an extremely resource-intensive process that is impossible to complete using a small learning sampling. For this reason it is required to select a number of different neurons and their synapses on a basis of a principle of work of any used functional, much relying on an intuitive approach and empirics.

It is self-explanatory that a new neuron must be efficient, that means it makes errors as rare as possible. To provide non “zero” contribution of a new neuron, it is required to build it based on another functional or that it processes other (unique) combinations of features. In this paper we take three types of functionals and three subnets consisting of neurons based on corresponding functionals (Fig. 1). A number of neurons of every subnet may be controlled independently. Gradually increasing a number of neurons in the network we can come to a situation when they all will process a significantly intersecting set of features and therefore a larger number of neurons will make similar decisions. It is necessary to find a moment when a further increase in a number of neurons of a certain type does not influence a decrease in error probability of pattern recognition.
The work [1] state that to process the considered biometric features with $\phi > 0.5$ it is necessary to use difference (6) and two type of hyperbolic (7) and (8) Bayes functionals (using features with $\phi < 0.5$ does not lead to a significant gain in recognition reliability). Researches showed [1, 8, 12] that the networks based on above mentioned Bayes functionals can be configured in the same way and produce the similar results on average, but at the same time their particular solutions differ. Thus, functional (6), (7) and (8) complement each other. A procedure of defining a configuration of Bayes-Hamming network is suggested in [1]. This procedure may be applied one-time to build three Bayes-Hamming subnets at once (three segments inside one network) with the same number of neurons and the same synapses that differ only in a functional in a basis of a neuron. This approach was used in this experiment.

To process features with $\phi < 0.7$ a single-layer perceptron configured according to the GOST R 52633.5-2011 was used. To define a minimal required number of neurons it is possible to rely on a principle of minimal complexity of a neural network [17], the maximum limits of the network size may be found based on results of the previous experiment on estimation of the reliability of solutions made by perceptrons while recognizing signature, face and key stroke patterns [1, 10]. A number of neurons and inputs was selected empirically taking into account these data.

To process features with $\phi < 0.5$ a subnet of quadratic forms consisting of 3 segments based on different functionals was used: Pearson measure (3), a Chi-module (4) and Mahalonobis (5). A number of neurons and their inputs is selected empirically but focusing on the results of the works [1, 10]. The usage of a wider range of features than when $\phi < 0.3$ is explained by the fact that significant errors in calculating correlative coefficients are met when the sampling is small [8].

Thus, this simulation experiment consisted of several series of tests, in each series parameters of neural networks being generated change in a certain range. Each network was trained using 20 examples of corresponding biometric patterns of a certain person (“Own”) and 64 examples of other persons (“Non-Own”). The process of learning was based on biometric samples obtained in the first day of the experiment. Other patterns were used to evaluate the reliability of person’s recognition (more than 8000 of every type). Error probabilities were evaluated for two cases:

1. Immediately after learning. To test the neural networks, biometric patterns obtained in the first day of the experiment were used (an ideal variant).

2. During a month after learning. To test neural networks biometric patterns were used obtained during the next period of time of the experiment. In this case an aspect of variability of a personal biometric pattern in a course of time is taken into account. This aspect was not considered in previous experiments [1, 7, 10, 13]. This test scenario meets real conditions.

The results of the experiment is shown in Figures 3-5.

**Figure 3.** Estimation of errors of generating keys from signatures (depending on a number of
corrected bits): with regard to (on the right) and without regard to variability of features over time (on the left).

While testing hybrid networks every person was considered “Non-Own” in relation to other persons. Thus, FRR and FAR were computed based on data from different experiments, in the first case keys were generated from the “Own” patterns, in the second case they were generated from the “Non-Own” patterns correspondingly.

Figure 4. Estimations of errors of generating keys by a two-factor system based on face and key stroke patterns (depending on a number of corrected bits): with regard to (on the right) and without regard to the variability of features over time (on the left).

Figure 5. Estimations of errors of generating keys by a three-factor system based on signatures, a face and a key stroke manner (depending on a number of corrected bits): with regard to (on the right) and without regard to the variability of features over time (on the left).

5. Discussion of results and its comparison with previous ones
As shown in Figures 3-5 the network configurations used allow generating a key with a length up to 2048 bits (each neuron generates one bit) in all cases. This is not a limiting ability of a wide network, however according to the calculations a further increase in a number of neurons does not lead to a
decrease in error probabilities, at least if functionals described in this work are used. For comparison, we give graphs of signatures verification errors by the Bayes-Hamming networks (Figure 6). They show that the use of a network of one type of functional gives more errors and a slightly different picture of the characteristic curves, which indicates that the measures (6), (7) and (8) are not completely correlated.

Figure 6. The results of verification of signatures by the Bayes-Hamming networks with regard to the variability of features over time.

If a biometric system is tested immediately after its learning (or using testing samplings) the hybrid wide networks divide users’ patterns almost error-free. An equal error rate for such ideal case is:

- EER=0.5% when a user is recognized/a key is generated using a handwritten pattern;
- EER=0.02% when a user is recognized/a key is generated using a key stroke manner and a face;
- EER<0.02% when a user is recognized/a key is generated using a handwritten pattern, a face and a keystroke manner.

These results significantly exceed the previous ones [1, 7, 10, 13] that proves high efficiency of wide hybrid neural networks.

As you see, due to the variability of patterns of key strokes, signatures and photography conditions in an extended period, the reliability of personal recognition decreases. Researches show that time variations of dynamic biometric features are spontaneous and cannot be forecasted. However even considering this, the system may be configured to the following reliability indicators:

- When a person is recognized/a key is generated using a handwritten pattern: FRR=31.5% in case of FAR<0.01% (EER=5.1%, Fig. 3);
- When a person is recognized/a key is generated using a key stroke manner and a face: FRR=9.2% in case of FAR<0.01% (EER=2.28%, Fig. 4);
- When a person is recognized/a key is generated using a handwritten pattern, a face and a keystroke manner: FRR=3.5% in case of FAR<0.01% (EER=1.15%, Fig. 5).

These estimations are generalized for all users. In practice a trigger threshold of a protection system must be configured for every person individually. A basic threshold value (Fig. 3-5) must be corrected on a basis of a neuron response to patterns of a learning sampling, that enters a hybrid network immediately after learning. The custom configuration allows decreasing the obtained estimations by 10-20%.

6. Conclusion
This work suggests a model of a wide hybrid neural network based on perceptrons, quadratic form networks and multidimensional difference and hyperbolic Bayes functionals. It was experimentally proved that this model is highly efficient for biometric authentication and generating a digital signature activated biometrically. The work suggests methods of generating keys of a digital signature, and authenticating persons by handwritten patterns, a key stroke manner and facial parameters. While attempting to generate a digital signature activated biometrically based on a handwritten pattern immediately after system learning, the erroneous solution rates were about 0.5%, and for a multi-factor system EER≤0.02%. Taking into account changes in dynamic biometric features over time (a time period of about a month is considered) the erroneous solution rates increase many times. However even taking into account the variability of patterns over time, with fine-tuning of the biometric system according to the peculiarities of every user’s patterns the reliability rates were:
- When a person is recognized/a key is generated using handwritten patterns: FRR=24.5% in case of FAR<0.01% (EER=3.9%, Fig. 3);
- When a person is recognized/a key is generated using a key stroke manner and a face: FRR=8.3% in case of FAR<0.01% (EER=2%, Fig. 4);
- When a person is recognized/a key is generated using handwritten patterns, a face and a keystroke manner: FRR=3% in case of FAR<0.01% (EER=0.9%, Fig. 5).

These indicators are enough for authentication systems.

The result of this work may be used in practice. However it is recommended to start learning the recognition system over time again, in this case erroneous solution probabilities will be lower.

Researches show that for different persons the recommended period of time differs, and it ranges from two weeks to several months.

7. References
[1] Ivanov A I, Lozhnikov P S, Sulavko A E 2017 Evaluation of signature verification reliability based on artificial neural networks, Bayesian multivariate functional and quadratic forms Computer Optics vol 5 p 765-774
[2] Malygin A, Seilova N, Boskebeev K, Alimseitova Zh 2017 Application of artificial neural networks for handwritten biometric images recognition COMPUTER MODELLING & NEW TECHNOLOGIES vol 21(1) p 31-38
[3] Ivanov A I, Kulagin V P, Kunznetsov Y M, Chulkova G M, Ivannikov A D 2016 High-dimensional neural-network artificial intelligence capable of quick learning to recognize a new smell, and gradually expanding the database Digital Information Processing, Data Mining, and Wireless Communications (DIPDMWC), Third International Conference (Moscow)
[4] Volchikhin V.I., Ivanov A.I., Funtikov V.A. 2005 Fast learning algorithms of neural network mechanisms of biometric-cryptographic information protection (Penza: Penza State University Press) 273 p.
[5] Bezev A V, Ivanov A I, Funtikova U V 2014 Optimization of the structure self-correcting biocode, storing syndromes error as fragments hash-functions UrFR Newsletter. Information Security vol 3(13) p 4–13
[6] Epifantsev B N, Lozhnikov P S, Sulavko A E, Zhumazhanova S S 2016 Identification Potential of Online Handwritten Signature Verification Optoelectronics, Instrumentation and Data Processing vol 3(52) p 238-244
[7] Sulavko A E, Fedotov A A, Eremenko A V 2017 Users' identification through keystroke dynamics based on vibration parameters and keyboard pressure XI International IEEE Scientific and Technical Conference "Dynamics of Systems, Mechanisms and Machines (Dynamics) (Omsk: Omsk State Technical University) p 1-7
[8] Ivanov A I, Lozhnikov P S, Serikova Yu I 2016 Reducing the Size of a Sample Sufficient for Learning Due to the Symmetrization of Correlation Relationships Between Biometric Data Cybernetics and Systems Analysis vol. 52(3) p 379–385
[9] Akhmetov B, Doszhanova A, Ivanov A, Karbayev T, Malygin A 2013 Biometric Technology in Securing the Internet Using Large Neural Network Technology World Academy of Science,
Engineering and Technology (Singapore)

[10] Lozhnikov P S and Sulavko A E 2017 Usage of quadratic form networks for users’ recognition by dynamic biometric images XI International IEEE Scientific and Technical Conference "Dynamics of Systems, Mechanisms and Machines" (Dynamics) (Omsk: Omsk State Technical University) p 1-6

[11] Ivanov A I, Kachajkin E I, Lozhnikov P S 2016 A Complete Statistical Model of a Handwritten Signature as an Object of Biometric Identification Control and Communications (SIBCON) (Moscow) p 1–5

[12] Ivanov A I, Lozhnikov P S, Vyatchanian S E Comparable Estimation of Network Power for Chisquared Pearson Functional Networks and Bayes Hyperbolic Functional Networks while Processing Biometric Data Control and Communications (SIBCON) (Astan) p 1-3

[13] Lozhnikov P S, Sulavko A E, Eremenko A V, Volkov D A 2016 Methods of Generating Key Sequences based on Parameters of Handwritten Passwords and Signatures Information vol 7(4)

[14] Vasilyev V I, Sulavko A E, Eremenko A V, Zhumazhanova S S 2016 Identification potential capacity of typical hardware for the purpose of hidden recognition of computer network users X International IEEE Scientific and Technical Conference "Dynamics of Systems, Mechanisms and Machines" (Dynamics) (Omsk: Omsk State Technical University) p 1-5

[15] Cho H and Hwang SY J 2015 High-performance on-road vehicle detection with non-biased cascade classifier by weight-balanced training EURASIP Journal on Image and Video Processing

[16] Lozhnikov P S, Sulavko A E, Eremenko A V, Buraya E V 2016 Methods of generating key sequences based on keystroke dynamics X International IEEE Scientific and Technical Conference "Dynamics of Systems, Mechanisms and Machines" (Dynamics) (Omsk: Omsk State Technical University) p 1-5

[17] Vasilyev Vladimir 2016 Structural design of shallow neural networks on the basis of minimal complexity principle Control and Automation (MED) 24th Mediterranean Conference.

Acknowledgments

The research was supported by the Russian Scientific Foundation (project №17-71-10094).