UDC 004.89

Kostianikov Vladyslav, Korochkin Aleksandr.

USE OF NEURAL NETWORKS FOR SECURITY PURPOSES

The article describes the security spheres and the possibility of using in these areas systems based on the technology of artificial neural networks. An overview of modern solutions and problems they solve is given. It is proposed to improve the system for physical security, namely the access control system using the technology of wrapped artificial neural network.

Keywords: artificial neural networks, physical access control system, security.

Fig.: 2. Tabl.: 0. Bibl.: 5

Relevance of the research topic. Ensuring the safety of people is a hot topic of our time. In connection with the rapid elaboration of technologies of artificial neural networks (ANN), recent past few years, as well as an rise their accuracy and reliability. There was an opportunity to automate security sphere systems using this actual technology.

Target setting. Ensuring the safety of people is a complex task that requires different approaches for each type of theoretical danger, as well as the use of different security systems. The objective of this article is giving an overview of prevail problems and relevant automated systems and methods are use artificial neural network technology, as well as suggest improvement options using ANN in producing safety.

Actual scientific researches and issues analysis. Using an artificial neural network has found its applying in many spheres of security. There is a lot of researches about safety, in many cases: when driving in vehicles and air transport, ensuring physical or information security, forecasting in biological, economic and environmental safety spheres. Fundamental researches the theory of neural networks is also developing thick and fast.

Uninvestigated parts of general matters defining. Despite versatile research in the theory of neural networks, presently this technology is yet very demanding on resources for training. Research and the search for effective learning algorithms are needed. New efficient mass parallelization algorithms could also increase performance. And also a promising research topic is the development of specialized hardware for purposes training and use in end devices.

The research objective. The aim of this work is to review a set of measures to ensure the safety of people, search for existing solutions based on ANN, and exposition their main ideas. In conclusion of this article, the best solution will be proposed to ensure high reliability the system for one of the considered security types.

The statement of basic materials. Artificial neural networks are software algorithms that, during training, adjust the internal parameters of variables so that they with high presumprion correspond to certain data sample and do not reduce efficiency when adding new data. Accordingly, these algorithms can be effectively used to solve a wide range of problems, classifying images and texts, clustering and categorizing data, approximating functions, building forecasts and predictions, and many others, this is only a part of the functionality that can be used to ensure security. The classification task usually comes down to recognition of images and texts, and provides a search for objects in the image, the search for unique identifying signs and performing some actions based on this.

Clustering or categorizing data is a process in which a set of input data, be it symbolic text or an image, can be divided into classes or categories according to some criteria, which will highlight the algorithm itself.

Approximation of functions is reduced to finding some simple function similar to a complex function for which a set of points is known to points. This method is also a subsection of this task; extrapolation of functions can be used to build forecasts and predictions of certain values from known data.

Personal safety of a person consists of many factors, because every day a person faces many dangers, while walking on the street, while paying with a card on the Internet, and even while breathing. I will choose for review some spheres of safety in which systems based on artificial neural networks or can be based.

Road safety is regulated by law, has clear rules, and also participates in the lives of most people in the world. More than 20 million people suffer from road accidents each year, more than a million of them die [1]. These facts indicate the high relevance of the task of automating vehicle control to minimize the effect of the human factor. For this task, researchers use neural networks capable of identifying objects in the vicinity of the machine and assist in management. The most famous engineering solutions in this area are Tesla cars, as well as the Nvidia DRIVE AGX device that is installed in cars of world manufacturers such as Audi, Toyota, Volvo, Volkswagen, Mercedes-Benz. According to Tesla`s report, using all the automation technologies available to them, the accident rate is one car accident per 7.5 million kilometers, which is 3.4 times better than without using systems.

Environmental safety is a set of studies and actions that are aimed at studying the anthropogenic influence on the ecological encircling as well as the inverse effect of environmental hazards on life and health all life species. It includes comprehensive monitoring and assessment of factors, as well as the adoption of measures to prevent or reduce the effects of pollution. In this area of security, modeling and forecasting methods are widespread. Given that artificial neural networks can be used for modeling and forecasting. As well as the fact that ecological safety affects the lives of absolutely all people on earth, we can conclude that research in this area is very relevant. In December 1998, an international seminar was held on the use of artificial neural networks in environmental modeling, where even then they suggested using different data for building models and forecasting, starting from using data from radars to skulls of ancient rodents. Since then, forecasting methods in the field of ecology using artificial neural networks have constantly improved. Now there are many models that mainly study the effect of the ecology on different animals, the effects of global warming or the spread of diseases. Also in London there is a project which consists in controlling traffic lights via a neural network for the purpose distributing traffic and reduce the level of city pollution.

Information security basically implies the safety of data and means of storage and strong access to this information, as well as providing access to it only an authorized users [2]. It also implies the safety of personal information, the safety of funds in bank accounts etc. In this area, there are two main approaches for the use of artificial neural networks. The first is to use neural networks to test system vulnerabilities in union vulnerability scanners, this treatment saves up to 70% of testing time. The second is the use of active information protection systems whose main idea is continuously analyze user actions and identify suspicious ones which are may harm all system or be able to indicate the loss of an account by real owner.

Physical security is a fairly broad term that includes ensuring the safety of life and health of people and the preservation of their property. In this sphere, neural networks have been extensively applying for object and pattern recognition or the timely detection of dangerous objects or events. So, the government of certain countries is introducing systems that expand the capabilities of street cameras, performing the functions of searching for criminals or detecting offenses. There is also another way of intercalation artificial neural networks in ensuring security in physical range is the automation of physical access control systems.

The physical access control system(PACS) provides a hardware and software system for identifying and authorizing the identity of people who are trying to go to a protected area or gain access to sensitive information. ACS systems involve the use of sensors; currently, sensors for reading cards identifying a person are widespread. However, a duplicate of this card can be easily falsified and used for unlawful purposes. A more reliable way of identifying a person is identification by individual biological characteristics. Sensors for biological identification record the following types of individual signs: facial appearance, fingerprint, location of veins on the wrist, iris coloring.

I believe that to increase the accuracy of identification it is necessary to use several sensors at the same time, having reviewed all possible options, I consider that in addition to the camera of the visible spectrum to identify the appearance of the face, using the camera in the infrared spectrum to identify the heat map of the face will have an advantage. Also, this approach can give an advantage due to the use of the parallax effect. Consider the benefits that the parallax effect will bring. A stereo pair of images can make it possible to build a depth map of an object, which will can allow build a three-dimensional model, also therefore increase amount of data used for training and recognition, which will positively affect on accuracy. Also, the use of a stereo pair of images can reduce the relation accuracy on angle of rotation of the identified object. In addition, an important function of using a stereo pair can append possibility of determining an attempt to use a two-dimensional image as a key for identifying a person. Infrared sensor is also provides possible to detect an attempt to identify using a three-dimensional face model, because the model will not have the same heat map.

There are several basic types of artificial neural networks. However, the best indicators at the moment for pattern recognition tasks are shown by convolutional neural networks, CNN and deep convolutional neural networks, DCNN). An example of this can be AlexNet, GoogLeNet, VGG, and others that were presented as part of the Large Scale Visual Recognition Challenge (ILSVRC) [3].

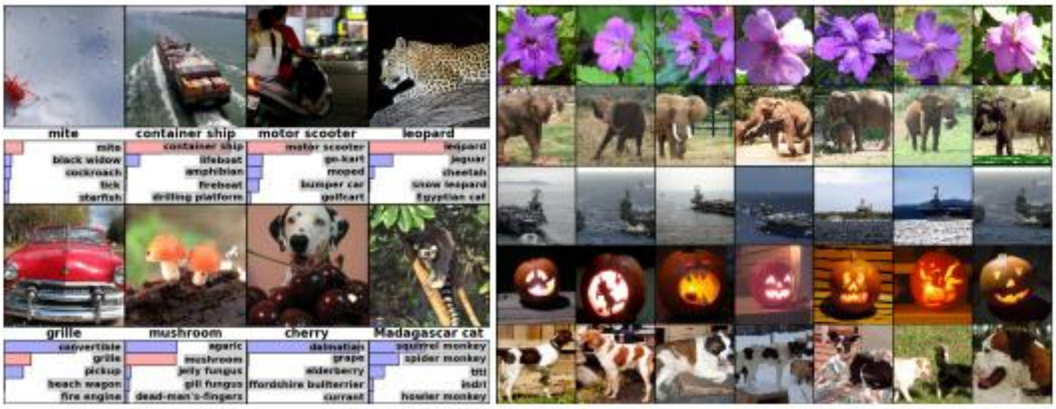

Fig. 1. Images what used in test ILSVRC-2010 [4]

According to the results of the competition, the results were obtained that when using deep convolutional neural networks, you can get the accuracy of determining images comparable to the accuracy of a person. The main idea of such networks is the use of the image convolution operation, which can display the similarity of functions in this case, the similarity of a part of the input image with some convolution kernel, this operation allow find crucial features [4]. Also, in add to convolution, the subsampling operation used, it allows reduce amount of processed information without significant data loss.

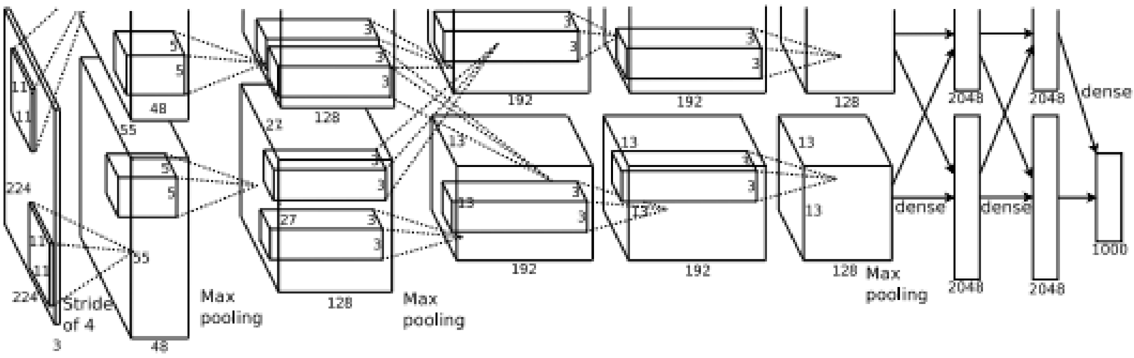

Fig. 2. An CNN architecture illustration [4]

Special attention is paid to the training algorithm is used in modern artificial neural networks [5]. This algorithm is called backpropagation, the essence of this method can be described as the development of the gradient descent algorithm, the essence of which is to find the function infinum, in our case error function, due to movement along their gradient. The main innovation of backpropagation is the correction of neural network weights starting from the penultimate one based on how much the gradient of the received value differentiate of clean value.

Conclusions. The wide possibilities of using neural networks in ensuring the safety of a pearson. ANN are broadly employ in all directions and successfully perform their functions increasing the reliability systems and the safety of people's lives. Given the low security of most modern access control management systems, I believe that the make use of ANN for automation purposes and for increase the reliability of these systems is justified. As a system sensor, it is necessary to use a stereo pair of images captured in different spectrum, one picture in visible spectrum and another one in the infrared. The main architecture design of such system with neural network should based on deep convolutional neural networks and with backpropagation algorithm for learning. This solution will allow high accuracy of identification of a person by a person’s face in a wide range of rotation angles, and will also be protected from attempts to penetrate by counterfeit identifying signs.

References

1. WHO. (2009). Global status report on road safety: time for action. [Online] Retrieved from: https://apps.who.int/iris/bitstream/handle/10665/44122/ 9789244 563847_rus.pdf

2. Tramer`, F., Kurakin, A., Papernot, N., Goodfellow, I., Boneh, D., and McDaniel, P. (2018). Ensemble Adversarial Training: Attacks and Defenses.

3. Krizhevsky A, Sutskever I, Hinton G E. (2012). ImageNet Classification with Deep Convolutional Neural Networks. Advances in Neural Information Processing Systems.

4. Domínguez A.(2015). A History of the Convolution Operation Vol. 6, pp. 1-49.

5. LeCun Y.(1998). Gradient-based learning applied to document recognition.

AUTHORS

Vladyslav Kostianikov – student, Department of Computer Engineering, National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”.

E-mail: VKostianikovIO51@office365.fiot.kpi.ua

Aleksandr Korochkin (supervisor) – Associate professor, PhD of Computer Science, Department of Computer Engineering, National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”.

E-mail: avcora@gmail.com