World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:7, No:7, 2013

Biometric Technology in Securing the Internet Using Large Neural Network Technology

B. Akhmetov, A. Doszhanova, A. Ivanov, T. Kartbayev, and A. Malygin

***Abstract*—**The article examines the methods of protection of citizens' personal data on the Internet using biometric identity authentication technology. It`s celebrated their potential danger due to the threat of loss of base biometric templates. To eliminate the threat of compromised biometric templates is proposed to use neural networks large and extra-large sizes, which will on the one hand securely (Highly reliable) to authenticate a person by his biometrics, and on the other hand make biometrics a person is not available for observation and understanding. This article also describes in detail the transformation of personal biometric data access code. It`s formed the requirements for biometrics converter code for his work with the images of "Insider," "Stranger", all the "Strangers". It`s analyzed the effect of the dimension of neural networks on the quality of converters mystery of biometrics in access code.

***Keywords*—**Biometric security technologies, Conversion of personal biometric data access code, Electronic signature, Large neural networks, quality of converters "Biometrics - the code", the E-government.

I. Introduction

CREATION of E-government requires the construction of a distributed state-wide system of public administration that implements the solution of a complete range of tasks associated with managing documents and processes of their processing. The introduction of E-government provides citizens and businesses access to high quality services and government agencies at the same time reduces the cost of those services [1].

Formation of E-government requires a complex solution of the following tasks:

- Full automation of government based on modern information and communication technologies,
- The reform of the institutions of government,
- Provision of government web presence,
- A high level of telecommunications infrastructure,
- Increase the level of readiness of the population to use information services.

Bahytzhan Akhmetov and Aliya Doszhanova are with the Institute of Information and Telecommunication Technologies, Kazakh National Technical University, Almaty, 050013, Kazakhstan (phone: 777-552-8911; e-mail: b_akhmetov@ntu.kz).

Timur Kartbayev is with the Institute of Information and Telecommunication Technologies, Kazakh National Technical University, Almaty, 050013, Kazakhstan (corresponding author to provide phone: 701-547-4248; e-mail: kartbaev_t@mail.ru or kartbaev_t@kazntu.kz).

Malygin Aleksandr and Aleksandr Ivanov are with the Penza Research Electrical Engineering Institute, Penza, 440000, Russia (e-mail: mal@stup.ac.ru).

In turn, the government's web presence (as classified by the European Commission) is characterized by sequential passage of the five stages [2]:

Information – means 20% bonus web presence and involves the creation of regularly updated government websites posting on them, the main government information (regulations, directives, decisions, etc.) links to the ministries and government departments (education, health , finance, etc.);

One way interaction – implies a 40% bonus web presence and is the organization of passive interaction between clients and the government. It implies, for example, providing access to an electronic form to the various form of documents required for citizens and businesses to interact with government. The required form can be printed, but will have to send it the traditional way, but not via the Internet. Or, for example, search for jobs in government organizations based on user-defined criteria;

Two way interactions – means 60% bonus web presence and is implemented through an interactive two-way interaction. At this stage, online services become interactive and an opportunity to request information on various presentations and discussions, to contact government officials via E-mail, participate in online discussions or post comments on message boards, etc.;

Transaction – assumes 80% bonus web presence and is characterized by transactional interaction, making possible the provision of services feasible in online mode at all stages. An example is the filing of applications in electronic form for the licenses for professional activity, filing tax returns, applications for exchange of documents, etc. At this stage, one of the major challenges is to ensure safety;

Targetisation – means 100% of web presence and is characterized by the fact that the government not only provides citizens and businesses and services, including but involves citizens in decision-making and two-side dialogue based on interactive services.

In general, "E-government" is defined as a specialized complex system of interaction of the executive authorities with citizens, civil society and business organizations through the Internet. The two distinct levels of interaction [3]:

C2B (customer-to-business) – between citizens and private companies;

B2B (business-to-business) – between private companies;

G2C (government-to-citizen) – between public services (at the level of governments, departments and regions) and citizens;

G2B (government-to-business) – between the state and

private companies;

G2G (government-to-government) – among governments.

The concept of "E-government", the whole system of executive power, functioning as a single service organization dedicated to providing services to the public. The activities of «E-government» should be open enough information transparent and accessible to the citizens. Particular attention is paid to the principle of feedback; speed and quality of service delivery through the use of centralized systems are widely internet. All this is intended to improve the quality of the provision of services to the population and the functioning of the government itself [4].

Practical implementation of e-government in Russia and Kazakhstan goes along the same lines, and its structure is shown schematically in Fig. 1.

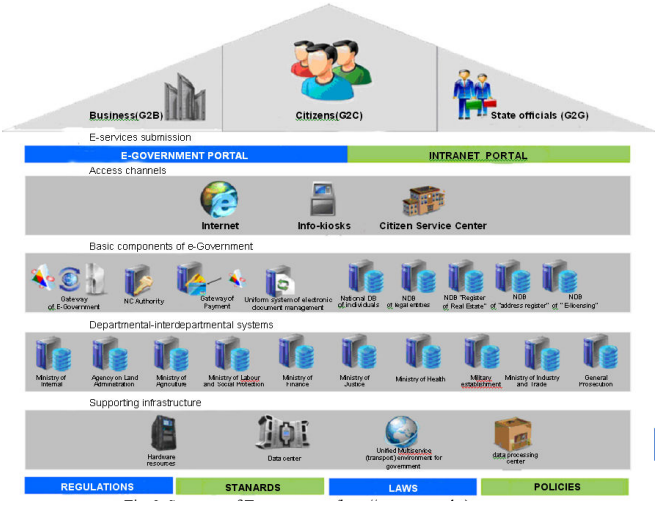

Fig. 1 The structure of the electronic government (http://www.e.gov.kz)

In this E-government needs a reliable electronic authentication of citizens, and citizens are in need of reliable protection of their personal information used (created) E-government and allocated over the Internet to a citizen.

II. Electronic Digital Signature

Authorization and integrity of electronic documents created electronically by the government to the citizen can be ensured through the formation of an electronic digital signature (EDS) E-government under the document. Fundamentally important is the fact that the storage of keys forming a digital signature of E-government and businesses are well exhaust problems [5]-[7].

Today the technology of digital signatures to electronic document is one of the basic technologies of the information society. The classical scheme of digital signature is shown in Fig. 2.

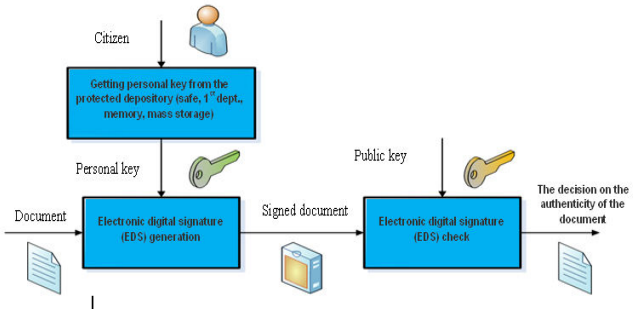

Fig. 2 The classic pattern of use of digital signature

A typical user may not provide reliable storage of his personal key in his computer in his safe for its recording medium and its use only in a trusted computing environment. All of it is dangerous to provoke an attack on a citizen. In this regard, the government must provide the citizen with the means of safe storage of private keys and digital signature algorithm trusted computing environment for their application in the face of certification authorities [8], [9].

However, the existing certification authorities do not increase the information security of the average user, but rather reduce it. They provide services only to support public-key certificates of citizens, but citizens do not want to officially register your public key to verify the signature of legally significant. The problem is that along with the registration of a public key citizen inevitably gets an extra risk of compromise of its private key digital signature algorithm. Anyone who has stolen the private key of person is able to generate on its behalf EDS any electronic document.

III. Biometric Technology

One of the most appropriate ways to solve this problem is to link the code to the user's biometrics. This technology is currently being actively developed [10]-[13]. Its main task was to create devices and programs that could very likely recognize its owner, and with even higher probability to recognize intruders trying to masquerade as legitimate users. Common Market for biometric systems is projected International Data Corp steadily increased by about 40% per year [http://www.biometricgroup.com/].

The basic postulate of such funds is to use static person's biometric data. Their peculiarity is that they are given to person by birth and cannot be changed [14]. These include the identification of: a drawing iris pattern leather fingertips (on the pattern of papillary lines), the parameters of two-and three-dimensional geometry of the hand, two-and three-dimensional geometry of the human face, drawing blood vessels: the fundus of the eyeball, the back side of the hand, the geometry of the ears, electrocardiogram of the heart, body odor, DNA analysis, ion spectrum traces of sweat.

A potentially more powerful are the so-called behavioral biometric images of the individual, which on one hand are sensitive to the current psychophysical state of person, and on the other hand can be changed by the will of man. These so-

called dynamic biometric characteristics of the person, such as a signature, handwriting keyboard, voice. In its pure form, they have limited use because of their low resistance to attacks of selection; however, they are well suited remote user identification.

In both cases, on the basis of these data formed the biometric template, which is signed by electronic signature and shall be published (stored) in the system of biometric identification certifying centers [15]. Encrypt the biometric template is impossible, as it should be used identification system. This approach to the problem is potentially dangerous because of the threat of loss of the base of biometric templates, but it is quite acceptable for police applications, passport and visa control and corporate applications of biometric access control.

Due to the fact that the biometric identification center (BIC) is a commercial organization providing a trusted computing environment and public key certificates, the user should not trust him keeping his secret biometrics. Exclusion of possible abuse by the staff of biometric identification center provided assistance of external guarantors of anonymity (confidentiality, anonymity). Guarantor of the confidentiality of their biometric and other personal data, the user chooses by himself [16].

The guarantor can be any person who has agreed to perform this function and has a public key certificate.

If you want to preserve the confidentiality of personal data person, then they are encrypted with a public key and a private key guarantor of the user. Further, this cipher text is stored in the biometric certification center in conjunction with a public key donor biometrics. Staff biometric identification center cannot decrypt personal data because it does not have the private key guarantor of anonymity and the client. If you want to disavow the confidentiality of biometric and personal data of a person against his will, the law enforcement agencies must apply to biometric identification center to get the cipher text biometrics and personal data. Further, they must apply to the guarantor of confidentiality that using his private key can decrypt personal data. Privacy Guarantor is not able to abuse their status, because they do not have cipher text personal data. He gets a cipher text only if it is accessed by law enforcement or biometric identification center.

Thus, biometric certification centers have a much more viable business model. They do not try to sell additional risks, and provide users with additional electronic identity card, his trusted computing environment (e.g., in the form of remote terminals remote biometric authentication). Relying on the services of biometric identification centers, end users are able to ensure their anonymity in electronic voting or impersonality of doing their histories. Due to the growing volumes of biometric identity centers are able to lower their prices to micro and completely remove the threat of compromising the secret of biometric images citizen in conjunction with its private key. E-government and e-business in the face biometric identification centers actually has an intermediary specializing in the provision of secure cryptographic and biometric services to the citizens of the information society. Micropayments for the provision of these services arise from the fact that the cost of maintaining a workable trusted computing environment and a highly reliable biometric passed on to all users of biometric identification centers.

If you are using *Word,* use either the Microsoft Equation Editor or the *MathType* add-on (http://www.mathtype.com) for equations in your paper (Insert | Object | Create New | Microsoft Equation *or* MathType Equation). “Float over text” should *not* be selected.

IV. Biometric Technology Using Large Neural Networks

The main problem is the threat of biometrics simple "mark of the beast" [15]. Unfortunately, the biometric template pattern your fingerprint or iris your get not only your card biometric data, but also the corresponding central database. This may be a corporate biometric database which may accumulate about 1000 times more sensitive biometric information, people working in the corporation and interacting actively with the corporation side. The largest volume of sensitive biometric information can be stored in the state of biometric databases. Shoot people of their biometrics and place it in a large database is extremely dangerous.

To eliminate the threat of compromised biometric templates to create new biometric technology, which on one hand can reliably (Highly reliable) to authenticate a person by his biometrics, and on the other hand make biometrics a person is not available for observation and understanding. One of the ways to reach the goal of partial confidentiality and anonymity of biometric data is to use neural networks large and extra-large size [16]-[18].

A positive aspect of neural network solutions is that disappeared biometric template has been stored previously in explicit form. Instead, it appears neural container user's biometric data. In fact, this table is a neural network connection of neurons and synaptic connections table (weights) trained to recognize "their" neural network (Fig. 3). Means carried by the block diagram of Fig. 3 is highly reliable because the application of neural network based on biometrics code converter (block 3 and block 4).

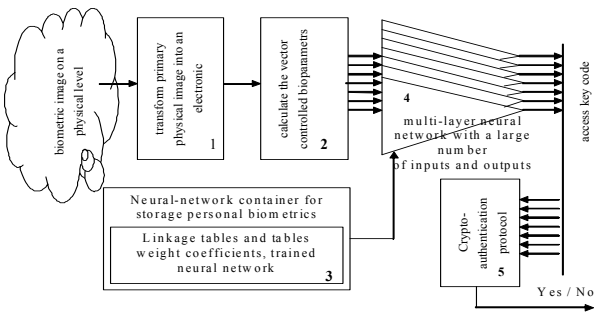

Fig. 3 A typical block diagram of the organization means a highly reliable biometric authentication

Mystery of biometrics using block diagrams of Fig. 3 provided by the fact that the tables relations trained neural network, and the tables of weights to calculate the donor biometrics (find a person based on biometric images) is technically very difficult. Privacy biometrics, placed in the container, the neural network is provided at a level comparable to the confidentiality provided by encryption.

The key point is that the neural transmitter biometrics code according to GOST (Government standard) R 52633.0 must be trained in advance to convert secret biometric image of "Insider" in the user's private key. Any other biometric image of the "Stranger" Biometrics neural transmitter code must be converted to a random key. If the private key and biometric image of "Insider" unknown to outsiders, the attacker can pick it up after 1 billion attempts (resistance to attacks selecting 109) degree. On the selection of the attacker must go 3 × 109 seconds, or about 300 years, if the attacker is allowed to present one of the random biometric images in three-second intervals.

If a biometric image of a person is compromised, then its residual resistance to attack selecting drops to 103 attempts (selection time is reduced to 1 hour). Ensuring the secrecy of biometrics is much more effective than most biometrics.

It should be emphasized that the key length of 256 bits - it's a very, very serious protection that is used, for example, to generate a digital signature of the citizen to the Russian national standard and in accordance with the algorithms [16], [19]. If the English were collected from the Russians would not their fingerprints in an explicit form, and neural networks containers drawings Russian finger prints, no further claims against them could not be. With such a container, you can always make sure that before you master it. Moreover, these fingerprints are not stored anywhere and nowhere to shine. Figures fingerprints are "dissolved" in the parameters of neural networks. Place a man and lay out in the open access his fingerprints, no one can - in this case, human rights truly respected.

The use of highly reliable biometrics, neural networks store the user's key signature is proposed to introduce a portable flash media and national biometric identification centers digital signature algorithm. National Buts not only provide traditional services for certification of public keys of individuals and entities, but also perform very different services on a local and remote biometric authentication personality. Man enough to appear in person once a certification authority for its biometric registration, then one can prove the authenticity of biometric e-government, e-business, other citizens using the services of an intermediary safe - biometric identification center of the new generation (Fig. 4).

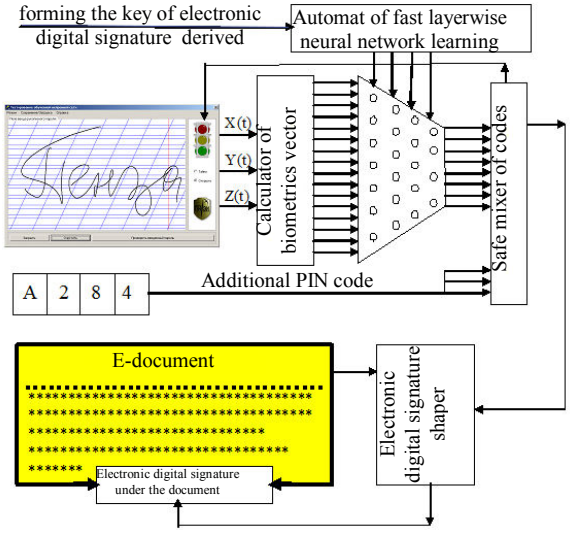

Fig. 4 Structure of the personal signature generator with a highly reliable biometric authorization

Strengthening the resilience of biometric authentication can be achieved through the use of multiple biometric technologies (Fig. 5). Thus, each key part is formed from individual tiles, each formed of a biometric parameter.

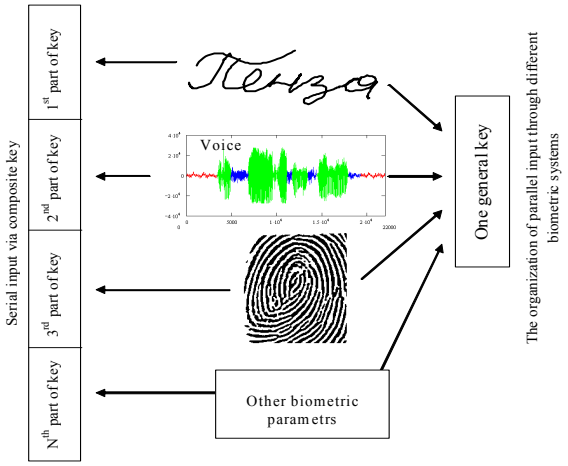

Fig. 5 Diagram of the formation of multi-biometric key code

Thus, biometric electronic identity card that is stored in the Internet and intended for use in open information spaces must have biometrics placed in closed containers of neural network that can be easily opened their host and cannot be guaranteed to be open to other biometrics another person. Themselves open containers neural network should be set up according to the requirements of GOST R 52633.4, GOST R 52633.0, GOST R 52633.5 [19], [20], [22], and further self-defending (crash). Apparently, and other personal data of the person in front of their placement in an electronic biometric ID card should also be encrypted on the key of the holder. Next, the electronic identity card must be signed by electronic signature authority issued it, after that anonymous electronic identity card may well be stored in the Internet (cloud storage of data).

The main elements of this technology are illustrated by Fig. 6.

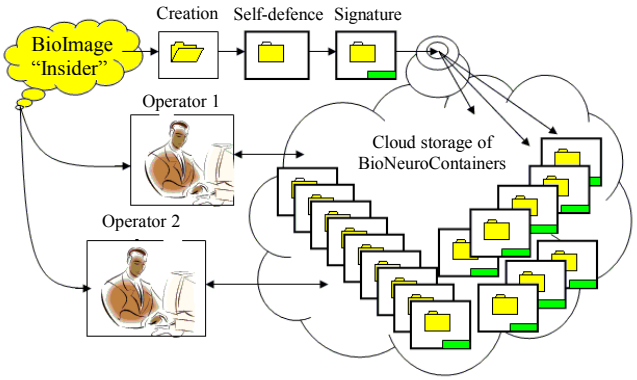

Fig. 6 Cloud storage technology electronic identity

This technology allows not having any documents. In order to confirm their authority to any one of us would be enough to give his name and show your biometric image of a particular operator to provide certain information services. By name and the image of this operator information services or the user finds the desired cloud storage electronic identity card. Use your biometric identity can only the user to the presence of the operator or service remotely (identity card for local authentication and remote are different).

V. Transformation of Personal Biometrics into Access Code

Formally continuous conversion biometric data (parameters) in the output code can use conventional analog-to-digital converters (ADCs) and use them to implement a conversion of each of the plurality of continuous variables in the corresponding biometric binary code. An example of such a transformation continuous parameter v1 biometric image of "Insider" and similar parameter ξ1 biometric images all "Strangers" in a 4-bit binary code is shown in Fig. 7.

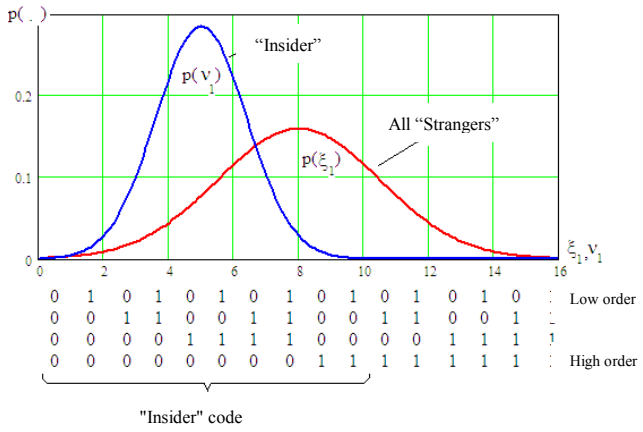

Fig. 7 The transformation of continuous biometric v1 image of ξ1 and images of all the "Strangers" in the digital code

Obviously, before the analog-to-digital conversion must be scaled and converted to center all the biometric parameters so that the dynamic range of the ADC has coincided with an input dynamic range of images of all the "Strangers". In this case, each ADC output code will correspond to a situation of continuous biometric input. In this part of the output code will match the biometric image of "Insider."

In the first approximation, the density distribution of the values of the input biometric image «Insider» - p(vi) can be considered normal. It can be considered as the normal density values of biometric images "Strangers" – p (ξi). Biometric data of the image of "his" are considered stable if the dynamic range of their change is less than 30% of the dynamic range of images all "Strangers." Biometrics high stability has a dynamic range of 30% to 60% of the possible dynamic range of all the "Strangers". Unstable biometrics has a dynamic range of between 60% and 90% of the possible dynamic range of images of all the "Strangers".

GOST R 52633.1-2009 [21] defines a measure of strength of biometrics as the ratio of the standard deviations of the parameters of images of all the "Strangers" and the image of "Insider":

$$s_i = \frac{\sigma(\xi_i)}{\sigma(v_i)} \quad (1)$$

where $\sigma(\xi_i)$ - the standard deviation of the ith biometric images of all the "Strangers" on the i-th input of the converter biometrics code;

$\sigma(v_i)$ - the standard deviation of the ith biometric image of "Insider" in the ith input of the converter biometrics code.

In addition, GOST R 52633.1-2009 further defines a unique measure of biometrics:

$$u_i = \frac{|E(\xi_i) - E(v_i)|}{\sigma(\xi_i)} \quad (2)$$

where $E(\xi_i)$ - the expectation of the i-th biometric images of all the "Strangers" on the i-th input of the converter biometrics code;

$E(v_i)$ - The expectation of the i-th biometric image of "Insider" in the i-th input of the converter biometrics code.

Indicator unique ui allows you to numerically evaluate how the distribution center *p(vi)* of a biometric parameter is different from the so-called average distribution *p(ξi)*. An indicator unique biometric image typically varies from 0 to 4. Typical, the unique parameters of extremely small, so for example, a measure of the uniqueness of the parameters a 1 to the average image of "his" is less than 25%.

Obviously, the higher the stability of the average E(si) and the higher the average uniqueness of E(ui) biometric image of "his", the easier it is to solve the challenge of transforming a biometric image of "his" in the output code is unambiguous.

In addition, it should be noted that is widely used in the last century practice of allocating and using the most informative parameters [23]-[26] for a highly reliable biometric unacceptable for the following reasons. First the use of only the most informative parameters significantly compromised biometric image of "Insider", as each unique biometric image of the most informative biometrics have their own unique layout. Secondly the use of only the most informative parameters significantly reduces the quality of the final solutions.

Since experience has shown that the use of only 16 of the most informative parameters gives the probability of error of the second kind (the probability of false pass "Stranger") at 10-3 with identity authentication on the dynamics of the play written word, "Penza". If we refuse from the practice of using only the most informative parameters and increase the number of metered parameters to 416, the probability of error of the second kind is reduced to a value of 10-12. A reduction in the probability of error is a billion times by increasing the dimension of the problem being solved with the 16 parameters analyzed to 416 Biometrics.

The information contained in 16 of the most informative parameters of the written word, "Penza" reserves of about 10 bits (P2 ≈ 10-3 ≈ 2-10). The information contained in the 416 parameters of the handwritten words "Penza" reserves of about 40 bits (P2 ≈ 10-12 ≈ 2-40). That is, 400 relatively poor in terms of information parameters is located 30 bits of information. Much of the information (3/4) is contained in so-called bad data. In good data contains a minority (1/4) of biometric information of the image.

As a consequence, efficient converters of biometrics code cannot be constructed a simple digitization of biometric parameters (Fig. 7, as well as the classic procedures of recognition biometric images [23]-[26]. With a simple digitization of data [17], the output code of the images of «Insider» is very unstable and they cannot be corrected by classical methods of error detection and correction [27]-[30]. Attempts to pre-processing of data (up to digitization) classical procedures of artificial intelligence [23]-[26] there are significant information loss; the vast majority of the information is released.

The requirements for biometrics converter code for his work with the images of "Insider." Currently, there are two approaches to the formulation of requirements for the converter biometrics code (PBC) on presentation of the image of "Insider". Foreign researchers from USA and Canada [10], [11], [31], [32] form a unique key based on the uniqueness of the biometric image of "Insider". Russia is developing its technology GOST R 52633.0-2006 [20], in which the cryptographic key "Insider" at the inverter output biometrics code can be anything, as it is given from the outside during training the neural network of the converter. Both of these areas are complementary.

Scholars from abroad are trying to create a so-called biometric hash function that gives a random number, which is characteristic for a particular biometric image of "Insider." In this case, all examples of the image of "Insider" rise to the corresponding vector of biometrics $\overline{\nu}_1, \overline{\nu}_2, \overline{\nu}_3, ..., \overline{\nu}_K$, must provide biometrics at the converter output code is the same random binary code - consisting of a sequence of states "0" and "1".

The same demands and domestic standard [20], that is, converters biometrics code of any type are described in the following vector equation:

$$\begin{bmatrix} ПБК \\ N \times n \end{bmatrix} \cdot \overline{\nu}_i = \overline{c}\,, \tag{3}$$

where $\overline{\nu}_i$ - the vector of N input biometric parameters obtained from the i-th example of the image of "Insider";

$\overline{c}$ - Binary code of n bits (binary vector of n states of each of the bits of code) corresponding to the response of PBC on the image of "Insider";

$\begin{bmatrix} ПБК \\ N \times n \end{bmatrix}$ - Some non-linear transformation matrix

is sampled (convert) the input vector of continuous biometric data in the output code.

Obviously, the examples of biometrics image of "Insider" have a non-zero uncertainty (volatility). That is, the entropy of the input vector "Insider" is always different from zero:

$$H(\overline{\nu}_i) \neq 0.0 \tag{4}$$

In contrast, the output of the converter $\overline{c}$ code when exposed to examples of biometric image of "Insider" - $\overline{\nu}_1, \overline{\nu}_2, \overline{\nu}_3, ..., \overline{\nu}_K$ always stable (always the same). That is, the entropy of the output code for the image of "Insider" is almost zero:

$$H(\overline{c}) \cong 0.0 \tag{5}$$

Biometrics can be interpreted converter code as a device that performs almost full compensation of entropy inherent biometric image of "Insider".

It is also clear that the biometric data of the image of "Insider" have significant correlations between pairs of biometrics [12], [18]:

$$\left| r_{\nu_i, \nu_j} \right| \neq 0.0 \tag{6}$$

where $\left| r_{\nu_i, \nu_j} \right| = \frac{1}{K} \sum_{k=1}^{K} \frac{(E(\nu_{i,k}) - \nu_{i,k}) \cdot (E(\nu_{j,k}) - \nu_{j,k})}{\sigma(\nu_{i,k}) \cdot \sigma(\nu_{j,k})}$ - the correlation coefficient between pairs of input biometric parameters;

$\nu_{i,k}$ - I-th biometric k-th example of the image of "Insider";

$\nu_{j,k}$ - J-th biometric k-th example of the image of "Insider";

K - total number of examples of the image of "Insider" used in calculations.

The correlation coefficient between pairs of input biometric image of "Insider" is a random variable, is well described by a normal distribution of values. It is evident that the condition (6) for an absolute majority pair correlation coefficients leads to the expectation that the module pair correlation is as different from zero:

$$E\left(\left|r_{\nu_i,\nu_j}\right|\right) \neq 0.0 \tag{7}$$

For real biometric images module expectation pair correlation coefficients significant value from 0.2 to 0.6

Naturally, the estimates of the form (7) can be performed not only in relation to biometric input of the converter, but also in relation to the outputs of the converter biometrics code [33], [34]. For the image of "Insider," correlations between pairs of bits output code is always close to its limiting value:

$$E\left(\left|r_{c_i,c_j}\right|\right) \cong 1.0 \tag{8}$$

Calculations of pair correlations bit output codes appropriate to carry out a special formula built on the transition to a different system:

$$\begin{cases} \widetilde{c}_i = 1 & if \;\; c_i = \text{"1"}; \\ \widetilde{c}_i = -1 & if \;\; c_i = \text{"0"} \end{cases} \tag{9}$$

The transition to the new system (9) simplifies the calculation of the correlation coefficients due to the exclusion from the formula of the standard deviations of discrete values:

$$r_{c_i,c_j} = r_{\widetilde{c}_i,\widetilde{c}_j} = \frac{1}{K}\sum_{k=1}^{K} \widetilde{c}_{i,k} \cdot \widetilde{c}_{j,k} \,, \tag{10}$$

where $\widetilde{c}_{i,k}$ - state of the i-th bit of the output code in response to the k-th sample image of "Insider" after the transition to the new system of coordinates (9).

Good converter biometrics code when exposed to examples of the image of "Insider" should act as an amplifier input pair correlations to the maximum possible correlation coefficients:

$$\left|r_{c_i,c_j}\right| \cong 1.0 \tag{11}$$

Strengthening the pair correlations is a consequence of the reverse effect of weakening the entropy transmitter outputs biometrics code for the images "Insider".

The requirements for biometrics converter code for his work with the images of "Stranger". We emphasize that the intrinsic entropy and pair correlation image of "Insider" are similar to those parameters of the image of "Stranger", but the converter biometrics code must respond to this in a different way. All examples of the image of "Stranger" that generate the corresponding vector of biometrics, $\overline{\varsigma}_1, \overline{\varsigma}_2, \overline{\varsigma}_3, ..., \overline{\varsigma}_K$ should give the inverter output biometrics-random code that do not coincide with each other, binary codes - $\overline{x}_1, \overline{x}_2, \overline{x}_3, ..., \overline{x}_K$. This situation is described by the vector equation:

$$\begin{bmatrix} ПБК \\ N \times n \end{bmatrix} \cdot \overline{\varsigma}_i = \overline{x}_i, \tag{12}$$

As the output code image of the "Stranger" does not coincide with each other:

$$\overline{x}_i \neq \overline{x}_j \tag{13}$$

their entropy cannot be zero:

$$H(\overline{x}_i) \rangle 0.0 \tag{14}$$

Studies of neural transmitters' biometrics code showed that for them the natural entropy of the input image of the "Strangers" is significantly enhanced:

$$H(\overline{x}_i) \rangle H(\overline{\varsigma}_i) \rangle 0.0 \tag{15}$$

As a result, the pair correlation of input biometric image of the "Stranger" destroyed

$$E(\left|r_{\varsigma_i,\varsigma_j}\right|) \rangle E(\left|r_{x_i,x_j}\right|) \rangle 0.0 \tag{16}$$

National Standard GOST R 52633.0-2006 [20] admits the existence of the expectation modules residual correlations less than 0.15, or:

$$0.15 \rangle E(\left|r_{x_i,x_j}\right|) \rangle 0.0 \tag{17}$$

The requirements for biometrics converter code when working with images of all the "Strangers". During the transition to a set of random images of all the "Strangers", generating vector $\overline{\xi}_1, \overline{\xi}_2, \overline{\xi}_3, ..., \overline{\xi}_K$ their entropy increases significantly when compared to the entropy of a biometric image of the "Stranger":

$$H(\overline{\xi}_i) \rangle H(\overline{\varsigma}_i) \tag{18}$$

The vector equation for images of all the "Strangers" is a complete analogue of (12):

$$\begin{bmatrix} ПБК \\ N \times n \end{bmatrix} \cdot \bar{\xi}_i = \bar{z}_i \qquad (19)$$

Equations (12) and (19) differ only in quantitative ratios. Firstly the entropy increases output codes:

$$H(\bar{z}_i) \rangle H(\bar{x}_i) \qquad (20)$$

Second, according to the standard [20] for the codes, responses to the images were "Strangers" requires equally probable states "0" and "1" for each k-th digit zk:

$$P(z_k = "0") \approx P(z_k = "1") \approx 0.5 \qquad (21)$$

For k = 1, 2, 3 … n.

Third, the basic standard [20] requires the provision of pairwise independent (uncorrelated) discharges the output codes:

$$r_{z_i, z_j} \cong 0.0 \qquad (22)$$

The last two requirements are technically hard to implement, but they will eventually allow for a high level of confidentiality of secret storage of biometric images in the learning parameters (tuned) converter biometrics code.

The influence of the dimension of neural networks on the quality of converters mystery of biometrics in access code. Experience in the development of neural network-equipment biometrics authentication identity showed that the increase in the input and output dimensions, the problem, a strong effect on the value of the probability of type II errors (false acceptance "Stranger" for "Insider"). The transition to accounting for 416 of biometric parameters (instead of the commonly considered 16 ... 32 parameters) and the transition from a single-bit control "Insider" / "Stranger" to the vector control key, which consists of 256 bits allowed to reduce the probability of type II errors of about a billion times [12], [16]-[18], [35].

It is well established that there is exponential growth of communications input-output dimension of the problem with the quality of its solutions [17]. Customary norms was related to the "Occam's Razor", which prohibits inflate the dimension of computing beyond what is necessary. In our case, it turns out that Occam is not right, in nature there are conditions under which artificially inflate the dimension is very, very profitable. In this regard, we will dwell upon these conditions.

In accordance with the requirements of GOST R [20], a highly reliable transmitter of biometrics in highly resistant key code should provide equally probable state "0" and "1" in each bit output code when the input action on the transmitter randomly "Stranger". The second most important condition is to ensure the independence of the (uncorrelated) output when exposed to the converter biometrics code randomly "Stranger".

The fulfillment of these conditions is equivalent to creating a multi-dimensional orthogonal neural network monitoring system. The operation of this system to its simplest two-dimensional case has a graphical interpretation, which is displayed in Fig. 8.

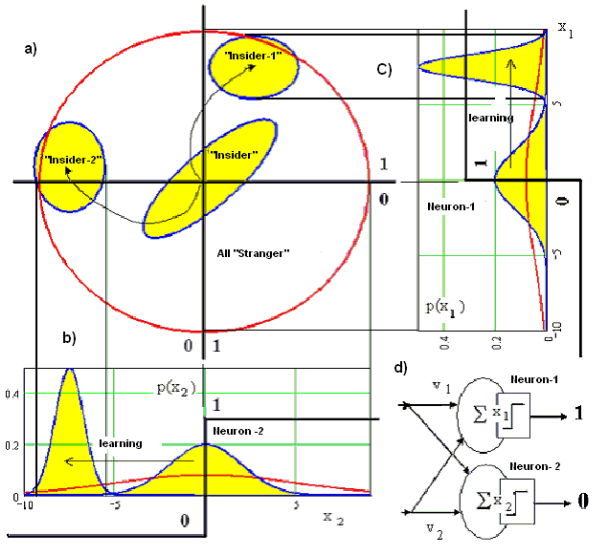

Fig. 8 Education two neighboring neurons single-layer artificial neural networks, leading to the orthogonality of dividing functions

The data can be seen that the two neighboring neuron layer neural network to be trained in different ways. Usually the biometric image of "Insider" is in the center of a set "All Strangers" and training All “Strangers” of neurons that image is pushed to the periphery of the multitude of "all strangers." Fig. 8 shows the two trajectories pushing the image of "Insider - 1" when learning neuron-1 and trajectory "Insider -2 ", occurs when learning neuron-2.

Looking at the picture it is easy to see that after the training neurons 1 and 2, the image of "Insider" will respond to the state of the code "10". If these same two neurons exposed to random images "Stranger", the states "0" and "1" bits of the output code will be equally probable, since the linear separating function of the neuron-neuron-1 and 2 pass exactly through the center of the distribution of images of "Strangers" Mutually orthogonal (perpendicular) sharing features makes state of the output bits of code independent (uncorrelated).

As a consequence of neuron-1 recognizes "Insider" never make mistakes, but with a probability of 0.5 can take the "Stranger" for "Insider". When there are two conflict neuron passes "Alien" occur with a probability of 0.52 = 0.25. It is easy to show that the capacity dimension of input and output data is the exponential decrease the probability of collision "Insider" / "Stranger". If you take the 256 inputs and outputs, the probability of collisions will be 10-77 = 0.5256. This is an extremely small value, which coincides exactly with the probability of guessing the key length of 256 bits.

Thus, increasing the number of inputs and outputs of the neural network is theoretically possible somehow greatly reduce the likelihood of conflicts in the decisions taken by the

neural network artificial intelligence. This is a purely theoretical conclusion without taking into account the real practical limitations.

In practice, the full higher dimensional orthogonal neural network observer cannot be reached. Between discharges the output codes are residual correlations; their value is strictly regulated by the IEC [20]. In addition, it was found that only technically meaningless to increase the length of the output code. Fig. 9 shows a graph of the logarithmic connection indicator output quality of decisions-q and the length of the output code (the number of neurons in the same layer of the neural network). It can be seen from the data that the increase in the quality of decision neural network code converter biometrics solutions at about 400 outlets practically stops. There is a very real technical limit increasing the length of the output code of the key. Just step up output of the neural network without increasing the number of its inputs cannot.

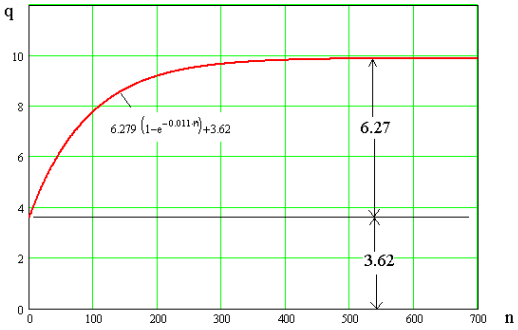

Fig. 9 Exponential growth restriction indicator of the quality of decision-making neural network as the number of output neurons

However, the transition from small neural networks with a small number of inputs and outputs to the large neural networks with a large number of inputs and outputs and is very highly effective techniques. So the bottom part of the graph in Fig. 2 quality (q = 3.62) corresponds to a two-layer neural network with one input and 416 output, which provides the possibility of faulty collisions at 10-6. Upper graph (q = 9.89) corresponds to a two-layer neural network 500 neurons in each layer (each neuron has to input 24) that together process 416 input biometrics. In this case, the neural network by number of neurons and connections between them has increased by about 300 times, and the probability of error has decreased to a value of 10-22 times (16 orders).

Save on their natural Occam brains can and should be. Save for Occam on artificial intelligence makes no sense. Quite the contrary, it makes sense to artificially inflate the dimension of the problem, solve it in spaces of high and ultra-high-dimensional, and then turn off the dimension for a satisfactory understanding of the human sense solutions.

VI. Conclusion

Experience in the development of neural network-equipment biometrics authentication identity showed that the increase in the input and output dimensions, the problem, a strong effect on the value of the probability of type II errors (false acceptance "Stranger" for "Insider"). The transition to accounting for 416 of biometric parameters (instead of the commonly considered 16 ... 32 parameters) and the transition from a single-bit control "Insider" / "Stranger" to the vector control key, which consists of 256 bits, helped to reduce the likelihood of type II errors of about a billion times.

References

[1] Chugunov A.V. “E-government: the formation of its legal framework in Russia”, Bulletin of the FSI "State Registration Chamber", no. 4, pp. 34 – 46, 2009.
[2] Shlyakhtina S. “Internet Facts and Figures”, Computer Press, no. 2, pp. 8-19, 2003.
[3] Prokhorov. A. “E-Government at a Glance”, Computer Press, no. 5, pp.144-150, 2006.
[4] Irkhin Y.V. "Electronic Government: theory and practice”, Public service, no. 4, pp. 163-173, 2008.
[5] Srivastava, A. From Manuscript to Electronic Signature: Background, Technology and Case Laws. In Electronic Signatures for B2B Contracts, (pp. 7-30). Springer India.
[6] Sano, T., Kakizaki, Y., Inamura, M., & Iwamura, K. Digital Signature Scheme Enabling Pre-Control of Content Editing for Secondary Use.
[7] Barik, N., & Karforma, S. (2012). A Study on Efficient Digital Signature Scheme for E-Governance Security. Global Journal of Computer Science and Technology, 12(3).
[8] Akhmetov B.S., Ivanov A.I., Trifonov S.E. Biometric identity centers walking distance / / News Science of Kazakhstan. - 2011. - № 3-4. - S. 34-41
[9] Bautin V.M. ,Tabolina M.S. (2012). Ways to Improve the Quality of Public Services in russia. Series "Innovation Economy: The Human Dimension '51.
[10] Soutar, C. (1999). D. roberge, A. Stoianov, R. Gilroy, and BVK Vijaya Kumar,“Biometric Encryption”, ICSA Guide to Cryptography.
[11] A. Cavoukian, A. Stoianov, "Biometric Encryption: A Positive-Sum Technology That Achieves Strong Authentication, Security And Privacy," White Paper, Office of the Information and Privacy Commissioner of Ontario, 2007
[12] Ivanov A.I. Biometric identification on the dynamics of unconscious movements. - Penza: Publishing House Penz. State. University Press, 2000. - 188 p.
[13] Nixon, M. Gait biometrics. Biometric Technology Today, Volume 16, Issue 7-8, 2008-07-01, Pages 8-9
[14] Ball Rood and others. Management on biometrics. / Ball Rood, Jonathan H. Connell, Sharath Pankanti, Nalini K. Ratha, Andrew W. Senior / / Moscow: Technosphere, 2007. p-368.
[15] Akhmetov B.S., Volchikhin V.I., Ivanov A.S., Malygin A.Y. Highly reliable multi-biometric authentication of the human person authorized to support the interaction of citizens with e-government and e-business / / Bulletin of KazNTU, 2012. - N3. - P.181-184.
[16] Volchikhin V.I., Ivanov A.I., Funtikov V.A. Fast algorithms for learning neural mechanisms
[17] Malygin A.Y., Volchikhin V.I., Ivanov A.I., Funtikov A.Y. Fast algorithms for testing neural mechanisms of biometrics, cryptographic protection of information / Penza, 2006, Publisher of Penza State University, 161 p.
[18] Ivanov A.I. Neural network algorithms for biometric identification. Book 15, the series "Neurocomputers and their Applications" M. radio engineering, 2004, p.144.
[19] GOST R 52633.4-2011 Information Security. Security technique. Interaction interfaces with neural network converters Biometrics Access Code
[20] GOST R 52633.0-2006 "The protection of information. Security technique. The requirements for a highly reliable means of biometric authentication "
[21] GOST R 52633.1 "The protection of information. Security technique. Requirements for the formation of the natural bases of biometric images designed to test a highly reliable means of biometric authentication "

[22] GOST R 52633.5-2011 "The protection of information. Security technique. Automatic learning of neural transmitters Biometrics Access Code "
[23] R. Duda, Hart P. Pattern recognition and scene analysis. – M., Mir. 1976, p.511.
[24] Fukanaga K. Introduction to the theory of statistical pattern recognition. Nauka, Moscow, 1979, p. 368.
[25] Tu J., Gonzalez R. The principles of pattern recognition. - M.: Radio and Communications, 1980, p. 408.
[26] Hunt E. Artificial Intelligence. – M., Academic Press, 1978, p. 550.
[27] R. Morelos Zaragoza. Art of error-correcting coding M. Technosphere, 2007, p. 320.
[28] Peterson W.W., Weldon E. Error correcting codes/ Monograph, ed. Dobrushin R.L., Samojlenko S.I. / /-M.: MIR, 1976, p. 364.
[29] Samojlenko S.I. Error Coding. M.: Radio and Communications, 1968, p. 240.
[30] Borodin P.F. Introduction to the theory of error-correcting coding. M.: "The Soviet radio", 1968, p. 708.
[31] Monrose F., Reiter M., Q. Li, Wetzel S. Cryptographic key generation from voice. In Proc. IEEE Symp. on Security and Privacy, 2001.
[32] Dodis Y., Reyzin L., Smith A. Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy, Data April 13, 2004.
[33] Ivanov A.I. Evaluation of residual correlations for testing neural transmitters biometrics code "Neurocomputers: development, application» № 12, 2007, pp.25-26.
[34] Nadeev D.N., Ivanov A.I. Contact pair correlation coefficient outputs neurotransmitter biometrics code with a standard deviation measures the Hamming images of "Strangers", "Neurocomputers: development, application» № 12, 2007, p.27-29
[35] Ivanov A.I., Kislyaev S.E., Gelashvili P.A. Artificial neural networks in biometrics, medicine and healthcare. Samara: LLC "Etching", 2004, p. 236.