UDC 538.913,159.923

Mykhaylo MAR'YAN,
DrSc, Professor,
Department of Solid-State Electronics & Information Security Faculty of Physics, Uzhgorod National University, Ukraine;
Nataliya YURKOVYCH,
PhD, Ass. Prof. ,
Department of Solid-State Electronics & Information Security Faculty of Physics, Uzhgorod National University, Ukraine

SYNERGETICS OF THE NEURAL NETWORKS IN THE CYBER SYSTEMS: SELF-ORGANIZATION AND FRACTALITY

Intelligent systems based on artificial neural networks allow you to successfully solve problems of image recognition, execution of forecasts, optimization, associative memory and management. Traditional approaches to these problems do not always provide the necessary flexibility in cyber systems. Many software applications are implemented in cybersecurity using neural networks [1]. Since artificial neural networks are electronic models of the neural structure of the brain, the natural analog shows that the set of problems that are not yet subject to the resolution of existing computers can be effectively solved by the synergy of neural networks [2].

The purpose of this work is to explore the possibility of using neural networks with Hebb's algorithms and direct distribution in cybersecurity and creating a composition of neural networks to reproduce symbolic data encoding in C ++, Ruby programming languages. The method of teaching Hebb with the change of weights $W_{ij}(t)$ by the ratio [2]:

$$W_{ij}(t) = W_{ij}(t-1) + \alpha y_i^{(n-1)} y_i^n , \quad (1)$$

where $y_i^{(n-1)}$ is the initial value of a i neuron of a $n-1$ layer вихідне, $W_{ij}(t)$ is weight coefficient of synapse joining i j neurons in iterations t and t-1 layers respectively, α is the rate of learning. When studying this method, the relationships between excited neurons increase and the coefficient modification α in the learning process is used. Along with (1) the differential method of Hebb's teaching is use]:

$$W_{ij}(t) = W_{ij}(t-1) + \alpha\left[y_i^{n-1}(t) - y_i^{(n-1)}(t-1)\right]\cdot\left[y_j^{(n)}(t) - y_j^{(n)}\right] \quad (2)$$

The most effective learning is in accordance with (2) the synapse connecting the neurons, the outputs of which most dynamically changed

toward the increase. The complete learning algorithm using the above formulas looks like this:

1. At the initialization stage, all weight coefficients are assigned small random values.

2. The inputs of the network are represented by the input image, and the excitation signals are propagated in layers according to the principles of classical networks of direct propagation (feedforward), that is, for each neuron, a weighed sum of its inputs is calculated, to which then the activation (transfer) function of the neuron is applied, which results in its initial value y_i^n, $i = 0..M_i - 1$, where M_i is the number of neurons in the stratum *i*, *n = 0 ... N-1*, and *N* is the number of layers in the network.

3. Based on the obtained initial values of the neurons by the formulas (1), (2) the change in weight coefficients is given.

On the basis of the correlations (1) - (2) we created applications in the programming languages C ++, Ruby. Their purpose is to recognize patterns of figures and Latin letters. The implemented neural network as a transfer function uses a binary threshold function [1].The neural network is modeled in two classes: RecognizeNeuron and RecognizePerceptron. In addition to them, two more classes are created: CodeNeuron and CodePerceptron, which is a direct distribution neural network. The neural network itself consists of 36 neurons, each of which is responsible for a certain symbol. During testing, only a neuron is trained with the corresponding one. (The influence of the number of neurons in the 102 ÷ 106 range on the efficiency of image recognition in the presence of noise (white and color) is also considered).

A separate module implemented an algorithm for entering the access code and blocking the system under certain predetermined conditions. It connects to the CodeCheckBox switch. As a result, the principle of the program changes. The CodeEdit and BlockCheckBox components are available. The Teach button is blocked because it is not needed in this mode. The SymbolEdit field becomes unavailable for editing - the user input process is displayed here (Fig. 1,2).

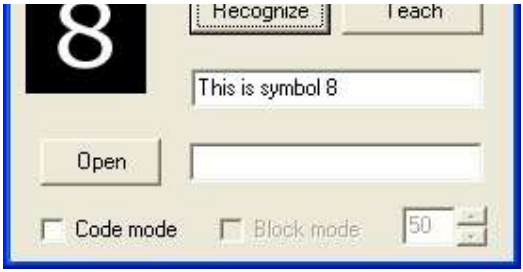

Fig.1. Enter user access code.

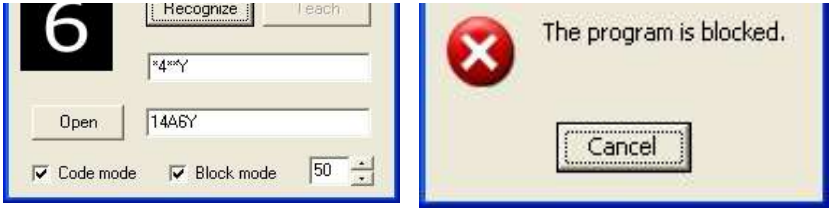

Fig.2. Blocking the program after reaching the specified percentage of recognition.

The essence of the module is that trying to enter an access code (regular password, fingerprint, electronic card), the program compares the entered data with the standard. In lock mode (BlockCheckBox switches on) when a certain percent of the input data recognition is reached (that is, the match between the characters represented by the reference image), the program is blocked. Thus, there is protection against unauthorized access by the attacker (Fig. 2,3). These neural networks can be used as an alternative to the existing development of systems for the reproduction and protection of electronic digital signatures.

Fig.3. Recognized drawn numbers and converted input image.

To verify the feasibility of using neural networks in electronic digital signature mechanisms, a comparison of the speed of recognition of input images based on the neural network and the normal cycle was made. As a

result, the neural network was much faster. The results for the same images in seconds are presented in the table 1.

Table 1.

Time of recognition of incoming images.

Input image	Time of recognition of incoming images of neural network	Cycle
0	0.00251233	0.078437902
1	0.002435225	0.091464138
3	0.002361752	0.11771464
5	0.002332978	0.126973121
6	0.002681905	0.203201804
9	0.002495569	0.240412119

This is due to the fact that for the neural network, the number of incoming images is insignificant. After learning once, the network can recognize a favorite input at the same speed. The speed of the cycle directly depends on the number of images with which to compare the input. Another advantage of the neural network in this case is that it can recognize even partial matches. In order to do this in the usual way, you need to connect additional resources, which will further increase the recognition time [3].

The peculiarity of the work is connected with the complementarity of the knowledge spheres, which are mostly considered separately and isolated, namely: programming and computer modeling, cybernetic systems and education. This integrity is achieved owing to the fractal application of synergetics and the possibility of obtaining completely new properties at the junction of adjacent spheres. The synergetics and fractality approach allows describing systems of a diverse nature as a whole, while preserving their uniqueness and originality. Also shown is the possibility of implementation of the results of the study of processes in the structuring of information, cybernetic, educational systems.

Conclusions. Thus, the possibility of using neural networks and examples of their software implementations in cyber security is shown. Developed applications for the symbol recognition, reproduction and protection of electronic digital signatures using the Hebb's network and direct distribution in C++, Ruby programming languages. The testing and diagnostics of the model have been carried out, and interfaces have been developed. A module for implementing the algorithm for recognizing the sequence of symbols and their comparison with a specific password has been created. The possibility of blocking the program's operation has been realized with the achievement of the specified percentage of recognition and access is simulated.

References

1. Mar'yan M., Seben V., Yurkovych N. *Synergetics and Fractality in Science Education*. University of Presov in Presov Publishing, Presov, 2018. P. 168.

2. Mar'yan M., Seben V., Yurkovych N. *Synergetics of Computer Modeling, Research and Technology Education. Concepts&Methods.* Lambert Academic Publishing, Riga, 2018. P. 120.

3. Mar'yan M. I., Seben V., Yurkovych N. V. Synergetics of thermoinduced instabilities and hypersensitivity of the non-crystalline materials in sybersecutity systems. IV International Scientific and Practical Conference «Actual Issues of Ensuring Cybersecurity and Information Protection». February 21-24, 2018, Kyiv, European University (Ukraine), P. 148-150.

Одержано 23.10.2018

УДК 343.43

Олександр Маркович БАНДУРКА,
доктор юридичних наук, професор,
академік Національної академії правових наук України, заслужений юрист України,
професор кафедри теорії та історії держави і права
факультету № 1 (слідства)
Харківського національного університету внутрішніх справ;
ORCID: https://orcid.org/0000-0002-0240-5517

ПРИВАТНІ ОНЛАЙН-ПРОЕКТИ ЯК СУЧАСНИЙ ІНСТРУМЕНТ ДЛЯ ПРОТИДІЇ ЗЛОЧИННОСТІ

Трансформація суспільних процесів у сучасному світі відбувається надшвидкими темпами. Те, що працювало ще місяць тому, сьогодні може виявитися застарілим і малопридатним для застосування у практичній діяльності.

Все це стосується і правоохоронної сфери. Її реформування відбувається весь час, проте стара ієрархічна структура управління не дозволяє ефективно та своєчасно відповідати на виклики сьогодення. Поряд із необхідністю заохочення ініціативи в частині запровадження інновацій на місцях потрібно також звернути увагу на більш широке делегування частини забезпечувальних функцій діяльності поліції приватному сектору. Особливо це стосується інформаційної сфери. Професійне супроводження окремого інформаційного завдання потребує залучення значних матеріальних та фінансових ресурсів, а також кваліфікованого персоналу. Вказана обставина в сучасних умовах унеможливлює ефективне виконання таких завдань поліцією, а тому було б цілком логічним залучати до їх виконання приватних підрядників.

Окремі приватні компанії та громадські формування продемонстрували достатньо великий потенціал розвитку онлайн-проектів, які можуть бути задіяні у протидії злочинності, та не могли б бути швидко та якісно виконані у забюрократизованих державних органах.

Наведемо декілька таких проектів: