Application of Chaotic Neural Network in Cryptography

Suhrid Das
ECE Department, Jalpaiguri Government Engineering College
Jalpaiguri, India

Shankha Shubhra Mukherjee
ECE Department, Jalpaiguri Government Engineering College
Jalpaiguri, India

Sudip Mandal
ECE Department, Jalpaiguri Government Engineering College
Jalpaiguri, 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. 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). In this paper, data or information are encrypted and decrypted using artificial neural networks based on chaotic algorithm. Chaotic system generates random numbers which is highly sensitive to initial conditions. So, in this cryptosystems, we have utilized the advantages of randomness of chaotic theory, rigorous structure of ANN for encryption and decryption. Chaotic Neural Network (CNN) has been implemented for encryption and decryption of on array of numbers, a word and RGB image. Results indicated that Chaotic Neural Network can be used effectively in cryptography.

Keywords
Cryptography, Chaos theory, Artificial Neural Network, Chaotic Neural Network, Word Encryption, Image Encryption and Decryption

1. INTRODUCTION
With the advent of modern internet technology, both convenience and the need for security have come to the lime light. The world now prefers all actions to be done in the digital domain since it time saving and much more reliable. Throughout the years numerous methodologies have been applied to increase the security related to modern day data transfer and transactions. Right here, the concept of cryptography [1] emerges. In elementary terms, cryptography is the process of converting a message or a signal by the help of an algorithm into a certain form which is unrecognizable by anyone other than the ones who have access to the algorithm. The process of conversion of the message signal is termed as encryption and the reverse procedure is called decryption. Mathematicians and computer scientists are always on the move to evolve new encryption techniques to increase security and make the process of communication more dependable. Data security in cloud systems by a novel venture using encryption and steganography has been discussed in [2]. Description of design and employment of simple algorithms based on Data Encryption Algorithm (DES) algorithm [3] has been described. The necessity to secure databases and a corresponding encryption strategy has been presented in [4]. In this paper, a high security image encryption algorithm based on Artificial Neural Network (ANN) [5] and chaotic system [6] is used. ANN is a computational paradigm influenced by the layout of the human brain. 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 [7]. Chaotic Neural Network (CNN) has been used for the encryption and decryption purpose. The rest of the paper is organized is as follows. In next section, literature survey on ANN and Chaotic Neural Network has been given in details followed by prerequisite theoretical background which is necessary to understand this work. Proposed methodology is elaborated Section 4. Different results corresponding to Chaotic Neural Network are shown in Section 5.

2. LITERATURE SURVEY
The development of the Artificial Neural Network [8] began back in the 1800s with scientific endeavors to study the activity of the human brain. In 1890, William James published the first work about brain activity patterns. In 1943, McCulloh and Pitts [9] created a model of the neuron, which became the basic building block of the Artificial Neural Network. Subsequently in the next few years, many works about modelling and learning schemes of ANN were published. Later, there were endeavors to use neural network procedures for character recognition. This gave birth to the idea of perceptron. Perceptron was a linear system and was valuable for solving issues where the in- put classes were linearly separable in the input space. Despite the early success of perceptron and artificial neural network research, it had many limitations. The prime limitation of ANN [10] was that it was not capable of distinguishing patterns that are not linearly separable in input space with a linear classification problem. After over two decades of tackling its limitations and when ANN research [11] was of minimum interest, Hecht-Nielsen showed a two-layer perceptron in 1990. The backpropagation problem, which was rediscovered in 1986, is a type of gradient descent algorithm used with artificial neural networks for reduction and curve-fitting.

A network is called chaotic neural network (CNN) [12], [13] if its weights and biases are determined by chaotic sequence. Many works already have done in cryptography as well as others engineering area. H. Kaur et al. [14] have studied the CNN for image encryption for different initial condition for the chaotic sequence generator. Min Long et al. [15] have used CNN for image and video encryption. Kuwar et al. [16] used CNN algorithms for data encryption and compared results with such as DES, AES, Blowfish, Elliptic curve cryptography. In 2012, Shweta et al. [17] utilized CNN with triple key for image encryption purpose. On the hand, Shukla et al. [18] have used sequential machine and the CNN for image cryptography purpose. Liang et al. [19] employed CNN for wireless communication with satisfactory accuracy. Maddodi et al. [20] hybridized heterogeneous CNN and DNA encoding for the encryption. Chen et al. used novel fractional-order discrete chaotic neural network and DNA sequence operations for the image encryption. Recently, Liu et al. applied Hopfield chaotic neural network for scrambling and image encryption. So, in this review paper we are aiming at the use of CNN for encryption and decryption of numbers, words and images and check if it worked accurately or not..

3. PRELIMINARY CONCEPT
An ANN is developed on the basis of a group of linked nodes

mimicking the structure of the biological neural network. Each node of the ANN possesses the ability to transfer signals to other such neurons, and the signals are modelled by real numbers. The output of each neuron is computed by a non-linear function of the sum of each of its inputs. Hence, the connection between the neurons is associated with a weight and a threshold. A node is activated if the output of an individual node exceeds the certain threshold value that has been specified. If the value is less than the threshold, then no data is sent over to the following node. In general, the nodes are associated in layers, hence the signals travel starting from the first layer through one or many intermediate layers and finally reaches the last layer. The intermediate layers are termed as hidden layers. The working of Neural Networks is centered on training data. By the means of training ANNs augment their accuracy over time, and on optimization they serve as powerful and reliable computational tools able to work on a large amount of data.

Chaos is statistically indistinguishable from randomness, and yet it is deterministic and not random at all. Chaotic system will produce the same results if given the same inputs, it is unpredictable in the sense that you cannot predict in what way the system's behavior will change for any change in the input to that system. In case of Chaotic Neural Network, the weights of neural network are obtained based on chaotic sequence. The chaotic sequence (based on initial condition) thus generated is forwarded to ANN and the weighs of ANN are updated, which influence the generation of the key in the encryption algorithm. Here, we exploit its unique properties for encryption of an array of integers. Chaotic system is highly sensitive to initial conditions.

In the first instance, two keys are taken manually by the user: μ and x(0), to encrypt an array. Consider the length of the input sequence to be N. We generate a chaotic sequence x, with length N, using the two unique keys. The first element of this chaotic sequence is $x(0)$. The subsequent elements are generated using the formula:

$$x(i) = \square x(i-1)(1-x(i-1)) \quad (1)$$

The individual elements of the array x are first scaled and then type casted into unsigned integer (with range 0-255). The binary form of this converted array is then stored in another matrix b. Each row of the matrix b represents the binary form of the converted elements from the array x. Thereafter, a weight matrix is generated for each of the individual rows of the matrix b. These weight matrices are diagonal matrices, where each diagonal element is either 1 or -1. The essence of distinctiveness of the algorithm lies on its simplicity where each of the diagonal elements represents a bit from a row of the matrix b. The element on the diagonal of i^{th} row of the j^{th} weight matrix will be 1 if the i^{th} element of the j^{th} row of matrix b is 0 and -1 if it is 1.

For every bit of matrix b, there is a corresponding value of θ. The value of θ is -1/2 if the corresponding bit from matrix b is 0 and 1/2 if the bit value from matrix b is 1. An entire row of the weight matrix is element wise multiplied with the binary form of the corresponding input element. If the summation of this entire element wise multiplied array is greater than or equal to zero then a temporary value of 1 is stored in a variable. If the summation is negative, then a zero is stored in that variable. This value is added with the corresponding value of θ for that row. This is finally stored in a matrix dx. The dimension of the matrix dx is $N \times 8$. The i^{th} row of the j^{th} column of the matrix dx represents the element from the i^{th} row of the j^{th} column of matrix b. We consider each row of the matrix dx as an entire binary sequence. This sequence is then converted into its corresponding integer form. All the N rows from the matrix dx is converted into a subsequent integer. These N integers are the final encrypted output.

This entire process is unique and it generates a different output for every different set of keys. Furthermore, this process is reversible and the same algorithm can be used to decrypt the encrypted data, given that the keys are same. A data can be encrypted and then obtained cipher was decrypted by using the chaotic dynamics. It is accepted that the initial conditions which were used in the training phase of the chaotic NN model and the system parameters are known by both the transmitter and the receiver. The critical aspect here is to design a neural network that exhibits the property of chaos.

4. METHODOLOGY

Here, 8bit is considered to represent the unsigned integer value during encryption as maximum allowable integer value is 255 (for this study). Now, this 8 binary bit will encrypted based on chaos theory and will create different 8bits pattern. Hence, the number of input and output nodes of Chaotic Neural Network is 8 for both input and output layer respectively. So, we are 8x8 CNN for cryptography. At the end, the output binary value will be converted back to integer value again which will indicate the encrypted data. CNN has been applied for 3 different cases of data encryption those are array of numbers, a word, and a RGB image.

Case-1: First, an array consisting of a set of random numbers is taken as input and feed it to the algorithm working on the principle of Chaotic ANN. Initial random values of the two keys $x(0)$ and μ are required to generate the chaotic sequence. Next, the chaotic neural network (8x8) is designed based on the input adaptive weights, activation function and bias. 3. Once the chaotic neural network is designed, the input numbers are applied to the network to obtain the cipher. Subsequently the cipher numbered will be displayed. This cipher numbers will be again decrypted by same CNN algorithm.

Case-2: Further, the algorithm is employed on a set of words. Initially, the plain text is entered by the user and it is displayed and stored. Subsequently, the plain text is converted into its ASCII equivalent and the ASCII equivalent of the plain text is displayed. Chaotic neural network (8x8) is created again same as earlier one. Once the chaotic neural network is designed, the ASCII equivalent of the input is applied to the network to obtain the cipher text. Subsequently the cipher text is displayed. The cipher text is then applied to the chaotic network again for decryption and then the plain text is extracted from the cipher text. The plain text obtained through the decryption mechanism is displayed.

Case-3: Last, after successful results for both numbers and words; the algorithm is finally operated on a standard RGB image. An image in computational terms is a set of pixels; each assigned a different value that depicts a different color by the combination of the three basic colors: red, blue, and green. Hence, an image can be represented straightforwardly through a 3-Dimensional matrix comprising the different values of the pixels of which the image is made up. The 3D matrix can be broken down into 3 matrices having values of the 3 basic color components separately. Nethaotic neural network (8x8) same as earlier one. Now, the CNN algorithm is applied on the three matrices (pixel value) independently

and the derived results are then reverted back in the form of a 3D matrix that displays the encrypted RGB image. Similarly, the cipher image has been decrypted using same CNN.

5. RESULTS AND DISCUSSION

Chaotic Neural Network has been employed for above mentioned three cases are array of numbers, a word, and a RGB image using MATLAB. All simulations have been performed on a laptop containing Windows10 Operating System, 8 GB RAM and i5 processor. The initial values of CNN generator are set as $x(0) = 2$ and $ = 3$ respectively.

Case-1: For first case, an arbitrary array of integers: [0 13 28 37 62 15 123 52 52 85] is considered for encryption. Now after applying CNN, the encrypted values become [127 114 99 90 65 112 4 75 75 85]. Same CNN was applied for decryption purpose and it decrypted the array of integers accurately. Fig. 1 and Fig. 2 show the encrypted and decrypted output using MATLAB respectively.

```
>> Encryption_chaotic_neural_network

inp =

     0    13    28    37    62    15   123    52    52    85

x(1)=
     2

mu =

     3

outx =

   127   114    99    90    65   112     4    75    75    85
```

Fig. 1: Encryption of an array of integers

```
inp =

   127   114    99    90    65   112     4    75    75    85

x =

     2

mu =

     3

outx =

     0    13    28    37    62    15   123    52    52    85
```

Fig. 2: Decryption of the encrypted array of integers

Case-2: In second case, the word "Encoding" is considered for encoding. Now, standard ASCII values corresponding to this word can be expressed as [69 110 99 111 100 105 110 103]. Now, this ASCII sequence is being encrypted by the CNN (8x8). The corresponding encrypted output sequence is given by [58 17 28 16 27 22 17 103]. Next, CNN has been applied for decryption and we found that the word corresponding to the decrypted ASCII values is exactly same as input word i.e. "Encoding". It indicates that CNN can be applied for word encryption and decryption accurately. Fig.3, Fig. 4 and Fig. 5 are showing the input word, encrypted ASCII values, and decrypted ASCII and corresponding word respectively.

```
inp='Encoding';
```

Fig. 3: Input word

```
outx =

    58    17    28    16    27    22    17   103


ans =

    ':□□□□□□g'
```

Fig. 4: Encrypted result of the input word

```
Inp=
:□□□□□□g

x =

     4

mu =

     7

outx =

    69   110    99   111   100   105   110   103

ans =

    'Encoding'
```

Fig. 5: Decrypted result of the Input Word's Encrypted sequence

Case-3: Next, CNN have been implanted on a standard RGB image (Fig. 6a) where the pixel values of Red plane, Blue plane and Green plane are encrypted individually. After reconverting these encrypted values into a RGB image, the encrypted image has been obtained which is shown below in Fig.6b. It has been observed that encrypted image become unidentifiable in normal view as it very much differ from original one. By using same CNN for decryption of individual Red, Blue and Green Plane of the encrypted image, it has been observed that decrypted image (Fig.6c) is same as input image. It indicates the effectiveness of using CNN for image encryption. Moreover, to analyze the encrypted image and observe the differences we have evaluated the probability density functions (PDF) of both the original and the encrypted image. From Fig. 7a and Fig. 7b, it can be easily observed that the frequency components differ considerably for encrypted and decrypted images. Hence, it can be confirmed that the process of encryption and decryption using Chaotic Neural Network has yielded a satisfactory accuracy.

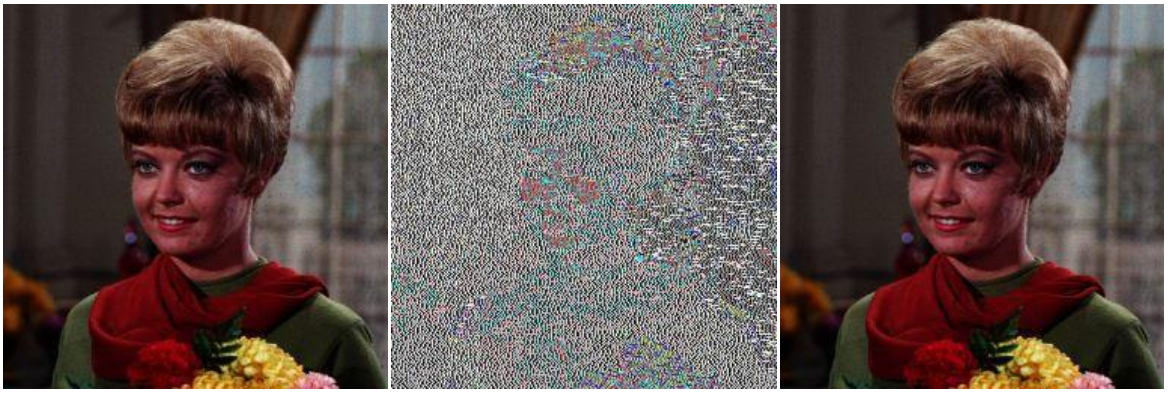

Fig. 6a: Original Image **Fig.6b: Encrypted Image** **Fig. 6c: Decrypted Image**

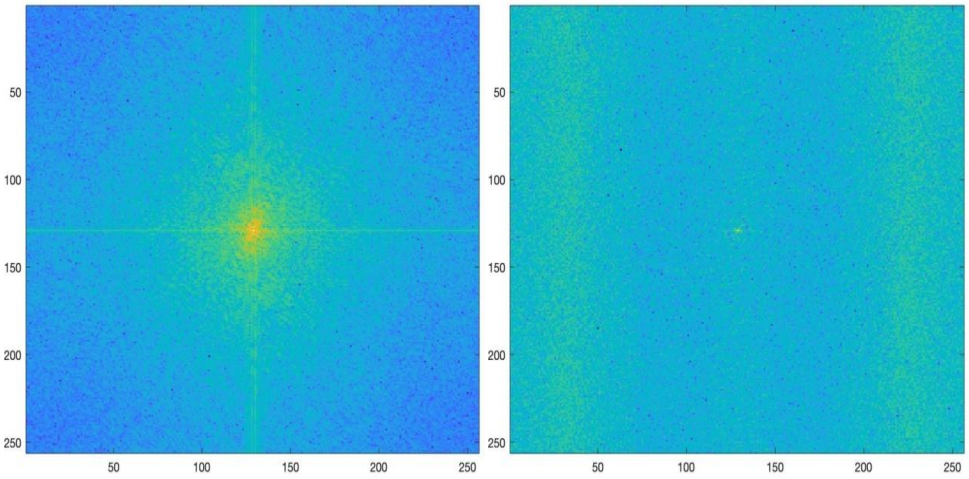

Fig. 7a: PDF of original image **Fig. 7b: PDF of encrypted image**

6. CONCLUSION

Cryptography is the exchange of information among the users without leakage or loses of information to others. Chaotic systems are sensitive to initial conditions and system parameters. Noise like behavior of chaotic systems is the main reason of using these systems in cryptology. Chaos is statistically indistinguishable from randomness, and yet it is deterministic and not random at all. By using the features of both Neural Network and chaos system, Chaotic Neural Network (CNN) is used to generate secret key for encryption. A binary sequence generated from a chaotic system, when the biases and weights of neurons are set. This research aims mainly at CNN based cryptosystems for the encryption and decryption of numbers, words and image data. The results show that CNN can be applied in cryptography with great accuracy. In future, different chaotic systems may be incorporated to observe the effectiveness of the encryption.

7. REFERENCES

[1] William Stallings, ―Cryptography and Network Security: Principles and Practice‖, (5th Edition), Prentice Hall, 2010.

[2] N. Subramanian, O. Elharrouss, S. Al-Maadeed and A. Bouridane, "Image Steganography: A Review of the Recent Advances," in IEEE Access, vol. 9, pp. 23409-23423, 2021, doi: 10.1109/ACCESS.2021.3053998.

[3] Seung-Jo Han, Heang-Soo Oh and Jongan Park, "The improved data encryption standard (DES) algorithm," Proceedings of ISSSTA'95 International Symposium on Spread Spectrum Techniques and Applications, 1996, pp. 1310-1314 vol.3, doi: 10.1109/ISSSTA.1996.563518.

[4] T. P.Wasnik , Vishal S. Patil , Sushant A. Patinge , Sachin R. Dave , Gaurav J. Sayasikamal, "Cryptography as an instrument to network security‖, International Journal of Application or Innovation in Engineering & Management (IJAIEM), Vol. 2, Issue 3, 72-80, 2013.

[5] Wang SC. (2003) Artificial Neural Network. In: Interdisciplinary Computing in Java Programming. The Springer International Series in Engineering and Computer Science, vol 743. Springer, Boston, MA. https://doi.org/10.1007/978-1-4615-0377-4_5.

[6] K.Kaneko, I. Tsuda, Complex Systems: Chaos and Beyond, Springer, New York, 2000, pp.57–162.

[7] Wolfgang Kinzel, IdoKanter, ―Neural Cryptography‖, Proceedings TH2002 Supplement, Vol. 4, 147 – 153, 2003.

[8] Wang SC. (2003) Artificial Neural Network. In: Interdisciplinary Computing in Java Programming. The Springer International Series in Engineering and Computer Science, vol 743. Springer, Boston, MA. https://doi.org/10.1007/978-1-4615-0377-4_5.

[9] McCulloch, W.S., Pitts, W. A logical calculus of the ideas immanent in nervous activity. Bulletin of Mathematical Biophysics 5, 115–133 (1943). https://doi.org/10.1007/BF02478259.

[10] S. Mandal, and I. Banerjee, "Cancer Classification Using Neural Network", International Journal of Emerging

Engineering Research and Technology, vol. 3(7), pp. 172-178, 2015.

[11] S. Mandal, G. Saha, and R. K. Pal, "Neural Network Training Using Firefly Algorithm", Global Journal on Advancement in Engineering and Science, vol. 1(1), 2015, pp. 07-11,

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

[13] M.S. Baptista, "Cryptography with Chaos," Physics Letters A, 240, pp.50-54, 1998.

[14] Kaur, H. and Panag, T.S., 2011. Cryptography using chaotic neural network. International Journal of Information Technology and Knowledge Management, 4(2), pp.417-422.

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

[16] Kuwar, L.M. and Pathan, A.I., Implementation Of Chaotic Neural Network Using Chaos For Data Encryption. IJSART - Volume 4 Issue 5 –MAY 2018

[17] Shweta B. Suryawanshi, Devesh D. Nawgaje, ―A triple-key Chaotic neural network for cryptography in image processing‖, International Journal of Engineering Sciences & Emerging Technologies, Vol. 2, Issue. 1, 46-50, 2012.

[18] Nitin Shukla, Abhinav Tiwari, ―An Empirical Investigation of Using ANN Based N-State Sequential Machine and Chaotic Neural Network in the Field of Cryptography‖, Global Journal of Computer Science and Technology Neural & Artificial Intelligence, Vol. 12, Issue.10,No. 1,17-26, 2012.

[19] Liang, C., Zhang, Q., Ma, J. and Li, K., 2019. Research on neural network chaotic encryption algorithm in wireless network security communication. EURASIP Journal on Wireless Communications and Networking, 2019(1), pp.1-10.

[20] Maddodi, G., Awad, A., Awad, D., Awad, M. and Lee, B., 2018. A new image encryption algorithm based on heterogeneous chaotic neural network generator and dna encoding. Multimedia Tools and Applications, 77(19), pp.24701-24725.

[21] Chen, L.P., Yin, H., Yuan, L.G., Lopes, A.M., Machado, J.T. and Wu, R.C., 2020. A novel color image encryption algorithm based on a fractional-order discrete chaotic neural network and DNA sequence operations. Frontiers of Information Technology & Electronic Engineering, 21(6), pp.866-879.

[22] Liu, L., Zhang, L., Jiang, D., Guan, Y. and Zhang, Z., 2019. A simultaneous scrambling and diffusion color image encryption algorithm based on Hopfield chaotic neural network. IEEE Access, 7, pp.185796-185810.

8. AUTHORS' PROFILES

Suhrid Das is a B.Tech. student of Electronics and Communication Engineering Department, Jalpaiguri Government Engineering College, Jalpaiguri, India.

Shankha Shubhra Mukherjee is a B.Tech. student of Electronics and Communication Engineering Department, Jalpaiguri Government Engineering College, Jalpaiguri, India.

Dr. Sudip Mandal received his PhD degree from the Department of Computer Science and Engineering, University of Calcutta, India in 2019. He received his B.Tech. and M.Tech. in Electronics and Communication Engineering from Kalyani Government Engineering College, India in 2009 and 2011, respectively. Currently, he is working as the Assistant Professor of Electronics and Communication Engineering Department, Jalpaiguri Government Engineering College, Jalpaiguri, India. He was the former Head of ECE Department, Global Institute of Management Technology, Krishnagar, India. His current research interests include computational biology, tomography, artificial intelligence and optimization. He is a member of the IEEE Computational Intelligence Society. He has 42 publications in peer-reviewed journals, and in national and international conferences. He also published 2 Indian patents so far. Dr. Mandal has authored 2 Books so far. He is also editorial and review board member of many peer review international journals.