SECURED COMMUNICATION SYSTEM WITH NEURAL ENCODER

Mahmoud I. Abdalla

Dept. of Electronic and Electrical Communication, Zagazig Univ., Egypt.

نظام اتصال مأمون بإستخدام الدوائر العصبية

الملخص العربى

هذا البحث يعرض نظام اتصال بإستخدام الدوائرالعصبية؛ فقد أمكن استخدام خواص الدوائر العصبية فى تصميم وحدتى تشفير يمكن ان تستخدم فى الاتصالات السرية و التطبيقات العسكرية؛ و تم تحسين هذا النظام بإستخدام خوارزم encryption/decryption و قدأستخدم خوارزم

generalized delta rule for feed forward with back propagation لتعليم الدوائر العصبية

وتم تحليل ودراسة أداء النظام و وحدات التشفير عند قيم مختلفة من نسبة شدة الأشارة الى شدة الضوضاء كما تم دراسة تأثير الضوضاء على هذا النظام عن طريق المحاكاه ؛ و البحث يوضح كيفية وخطوات تصميم وحدات التشفيرو وحدات فك التشفير حتى يمكن تنفيذ ذلك لمن يرغب فى حالات الاتصالات السرية. و أجريت مقارنة بين أداء شفرة الخلايا العصبية و الشفرات التقليدية وقد وجد أن كسب الشفير لشفرة الخلايا العصبية هو 5 ديسبل عند احتمال خطأ مقداره 10^{-4}و10^{-8}و البحث يقدم دراسة عملية وتطبيقية لنظام اتصالات جديد.

ABSTRACT

A Secured communication system with neural encoder /decoder is designed and enhanced by providing an Encryption and Decryption algorithm based on a one-dimensional reversible cellular automata.. The capabilities of neural networks are used to design a neural encoder /decoder for secured data communications. The generalised delta rule for feed forward with back-propagation technique is used for designing the neural network. Using computer simulation the performance of the system is evaluated for different signal to noise ratios. The design algorithm of the neural encoder /decoder together with the encryption decryption algorithm is given Comparisons between the performance of neural decoders and that of several conventional ones are discussed. At probabilities of error of 10^{-4} and 10^{-8}, the neural coding gain is found to be about 5 dB.

Accepted August 3. 1998

1. INTRODUCTION

Digital communication systems have three types of coding namely; source codes, secrecy codes and error control codes (also called channel codes). The source codes include codes used to format the data for specialised modulator. Secrecy codes encrypt information so that the information cannot be understood by anyone except the intended recipient. Channel codes are used to increase its immunity to noise. This is accomplished by inserting controlled redundancy into the transmitted information stream[1] that leads to a decrease in the information transmission rate. Such rate can be increased by using the neural coding. As electric communication replaces written communication, security becomes increasingly important, it must be assured that only the intended receiver can extract the message. An artificial neural network can be trained to recognise a number of patterns. If a version of one of these pattern, is corrupted by noise, and then presented to a properly trained network, the network can provide the original pattern on which it was trained[2].

Any task that can be done by traditional descriminant analysis can be done at least as well (and almost always much better) by neural networks[2]. Also neural networks can be used as a prediction tool. Neural networks are non-linear parametric models that can approximate any input-output relation. Coding is to convert M possible messages into M possible codewords. The codewords should be selected to achieve objectives such as efficiency and security. Neural networks can be used to satisfy the function of the encryption and the channel codes to form a neural communication system. For various applications, the generalised delta rule for feed-forward with back-propagation technique can be used for designing the neural network[3,4,5]. The learning paradigm is summarised in reference[6]. The widest application of this code may be in military communication systems

2 .SYSTEM OVERVIEW

The proposed Secured communication system consists of a transmission Subsystem, the Communication channel and the receiver Subsystem. The transmission Subsystem consists of the following stages:

1- A private key encryptor to receive a frame 2L bytes in Length and to produce the Ciphered frame with the same length.

2- A Dequeue System to receive the Ciphered frame and present it one nibble at a time to the Neural encoder.

3- The Neural encoder which maps the input nibble into a code vector.

The receiver will consist of equivalent subsystems to map the transmitted code vector into the equivalent message nibble, followed by an Enqueing system to form the Ciphered frame which is then decrypted using the Encryption Key

3. DESIGN TECHNIQUE

3.1 The Encryption/Decryption Systems

In the present design, we use an encryption/decryption algorithm based on Time Reversal Transformation [7] in One-dimension. The advantages of this algorithm are its computational simplicity, conservation of information, high performance (can be implemented as a parallel algorithm) and the possibility of having keys as arithmetic functions which provides astronomical numbers for the possible key combinations. In ref. [7], such algorithm has been modelled as N-D Reversible Cellular Automata. In the 1-D case, a simple rule (key function) can be used to encrypt a Symbol (byte) using its immediate neighbours.

The encryption/decryption Scheme is designed to receive a frame of symbols U and using the Time Reversible Transformation[7]:

$$U_i(t-1) = f[\{U_i(t)\}] - U_i(t-1) \bmod 2 \qquad (1)$$

with the key function operates on the symbol and its immediate neighbours.

$$f[\{U_i(t)\}] = W_1 U_{i-1}(t) + W_2 U_i(t) + W_3 U_{i+1}(t) \qquad (2)$$

where W_1, W_2, W_3 are arbitrary key weights. The time evolution of the above scheme is completely reversible and the entropy of the frame increases linearly with time steps (t). Notice that the Decryption System will follow the same outlined steps since the algorithm is completely reversible

3.2 The Neural Transmitter

Fig. (1) illustrates the neural network that is used to design the neural encoder. Different structures of hidden layers with different nodes were tried. The proper structure is fouud to be two hidden layers with twenty uodes such that the error can be minimised rapidly. The generalized delta rule formulated by Rumelhart, Hinton , and Williams (1986)[9,10] is used for learing the network.

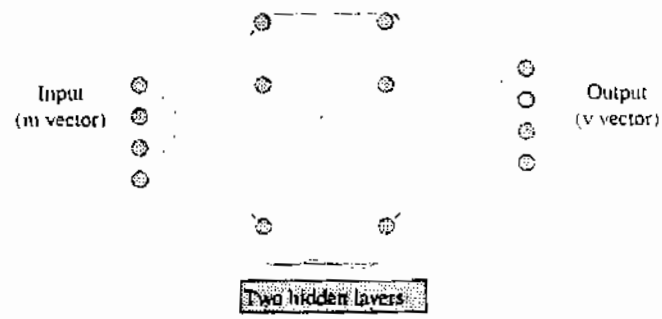
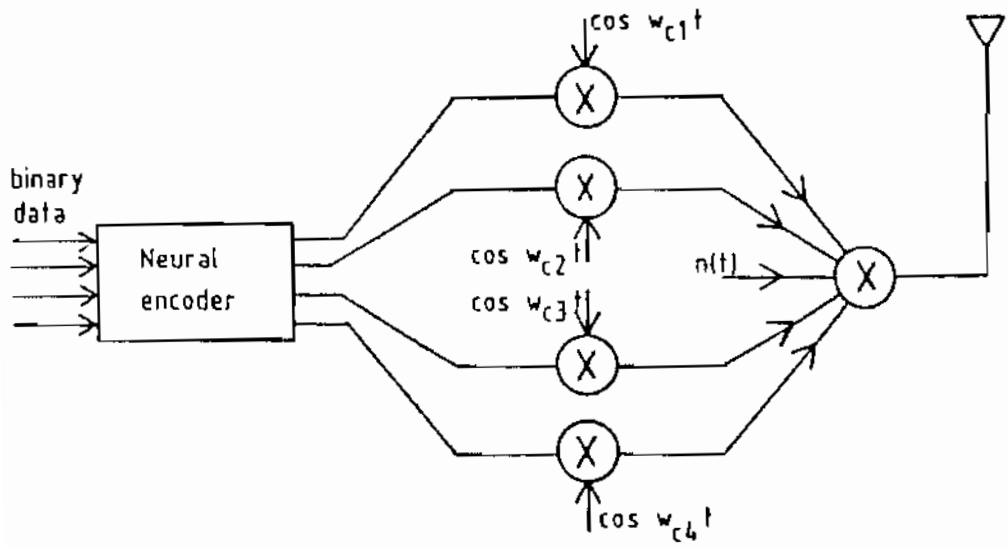


Fig. (1) Neural Encoder Architecture

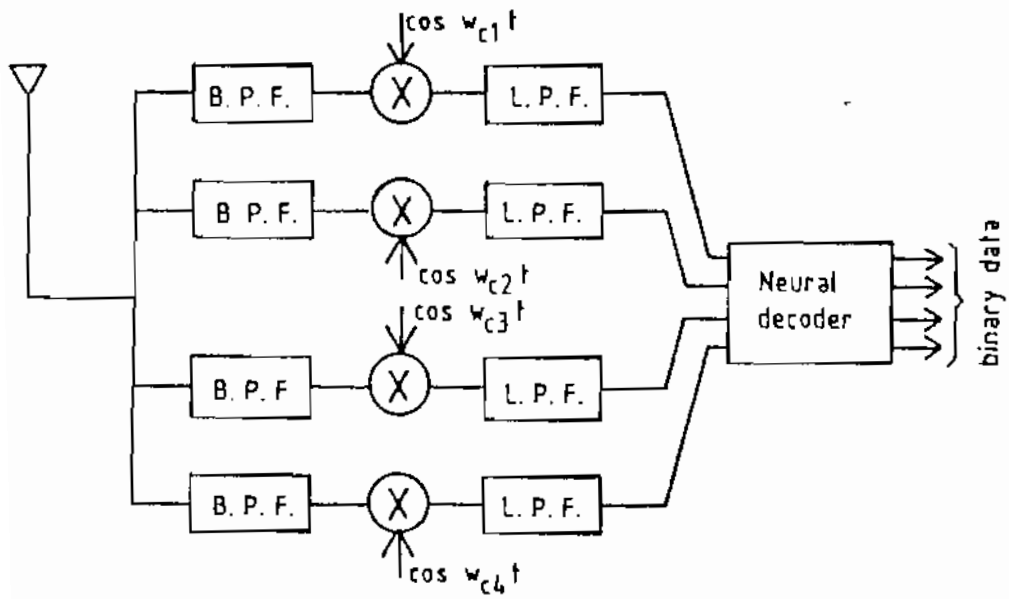
Let $m = \{m_1, m_2, m_3, m_4\}$ be the input information bits and $v = \{v_1, v_2, v_3, v_4\}$ be the encoded-word, the neural network has to map the vector m into a vector v at the transmitting side of the communication system. At the receiver the neural decoder has to map the vector v into vector m. Fig. (2) shows the block-diagram of a neural data transmitter. The encoder has 16 possible messages. The code vectors are shown in Table (1).The code vectors have been chosen randomly, however the hamming distance between any pair is 4. It is to be noted that the transmitted signal is in a form similar to that of PAM, thus any unauthorised receiver will not be able to extract the transmitted information.

The design algorithm of neural encoder can be summarised as follows:

1- Choose the number of code messages to be coded and form the code messages.



a- Neural encoder communication system



b- Neural decoder communication system

Fig. (2) Neural encoder/decoder communication system

2- Form code words of the encoder such that the hamming distance between two codes words is as large as possible.

3- Design the neural network architecture with the number of input nodes N such that:

$M=2^N$. where M is the number of codewords. The neural network output layer will also have N nodes.

4- The ciphered nibbles will be the input to the neural network while the associated codewords will be the output.

5- Design the neural network to obtain the weights of the neural network.

6- Implement the neural encoder using software or hardware technique.

Table (1) Encoder code-vectors

Code-vector	Code-Word
0 0 0 0	.5 .1 .6 .8
0 0 0 1	.2 .4 .2 .6
0 0 1 0	.4 .6 .3 .7
0 1 0 0	.3 .3 .9 .5
1 0 0 0	.8 .5 .7 .2
0 0 1 1	.7 .2 .8 .55
0 1 1 0	.2 .9 .5 .3
0 1 0 1	.8 .7 .85 .8
1 0 0 1	.5 .18 .5 .9
1 0 1 0	.1 .8 .6 .8
1 1 0 0	.3 .7 .2 .4
0 1 1 1	.25 .85 .1 .5
1 1 0 1	.4 .1 .7 .2
1 1 1 0	.85 .25 .15 .6
1 0 1 1	.1 .9 .8 .1
1 1 1 1	.6 .7 .3 .9

3.3 Neural Receiver

The neural decoder is built using the same neural architecture (see Fig. (3)). After adjusting the weights, the network was tested. On the basis of experimental results, it has been considered that if the output is greater than .7, then it will be considered one (1 binary) and if it is less than .5 it will be considered zero (0 binary). The network can easily recognise the inputs and map it into the original message. The network maps the vector v={v1, v2, v3, v4} into the vector m={m1, m2, m3, m4}. The neural receiver is shown in Fig. (2-b).

The design the decoder follows the same steps for the design the neural encoder expects that the input to the neural network will be the code-word while the output will be the ciphered message.

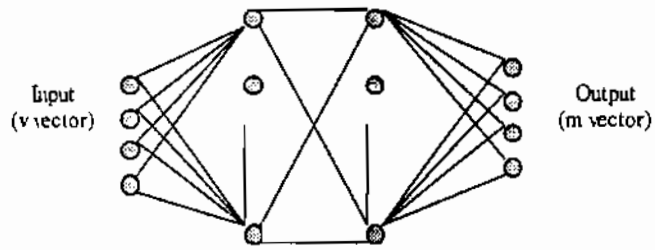


Fig. (3) Neural Decoder Architecture

3. RESULTS AND CONCLUSION

After adjusting the weights, the network can easily recognise the input and map the input messages to the code-words at the transmitting terminal. Four bits are transmitted at the same time and there is no parity check bits. So the coded-word has the same number of bits as the uncoded one. Hence the rate of information transmitted is the same in the two cases with the same bit duration. The neural network maps the input vector m={ m1, m2, m3, m4 } into the code-word vector v={v1, v2, v3, v4} without mistakes. The vector v can be transmitted using four different carriers (carrier for each information bit). Frequency synthesisers can be used to generate the carrier frequencies required. Frequeney hopping techniques can be applied to increase the security as well as obtaining its advantages[11].

Computer simulation is used to investigate the performance of the neural receiver. Since the input bits are transmitted at the same time, we assumed that the input bits are subjected to the same noise level. The neural decoder is trained with 192 input patterns with different noise levels.

The probability of error is given by[12,13]:

$$P(e) = P(x>a) = \int_{\sigma}^{\infty} \left(\sqrt{2\sigma^2\Pi}\right) e^{-\left[x^2 \; 2\sigma^2\right]} dx \qquad (4)$$

where σ is the variance of the random variable x

$$P(e) = P(x>a) = \int_{a\;\sigma} \left(\sqrt{2\Pi}\right) e^{-\left[x^2 \; 2\right]} dx \qquad (5)$$

The value of the variance a/σ is calculated at different signal to noise ratios.

Using this computer simulation the value of a is calculated. The value of variable a {in equ. (5)} is the maximum noise level at which the performance of the decoder is perfect. The probability of error is obtained using equ. (5). Fig. (4) shows the probability of error for various SNR for the two cases, namely, the neural system, and the conventional one. Clearly coded transmission results in low probability of error than uncoded transmission that uses ASK modulation technique overall signals to noise ratios. A comparison between the probability of error for coded transmission using neural code and coded transmission using block-code (4,7)is given in Fig. (5). Clearly the probability of error in the case of neural coding is lower than that of block-code.

Table (2) gives the coding gain for various coding techniques when referred to binary PSK transmission system for the two values of p(e), namely, $p(e)=10^{-5}$ and 10^{-8}[14].

The coding gain is used as the basis of comparison. The coding gain refers to the number of dB that the signal to noise ratio can be reduced from the value required when there are no coding and still provide the same bit error rate. This means that the coding gain A is:

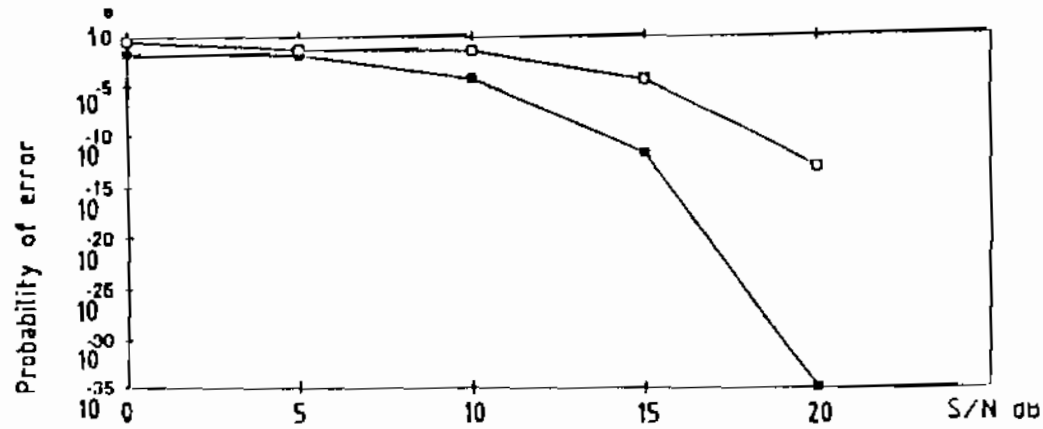


Fig. (4) Probability of error for neural decoder and uncoded using ASK modulation technique.

neural coding
uncoded ASK

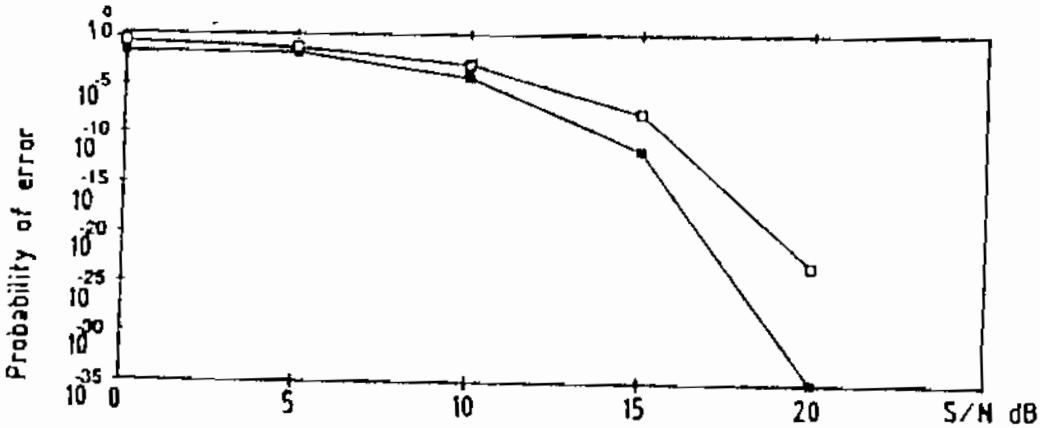


Fig. (5) Comparison between the probability of error of neural coding and block coding.

neural coding
block coding

$$A = \frac{[\text{signal to noise ratio}]_{\text{intended}}}{[\text{signal to noise ratio}]_{\text{coded}}}$$

The neural communication system is a secure code with high rate of information and it has low probability of error with coding gain of 5 dB at $p(e)=10^{-5}$and 10^{-8}. The system parameters were changed step by step and test the neural network by the input code vectors The tolerance of the input weights is found to be 3.5% for the input and output weights while it is 4.5% for the weights between the two hidden layer

Table (2) Comparison of coding techniques on a Gaussian channel

coding technique	coding gain	
	$P(e)=10^{-5}$	$P(e)=10^{-8}$
Neural codes	5	5
Block codes (hard decision)	3- 4	4.5 - 5.5
Convolutional coding with sequential decoding	4- 5	6 - 7
Convolutional coding with viterbi decoding	4- 5.5	5 - 6.5

4- REFERENCES

1- Wieker, Stephen B., "Error Control System for Digital Communication and Storage "Prentice-Hall, Inc,USA.1995.

2- Masters, Timothy. "Practical Neural Network Recipes in C++ Academic Press, Inc. Newyork, 1993.

3- Werbos. P. J.. "Backpropagation Through Time: What it Does and How to Do it", Proceedings of the IEEE, Vol. 78, No. 10, October 1990.

4- Nguyen, D. H. and Widrow B., " Neural Networks for Self- Learning Control Systems", IEEE Contr. Syst. Mag., vol. 10, No. 3, April 1990.

5- Beale, R. and Jackson, T., "Neural Computing: An Introduction", Adam Hilger (IOP), New York 1990.

6- Abdalla, M. And Abo-Elfadel, M. "Modelling Traffic Noise with Neural network" The Egyptian Computer Journal ISSR, Cairo Univ., Vol.22,No.1,1994.

7- Goneid, A., "Image Encryption using N-Dimensional Reversible Cellur Automata", Proc. IASTED Int. Conf. On Modelling, Simulation & Identification. Wakayama, Japan, 1994,100-103.

8- William A. Shay "Understanding Data Communication and Networks", PWS publishing Company, 1995.

9- Pao, Y., "Adaptive Pattern Recognition and Neural Networks", Addison-Wesley Publishing Company, Inc., New York 1989.

10- Bhat, N. N., Minderman, P. A., Jr., McAVOY, T. and Wang, N. S., "Modelling Chemical Process Systems Via Neural Computation:, IEEE CONTR. Syst. Mag., vol. 10, no. 3.April 1990.

11- Simmon, M. K., Huth, G. K. And Polydoros, A., "Differentially Coherent Detection of QASK for Frequency Hopping Systems -part 1", IEEE Transaction on communication, Vol.com-30, N0. 1, January 1982.

12- Shanmugan, K. S., "Digital and Analogue Communication Systems", John Wiley & Sons, New York 1979.

13- 11-Ziemer, R. E. and Peterson, R. L., "Digital Communication and Spread Spectrum System", Macmillan Publishing Company, New York 1985.

14-Tauh, H. and Schilling, D., "Principles Of Communication Systems". McGraw-Hill Company, New York 1986.