ARTICLE OPEN

Multistage encryption system using bidirectional associated memory neural network

Assitent.lecture. Angham k.hussein

Al-turath University College

Corresponding Author email: Angkhalid23@gmail.com

Abstract:

In this paper an encryption system is designed .this system is in two stage in each stage an neural network of (BAM) are used. the purpose of using neural network is to increase the complexity of encryption process so the decryption will be complicated and the original information will not easily discovered.

Keywords: ANN: artificial neural network. ,BAM: bidirectional associated memory.

1 Introduction:

Information security is generally essential to modern business and technology, both for privacy of transactions and communications, as well as for defense against malicious intruders. Cryptography is the study of information security and the feasibility of communication over an insecure channel while preserving the secrecy of the information transmitted. Cryptographic techniques should offer at least the three security features concerning data transmission: confidentiality, authentication and integrity. Confidentiality is fundamental third parties are expected to see the encrypted data but should not be able to decipher it. Authentication methods allow the receiver to verify that the sender is legitimate. Integrity of the transmitted data must be verifiable, i.e., the receiver should be able to check that no part of the message was lost or altered during transmission. As the sophistication of cryptanalytic attacks increases and their cost decreases, there is constant pressure to improve cryptographic methods on all three of these fronts [1].

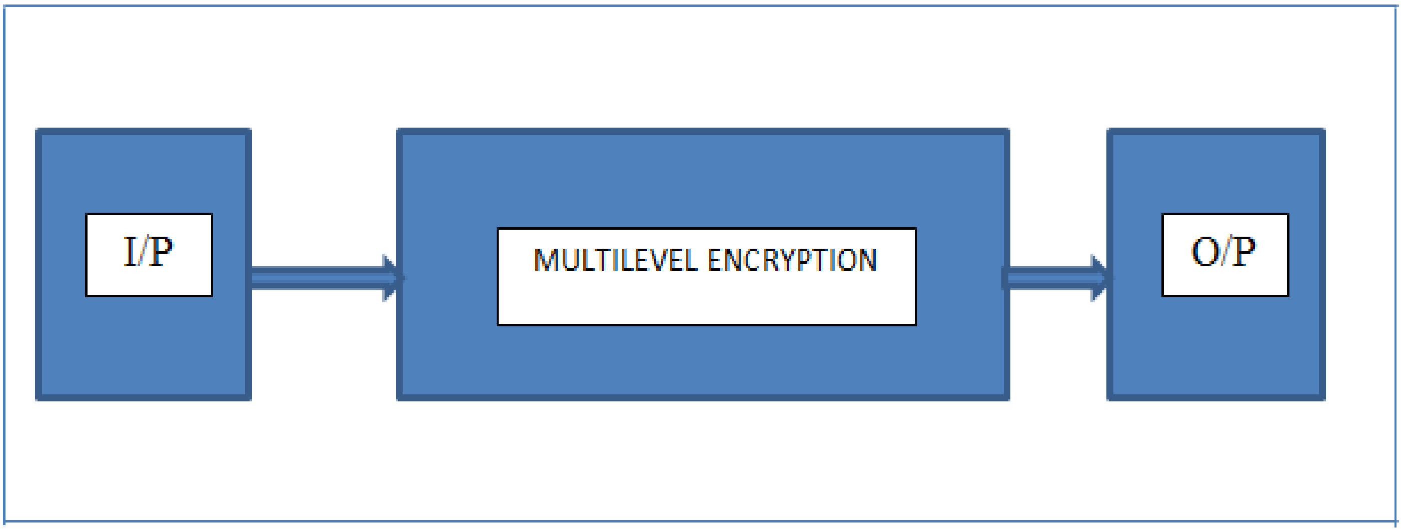
Work on artificial neural network has been motivated right from its inception by the recognition that the human brain computes in an entirely different way from the conventional digital computer. The brain is a highly complex, nonlinear and parallel information processing system. It has the capability to organize its structural constituents, known as neurons, so as to perform certain computations many times faster than the fastest digital computer in existence today. The brain routinely accomplishes perceptual recognition tasks, e.g. recognizing a familiar face embedded in an unfamiliar scene, in approximately 100-200 ms, whereas tasks of much lesser complexity may take days on a conventional computer [2].

Neural network has important feature which is the capability of learning and explore the solution space of the problem to gain the best result. This feature are used in many fields one of these fields are cryptosystems where a single layer neural network consist of input values ,a set of weights that changed according to learning algorithm and activation function and output .Bidirectional associative memory (BAM) is a type of neural

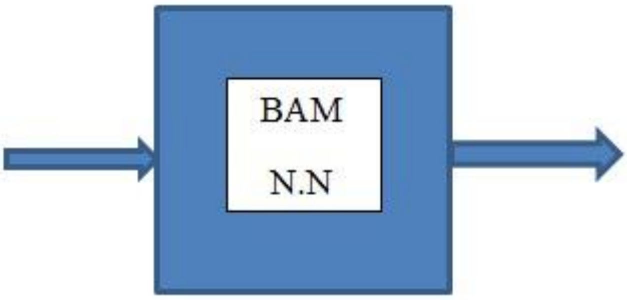
Network BAM was introduced by Bart Kosko in 1988. BAM is hetero-associative, meaning given a pattern it can return another pattern which is potentially of a different size. It is similar to the Hopfield network in that they are both forms of associative memory.[3]

2 Encryption system

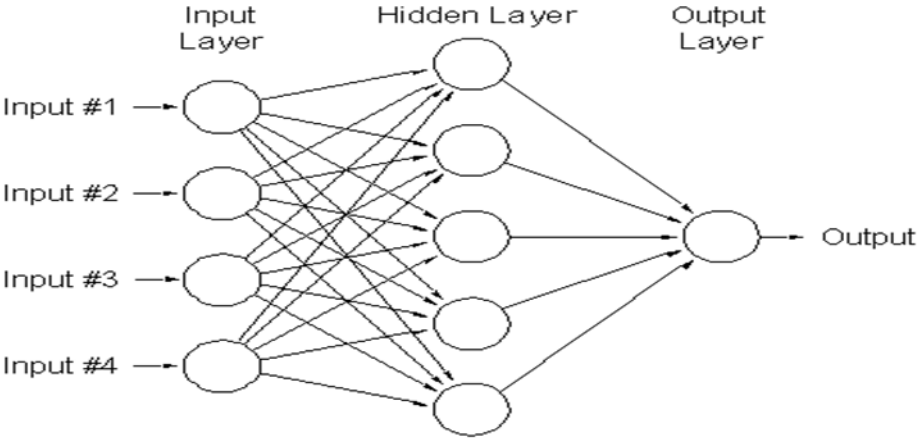
Cryptography has interest of building systems with high security of information, to gain this level of security. The encryption key must have many heavy calculations to grantees the immunity against decipher. The power of any encryption system are lying in the complexity and the number of stages of that system for this purposes a multistage symmetric key encryption system with neural network are used, the BAM neural network are chosen .The system consist of three stages as shown in fig(1) , the first stage is the input ,the second stage is the cyphering stage ,and the third one are the output



Fig(1) Encryption System Stages Each stage consist of the following:



Fig(2) Content of a single stage The BAM N.N are as shown in the fig (3):



Fig(3) BAM NN architecture

The BAM functionality differ from other neural network 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 information is propagated forward and back between layers x Andy 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)[4].

3 Practical application and Results:

The system are consist of 2 level of encryption each level has an input stage as a first stage and second BAN NN stage and output .The output of the first stage will be as input to the second stage as shown in the fig(4) below

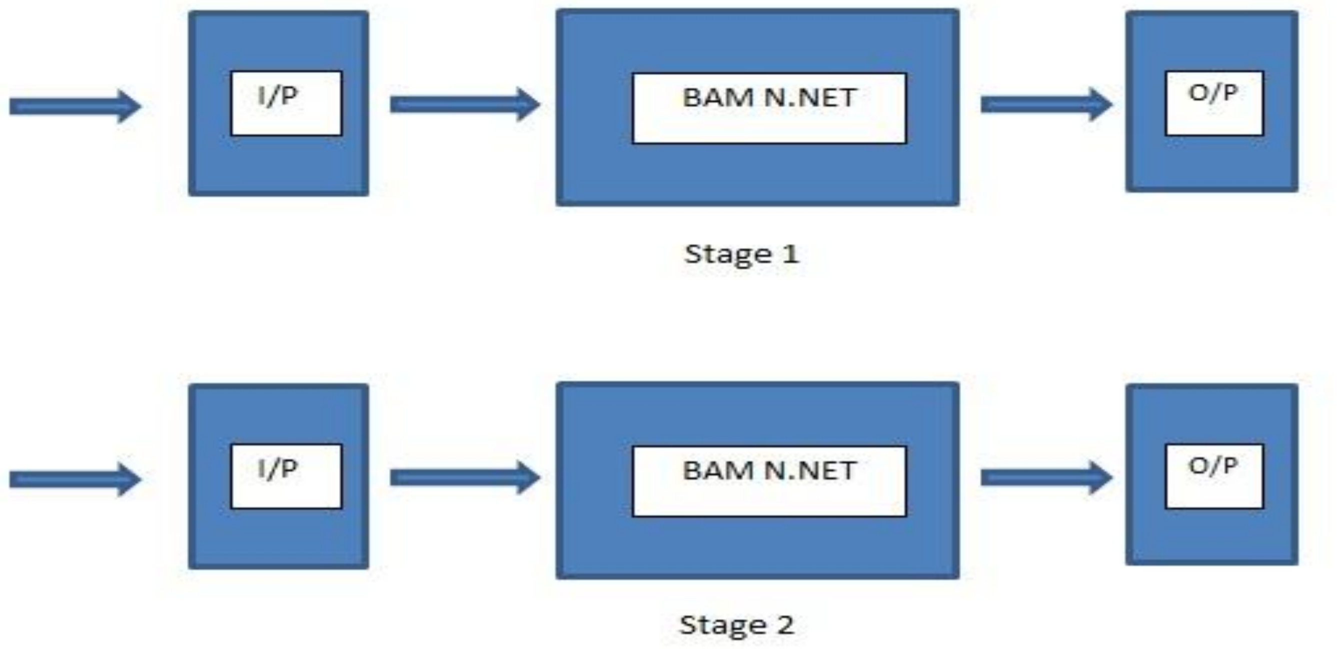


Fig (4) encryption system

Our input of the first stage is any text message ,each letter is converted to ASCII code and then each code to 64 bit stream long to by ready for the next stage, in the next stage each bit is multiplied by initial weight which is chosen randomly between (0~1) as shown in the Eq.1

$O/P1=\sum W_{ij} *Xi$ ……. Eq.1

Each weight (W_{ij}) are updated as shown in Eq.2

$W_{new}=W_{old}+\Delta W$ ……. Eq.2

Where Wnew is the new updated weight, Wold is the weight of previous iteration and ΔW is determined by the Eq.3

$\Delta W = X_{ij}*Y_{ij}$ …. …... Eq.3

Where X_{ij} is the input and Yij is the output [3]

This process is continue until there is no more weight update and weight remain constant at this point the output of the first stage is move to the input of the second stage and the same process of the first stage are applied on the seconds stage. The result of the first stage are shown in the following table (1)

Table (1) input data and output result.

Input	**Encryption result of first stage**	**Encryption of second stage**
h	**16.6420**	**13.1794**
e	**61.2911**	**56.4989**
L	**52.4861**	**38.7456**
l	**96.2603**	**16.9674**
o	**84.5927**	**34.3198**
W	**22.5688**	**13.3960**
O	**21.4709**	**10.6614**
R	**77.7734**	**69.9782**
l	**32.6986**	**26.8661**
d	**54.1674**	**34.9331**

4 Conclusion and future work:

To obtain more protection for information it is necessary to use a high complicate encryption technique for this reason a multistage are used and to increase the complexity the neural network at each stage are applied. For future it is possible to add more stages and use different type in each stage.

5 Reference

[1]"Cryptography using artificial neural network",Swsaen S.Abod,Depattmrnt of chemistry science, collage of ibn alhaitham, dananeer journal,pages:388-402.

[2]"Cryptography using artificial neural network", Vikas Gujral project report submitted to Department of Electronics and Communication Engineering National Institute of Technology

[3]"Bidirectional Associative Memories", Bart Kasko, IEEE transection on systems, man and cybernet ,Vol 11, No 8.

[4]"Encryption using BAM neural network", Angham K.hussein,Al.Turath university college journal,Vol.2014,Issue 15,Pages 53 -61.