# A Novel Neural Network Approach for Digital Image Data Encryption/Decryption

Saraswati D. Joshi [1], Dr. V. R. Udupi [2], Dr. D. R. Joshi [3]

*[1] Assistant Professor, Department of Electrical and Electronics, Gogte Institute of Technology, Belgaum.*

*[2] Professor, Department of Electronics and Communication, Gogte Institute of Technology, Belgaum..*

*[3] Principal, Arvind Gavali College of Engineering, Satara.*

*[1,2,3] India*

[1] saraswatidjoshi@rediffmail.com
[2] vishwa_u@yahoo.com
[3] drj5@rediffmail.com

***Abstract*— with the increased popularity of multimedia applications, there is a great demand for secured data storage and transmission techniques. Information security has traditionally been ensured with data encryption and authentication techniques. Through the years, different generic data encryption standards have been developed. The secrecy of communication is maintained by secret key exchange. In effect the strength of the algorithm depends solely on the length of the key. The presented work aims at secure image transmission using randomness in encryption algorithm, thereby creating more confusion to obtain the original data. The security of the original cipher has been enhanced by addition of impurities to misguide the cryptanalyst. Since the encryption process is one way function, the artificial neural networks are best suited for this purpose as they possess features like high security, no distortion and its ability to perform for non linear input-output characteristics, In the presented work the need for key exchange is also eliminated, which is otherwise a perquisite for most of the algorithms used today. The proposed work finds its application in medical imaging systems, military image database communication and confidential video conferencing, and similar such application. The results are obtained through the use of MATLAB 7.0.1.**

***Keywords*— Artificial neural networks, backpropagation algorithm, cipher, decipher, decryption, encryption, normalization.**

## I. Introduction

In the past few years there have has been an explosion in the use of digital media. Industry is making significant investment to deliver digital audio, image and video information to the consumers by networked information system, because of which illegal data access and unauthorized data reproduction have become easier and more prevalent [4]. Hence security of multimedia data has become more and more important.

Information security has traditionally been ensured with data encryption and authentication techniques. Through the years, different generic data encryption standards have been developed. Data encryption standard (DES) has been the main encryption standard from 1977. However in the year 1998 it has been shown to be vulnerable to brute force attacks, differential cryptanalysis and linear cryptanalysis. Acknowledging the need for a new encryption standard, several ciphers have been proposed such as AES, 3DES, MARS, RSA, Serpent, two fish, blowfish, IDEA and GOST were used [3]. Because of voluminous data involved in image/video, other encryption methodologies such as affine transform, the chaotic system and the frequency domain algorithms have been developed [4],[5].

Neural network plays a very important role in information security and lot of work has been going on in this direction. Khalil shihab [3], Liew Pal Yeh and Liyanage C. De Silva [2], Munukur R. K. [1] and many others have used neural networks for encryption/decryption of either text or image.

Whether it is image processing or otherwise, most of the algorithms used are generic, because of which the key exchange has become a prerequisite prior to exchange of the data. Hence the strength of such encryption solely lies on the key length. In the presented work, encryption process uses random substitutions, and impurity addition (doping) creating more confusion and misguide the cryptanalyst to obtain the cipher. At the receiving end, it uses artificial neural networks to obtain the original image. The elimination of the key exchange and the usage of artificial neural network for high security are the major strengths of the presented work.

The paper is organized as follows. Section II gives a brief introduction to artificial neural network. Section III describes the design aspects, Section IV discusses the results. Performance analysis is discussed in Section V and finally in Section VI some conclusions are presented.

## II. Artificial Neural Network

Artificial Neural networks (ANN) are simplified models of the biological nervous system. An ANN, in general, is a highly interconnected, massively parallel distributed processing network with a large number of processing elements called neurons in an architecture inspired by the brain, which has a natural propensity for storing experimental knowledge and making it available for later use. Each neuron is connected to other neurons by means of directed communication links each with an associated weight. Each neuron has an internal state, called its activation or activity level, which is a function of the inputs it has received. Typically, a neuron sends its activation as a signal to several

978-1-4673-0449-8/12/$31.00 ©2012 IEEE

other neurons. There are several architectures in which the neurons can be connected. By choosing the suitable model and appropriately training the network, it can be used as a mapping function. Among the various architectures, feedforward networks using backpropagation learning algorithm are used.

In the backpropagation neural networks, perceptron and other one layer networks are seriously limited in their capabilities. Hence multilayer Feedforward (MLFF) networks with Backpropagation learning and non linear node functions are used to overcome these limitations,. Multilayer feedforward network [MLFF] is made up of multiple layers. Thus, architectures of this class, besides possessing an input and an output layer also have one or more intermediary layers called hidden layers. Here the neurons of one layer are connected to the neurons of the next layer and so on till the output layer. The hidden layer aids in performing useful intermediary computations before directing the input to the output layer. Backpropagation neural nets are those feed forward networks which use backpropagation learning method for their training. The training of a network by back propagation involves three stages: the feed forward of the input training pattern, the calculation and back propagation of the associated error, and the adjustment of the weights. Once the process converges, the final weights are stored in a file. After training, application of the network involves only the computations of the feed forward phase [1][3], [6].

## III. System Design

Fig. 1 depicts the schematic diagram of the presented work.

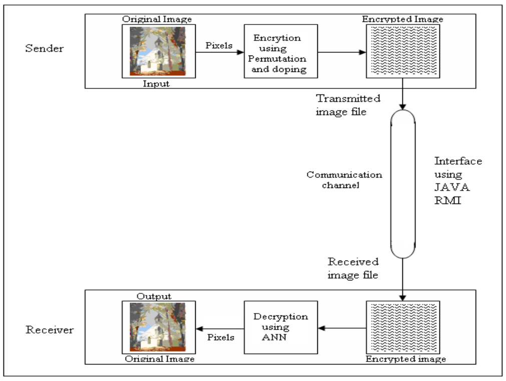


Fig. 1 Block diagram of the image transmission and reception

The system designed can be split into three modules-encryption, decryption and the interface module [8]. Whenever the sender wishes to send an image, he feeds the image to be sent to the encryption module. The image data is encrypted in the encryption module and the encrypted data is fed to the interface module. This module transfers the encrypted image data to the remote system. At the receiving end the user in the remote system decrypts the image data by feeding the received data to the decryption module. Encryption and decryption module are implemented using MATLAB 7.0.1 [7], [9]. All the above three modules have to be present in every user's system who wish to use of secured image transmission and reception facility.

### A. Encryption Module

The image to be encrypted is read pixel by pixel and the transformation is done on these pixels using permutation, substitution and impurity addition. Two levels of encryption are used to obtain high level of image encryption. The algorithm shown does the necessary transformation.

Algorithm :

*First level of encryption (steps 1 to 8):*

Step1: Get the pixel value of the image file, [67] [01000011].

Step2: Divide the pixel byte value into two parts (nibbles), [0100 and 0011].

Step3: Exchange the nibbles and concatenate to form a byte, [00110100].

Step4: Calculate the impurity by EX-ORing the original msnibble and lsnibble,[0111].

Step5: Shift the bits of the impurity by 5 bits to the right. Now we get 9 bit number, [011100000].

Step6: EX-OR the results of step3 and step5 [011010100] = [212].

Step7: Add impurity2 to the obtained result in step6. Impurity value chosen is 117, [212+117=329].

Step8: Continue step1 to 7 for all the pixels of the image file

*Addition of two columns:*

Step9: Additional two columns are added and the value of 117 is added to the first new column and 627 is added to the second new column. This is required for normalization of the matrix.

*Second level encryption:*

Step10: Add another level of impurity to the resultant matrix obtained in step9 to the result obtained in step 9 such that impurity changes with respect to the position of the pixel.

Table I shows the transformation of the sample pixel values after first level of encryption.

Table I
Sample First Level Encryption Results

| Original Pixel Value | Pixel Value after 1st level Encryption |
|---|---|
| 1 | 165 |
| 6 | 277 |
| 45 | 473 |
| 67 | 329 |

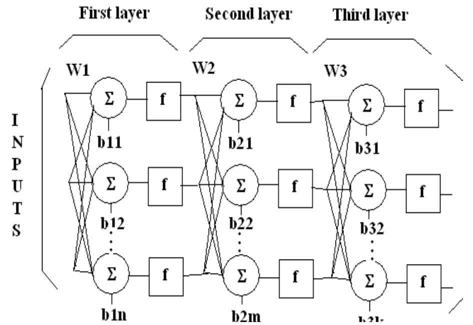
Table II shows how the pixel value (12) changes with respect to its position during the second level encryption.

TABLE II
SAMPLE RESULTS OF A PIXEL AFTER 2ND LEVEL ENCRYPTION

| Pixel position | Original pixel value | Pixel value after 1st level encryption | Pixel value after 2nd level encryption |
|---|---|---|---|
| (1,1) | 12 | 437 | 537 |
| (4,68) | 12 | 437 | 708 |
| (10,34) | 12 | 437 | 1050 |
| (15,29) | 12 | 437 | 1335 |
| (19,8) | 12 | 437 | 1563 |

### B. *Decryption Module*

At the receiving end, decryption is achieved using an artificial neural network. The neural network is trained for the standard mapping value and the weights and biases are stored before applying the input to it [1]-[3], [6]. MATLAB's neural network tool box is used for implementing and training the neural network.



Wi- weight matrix of the i$^{th}$ layer
f- activation function
bij- bias of the jth neuron in ith layer

Fig. 2 Block diagram of s 3 layer backpropagation net [1]

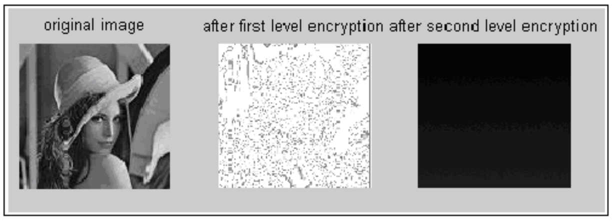
The system is designed for three layers-input, output and the hidden layer. The input and output layers have only one neuron and the hidden layer has 695 neurons. Large numbers of neurons are essential for achieving high accuracy. The decryption process is achieved in three steps. During the first stage, the impurity which was varying with respect to the position of the pixel is removed. In the he second stage, the additional columns from the matrix which were added during encryption is deleted. During the third stage, the received image data and weights which were stored after training are used to simulate the network. The output of this stage is the recovered image, the results of which are shown in Fig. 4.

### C. *Interface Module*

The system was tested by connecting two computers in the network. File transfer from the host system to the remote system was done using the JAVA remote method invocation [10]-[12].

## IV. RESULTS AND DISCUSSION

The results of the encryption module are shown in Fig. 3.



.

Fig. 3 The Output of the encryption module

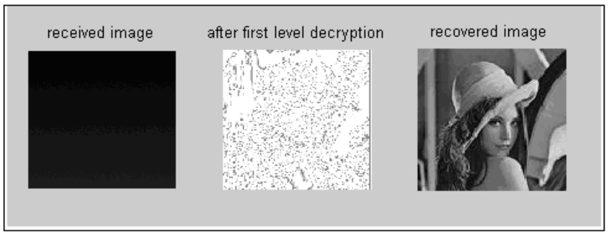


Fig. 4 Output of the decryption module

### A. *The Need for Two Levels of Encryption*

As already mentioned, there are two levels of encryption in the encryption module. It is required, because, for some of the images, a sample of which is as shown in Fig. 5, 1st level encryption does not suffice. From the Fig. 5, it is very clear that although the intensity of the pixel has changed drastically, the picture is still in an understandable form.

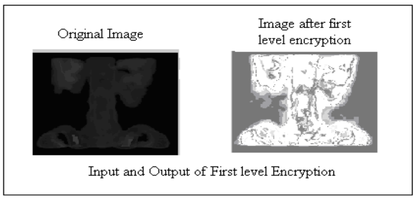

Original Image
Image after first level encryption
Input and Output of First level Encryption

Fig. 5 Input and output images of first level encryption

The reason behind this is that, although the pixel value changes after first level of encryption all the pixels with same original value will have the same encrypted value, because of which intensity changes but image can be still visible.

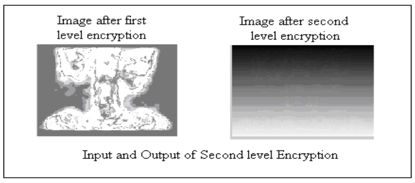


Image after first level encryption
Image after second level encryption
Input and Output of Second level Encryption

Fig. 6 Input and Output images of second level encryption

To overcome this problem, the second level encryption is used. During the second level encryption the impurity changes with respect to the pixel position (shown in table 2) it means that the pixel with same original value will have two different values after the second level of encryption depending on the pixel position. The output after the second level of encryption is shown in Fig. 6.

### B. Need for Normalization:

As mentioned earlier ANN is used for decrypting the image. ANNs require training before they are used for any application The results of training were not converging for the given input data set having 256 values. This problem was solved by the normalization of the input data. Normalization is the process of transforming the data set to the values ranging from -1 to 1 [6].

### C. Requirement of Additional Two Columns during Encryption:

The image matrix was treated as a series of vectors (one row as one vector input) while simulating the network. Thus it became mandatory to have minimum and maximum pixel values in each row for achieving accurate normalization of the vector.

## V. Performance Analysis

### A. Network Performance:

The training of the ANN is done using 'trainlm' function available in MATLAB's neural network tool box. It updates weight and bias values according to Levenberg-Marquardt optimization). This has been found faster compared to the other training algorithms. The convergence has been fastest when few hundreds of weights are present in the network. It uses the heuristic method based on the standard numerical optimization technique.

The accuracy of the network has been found very high. Network performance is shown in Table III. .For the performance goal of 1e-06 the accuracy is cent per cent. However, for such high accuracy, the number of neurons required in the hidden layer has been found as high as 695.

Table III
Network Performance with Variations in Performance Goals

| Sl. No | Performance goal set | No. of epochs | Time required in seconds | % error |
|---|---|---|---|---|
| 1 | 0.1 | 1 | 06.10 | 92 |
| 2 | 0.01 | 4 | 10.94 | 41 |
| 3 | 0.001 | 4 | 34.41 | 7 |
| 4 | 0.0001 | 5 | 52.01 | 1 |
| 5 | 0.00001 | 7 | 59.00 | 0 |
| 6 | 0.000001 | 11 | 104.63 | 0 |

### B. Application Performance

The presented work has been tested with many samples of JPEG, TIF and BMP files. Accuracy has been found to be very high. Table IV shows encryption and decryption time for the image. The decryption process was much slower than the encryption process. It is because of the fact that the simulation of the network during decryption process is done for each of the row separately.

Table IV
Encryption and Decryption Time

| Sl. No | Image file size in pixels | Encryption time in seconds | Decryption time in seconds |
|---|---|---|---|
| 1 | 100X100X1 | 0.07 | 00.14 |
| 2 | 256X256X1 | 1.13 | 15.71 |
| 3 | 48X 48 X3 | 0.24 | 02.43 |
| 4 | 256X256X3 | 1.48 | 58.71 |
| 5 | 377X464X3 | 1.69 | 112.96 |

## VI. Conclusion

The presented work discusses a novel neural network approach for image encryption and decryption. In order to make the decryption difficult for the eavesdropper, a random algorithm has been used to for encryption .Using the neural network at the receiver end has made random encryption possible at the senders end. Also the need for key exchange prior to data exchange has been eliminated. Faster training has been achieved by using the 'trainlm' function of MATLAB neural network tool kit. The accuracy of the system has been found very high. The presented work thus provides a means of robust, flexible, accurate and secure image data transmission and reception.

In future, authentication module can also be added to the existing encryption/decryption module. There is also lot of scope for enhancing this work to video encryption and decryption, there by making full-fledged video encryption /decryption system.

## VII. References

[1] Munukur, R.K.; Gnanam, V, "Neural network based decryption for random encryption algorithms," in *Proc.* 3rd Int. Conf. *Anti-counterfeiting, Security, and Identification in Communication, ASID*, pp. 603 – 605, Aug. 2009.

[2] Liew Pol Yee De Silva L.C., "Application of multilayer perceptron network as a one-way hash function," in *Proc. Int. Conf. Neural Networks, IJCNN*, vol. 2, pp. 1459-1462, May 2002.

[3] Khalil Shihab, "A backpropagation neural network for computer network security," in *Proc. Journal of Computer Science*, vol 2, 2006, pp. 710-715.

[4] Su, S.; Lin, A.; Jui-Cheng Yen "Design and realization of a new chaotic neural encryption/decryption network," in *Proc. IEEE Asia-Pacific Conf, Circuits and Systems*; *APCCAS*, pp. 335-338, Dec. 2000.

[5] Francia G.A., Ming Yang, Trifas M., "Applied image processing to multimedia information security," in *Proc. Int. Conf. Image Analysis and Signal Processing*, pp. 104-107, April, 2009.

[6] S. Rajasekaran and G.A Vijayalakshmi. *Neural Network, Fuaay Logic, and Genetic Algorithms, Synthesis and Applications.* Prentice-Hall India, 2003.

[7] Rafael C. Gonzalez, Richard E. Woods and Steven L. Eddins "Digital Image Processing using Matlab" Pearson Education,2008.

[8] William Stallings. *Network Security Essentials, Applications and Standards*, 3rd ed.. Pearson Education, 2009.

[9] *Basics of MATLAB and beyond.* Andrew Knight. CRC press-LLC,2000.

[10] [Online]. Available: http:/www.learn-rmi.thiyagaraj.com

[11] [Online]. Available: http:/www.scantips.com

[12] [Online]. Available: http/www.atalasoft.com