Image Encryption Using Chaotic Based Artificial Neural Network

Minal Chauhan[1], Rashmin Prajapati[2]

Abstract— Cryptography is the science to transform the information in secure way. Encryption is best alternative to convert the data to be transferred to cipher data which is an unintelligible image or data which cannot be understood by any third person. Images are form of the multimedia data. There are many image encryption schemes already have been proposed, each one of them has its own potency and limitation. This paper presents a new algorithm for the image encryption/decryption scheme which has been proposed using chaotic neural network. Chaotic system produces the same results if the given inputs are same, it is unpredictable in the sense that it cannot be predicted in what way the system's behavior will change for any little change in the input to the system. The objective is to investigate the use of ANNs in the field of chaotic Cryptography. The weights of neural network are achieved based on chaotic sequence. The chaotic sequence generated and forwarded to ANN and weighs of ANN are updated which influence the generation of the key in the encryption algorithm. The algorithm has been implemented in the software tool MATLAB and results have been studied. To compare the relative performance peak signal to noise ratio (PSNR) and mean square error (MSE) are used.

Index Terms— Chaotic maps, Image encryption, Chaotic cryptosystems, Artificial neural network- ANN, Peak signal to noise ratio- PSNR, Mean square error- MSE, Cipher text, Plain text

1 INTRODUCTION

In recent years, more and more electronic services and devices are available, like mobile phones and personal digital assistant PDAs, also started to provide the additional functions like saving and exchanging multimedia data. The prevalence of multimedia technology has promoted digital images and videos to play a more significant role than the traditional dull texts, which demands a serious protection of users' privacy and so the protection of multimedia data is becoming very important. There are so many different techniques should be used to protect confidential image data from unauthorized access. To fulfill such privacy and security needs in various applications, encryption of images is very important to aggravate malicious attacks from the unauthorized parties.

This paper is organized as follows In Section 1; general guide line about cryptography is presented. In Section 2, Propose method is presented. Finally, concluded in section 3.

Here is a quick introduction of chaotic systems and ANN systems.

1.1 What is Image Encryption?

Image encryption is a hiding of information. An original important and confidential plaintext is converted into cipher text that is apparently random nonsense. This cipher text can be saved or transmitted over the network. At the receiver, the cipher text can be transformed back into the original plaintext by using a decryption algorithm [2].

1.2 What is Chaotic Systems?

Chaos communications is application of chaos theory which is to provide security in the transmission of information. Chaos theory [2], [5], [9] describes the behavior of certain nonlinear dynamic system that under specific conditions exhibit dynamics that are sensitive to initial conditions. Properties of chaotic systems are the sensitivity to initial conditions. A large number of uncorrelated, random, deterministic signals can be generated by changing initial values to system. These sequences generated are called chaotic sequences. One of the simplest and most widely studied nonlinear dynamic chaos systems is the logistic map.

1.3 What is ANN?

A neural network [2], [12] is a machine that is designed to represent the way in which brain performs any particular task. The network is implemented by using electronic components or is simulated in software on a digital computer. The input images are encrypted with an encryption function on Artificial Neural Network and that images are decrypted using another ANN at receiver side in order to attain the initial image.

2 PROPOSE SYSTEM

There are many algorithms to encrypt image data may be simple symmetric key encryption algorithms or chaotic based or ANN based, each of them have their own advantages and limitations. So in proposed system we have combined these two approaches- chaotic cryptosystems and ANN based cryptosystems to make CNN--chaotic based ANN systems. Now why these two systems only that review research has already been done by us and available in our review paper [2].

Here is architecture of proposed system.

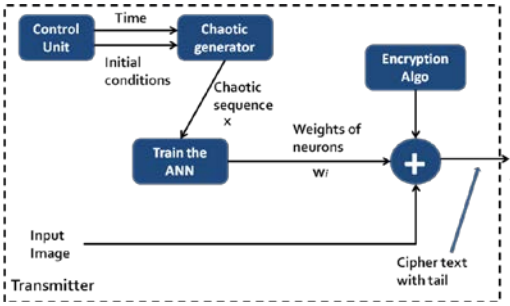

Fig. 1. At sender side

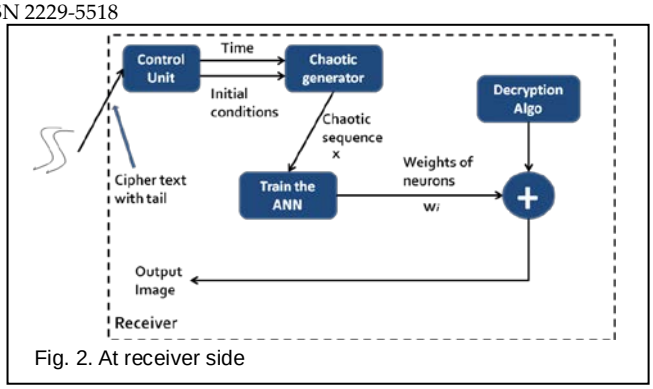

Fig. 2. At receiver side

2.1 Chaotic based Neural Network

A network is called a chaotic neural network if its weights and biases are determined by a chaotic sequence. Let g denote a digital signal of length M and g(n), 0 to M-1, be the one- byte value of the signal g at position n.

Step 1: Set the value of the parameter M.

Step 2: Determine the parameter, U and the initial point x(0) of the 1-D logistic map.

Step 3: Evolve the chaotic sequence x(l), x(2), ... , x(M) by x(n+l) = μ(n)(l-x(n)), and create b(O), b(l), ..., b(8M-1) from x(l), x(2), ..., x(M) by the generating scheme that 0.b(8m- 8)b(8m-7) ….. b(8m-2)b(8m-l) … is the binary representation of x(m) for m = 1, 2,. . . ., M.

Step 4: For n: 0 To (M - 1) Do

$$g(n) = \sum_{i=0}^{7} d_i \times 2^i \quad (1)$$

For i= 0 To 7 Do 1

$$w_{ji} = \begin{cases} 1 & if \quad j = i \quad and\, b(8\times n + i) = 0, \\ -1 & if \quad j = i \quad and\, b(8\times n + i) = 1, \\ 0 & if \quad j \neq i, \end{cases}$$

$$i \in (0,1,2,3,4,5,6,7) \quad (2)$$

$$\theta_i = \begin{cases} -1/2 & if \quad b(8\times n + i) = 0, \\ 1/2 & if \quad b(8\times n + i) = 1, \end{cases}$$

End

For i= 0 To 7 Do

$$d_i^{'} = f\left(\sum_{i=0}^{7} w_{ji} \times d_i + \theta_i\right) \quad (3)$$

Where f(x)` is 1 if x 2 0 and 0 otherwise,

End

$$g(n) = \sum_{i=0}^{7} d_i \times 2^i \quad (4)$$

End

Step 5: The encrypted signal g" is obtained and the algorithm is terminated.

The decryption procedure is the same as the above one except that the input signal to the decryption CNN should be g'(n) and its output signal should be g"(n).

In case of an image, pixels are processed by neurons according to (4). The desirable result of the encrypted image being completely disorder can be obtained. In the decryption phase of CNN, according to the initial state chaotic binary sequence is generated and forwarded to ANN which generates the weights to generate the key to obtain original image.

2.2 NN Architecture

A Neural network implemented using a Jordan network is used. In the Jordan network, the activation values of the output units are fed back into the input layer through a set of extra input units called the state units. There are as many state units as there are output units in the network.

To find the best ANN structure to produce chaotic dynamics by changing the number of hidden layers, the number of neurons in the hidden layers and the transfer functions in the neurons. After the training process, the ANN models were tested with sorted test data the suitable network structure is 8x10x8 trained with Back Propagation algorithm. This means that the number of neurons is 8 for the input layer, 10 for the hidden layer, and 8 for the output layer. The input and output layer neurons have linear activation functions and the hidden layer neurons have hyperbolic sigmoid activation functions, respectively. As the learning proceeds, the mean square error progressively decreases and finally attains a steady state minimum value.

Weight adjustments with sigmoid activation function:

The results from the previous section can be summarized in three equations:

1. The weight of a connection is adjusted by an amount proportional to the product of an error signal δ, on the unit k receiving the input and the output of the unit j sending this signal along the connection:

$$\Delta_p w_{jk} = \gamma \delta_k^p y_j^p \quad (5)$$

2. If the unit is an output unit, the error signal is given by

$$\delta_a^p = (d_a^p - y_a^p) F^{'}(\delta_a^p) \quad (6)$$

Take as the activation function F the 'sigmoid' function:

$$y^p = F(\gamma^p) = \frac{1}{1+e^{-\delta p}} \quad (7)$$

3. In this case the derivative is equal to:

$$F^{'}(\delta^p) = \frac{\partial}{\partial \delta^p}\frac{1}{1+e^{-\delta p}} = \frac{1}{(1+e^{-\delta p})^2}(-e^{-\delta p}) = \frac{1}{1+e^{-\delta p}}\frac{-e^{-\delta p}}{1+e^{-\delta p}} = y^p(1-y^p) \quad (8)$$

Such that the error signal for an output unit can be written as:

$$\delta_a^p = (d_a^p - y_a^p) y^p (1-y^p) \quad (9)$$

4. The error signal for a hidden unit is determined recursively in terms of error signals of the units to which it directly connects and the weights of those connections. For the sigmoid activation function:

$$\delta_h^p = F^{'}(\delta_h^p)\sum_{a=1}^{N_a} \delta_a^p w_{ha} = y_h^p(1-y_h^p)\sum_{a=1}^{N_0} \delta_a^p w_{ha} \quad (10)$$

5. Get an update rule which is equivalent to the delta rule, resulting in a gradient descent on the error surface if we make the weight changes according to:

$$\Delta_p w_{jk} = \gamma \delta_k^p y_j^p \quad (11)$$

Depending upon the size of the dataset the size of the hidden layer is changed as the complexity of the neural increases.

2.3 CNN based image encryption:

CNN based image encryption involves three steps:

1. **Generate Chaotic sequence**
   To generate the chaotic sequence first get the input sequence. Then chaotic sequence will be generated using logistic map,
   $x(n+l) = \mu(n)(l-x(n))$ (12)
   $x(i)=mu*x(i-1)*(1-x(i-1));$ (13)
2. **Generate ANN output**
   To generate the ANN network weights based on the chaotic sequence generated the output weights will be calculated by the logic below,
   if (bc,i = 0) & (i = j)
   $weight_{i,j} = 1;$
   elseif (bc,i = 1) & (i = j)
   $weight_{i,j} = -1;$
   elseif i ≠ j
   $weight_{i,j} = 0;$
   end
   $o/p = sum (weight_{ij} . x_{ij})+ \Theta$ (14)
   where, $\Theta = -1/2$ & $1/2$
3. **Encryption**
   To encrypt the image using the key generated by the output of the CNN system the asymmetric encryption algorithm AES [1] has been used.

2.4 Results

The CNN has been implemented in MATLAB tool version 7.10.0 (R2010a).

Result 1: lena image

Fig. 3. Original, encrypted and decrypted images

Result 2: monalisa image

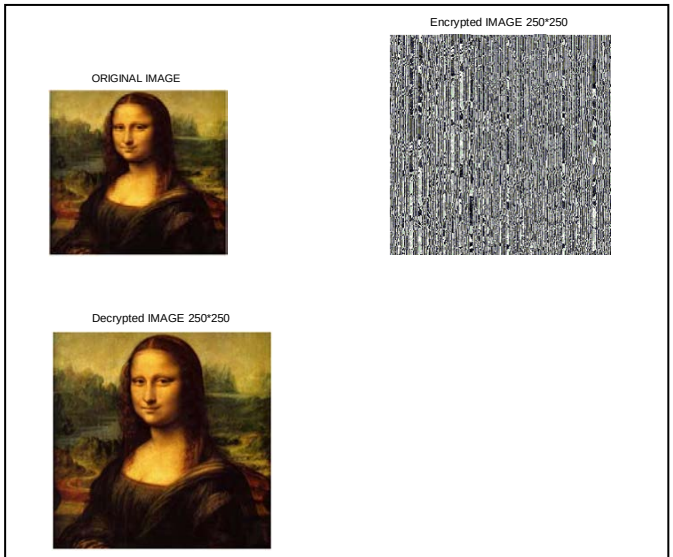

Fig. 4. Original, encrypted and decrypted images

Result 3: pepper image

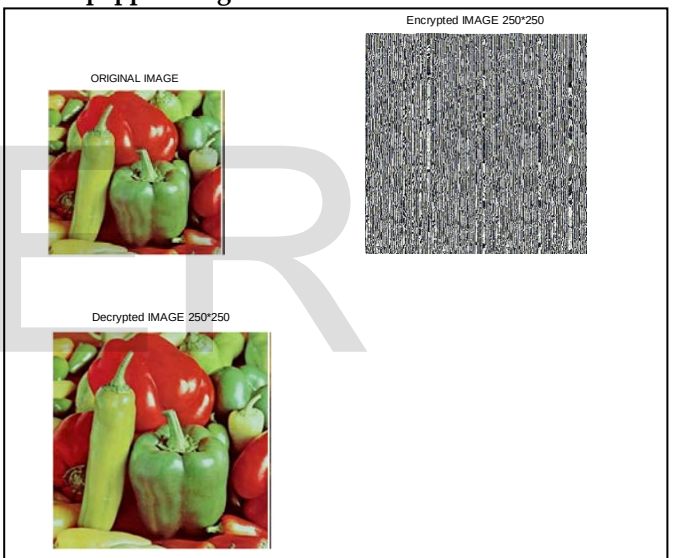

Fig. 5. Original, encrypted and decrypted images

Here, the first image is input-original image, second is encrypted image and third one is decrypted image.
The PSNR and MSE for these images are as below:

TABLE 1
PSNR RATIO OF CHAOTIC, ANN AND CNN SYSTEMS

Images	Chaotic Cryptosystem	Neural Network based Cryptosystem	CNN based Cryptosystem
Lena	7.9100	7.5070	8.5361
Pepper	8.7941	8.0158	9.0917
Monalisa	5.6778	5.9298	6.3215

TABLE 2
MSE RATIO OF CHAOTIC, ANN AND CNN SYSTEMS

Images	Chaotic Cryptosystem	Neural Network based Cryptosys-tem	CNN based Cryptosystem
Lena	10.1233e+03	10.1321e+03	9.4281e+03
Pepper	10.9081e+03	10.1214e+03	9.6522e+03
Monalisa	11.3216e+03	11.1231e+03	10.7112e+03

3 CONCLUSIONS

In this paper, we have proposed the combine method of chaotic and ANN cryptosystem which is CNN and incorporates the advantage of both the systems that are- randomness of chaotic theory, learning of ANN, good PSNR and also eliminates the limitation of the chaotic system and ANN like fewness of parameter and complexity of neural networks as the security is not only dependent on the neural network and so the complex structure of the ANN is not necessary.

Finally the comparisons of the parameters PSNR and MSE of the different input images using chart is shown below:

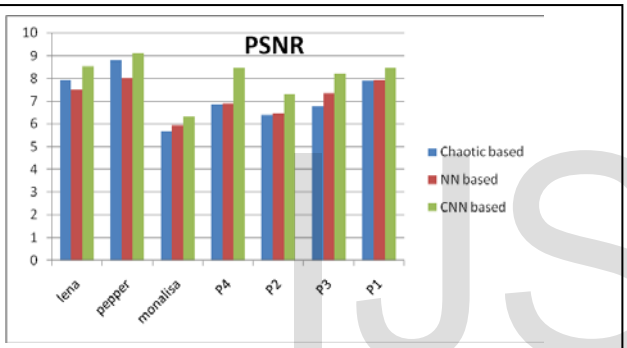

Fig. 6. Comparison of PSNR ratio

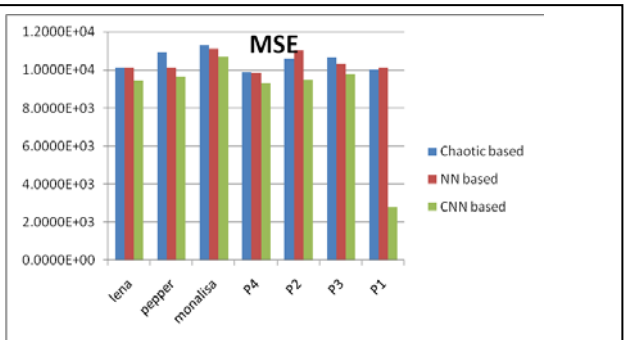

Fig. 7. Comparison of MSE ratio

Although not mentioned in this paper, there have been number of approaches in Image encryption in the context of chaotic systems, neural networks, using genetic algorithms and many more. The goal is to provide higher security and speed.

REFERENCES

[1] William Stallings, "Cryptography and Network Security: Principles and Practices", second edition.

[2] Minal Chauhan, Rashmin Prajapati "Image Encryption Using Chaotic Cryptosystems and Artificial Neural Network Cryptosystems: A Review", International Journal of Scientific & Engineering Research, Vol.5, Issue 5, May-2014.

[3] "Chaos Communication" Chaos%20communications%20-%20Wikipedia,%20the%20free%20encyclopedia.htm

[4] K.Deergha Rao, Ch. Gangadhar, "Modified Chaotic Key-Based Algorithm for Image Encryption and its VLSI Realization", IEEE, 15th International. Conference on Digital Signal Processing (DSP), 2007.

[5] Frank Dachselt , Wolfgang Schwarz, "Chaos And Cryptography", IEEE Transactions on Circuits And Systems- I: Fundamental Theory And Applications, Vol.48, 2001

[6] Zhang Yun-peng, Liu Wei, Cao Shui-ping, Zhai Zheng-jun, Nie Xuan, Dai Wei-di, "Digital Image Encryption Algorithm Based on Chaos and Improved DES", IEEE International Conference on Systems, Man and Cybernetics, 2009.

[7] Min Long, Li Tan, "A chaos-Based Data Encryption Algorithm for Image/Video", IEEE, Second International Conference on Multimedia and Information Technology, 2010.

[8] Kuldeep Singh, Komalpreet Kaur, "Image Encryption using Chaotic Maps and DNA Addition Operation and Noise Effects on it", International Journal of Computer Applications (0975 - 8887) Vol.23, No.6, June 2011.

[9] Qais H. Alsafasfeh, Aouda A. Arfoa, "Image Encryption Based on the General Approach for Multiple Chaotic Systems", Journal of Signal and Information Processing, 2011.

[10] J. K. Mandal, Arindam Sarkar, "An Adaptive Neural Network Guided Secret Key based Encryption through Recursive Positional Modulo-2 Substitution for Online Wireless Communication (ANNRPMS)", IEEE, International Conference on Recent Trends in Information Technology (ICRTIT), June 2011.

[11] G.A.Sathishkumar, Dr.K.Bhoopathy bagan and Dr.N.Sriraam, "Image Encryption Based on Diffusion and Multiple Chaotic Maps" International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.2, March 2011.

[12] Eva Volna, Martin Kotyrba, Vaclav Kocian, Michal Janosek, "Cryptography Based on Neural Network", 26th European Conference on Modelling and Simulation, 2012.

[13] Hüsamettin UYSAL, Sinem KURT, Tülay YILDIRIM "Automatic Decryption of Images through Artificial Neural Networks", Trends in Innovative Computing - Intelligent Systems Design, 2012.