Available online at www.sciencedirect.com

ScienceDirect

Procedia - Social and Behavioral Sciences 191 (2015) 2261 – 2266

Procedia
Social and Behavioral Sciences

WCES 2014

Testing The Quality of Teaching The Biometrical-Code Transformers

Akhmetov B.S. [a], Ivanov A.I.[b], Kartbayev T.S. [a]*, Kalizhanova A.U.[a], Mukapil K.[a], Nabiyeva G.S.[a]

[a]*Institute of Information and Telecommunication Technologies, Kazakh National Technical University named after K.I. Satpayev, Satpayev street,22, Almaty, 050013,Kazakhstan*
[b]*Penza Scientific-Research Electrical Institute, Sovetskaya street, 9, Penza, 440000, Russia*

Abstract

The article herein considers the problems of testing the quality of teaching the biometrical-code transformers as nowadays big attention is given to biometric technologies development. In the result of higher school students testing in the real mode in the frame of works carried out by interbranch laboratory on biometrical devices and technologies testing there have been received certain results.

Selection and peer-review under responsibility of the Organizing Committee of WCES 2014

Keywords: Biometrics, neural network, authentication, infromation protection, biometrical-code transformers;

1. Introduction

Rampant development and wide use of information-telecommunication systems gave a possibility for the mankind to transfer to the new step of its development. The given systems transformed not only the collection, processing and transfer principles and forms but they started to influence sufficiently at all facets of the society's life becoming one of the key factors of its sustainable development maintenance. Amount, technical level and accessibility to information-communication systems determine the level of any state's education development at present. However along with the development and accessibility there appeared the problem of the given systems safety security. The system herein represents an entire tasks complex which is solved through perfecting educational

* Kartbayev Timur, Tel.: +7-707-547-4248
E-mail address: kartbaev_t@mail.ru

Selection and peer-review under responsibility of the Organizing Committee of WCES 2014
doi:10.1016/j.sbspro.2015.04.557

resources applying information technologies, methods and means of their elaboration. All above mentioned proves significant attention drawn to biometry and biometrical technologies development. Biometrical systems' common market sustainably increases within the recent years approximately for 40% annually [http://www.biometricgroup.com/] according to forecast of International Data Corp.

1.1. Solution of the problem

Use of super-reliable biometrical means having been developed in compliance with the state standard requirements (GOST, 2006) puts a number of questions to a user. Biometrical password (written or voiced) shall be kept in secret by a user. A user shall independently form digital combination, word, phrase convenient for him/her. At that a user shall not trust statistically average characteristics stated by producer. Therefore testing of neuron network solutions becomes an integral element of their training (programming). Classical recommendation is fractionation of all examples in halves and use of the first part for training and the second one for testing. (Galushkin and Tsypkin, 2002; Galushkin, 2000; Gorbanj and Rossiyev, 1996; Ossovsky, 2002)

On the one hand to waste a half of training examples for intermediate testing is squander, but on the other hand such approach is guaranteeing statistical balance of training and testing procedures. Actually along with examples number growth in training sampling the problem of their statistical balance weakens. To illustrate the above relation distribution approximations of written images samples "a" (center -m1), written images «в» (center - m2) and images test sampling «a» (center - mt) are given on Fig1. From charts given on Fig. 1it is obvious that test selection from 6 images «a» differs approximately for 35% from similar training selection of the same image. If to increase the test and training selection up to 16 examples we can reach the situation shown on Fig. 2. In proportion to the testing and training sizes growth the false divergence between their distribution decreases. Presented graphs have been received in the neuron network systems modeling «Neuron teacher», designated for students' laboratory works. In this software product with the aim of displaying the values distribution laws there is used their approximation as a standard law of values distribution. This presentation form is not random. If to consider one of any neuron network outputs we will have a certain threshold element at integrator exit. Integrator (summer), as is known, is the normalizing element. According to the known statistics limiting theorem summing (Ventsel and Ovcharov, 1988; Pugachev, 1979) of independent (weakly dependent) values multiplicities with certain distribution laws results in distribution close to normal. That relation is asymptomatic, the more inputs has the summer the better it normalizes the output data. Naturally the latest neuron summer's weight numbers will be different but it will not influence the asymptomatic relation. At any weight numbers the summer is a normalizing element which gives a formal right to apply widely distribution laws normalcy hypothesis of output laws. Distribution laws normalcy hypothesis of the neuron summer's output laws is an effective tool for forecasting the expected quality of decisions taken by the latest neuron.

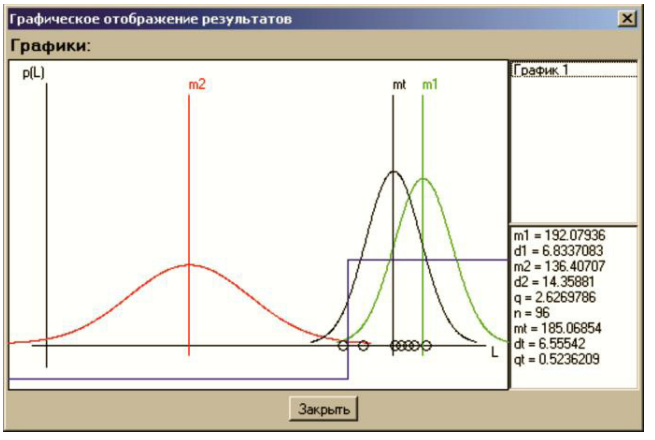

Fig. 1. Charts of training selection distributions from 6 images «a» with a center m1 and testing selection from 6 images «a» with a center mt

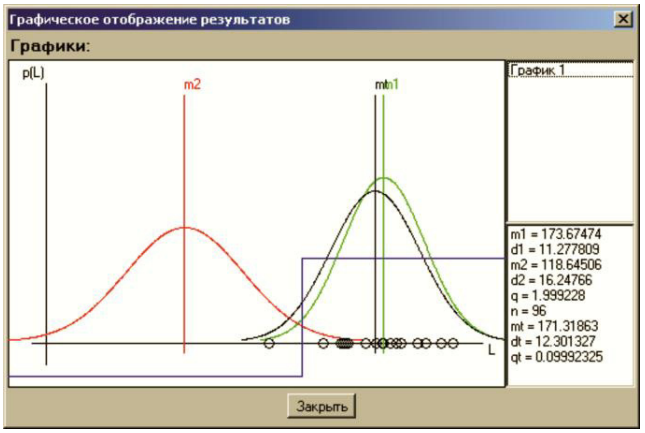

Fig. 2. Charts of training selection distributions from 16 images «a» with a center m1 and testing selection from 16 images «a» with a center mt

Use of this hypothesis allows to estimate first and second types errors probability in whole without attracting additional test examples per the following formula:

$$P_1 = P_2 \approx 0.5 - \frac{1}{\sqrt{2\pi}} \int_0^q \exp(\frac{-x^2}{2})dx = 0.5 - \Phi_0(q), \quad (1)$$

where $\Phi_0(.)$ – Laplace one-sided function (Laplace one-sided integral);

$$q = \frac{|m_1 - m_2|}{\sigma_1 + \sigma_2},$$

-logarithmic exponent of training quality;

where m1, m2 – mathematical expectations of first and second sharable multiplicities;

σ1, σ2 – mean-square deviations of first and second sharable multiplicities.

Having used the ratio (1) for error probability assessment for the situation (Fig. 1) we will receive $P1=P2=1-\Phi_0(2.6)=0.004$. For the situation with the bigger examples number (Fig. 2) we will receive worse forecasting results $P1=P2=1-\Phi_0(1.9)=0.024$.

Comparing the above given prognoses there can happen a mistake that using small training selections we can receive better training results. Testing sampling shows that it is far from it. Allowance for testing corrections is fulfilled as follows

$$P_1 = P_2 \approx 0.5 - \frac{1}{\sqrt{2\pi}} \int_0^{q-2q_t} \exp(\frac{-x^2}{2})dx = 0.5 - \Phi_0(q - 2q_t), \quad (2)$$

where qt – logarithmic exponent of examples distribution divergence of training selection and similar testing selection at trained neuron linear output.

Ratio (2) for the situation on Fig. 1 gives following outcomes:

$P1=P2=1-\Phi_0(2.6-1) = 0.05$, and for the situation on Fig. 2 we will receive

$P1=P2=1-\Phi_0(1.9-0.2) =0.036$.

Independent testing allowance gives much more correct predictions.

Biometrical systems are trained in a way to differentiate a narrow class “Own” from the general wide images class «Alien ». For that upon training an artificial neuron network there used several “Own” images samples, for instance shown on Fig. 3. It is obvious that number of “Own” images samples used upon training shall not be very big. It is connected not only with securing safety measures in artificial neuron network training process but as well with account of a user’s interests. Therefore producers try to create maximum friendly to users biometric systems. Upon real mode testing of Kazakh National Technical University students and military training institute attendees in the frame of works conducted by interbranch biometrical devices and technologies testing laboratory of Penza state university there were received definite results. It was revealed that an ordinary user having undertaken an introductory course with input devices of written password: pad or monitor of a palmtop and special software normally without specific voltage, can simulate up to 20 examples of the offered password consuming in average two-three minutes for it. Practical work on collecting the bases of password natural biometrical images writing shows that upon requirement to reproduce the bigger number of own biometrical images samples the user does it reluctantly. It seems that the systems requiring reproducing 40, …, 60 examples for training will have quite limited use upon access only to very responsible attachments. Number of “Alien” random images examples may be any. These images are not mandatory to produce with hand in training process they can be included into training software and correspondingly their number is defined solely according to technological demands of concrete algorithm training. On Fig. 4 there given 9 examples of such random written images which actually can present a part of wider training selection. Usually upon training completion relatively «weak» biometric-neuron network systems with one output have probability of first and second type errors at the level within 0.01, …., 0.05. Fig. 5 shows graphs of similar biometric protection system output distributions as an example. In the result of neurons training with fast decorrelation algorithms. (Volchikhin, 2005) there occurs extrusion of separated narrow biometric image “Own” to the periphery of the wider random images multiplicity “Alien”.

Fig. 3. Example of training selection «Own» from 9 password written random images «Penza»

Fig. 4. Example of training selection «Alien» from 9 password written random images

One of the important features of information protection biometric means is the fact that there is no problem of the first type error probability assessment for them (false refusal to «Own»). First, parameter P1 is not critical for operability of biometric protection and can change in the range of 0.01 to 0.25. This parameter value has psychological significance rather than practical. Even in the worst case P1=0.25 a user gets refusal to an access with a probability of 0.016 if the system affords him/her at least three attempts. If the method belongs to super reliable class then it can have no limitations in respect of access attempts. That is a real value P1 for «persistent» legal user of super reliable biometry is always zero.

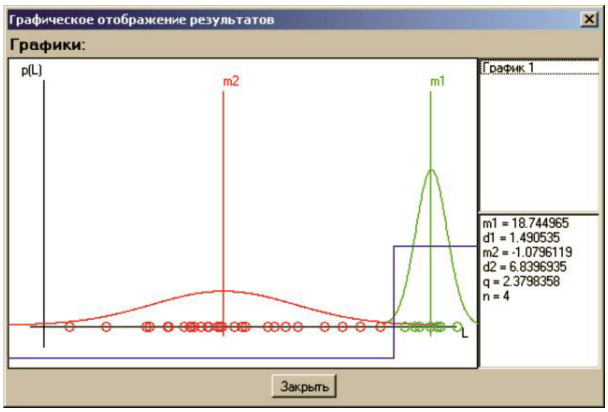

Fig. 5. Charts of results of one neuron training in separating a written image «Own» from random written images multiplicity «Alien» (PEE=0.008)

In connection with the above said they try not to sacrifice “Own” images samples in biometric protection methods on testing. All “Own” deficit images examples are used in training. Parameter P1 value forecasting problem is solved by calculating the parameters of normal distribution law of “Own” images output values. Testing on «Alien» images for biometric protection means with “Alien” letting pass probability P2≈0.001 is quite simple. For direct statistical estimations random biometrical images base of about 100 000 examples is enough. Similar test images bases collection, storage and use at availability of modern technical possibilities does not present any difficulties.

2. Conclusion

In conclusion it should be stressed that without doubt the new super reliable biometrical technologies require further studying but even today it is undisputable they will be demanded for protection from unauthorized access to information and for distant person authentication.

References

Akhmetov, B. , Doszhanova, A. , Ivanov, A. , Kartbayev, T. , Malygin, A. (2013). 'Biometric Technology in Securing the Internet Using Large Neural Network Technology'. World Academy of Science, Engineering and Technology, International Science Index 79, *International Journal of Computer, Information Science and Engineering, 7*(7), 136 - 145.

Akhmetov, B. S., Ivanov, A. I., Kartbaev, T. S., Malygin, A. U., & Mukapil, K. Biometric Dynamic Personality Authentication in Open Information Space. International *Journal of Computer Technology and Applications. India, 4*(5), 846-855.

Galushkin A.I. (2000) Theory of neuron networks. Volume 1 «Neuron computers and their use».

Galushkin A.I., Tsypkin Ya.Z. (2002) Neuron networks: background. Volume 5 of «Neuron computers and their use» series.

Gorbanj A.N., Rossiyev D.A. (1996) Neuron networks at personal computer, Novosibirsk:, Science. P. 276.

GOST P 52633.0 – 2006 «Information protection. Information protection techniques. Requirements to super reliable means of biometric authentication means».

Kartbayev, T. S., Volchihin, V., Akhmetov, B. S., Ivanov, A., & Malygin, A. (2013). Highly Reliable Human-Being Personality's Multi-Biometric Authentication to Support Citizens Interaction. *Global Journal on Technology, 3*.

Ossovsky S. (2002) Neuron networks for information processing. Finances and statistics.

Pugachev V.S. (1979) Theory of probability and mathematical statistics. Nauka. – p.495.

Ventsel Ye.S., Ovcharov L.A. (1988) Theory of probability and its engineering attachments. Nauka. – p. 480.

Volchikhin V.I., Ivanov A.I., Funtikov V.A. (2005) Fast algorithms of training neuron network mechanisms in biometrical-cryptographic information protection. – Penza: Edition of Penza State University, P.273.