Encryption System by Using BAM Artificial Neural Network

Angham Khalid Hussein
Al-Turath University Collage
Computer Science Department

Abstract

Data encryption is an important aspect Information security and protection the information against threats during its transferring in any communication network. Many techniques and methods are invented for this purpose ,one of this methods is to combine the artificial intelligent (A.I.) techniques with encryption methods, in this research an encryption system is built by using the BAM neural network which is one of the A.I. techniques and data encryption using a stream ciphering method with secure random key to protect information and increase the complexity of encryption process so become difficult to decrypted . In this system, the equations has been applied with input secret random key as input weight matrix for the BAM neural network and result an output encrypted secure information. A C++ programming language are used for this work.

العصبية الذكية (BAM) نظام تشفير باستخدام شبكة

م.م.انغام خالد حسين

قسم علوم الحاسوب

كلية التراث الجامعة

الخلاصة

ان تشفير البيانات يعتبر ناحية مهمة من نواحي حماية المعلومات ضد أي تهديدات اثناء نقلها ضمن شبكات الاتصالات.وهناك عدة طرق من اجل تحقيق هذا الهدف ,واحدة من هذه الطرق هي دمج تقنيات الذكاء الصناعي مع طرق التشفير.في هذا البحث تم بناء نظام باستخدام شبكة BAM العصبية الذكية بالدمج مع طريقة Stream Ciphering باستخدام مفتاح تشفيرعشوائي خاص من اجل حماية المعلومات وزيادة تعقيد عملية التشفير مما يؤدي الى صعوبة فك التشفر. في هذا النظام تم تطبيق المعادلات الخاصة بشبكة BAM العصبية الذكية واستخدام مفتاح التشفير السري العشوائي كمصفوفة وزن مدخل الى الشبكة وينتج عنها المخرجات والتي هي معلومات مشفره. تم استخدام لغة C++ البرمجية في بناء برنامج من اجل تنفيذ هذه العمل.

1-Introduction

Nowadays, information security has become an important aspect in every organization. The people have to be assured that the information is to be read by only the sender and the receiver. So, the basic need is to implement cryptography which can make use of an Artificial Neural Network. Artificial Neural Networks (ANNs) are simplified models of the central nervous system as shown in figure 1. They are networks of highly interconnected neural computing elements that have the ability to respond to input simulated. Among the capabilities of ANN, are their ability to learn adaptively from dynamic environments to establish a generalized solution through approximation of the underlying mapping between input and output. Neural networks can be regarded as a black-box that transforms an input vector of m-dimensional space to an output vector in n- dimensional space. This makes them ideal tools for black-box system identification [1].

Cryptography is the science of writing in secret code and is an ancient art. Cryptosystems are helpful for maintaining the integrity, confidentiality, and authenticity of all the information resources. This is very necessary to secure the data and resources from disclosure, to assure the authenticity of data and to secure systems from web - based attacks [2].in this paper a BAM network which is one of ANN type are used with random key encryption method in creating the cryptosystem for data encryption .

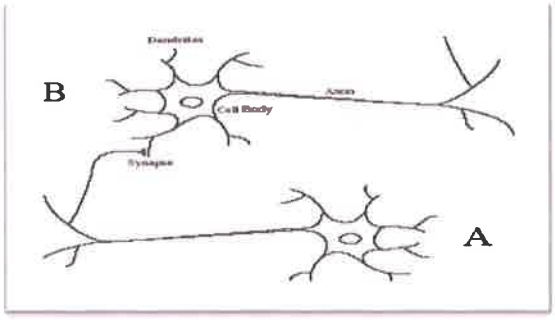

Figure 1

2- BAM Network:

Bidirectional associative memory (BAM) is a type of recurrent neural network. BAM was introduced by Bart Kosko in 1988. There are two types of associative memory, auto-associative and hetero-associative. BAM is hetero-associative, meaning given a pattern it can return another pattern which is potentially of a different size. It is similar to the Hopfield network in that they are both forms of associative memory.

2.1 The BAM Architecture

The BAM (Bidirectional Associative Memory) implements interpolative associative memory and consists of 2 layers of neurons fully interconnected. The figure 2 shows the net as M(x) =y but the input and output may swap places, i.e. the direction of connection arrows may be reversed and y play the role of input, using the same weight matrix Considering the weight matrix W then the network output is y = Wx, i.e. the activation function is identity f(x) = x. According to (1), the weight matrix may be build using a set of orthogonal {x} and the associated {y}, as:

$$W = \sum_{p=1}^{P} y_p \, x_p^T \qquad (1)$$

If the {y} are also orthogonal then the network is reversible. Considering y layer as input then: $x= W^T$ [3].

Y

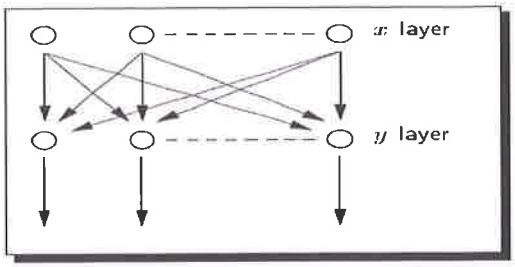

Figure 2

2.2 Network Running:

The BAM functionality differ from others by the fact that weights are not adjusted during a training period but calculated from the start from the set of vectors to be stored $\{x_p , y_p\}_{p=1,P}$.

The procedure is developed for vectors belonging to Hamming space H. Due to the fact that most information can be encoded in binary form this is not a significant limitation and it does improve the reliability and speed of the net.

The information is propagated forward and back between layers x and y till a stable state is reached and subsequently a pair {x`, y`} belonging to the set of exemplars is found (at the output of x respectively y layers).The procedure is as follows [4,5] :

- **At t = 0 the x(0) is applied to the net and the corresponding y(0) = Wx(0) is calculated.**

- **The outputs of x and y layers are propagated back and forward, till a stable state is reached, according to the formulas (for convenience $[W(:; i)]^T \equiv W(:; i)^T$) :**

$$x(t+1) = \text{sign}\,(W^T y(t)) + |\,\text{sign}(W^T\, y(t))|^C .\, x(t)$$

$$y(t+1) = \text{sign}\,(Wx(t+1)) + |\,\text{sign}(Wx(t+1))|^C .\, y(t) \qquad (2)$$

When working in reverse y(0) is applied to the net, $x(0) = W^T\, y(0)$ is calculated and the formulas change to:

$$y(t+1) = \text{sign}(Wx(t)) + |\,\text{sign}(Wx(t))^C|\, .\, y(t) \qquad (3)$$
$$x(t+1) = \text{sign}(W^T y(t+1)) + |\,\text{sign}(W^T y(t+1))|^C .\, x(t)$$

Encryption by using BAM Network:

A random secret key is generated to encrypt the input text this key is generated by using BAM network just like the method the weight generated and updated using initial input weights ,a stream ciphering method is used as encoding method to encode then input text to BAM network by using the key resulting from the BAM network, and here the encryption algorithm mean steps :

1- **Reading the input text message.**
2- **Preparing the weight matrix to fit the size of the input text.**
3- **Generate a random keys matrix in the same size of weight matrix.**
4- **Calculate the initial value y(0) and x(0) as in equation (1).**
5- **Calculate the x(t+1)than calculating y(t+1) as in equation (2).**

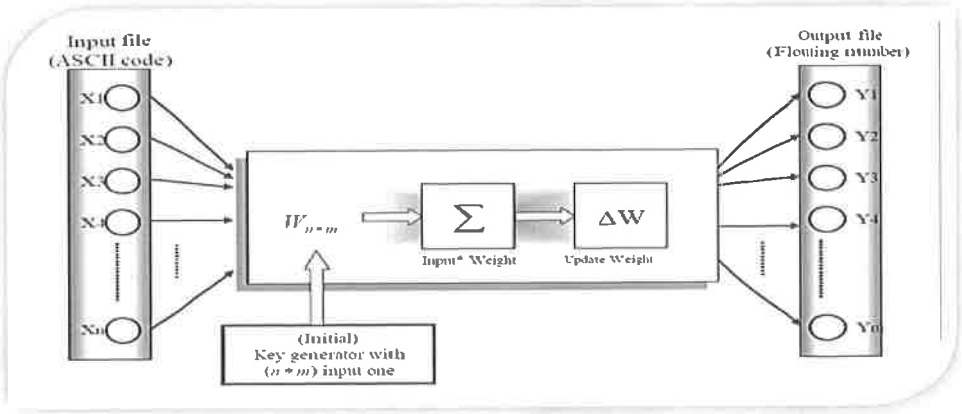

Figure 3

2-4 Encryption algorithm application example:

The text message (my computer) is encrypted and the result is shown in the table 1:

Table 1

m	Y	-	c	o	M	p	u	t	e	r
293	-503	-53	219	-30	-755	128	-759	-267	41	43

3- Conclusions and Future works:

Good information protection against many attacks during its transferring in any media is provided by using the benefits of ANN. Also the time required for encryption is relatively small. The next step

is using the same system to decrypt the information and trying to calculate the required time for this process.

References:

[1] Khaled M. Alallayah, Waiel F. Abd El-Wahed, Mohamed Amin and Alaa H. Alhamami ,"Attack of Against Simplified Data Encryption Standard CipherSystem Using Neural Networks", Journal of Computer Science 6 (1): 29-35, 2010 ISSN 1549-3636.

[2] Navita Agarwal, Prachi Agarwal, " Use of Artificial Neural Network in the Field of Security", MIT International Journal of Computer Science & Information Technology Vol. 3, No. 1, Jan. 2013, pp. 42–44 ISSN 2230-7621.

[3] Ugur Halici, "Artificial Neural Network", pp.43-58 , EE543 Lecture Notes. METUEEE , Ankara.

[4] R. M. Hristev, "The ANN Book",Edition 1, 1998.

[5] clien-pen chuang ,tin-ying and li-cliye, "Encryption and Decryption With Space Transformation for Bio-Directional Associated Memory", IEEE international conference,2008,pp.121-125.