International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 04 | Apr 2020 www.irjet.net p-ISSN: 2395-0072

Image Encryption using Deep Neural Networks based Chaotic Algorithm

Sangeetha S[1], Haseena P[2]

[1]*M.Tech Scholar, Dept. of ECE, Jawaharlal College of Engineering and Technology, Kerala, India*
[2]*Assistant Professor, Dept. of ECE, Jawaharlal College of Engineering and Technology, Kerala, India*

Abstract - *Cryptography is the method of protecting information and multimedia through the use of codes. So, that only the desired person can read and process the information. Cryptography is associated with two process: Encryption and Decryption. Encryption is scrambling plaintext into cipher text. Decryption is the process of retrieving the plain text back. In the recent years there has been quite a development in the field of artificial intelligence mainly the introduction of the artificial neural networks (ANN). The ANN is considered to an information processing unit which to a great extent resembles the working of the human brain. In this paper images are encrypted and decrypted using deep neural networks that are Convolutional Neural Network (CNN) based chaotic algorithm. Chaotic system is highly sensitive to initial conditions. The algorithm used for image encryption is Advanced Encryption Standard AES). This algorithm is been implemented in the software tool MATLAB and results have been studied. To compare the relative performance Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE) and Histogram are used.*

***Key Words*: Image encryption, Image decryption, Image security, ANN, CNN, Chaotic system, AES, MSE, PSNR**

1. INTRODUCTION

In recent years, more electronic devices like mobile phones have started to provide additional functions like saving and exchanging multimedia data. Digital images are widely used in the internet, how to protect image content has become an issue to be urgently solved. Information security is the most common word used by any man, any device or any peripheral since past two centuries. Protection from malicious sources has become a part of the invention of new technologies. Chaotic encryption schemes can generally be split into three main categories: Firstly they can employ chaos as a mean of performing complex permutations of coordinates with repeated iterations. Early adopters of chaos theory in encryption schemes used this method of chaotic coordinate transformation to mix the image topologically as much as possible, as in the case of the baker map. The Baker map exploits a `kneeling' and `folding' of two dimensional data iterated several times. This map is discretized for digital images and generalized to incorporate a secret key for the encryption process. Artificial Neural Networks (ANN) are parallel adaptive networks which consist of non-linear computing elements called Neurons. The working of ANN is weighted sum of input signal and the connecting weight. The sum is added with its threshold and resultant signal is then considered or proposed for sigmoid nonlinear function. For several years, chaotic maps have been used for cryptographic applications, due to the hyper-sensitivity to initial conditions and input parameters, producing pseudorandom and unpredictable behavior. In this paper, a high security image encryption algorithm based on ANN and chaotic system is used.. Chaotic behavior is seen in many natural systems, such as weather and climate. The objective here is to investigate the use of ANNs in the field of chaotic Cryptography. The weights of neural network are obtained based on chaotic sequence. The chaotic sequence thus generated is forwarded to ANN and the weighs of ANN are updated, which influence the generation of the key in the encryption algorithm. To increase security, the Convolutional Neural Networks(CNN) is used. The weights for this neural networks is given by chaotic generator. The algorithm used for image encryption is Advanced Encryption Standard (AES). This algorithm is been implemented in the software tool MATLAB and results have been studied.

2. PROPOSED METHOD

The system uses a encryption method based on CNN and AES algorithm to increase the security of image from unauthorized access. In the proposed system two approaches chaotic cryptosystems and ANN based cryptosystems are combined to make chaotic based ANN systems. The encryption phase consists of control unit, chaotic generator, ANN training and encryption algorithm. The decryption phase consists of control unit, chaotic generator, ANN training and decryption algorithm.

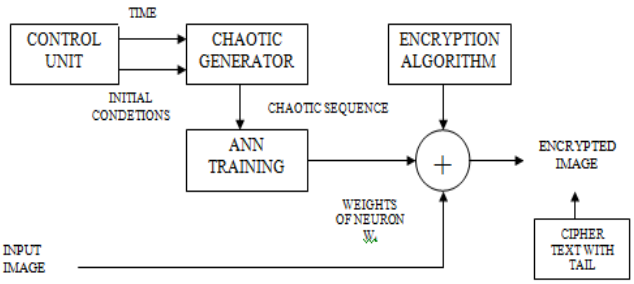

Fig. 1 Image Encryption

2.1 Chaotic Generator

Chaos communication is the application of chaos theory which provides the security in transmission of information. Chaos theory, describes the behavior of nonlinear dynamic

system under specific conditions that exhibit dynamics which is sensitive to initial conditions. The main characteristics of chaotic systems are the sensitivity to initial conditions.

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. The weights, w_i are added to the ANN using the chaotic generator. Chaotic systems exhibit emergence over scale, however, they do so in an unpredictable yet deterministic manner. In this common patterns may emerge, exact positions are highly unpredictable which are caused by hypersensitive dependence to the systems initial conditions. Chaotic systems are suitable for image encryption. Because of it's high initial condition sensitivity, randomness, unpredictability and are topologically mixing . Chaos can also be measured quantitatively, through means of the Lyapunov characteristic exponent(s) (LCE) of a given dynamic system, which describe the trajectory evolution of a dynamic (discrete) system,

$$\gamma(X_0) = \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln|f^{-1}(x_i)|$$

Where f (xi) gives the subsequent point xi, producing the Lyapunov exponent for the dynamic variable x. A spectrum of Lyapunov exponents is produced depending on the size of the phase space, i.e. a system with three dynamic equations will yield three Lyapunov exponents.

2.2 ANN Training

A neural network is a machine, designed to represent the way in which brain performs any particular task. ANN is used to generate the matrix code from the plain. At the end of this training process, the ANN produces the biases and weights matrices code, which are used in the first diffusion step. Encryption and decryption is done using Convolutional Neural Network. In deep learning, a convolutional neural network (CNN) is used. The CNN is a class of deep neural networks commonly applied to analyze visual imagery.

CNN is inspired by biological processes, that the connectivity pattern between neurons resembles the organization of the animal visual cortex. Individual neurons respond to stimuli only in restricted regions of the visual field, known as the receptive field. The receptive fields of neurons partially overlap such that they cover the entire visual field. CNN uses very little pre-processing compared to other image classification algorithms. Convolutional Neural Networks have a different architecture than regular Neural Networks. Ordinary Neural Networks transform an input data by putting it through a series of hidden layers. Each layer is made up of a set of neurons, where each layer is fully connected to all neurons in the layer before. In the final stage, there is a last fully connected layer the output layer that represents the predictions.

A CNN is able to successfully capture the Spatial and Temporal dependencies in an image through the application of relevant filters. The CNN architecture performs a better fitting to the image dataset due to the reduction in the number of parameters involved and reusability of weights. The network is trained to understand the sophistication of the image better.

3) AES Algorithm

AES algorithm is of three types: AES-128, AES-192 and AES-256. This classification is done based on the key used in the algorithm for encryption and decryption process. The numbers denotes the size of key in bits. This key size determines the security level as the size of key increases the level of security increases. The AES algorithm uses a round function. That is composed of four different byte oriented transformations: Substitution byte, Shift row, Mix columns, Add round key

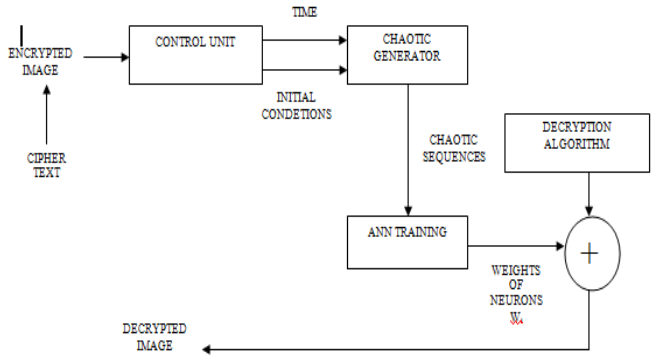

Fig 2 Image Decryption

2.3 Chaotic based ANN

In a Chaotic based Neural Network it's weights and biases are determined by chaotic sequence. Let, g denotes a digital signal of length M. Let g(n), M-1 be the one bit value of the signal g at position n. The following steps are given below:

STEP 1: Set the value of parameter M

STEP 2: Determine the parameter U and the initial point X(0) of one dimensional logistic map.

STEP 3: To develop the chaotic sequence X(0), X(1), X(2),...X(M) by X(n+1) = μ(n)(1-X(n)), and create binary representations b(8m-8), b(8m-7)....b(8m-2), b(8m-1) by using the generating scheme b(0), b(1), b(2),...b(8M-1),for m = 1,2,3,...,M

STEP 4: For n= 0 to M-1,

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

For, i = 0 to 1

$$W_{ji} = \begin{cases} 1 \; if \; j = i \; and \; b(8 \times n + i) = 0 \\ -1 \; if \; j = i \; and \; b(8 \times n + i) = 1 \\ 0 \qquad\qquad\qquad if \; j \neq i \end{cases}$$

$$\theta_i = \begin{cases} \frac{-1}{2} \; if \; b(8 \times n + i) = 0 \\ \frac{1}{2} \; if \; b(8 \times n + i) = 1 \end{cases}$$

I ϵ (0, 1, 2, 3, 4, 5, 6, 7)

For, i= 0 to 7,

$$d_i^1 = f\left(\sum_{i=0}^{7} w_{ji} \times d_i + \theta_i\right)$$

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

End

STEP 5: The encrypted image g^{11} is obtained.

In the Decryption is done same as the Encryption. The input signal to decryption is $g^{11}(n)$ and the otput is $g^1(n)$. In the case of images pixels are processed by neurons. The encrypted image with pixels that is disordered is obtained. In the decryption side, according to initial conditions chaotic binary sequence is generated and forwarded to ANN which generates the weights to generate the key to obtain original image.

2.4 NN Architecture

A neural network with deep learning neurons is used that is Convolutional Neural Network. It has 3 layers :

- Convolutional layers
- Pooling layers
- Fully connected layers

These 3 layers are combined to form CNN Architecture. To find the best NN structure to produce chaotic sequence is by changing the number of hidden layers, the number of neurons in the hidden layers, and the transfer functions in the neurons. Convolutional Neural Networks are simple neural networks that are convolution in the place of general matrix multiplication in at least one of their layers. After the training process, the ANN models were tested using the sorted test data, the suitable network structure is $8 \times 10 \times 8$, trained with back propagation algorithm. That means the number of neurons is 8 in the input layer, hidden layer it is 10, and In the output layer it is 8.

The input layer and output layer neurons have linear activation functions and the hidden layer has hyperbolic sigmoid activation functions.

The weights of neural network is given by, the complex substitution and sub-substition incorporates chained hill ciphers that resemble a fully connected neural network structure given by the equation,

$$y_i = \sum_{j=1}^{N} W_{IJ} X_J \; \forall \; i = 0,1,2,\ldots,M$$

However, the weights and inputs, w_{ij} and x_{ij}, will be treated as the elements of GF(2^8). The addition and multiplication operations are given in GF (2^8). The matrix is given by,

$$Y = Wx,$$

Where,

$$\begin{bmatrix} Y1 \\ Y2 \\ \vdots \\ YM \end{bmatrix} = \begin{bmatrix} W11 & \cdots & W1N \\ \vdots & \ddots & \vdots \\ WM1 & \cdots & WMN \end{bmatrix} \begin{bmatrix} X1 \\ X2 \\ \vdots \\ XN \end{bmatrix}$$

$$W_{ij}, x_i \sum (0, 1, 2, 3, \ldots\ldots\ldots, 255)$$

This can be cascaded as individual layers of an L – layer network within Chaos net.

$$Y_L = W_L(W_{L-1}(W_{L-2}, \ldots\ldots, (W_0(X))$$

A) Weight given to Sigmoid Activation functions

The weights of a connection is adjusted by an amount proportional to the product of an error signal, δ. There is k receiving input unit and j output unit.

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

- For the output unit, the error signal is given by,

$$\delta_a^p = \left(d_a^p - y_a^p\right) F(\delta_p^a)$$

The activation function F is the sigmoid function,

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

- In this the derivative is equal to,

$$F(\delta^p) = \frac{\partial}{\partial \delta^p} \frac{1}{1 + e^{-\delta p}}$$

$$F(\delta^p) = y^p(1 - y^p)$$

Error signal for the output is,

$$\delta a^p = (d\,a^p - y a^p) y^p (1 - y^p)$$

- The error signal for a hidden unit is determined recursively in terms of error signals of unit to which it directly connects.
- For Sigmoid activation function,

$$\delta_h^p = F^1(\delta_h^p) \sum_{a=1}^{N_a} \delta_a^p W_{ha}$$

$$= y_h^p (1 - y_h^p) \sum_{a=1}^{N_a} \delta_a^p W_{ha}$$

- The size of data sheet depends on the size of hidden layers. The size of hidden layer is changed as the complexity of the neural network increases.

2.5 Image encryption using deep neural network

STEPS:

I. Generation of chaotic sequence
To generate chaotic sequence first input sequence is selected. Then, the chaotic sequence will be generated by using logistic map.
X (n+1) = $\mu(n)\left(1 - x(n)\right)$
X (i) = mu$* X(i-1) * (1 - X(i-1)$

II. Generate CNN output
To generate CNN network, weights based on the chaotic sequence will be calculated. CNN extracts the features of images automatically. This effectively uses adjacent pixel information to down-sample the image first by convolution and then uses a prediction layer at the end. Thus it gives better accuracy

III. Image Encryption
In this stage AES algorithm is used to encrypt the image. AES tend to create a uniform image histogram that protects it from plaintext attack.

3. RESULT AND ANALYSIS

The deep neural network in chaos has been implemented MATLAB 2019a. To evaluate the quality of decrypted image the histogram, PSNR and MSE is applied.

Result 1) Lena Image

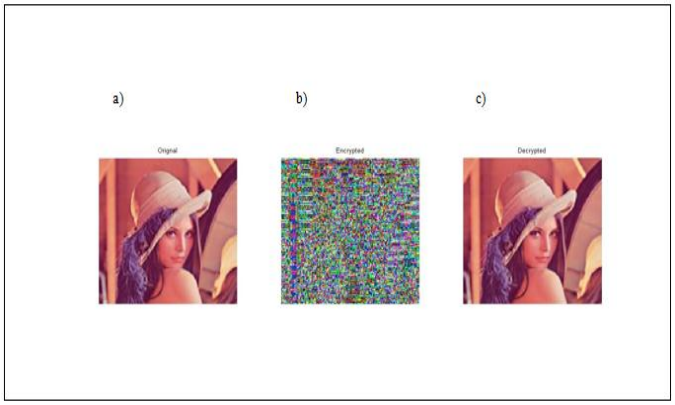

Fig 3: a) Original image I, b) Encrypted image, c) Decrypted image

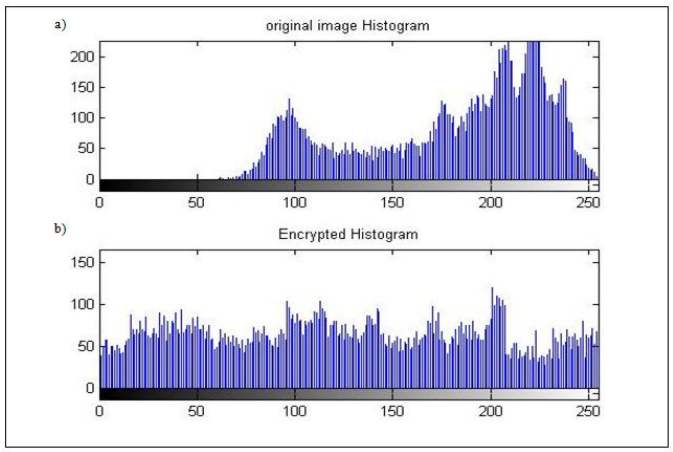

Fig 4: a) Original image histogram, b) Encrypted image histogram

Result 2) Bird Image

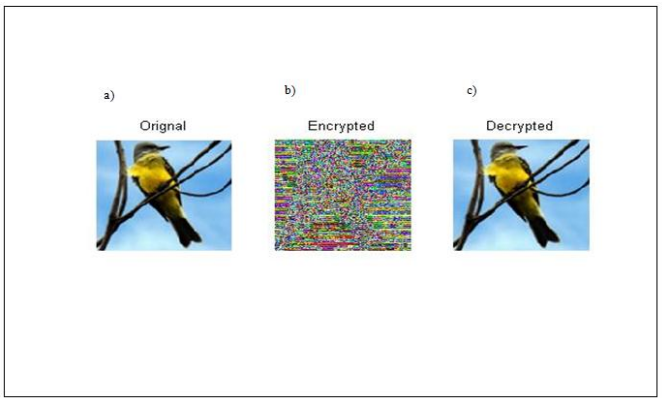

Fig 5: a) Original Image, b) Encrypted Image, c) Decrypted Image

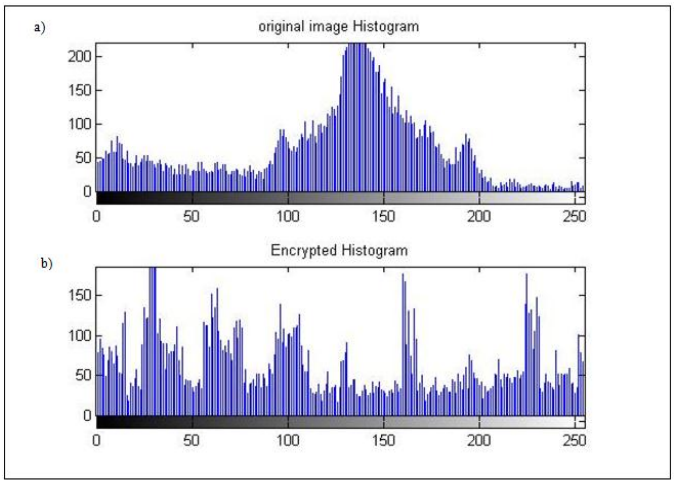

Fig 6: a) Original image histogram, b) Encrypted image histogram

The first image in fig (3a) and fig (5a) is the original input image. The image in fig (3b) and fig (5c) is the encrypted

image. The third image in fig (3c) and fig (5c) is the decrypted or original image. The Histogram for original and encrypted image is shown in fig (4) and fig (6).

Table I The PSNR and MSE ratios of original image to decrypted image

PARAMETERS	Lena Image	Bird Image
PSNR	+∞	+∞
MSE	0	0

Table II PSNR Ratio of Chaotic, ANN, and Deep Neural Network based chaotic systems.

Images	Chaotic cryptosystems	Neural cryptosystems	Deep Neural cryptosystems
Lena	7.9100	7.5070	8.5146
Bird	5.7941	5.0518	6.8951

Table III MSE Ratio of Chaotic, ANN, and Deep Neural Network based chaotic systems.

Images	Chaotic cryptosystems	Neural cryptosystems	Deep Neural cryptosystems
Lena	10.1233e+03	10.1321e+03	9.1541e+03
Bird	10.1453e+03	10.1120e+03	9.1452e+03

Table I shows the PSNR and MSE values of Lena image and Bird image by comparing the original and decrypted image. Table II and Table III shows the comparison of PSNR and MSE values of Chaotic cryptosystems, Neural cryptosystems and Deep Neural Network based cryptosystems. This table shows an increase in PSNR values and decrease in MSE values by using Deep Neural Networks.

4. CONCLUSION

In this paper, combination of Chaotic and Deep Neural Network cryptosystems are combined. Here the advantages of both systems are used. That is randomness of chaotic theory, learning of ANN, good PSNR eliminates the limitation of chaotic system and ANN cryptosystems. The security of image encryption is increased and the parameters PSNR and MSE of different input images are observed. There are number of approaches in image encryption in the context of chaotic systems, neural networks, using genetic algorithms, etc…The goal is to provide high security.

ACKNOWLEDGEMENT

I am ineffably indebted to my guide Mrs. Haseena P for her active guidance and encouragement to accomplish this assignment and Wikipedia for the correct source of information.

REFERENCES

[1] Eva Volna, Martin Kotyrba, Vaclav Kocian, Michal Janosek, “Cryp-tography Based on Neural Network”, 26th European Conference on Modelling and Simulation, 2012

[2] An Adaptive Neural Network guided secret key based encryption through recursive positional modulo-2 substitution for online wireless communication (annrpms) (j. K. Mandal1, Arindam sarkar2 department of computer science & engineering university of Kalyani, Kalyani- Nadia, West Bengal, India)

[3] Image encryption based on diffusion process and multiple chaotic maps (ameena marshnil n*, binish m c*, department of ece , kmea engineering college , kerala , india)

[4] Modified Chaotic Key-based algorithm for Image encryption and VLSI realization (K.Deergha Rao Ch. Gangadhar Research and Training Unit for Navigational Electronics Department of ECE, PVP Siddhartha Institute of Technology Osmania University Vijayawada , Hyderabad)

[5] A novel symmetric cryptography based on chaotic signal generator and a clipped neural network (Tsing Zhou, Xiaofeng Liao, and Yong Chen Department of Computer Science and Engineering, Chongqing University 400044, Chongqing, China).