MSC 62M45 DOI: 10.14529/jcem160304

APPLICATION OF NEURAL CRYPTOGRAPHY IN SOLVING PROBLEMS OF INFORMATION SECURITY

T. S. Ambrosova[1], tanyambrosova@mail.ru,
N. D. Zulyarkina[1], toddeath@yandex.ru.
[1] South Ural State University, Chelyabinsk, Russian Federation.

The paper is devoted to consideration of the actual problems connected with cryptographic methods of data protection, based on the use of mechanisms of artificial neural networks. Characteristics, as well as various approaches in implementation of cryptographic problems with use of artificial neural networks, are researched. The detailed overview of the artificial neural networks applied as data protection methods is carried out.

Keywords: cryptography, neurocryptography, artificial neural network.

Introduction

Complexity and heterogeneity of modern information and communication systems simplify the access to information, both for certain users, and for the big organizations. At the same time ease and speed of access to data are security threats. Though cryptographic methods of data protection provide the sufficient level of safety, rapid growth of capacities of computing systems can raise a question of their reliability. It is essential to research and develop new methods and mechanisms of information security. The perspective direction for the solution of practical problems of information security is a research about use of the device of the artificial neural networks (ANN) [1].

1. Artificial Neural Networks (ANN)

Multilayer neural networks (MLP) can model function practically of any complexity degree. Moreover, the number of layers and number of elements in each layer define the complexity of function. To determine the number of intermediate layers and number of elements in MLP is an important question during construction. MLP networks consist of several layers of computing blocks connected with themselves by direct connections. It is possible to use various methods of training for training of MLP network. The most popular one is the method of return distribution of a mistake.

Networks with the return and incomplete feedbacks are networks, such as Hopfield's network or Elman or Jordan network [2], where the signal can extend on a cyclic way, therefore the output signal depends not only on an entrance signal, but also on time. Feedback can proceed either from output, or from the hidden layer of neurons. It leads to a possibility to account results of information transformation by neural network at the previous step for processing of an input vector at the following step of a network functioning. From the systems point of view, the network can be considered as a finite-state machine. It allows to model a dynamic behavior. The main disadvantage is a big consumption of memory in comparison with linear structures [3].

Generalized and regression neural networks (GRNN) are networks intended for solution of problems by means of nuclear approximation [4]. The GRNN network has two buried layers (Fig. 1). They are a layer of radial elements and a layer of elements, which form a weighted sum for the corresponding element of an output layer. Signal x_i are applied. Gaussian nuclear function φ_i is placed in the point of location of each training observation. Weight coefficients ω_i of each neuron are calculated. The sum of neuron outputs in RBF layer υ_i forms an output signal of one neuron with number i. Each observation demonstrates some confidence that the response surface in this point has a certain height, and this confidence decreases during the withdrawal away from the point. The observation located in a specific point of space is taken as some probability density. Clusters from close lying points show that a probability density is big in this place. A trust to density level is big near observation. In process of moving further away from it the trust decreases and approaches zero.

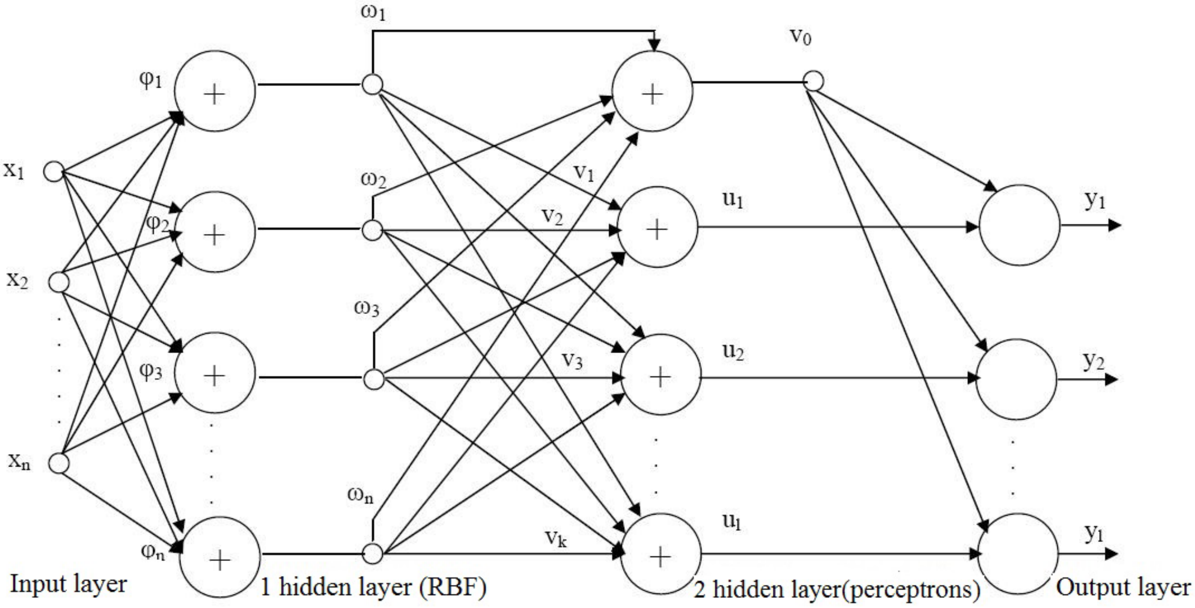

Fig. 1. Generalized structure of GRNN network

The output layer divides weighed sums into the sum of weights and issues the final forecast y_i. It is shown that, even with rare data in multidimensional space of measurements, the algorithm provides smooth transitions from one observed value to another [5,6].

The algorithmic form can be used for any regression problem in which an assumption of linearity isn't reasonable. The advantage of network is an almost instant training, because the network actually contains in itself all training data. On the other hand, such structure of a neural network is also its biggest disadvantage. Indeed, at large volume of the training data, the speed of network work falls, sometimes very significantly [7, 8], because of noticeable increase in complexity of an architecture.

Chaotic neural networks. Chaotic neural network is a single-layer recurrent network in which elements are connected with each other, without forming of a connection to themselves [9].

The behavior of elements in network is defined depending on chaoticity and correlative force of each cell. The cell leaves a cluster, when a chaoticity is high. On the other hand, each cell tends to remain in a cluster, when a correlative force among cells increases. If the level of chaoticity of each cell is constant, then the behavior of a cluster is defined depending on value of start state and correlative coefficient of each cell. If correlative coefficients among cells are high, then intercorrelations increase. As a result, the cluster is supported. Correlations among cells decrease, when correlative coefficients are small. Then distinctions of outputs of cells increase, and the cell falls out of the cluster.

2. Neurocryptography

Neurocryptography is a section of cryptography that studies the application of stochastic algorithms, especially neural network algorithms, for cryptoanalysis and encryption. An ability of neural networks to investigate space of decisions is used in cryptoanalysis. There is an opportunity to create new types of attacks to the existing algorithms of encryption, because any function can be presented by a neural network. One can crack an algorithm, then it is possible to find the solution, at least, theoretically. At the same time such properties of neural networks as mutual training, self-training, and stochastic behavior, and also low sensitivity to noise, inaccuracies are used [10].

Cryptography with use of ANN on the basis of von Neumann machine.The machine uses a recurrent network of Jordan [11]. The method of the return distribution of a mistake is used as a training mechanism. For encryption and decryption, a diagram of states is transformed to a table of states on the basis of which a training data set is generated. Input data include all possible entrances. Output data consist of the ciphered/deciphered data and transfer the machine to the following state.

An advantage of the solution of cryptographic problems is the following. Input and output data can have any type of relations, and the result depends on an initial state. The initial state is used as a key for encryption and decryption. If an initial state is unknown, then it is impossible to recover an initial data set even if tables or working sequence of states are known.

Consider the case of two states, such as it is unknown whether a state is "0" or "1". Then data can't be decrypted, and, therefore, the initial state works as a key [12].

Cryptography based on chaotic neural networks.The ANN model generates chaotic dynamics by means of the numerical solution of Chua chain [13]. Results of modeling show a dependence between chaotic dynamics of a network and amount of neurons in the hidden layer. There is no synchronization problem in this model of a neural network. Generation of a key for encryption and decryption of data is a result of the network work. A set of variations of chaotic dynamic is considered as an advantage of ANN, which is based on the chaotic generator. Results of modeling show that this model is rather effective, safe and can be used in systems of real time [14].

Use of ANN for implementation of hashing algorithms. The problem of an exchange of secret keys through an insecure channel can be solved using the algorithms of synchronization of neural networks. The multi-layer neural network of direct distribution and the chaotic map are used. A set of iterations of a piecewise linear function with the controlling parameter is applied as a chaotic map. A chaoticity of map is defined by a parameter value. It is shown in the paper [14] that output values of function are strongly differ in case of minor changes in input parameters, if a number of iterations of chaotic map is chosen rightly. To increase the number of operations required for hashing function calculation, a chaotic map is iterated only on input and output layers (more than 50 iterations are made). The hashing algorithm is constructed on the described above basis of the artificial neural network and the generator of keys. The generator of keys transform the user's key to a set of weight characteristics, offsets and the controlling parameters, for each layer. The algorithm transfers data of an arbitrary length to 128-bit value of a hash function. For this purpose the data is divided such that to be a multiple of the block having 1024 bits length. This block is given on an input of a neural network by the following algorithm. We add one "1" and remaining "0" in the last not multiple block. After that each block is given on an input of a neural network and the result is calculated.

In work [14] it is shown that the constructed algorithm of hashing with use of an artificial neural network has a property of sidedness, high sensitivity of output value to input data and the user's key. Moreover, the described algorithm is protected from attacks of "birthdays" and attacks of "a meeting in the middle".

Cryptography on the basis of GRNN networks. GRNN networks have three layers, each of which consists of several neurons depending on process type. An input message is divided into sequence of three bit data sets during encryption. There are 8 bits on the output after process of an encryption.

The results of modeling show more good result on productivity, than traditional methods of encryption. However, the test on cryptographic strength was not properly performed [15].

Conclusion

The considered cryptographic methods, which are realized with use of artificial neural networks, are capable to solve problems of classical cryptography, be applied to implement algorithms of an exchange of keys. Theoretical researches show a number of the advantages, which are connected, first of all, with complication of cryptanalysis of similar systems.

References

1. Ezhov A.A., Shumsky S.A. *Neurocomputing and Its Application in Economy and Business.* Moscow, MIFI Publ., 1998. (in Russian)

2. Zayentsev I.V. *Neural Networks: Main Models.* Voronezh, VGU Publ., 1999. (in Russian)

3. Boorakov M.V. *Neural Networks and Neurocontrollers.* SPb., GUAP Publ., 2013. (in Russian)

4. Specht D.F. The General Regression Neural Network – Rediscovered. *Neural Networks*, 1993, vol. 6, pp. 1033–1034.

5. Grubnik E.M., Lavrushin V.M., Uskov A.A. Simulation of Social and Economic Systems and Processes on the Basis of Device of Generalized Regression Neural

Network. *Fundamental and Applied Studies of the Cooperative Sector of Economics*, 2011, no. 1, pp. 58–63. (in Russian)

6. Soldatova O.P., Semenov V.V. Application of Neural Networks for the Solution of Forecasting Problems. *Electronic Scientific Journal "RESEARCHED IN RUSSIA"*, 2006, pp. 1270–1276. (in Russian)
7. Koshur V.D.,Pushkaryov K.V. Dual Generally-Regression Neural Networks for the Solution of Problems of Global Optimization. *Nauchnaya Sessiya NIYAU MIFI – 2010. XII Vserossijskaya Nauchno-Tekhnicheskaya Konferenciya «Nejroinformatika–2010»: Sbornik Nauchnyh Trudov. V 2-h Chastyah. CH. 2. – Scientific Session of NIYaU MIFI – 2010. XII All–Russian Scientific and Technical Neuroinformatics – 2010 Conference: Collection of scientific works. In 2 parts. P. 2.* Moscow, NIYaU MIFI Publ., 2010, pp. 219–227. (in Russian)
8. Kochetkova A.S. Application of Neural Networks for Safety Monitoring. *Science Journal of Volgograd State University Young Scientists' Research*, 2007, no. 6, pp. 163–166. (in Russian)
9. Kaneko K. Chaotic but Regular Posi-Nega Switch among Coded Attractors by Cluster-Size Variation. *Physical Review Letters*, 1989, vol. 63, issue 9, pp. 219. doi: 10.1103/PhysRevLett.63.219
10. Russell J., Cohn R. *Neural Cryptography.* VSD, 2013.
11. Jordan M.I. Serial Order: A Parallel Distributed Processing Approach. *Advances in Psychology*, 1997, vol. 121, pp. 471–495. doi: 10.1016/S0166-4115(97)80111-2
12. Bugayevsky M.Yu., Ponomarenko V.I. *Research of Chua Chain Behavior.* Saratov, GosUNTs "College" Publ., 1998. (in Russian)
13. Dalkiran I., Danis K. Artificial Neural Network Based Chaotic Generator for Cryptology. *Turk J Elec Eng & Comp Sci*, 2010, vol. 18, no. 2, pp. 240–255.
14. Chervyakov N., Evdokimov A., Galushkin A. *Application of Artificial Neural Networks and System of Residual Classes.* Moscow, Fizmatlit Publ., 2012. (in Russian)
15. *Neural Networks*, available at: http://www.statsoft.ru/home/textbook/modules/stneunet.html (accessed on 7 June 2016). (in Russian)

Tatyana S. Ambrosova, Undergraduate, Faculty of Mathematics, Mechanics and Computer Science, South Ural State University (Chelyabinsk, Russian Federation), tanyambrosova@mail.ru.

Natalya D. Zulyarkina, Doctor of Physics and Mathematics, Department of Differential and Stochastic Equations, South Ural State University (Chelyabinsk, Russian Federation), toddeath@yandex.ru.

Received June 27, 2016

УДК 004.056 DOI: 10.14529/jcem160304

ПРИМЕНЕНИЕ НЕЙРОННОЙ КРИПТОГРАФИИ ПРИ РЕШЕНИИ ЗАДАЧ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Т. С. Амбросова, Н. Д. Зюляркина

Работа посвящена рассмотрению актуальных проблем, связанных с криптографическими методами защиты данных, основанных на использовании механизмов искусственных нейронных сетей. Исследованы характерные особенности, а так же различные подходы в реализации криптографических задач с использованием искусственных нейронных сетей. Проведен детальный обзор искусственных нейронных сетей, применяемых в качестве методов защиты данных.

Ключевые слова: криптография, нейрокриптография, искусственная нейронная сеть.

Литература

1. Ежов, А.А. Нейрокомпьютинг и его применение в экономике и бизнесе / А.А. Ежов, С.А. Шумский. – М.: МИФИ, 1998.
2. Заенцев, И.В. Нейронные сети: основные модели / И.В. Заенцев. – Воронеж: ВГУ, 1999.
3. Бураков, М.В. Нейронные сети и нейроконтроллеры / М.В. Бураков. – СПб.: Изд-во ГУАП, 2013.
4. Specht, D.F. The General Regression Neural Network – Rediscovered / D.F. Specht // Neural Networks. – 1993. – V. 6. – P. 1033–1034.
5. Грубник, Е.М. Моделирование социально-экономических систем и процессов на основе аппарата обобщенно-регрессионных нейронных сетей / Е.М. Грубник, В.М. Лаврушин, А.А. Усков // Фундаментальные и прикладные исследования кооперативного сектора экономики. – 2011. – № 1. – С. 58–63.
6. Солдатова, О.П. Применение нейронных сетей для решения задач прогнозирования / О.П. Солдатова, В.В. Семенов // Электронный научный журнал «ИССЛЕДОВАНО В РОССИИ». – 2006. – P. 1270–1276.
7. Кошур, В.Д. Дуальные обобщенно-регрессионные нейронные сети для решения задач глобальной оптимизации / В.Д. Кошур, К.В. Пушкарёв // Научная сессия НИЯУ МИФИ – 2010. XII Всероссийская научно-техническая конференция «Нейроинформатика–2010»: Сборник научных трудов. В 2-х частях. Ч. 2. – М.: НИЯУ МИФИ, 2010. – С. 219–227.
8. Кочеткова, А.С. Применение нейронных сетей для мониторинга безопасности / А.С. Кочеткова // Вестник Волгоградского государственного университета. Серия 9. Исследования молодых ученых. – 2007. – №. 6. – С. 163–166.
9. Kaneko, K. Chaotic but Regular Posi-Nega Switch among Coded Attractors by Cluster-Size Variation / K. Kaneko // Physical Review Letters. – 1989. – V. 63, iss. 9 – P. 219.

10. Рассел, Д. Нейрокриптография / Д. Рассел, Р. Кон. – VSD, 2013.
11. Jordan, M.I. Serial Order: A Parallel Distributed Processing Approach / M.I. Jordan // Advances in Psychology. – 1997. – V. 121. – P. 471–495.
12. Бугаевский, М.Ю. Исследование поведения цепи Чуа / М.Ю. Бугаевский, В.И. Пономаренко. – Саратов: Издательство ГосУНЦ «Колледж», 1998.
13. Dalkiran, I. Artificial Neural Network Based Chaotic Generator for Cryptology / I. Dalkiran, K. Danis // Turk J Elec Eng & Comp Sci. – 2010. – V. 18, №. 2. – P. 240–255.
14. Червяков, Н. Применение искусственных нейронных сетей и системы остаточных классов / Н. Червяков, А. Евдокимов, А. Галушкин. – М.: Физматлит, 2012.
15. Нейронные сети, доступ: http://www.statsoft.ru/home/textbook/modules/stneunet.html (запрос 7 июня 2016).

Амбросова Татьяна Сергеевна, магистрант, факультет Математики, механики и компьютерных наук, Южно-Уральский государственный университет (г. Челябинск, Российская Федерация), tanyambrosova@mail.ru.

Зюляркина Наталья Дмитриевна, доктор физико-математических наук, кафедра дифференциальных и стохастических уравнений, Южно-Уральский государственный университет (г. Челябинск, Российская Федерация), toddeath@yandex.ru.

Поступила в редакцию 27 июня 2016 г.