Journal of
Engineering and
Applied Sciences

SINCE 2000
MEDWELL PUBLICATIONS

# A New Asymmetrical Crypto-Compression Application using Neural Network

Y. Benlcouiri, M. Benabdellah, M.C. Ismaili and A. Azizi
*Laboratory of Arithmetic, Scientific Computing and Applications, Faculty of Science, Mohamed First University, Oujda, Morocco*

**Key words:** Artificial neural networks, Multi-Layer Perceptron (ANN-MP), asymmetrical cryptography, crypto-compression

**Corresponding Author:**
Y. Benlcouiri
*Laboratory of Arithmetic, Scientific Computing and Applications, Faculty of Science, Mohamed First University, Oujda, Morocco*

Page No.: 89-93
Volume: 16, Issue 2, 2021
ISSN: 1816-949x
Journal of Engineering and Applied Sciences
Copy Right: Medwell Publications

**Abstract:** In this study, we propose a new application of asymmetrical crypto-compression system for images that is based on the artificial neural network to secure the transmission and the storage of images. The main idea of the security on this system consists on the problem of training in neural networks.

## INTRODUCTION

The digital revolution and the explosion of communication networks lead to increased circulation of documents multimedia (images, video, text, sound,…). The magnitude of this phenomenon is as critical issues facing now about the compression and protection of data exchanged. Indeed, by their nature digital documents Multimedia can be duplicated, modified, processed and distributed easily. Under these conditions and to transfer or to archive multimedia data, it becomes necessary to implement systems to enforce copyright, to control copies and protect the integrity of documents. In this context, the watermarking is quickly emerged as the “alternative” solution to enhance security of documents multimedia[1].

The Artificial Neural Networks (ANN) are tools for machine learning with a new approach information processing. The Multi-Layer Perceptron (MLP) is a neural network that uses a forward propagation type supervised learning to learn to perform a task. The compression of a set of data is the process of reducing the size of this body while preserving the integrity of that data. Cryptography is about the set of techniques to conceal the meaning of a message[2].

Standard encryption algorithms are not suited to the particular case of image data. The ideal would be applied to the images of asymmetric encryption systems in order not to have to transfer key. Due to the partial knowledge of the key (public key), the asymmetric systems require the use of large numbers above 512 bits. Therefore, as part of a secure transfer of images, the encryption of images is not feasible with for example the RSA algorithm. The use of symmetric algorithms requires having to transfer the secret key to the receiver. Conventional methods of image encryption require the transfer of the secret key by another channel or other means of communication[3, 4].

Cryptography technology remains essential to, first, protect the confidentiality of information transmitted over networks or stored on data servers and secondly, ensure the integrity of a document or to prove the authenticity of a transaction. It applies mathematical concepts and introduces paradigms computer to withstand potential attacks from attackers or to prove an almost sure that a procedure is incorruptible. The primary function of cryptography is to propose algorithms for encryption and electronic signature. In principle, the algorithm is standardized and known to all. The secret lies in the secret key. These algorithms are installed entities in personal trust (smart cards) or safes software computer servers[5]. The watermarking of image may also be a solution for secure image transfer. The purpose of the watermarking is inserted information in the image so invisible and indelible. The insertion of the message can be performed in space or frequency or in a combination of both areas[6, 7].

In Benlcouiri *et al*.[2], the compression and the data encryption are two technologies whose importance is growing exponentially in a myriad of applications. In addition, the excessive use of computer networks for data transfer must obviously obey to a double objective: the reduction of the volume of data in order to clutter the maximum possible public networks of communication and the confidentiality in order to ensure an optimum level of security. In this sense and in order to ensure the optimization and securing of the transmission and storage of still images, we propose a new approach for crypto-compression which the security reposes on the problem of training in compression neural network.

Our crypto-compression method has shown to be effective on the compression ratio, thus provides as well as the visual quality of reconstructed images. The principal advantages of our approach are the flexibility and the reduction of the processing time which incorporate simultaneously the compression and the crypto, at the time of the operations. Indeed, by our method, one can vary the processing time according to the desired degree of safety.

In this study, our works consist to construct the crypto graphical application based in the architecture of multilayer neural networks used for compressing still images. The application of Artificial Neural Networks Multilayer Perception (ANN-MP) to image compression seems to be well suited to achieve our crypto-compression, because it gives the propriety of irreversible function on its architecture.

On the other hand, the communication in asymmetrical crypto is based on two different keys: the public key in our case is the compressor part of ANN and the secret key is driven by the decompression one.

In what follows, we will discuss, initially, the still image compression by neural networks. Then, we will describe in detail the principles of our method and the results obtained after application. Finally, we conclude our article by introducing some perspectives.

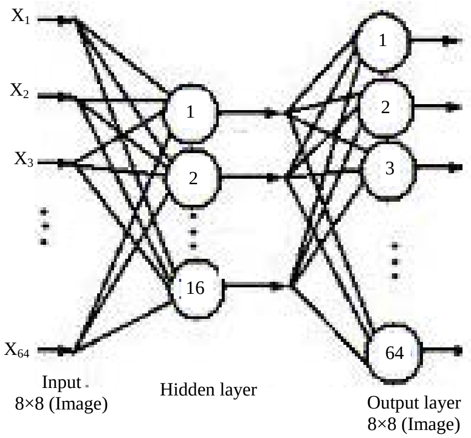


Fig. 1: Diagram of the neural network for compression and decompression

**Compression by ANNs:** Neural networks are originally attempted mathematical modeling of the human brain. The main idea of these networks is that one gives a single unit, a neuron which is able to perform some basic calculations. Then connected them a significant number of these units and trying to determine the computational power of the network, thus, obtained. It is important to note that these neurons manipulate numeric data and not symbolic.

Level image compression, there were already a number of comprehensive application of ANN and many algorithms learning and different architectures were used. We will use a system (Encoder/Decoder) which consists of two parts:

A compressor network consists of the input layer and of the hidden layer. And a decompression network which represents the sequence of the neural network (Fig. 1). The compression ratio is designated by the ratio of the number of neurons in the hidden layer and that of the input layer[8].

$X_i$ = The input of the cell i
$\overline{X}_i$ = The output of cell i
$h_j$ = The state of cell i in the hidden layer
$W_{ij}$ = The weight matrix between the input layer and the hidden layer
$W`_{ij}$ = The matrix of weight between the hidden layer and output layer

For an ANN, learning can be considered the problem of updating the weights of connections within the network, to succeed the task it is requested. Learning is the main characteristic of ANN, it can be done in different ways and with different rules and aims to adjust the connection weights, so that, the data presented to the input layer will be almost the same as those resulting from the layer output[9]. Using the back propagation algorithm using the sigmoid activation function as follows:

$$f(x) = \frac{1}{1 + e^{(-x)}}$$

$$f'(x) = f(x) \times (1 - f(x))$$

on training images divided into fixed-size block, we proceed as follows[2]:

**Repeat for each block:** Affect $X_i$ (data block) to cells in the input layer. As the square error is greater than the desired threshold on the outputs obtained from the inputs. Calculate hi (the states of neurons in the hidden layer):

$$h_j = \sum_i X_i \times W_{ij}$$

$$a_j = f(h_j)$$

Then $\overline{X_i}$ (the states of neurons in the output layer):

$$\overline{X_i} = \sum a_j \times W'_{ji}$$

$$a_i = f(\overline{X_i})$$

Calculate the error in units of cells in the output layer:

$$\delta_i = err_i \times f'(\overline{X_i})$$

then those of the hidden layer:

$$\delta_j = (\sum_i W'_{ji} \times \delta_i) \times f'(h_j)$$

Update weights on the output units and those of hidden units:

$$\Delta W'_{ji} = \varepsilon \times \partial_i \times a_j$$

$$\Delta W_{ij} = \varepsilon \times \partial_j \times X_i$$

Until the end. End repeat.

## MATERIALS AND METHODS

Our object is to use the architecture of ANN-MP on compression to construct an application of crypto-compression system[10].

In data compression, the ANN-MP makes a self-association on its hidden layer having a number of central neurons below the input layer, allowing the data reduction. To construct the crypto-compression application, our approach consists to use this architecture, for produce the public and private keys[11].

For this, we proceed in two phases; the first one is used to generate the keys of crypto-system (an ANN-MP adapted to compression of images) while the second is concerning to publisher the compressor part and preserve the decompression one as a secret key. We have defined a key of crypto-system to derive the encryption module and the decryption module of the ANN-MP architecture.

**Step (I):** Choose an architecture for our ANN-MP (N0 = number of input layer and output, N1 = number of hidden layer).

Apply the learning algorithm on our architecture chosen (Fig. 1) for the adjustment of connection weights between neurons.

**Step (II):** The result of the decomposition of the ANN-MP described above plays the role of key encryption and decryption (Fig. 2).

Publish the compressor part as a public key concerns the new section of compression (see diagram above) which we present the image to encrypt block by block of size N (the number of input layer). The encrypted message is obtained on the hidden layer.

Conserve secretly the decompression part as shown in the diagram above which encryption results are presented to the network block of size N1+N' '(the number of hidden layers of the new network). Thus, the results on the output layer with a length N0 resume their sites block by block for reconstruction perfect image.

**Scenario:** After the generation of Keys in step (I) and (II). The scenario between two interlocutors A and B is defined as follows:

**Encryption step:**

- A chooses a public key of B
- A applied the compressor RNA of B to all blocs on its images and send it for B

**Decryptions step:**

- B as a receiver, he applied the secret key (decompression part of his RNA) to all received blocs to reconstruct the images

**Security:** This assumption is based on the difficulty of the problem on training of neuron networks and then it can be reveals more difficult by fixed of one part of the network. Our method is ready to use for storage or transmission according to need and respect the compromise on the architecture ANN-MP between the number of neurons in the hidden layer and those of the input layer[12].

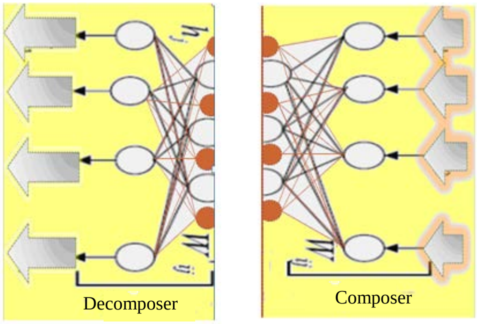
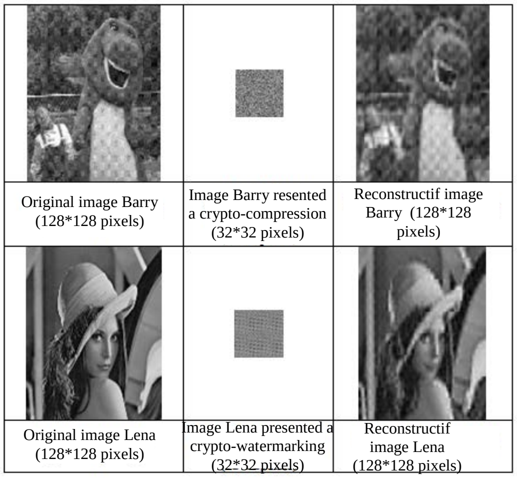


Fig. 2: Diagram of the two keys; the compressor section and the decompressor section



Original image Barry (128*128 pixels)

Image Barry resented a crypto-compression (32*32 pixels)

Reconstructif image Barry (128*128 pixels)

Original image Lena (128*128 pixels)

Image Lena presented a crypto-watermarking (32*32 pixels)

Reconstructif image Lena (128*128 pixels)

Fig. 3: Results obtained after applying our method on images Echo (1) and Lena (2)

## RESULTS AND DISCUSSION

To apply the proposed method, we chose an architecture of ANN-MP to the image compression whose has 8×8 = 64 neurons on the input and the output layer and 4 on the hidden layer neurons (N0 = 64; N1 = 8).

After fixing the ANN-MP and learning step for compression architecture, we present below the results obtained after applying our method on Barry and Lena images, presented in gray scale with a size equal 128×128 pixels (Fig. 3). Table 1 shows the overall results.

Figure 3 comparison between the original image (Image Barney and Image Lena) and the reconstructed image (Image Barney and Image Lena). (S.O.I = Size of the Original Image; P.S.N.R = Distortion measure; E.O.I = Entropy of the Original Image; E.R.I = Entropy of the Reconstructed Image; S.R.I = Size of the Reconstructed Image; T.(E/D) = Time of Encryption and Decryption.

Table 1: The overall results

| Image | S.O.I (Ko) | E.O.I | S.R.I (Ko) | E.R.I | P.S.N.R | T. (E/D) |
|---|---|---|---|---|---|---|
| Barry | 18.9 | 7.400 | 3.01 | 7.282 | 29.7170 | 10.01 |
| Lena | 19,1 | 7.574 | 2.95 | 7.521 | 26.2505 | 10.20 |

A compression by neural networks provides an interesting compression ratio and knowing that, the learning step is costly in terms of time required to adjust the weights appropriate to the neural networks that are responsible for the visual quality of the image processing and the asymmetrical compression coefficients which are not those of the decompression.

Moreover, our method provides a transmission with interlace (progressive transmission) which reduces the burden of bandwidth. As regards the time necessary for the crypto operation, it may vary depending on the images in treatment.

## CONCLUSION

In this work, we presented the use of RNA as a crypto-application of stills images in its asymmetric form. The security of our crypto-compression system is based on the problem of learning in the RNA on fixed all weight in the compressor part. Our method is more efficient and very important to absorb some forms of attacks that are based on detecting the length of the key and its composition or architecture and other attacks that take modern stochastic increasingly valuable in cryptanalysis. We plan to use the wavelet networks for a new application of crypto-compression of stills images.

## REFERENCES

01. Dugelay, J.L. and S. Roche, 1999. [Introduction to tattooing images (In French)]. Anal. Telecommun., 54: 427-437.
02. Benlcouiri, Y., M. Benabdellah, M.C. Ismaili and A. Azizi, 2012. Crypto-compression of images based on the ANNs and the AES algorithm. Int. J. Commun. Comput. Eng., 2: 1-6.
03. Benabdellah, M., F. Regragui and E.H. Bouyakhf, 2011. Hybrid methods of image compression-encryption. J. Commun. Comput. Eng., 1: 1-11.
04. Sinha, A. and K. Singh, 2003. A technique for image encryption using digital signature. Optics Commun., 218: 229-234.
05. Benabdellah, M., M. Gharbi, N. Zahid, F. Regragui and E.H. Bouyakhf, 2009. Encryption-compression method of images. Int. J. Comput. Sci. Inform. Syst., 4: 30-41.

06. Benabdellah, M., M.M. Himmi, N. Zahid, F. Regragui and E.H. Bouyakhf, 2007. Encryption-compression of images based on FMT and AES algorithm. Applied Math. Sci., 1: 2203-2219.
07. Shih, F.Y. and S.Y.T. Wu, 2003. Combinational image watermarking in the spatial and frequency domains. Pattern Recogn., 36: 969-975.
08. Jaara, E.M., 2000. [Parallel study and implementation of neural networks]. Ph.D. Thesis, College of Science, Oujda, Morocco. (In French)
09. Daoudi, E. and E. Jaara, 1999. Parallel methods of training for multilayer neural network. Proceedings of the European Conference on Parallel Processing, August 31-September 3, 1999, Springer, Berlin, Germany, pp: 686-690.
10. Benabdellah, M., F. Regragui, N. Zahid and E.H. Bouyakhf, 2007. Encryption-compression of echographic images using FMT transform and DES algorithm. INFOCOMP J. Comput. Sci., 6: 36-42.
11. Hogan, M.T., N.J. Hurley, G.C. Silvestre, F. Balado and K.M. Whelan, 2005. ML detection of steganography. Proceedings of the SPIE Conference on Security, Steganography and Watermarking of Multimedia Contents VII, March 21, 2005, ISOP, San Jose, California, USA., pp: 16-27.
12. Petitcolas, F.A. and S. Katzenbeisser, 2000. Information Hiding Techniques for Steganography and Digital Watermarking. Artech House, Norwood, Massachusetts, Pages: 220.