iJETRM
International Journal of Engineering Technology Research & Management

CHAOS AND ANN BASED CRYPTOGRAPHY

Siddharth Tathagat
Rahul R Sherekar
Dr. H. V. Kumaraswamy
R. V. College of Engineering, Bengaluru
siddhartht.tc16@rvce.edu.in
rahulrsherekar@gmail.com
kumaraswamyhv@rvce.edu.in

ABSTRACT

In this paper, an encryption-decryption scheme algorithm is presented which is proposed using chaos neural network.Chaos-based sequence is used to achieve neural network weights. The chaos sequence obtained is transmitted to the Artificial Neural Network, and ANN weights are modified, influencing key generation in the encryption algorithm. In order to address the demerits of chaos-based system, it is proposed to combine methods of ANN and chaotic cryptosystem. The resulting method, CNN, combines the advantages of both systems which are key responsiveness and hiding the connection between original message and encrypted message. The greater the level of architectural concurrency, to gather results from primary diagnosis to unexpected circumstances, efficiency, and reliability are some of the perks achieved through ANN.

KEYWORDS:

Chaotic Neural Network (CNN), Artificial Neural Network (ANN), Chaos-Based Cryptography, Cryptography.

INTRODUCTION

Cryptography is a method of network security which changes the stream of data into a form unreadable by non-authorized personnel. It is mainly used when data is communicated through an untrusted network, like the internet. It provides safety and validation of users. The methods to implement cryptography are based on key availability.

The working of digital computers and human brains is completely different. The human brain has structures called neurons which it organizes to complete a particular task. Especially, recognition functions are performed by a brain much faster than the most powerful computers. A neural network emulates the working of a human brain so as to complete a given task. Implementation is done either by software methods or by using electronic components.

Generation of an artificial neural network basically has two steps, first, a learning of the environment, and second, the strength of its interconnections. These can be used to perform tasks which might be too complex even for a human brain. Tasks can be performed based on learning and previous experience. Operating in real time and organizing by itself are more of its advantages.

An ANN has nodes, which are interconnected and tasks are performed based on the strength of these connections. It contains algorithms to determine effective input, updated input, bias input, and the

iJETRM
International Journal of Engineering Technology Research & Management

method of gathering information. Recurring network, forward-feed singular layer and forward-feed multiple layer are the network topologies used.

Process of learning includes three steps, namely, non-administered learning, administered learning and bolstered learning. To set the connection strengths, either prior knowledge or training methods can be used. Back propagation learning rule is used to deal with a multiple-layer network.

Chaotic mapping is the encryption of data using chaotic functions. Chaos is similar to randomness, but is not random and is deterministic. Logistics map contains a parameter which is used as a secret key for encryption purposes. Sinusoidal functions, non-linear shift registers, and logistics maps are some of the non-liner functions used to generate diffusion and confusion. There are various types of attacks that can be studied such as brute force attack, known encryption message attack, chosen encrypted message attack, known original text attack, chosen original text attack.

The cryptographic methods have their own sets of advantages and disadvantages. One method is superior in some aspect than the other and vice versa. So, in order to create a method such that the disadvantages of both the methods can be minimized and the advantages of both the methods can be maximized, the two methods (ANN and Chaos) are combined to make a chaotic neural network.

There are three major types of this system which are changing of positions, changing of values, and some combination of both operations. The proposed method provides high security, low distortion, and it expresses suitability for system integration. It also increases the system's memory capacity.

OBJECTIVES

The main objective of the study is to implement sequential machine using Jordan network, and implementation of combinational logic to choose between a 'fully connected' and a 'one-network-per-output' type neural network and also to implement chaos cryptography for encryption and decryption, and implementation of a combination of ANN and chaos cryptography which is Chaos-Neural Network cryptography (CNN).

METHODOLOGY

A Jordan network was used to implement a sequential machine of finite states. The output units contained activation values within the Jordanian network which are transmitted back to the input layer via a group of extra inputs which are named the state units. the number of state units and the number of output units are the same. The state and output units have a fixed weight of '+1' in their connection, and learning occurs only within the input unit-hidden unit connection and the hidden unit-output unit connection.

Back propagation methodology was used for the teaching of the Jordan topolgy. Therefore, applying the general delta rule requires a couple phases: x (input) is introduced and transmitted through the network during the first phase to determine the ypo (output) values for every node of the output. Comparing to its target output, an error signal is generated by this output for each unit of output. In the second phase, a reverse pass occurs through the network in which, each unit in the network receives the error signal and the calculation of appropriate weight changes is done.

iJETRM
International Journal of Engineering Technology Research & Management

For implementation of combinational logic, 2 types of ANN forward architectures have been used. The first type was a neural network which is completely connected, feed-forward. The other type does partition of the matter in independent sub-tasks which are lesser in size, and every sub-task is implemented through an ANN. Figure 1 shows the first type. It is a network which is fully connected, and depends on each input for obtaining each output. Figure 2, on the other hand, contains two networks, one for each bit of the output.

As every network in Figure 2 considers a single output which is independent, the problem size is required to be smaller, that allows less complexity in the neural networks and less time required for training. The first type of network has a target of combining every output bit's training and, hence, using lesser neurons and weights. The target of the second type of network was for each network to reduce the number of patterns, hence, to reduce the neuron count and the training time.

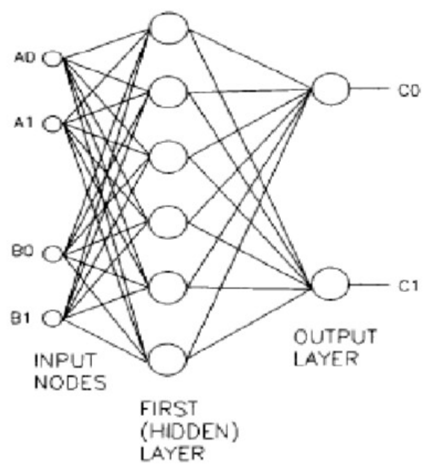

Figure 1: Fully connected network architecture

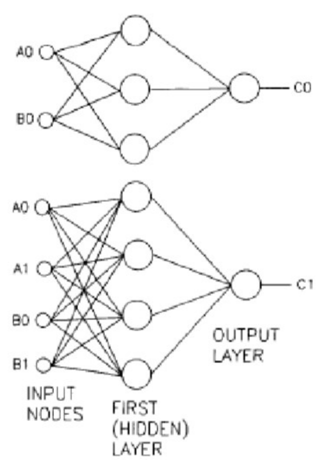

Figure 2: Architecture for 1 network per output

To find an optimized solution, a method with the minimum energy is preferred. Even if the algorithm of back-propagation does not find the very minimum always (i.e., the problem's easiest solution), the

ISSN: 2456-9348
Impact Factor: 4.520

iJETRM
International Journal of Engineering Technology Research & Management

algorithm would be good enough for the training. There was an alteration in the algorithm that weights were updated after each pattern was verified within the current repetition.

For chaos-based encryption and decryption of photos two separate keys generated from chaotic dual-map. Two different stages are required for cryptography using this method from the different keys created. Now to create a private key both the keys are EX-ORed with each other. Further this newly created private key is again EX-ORed with the original image. The measures taken in the encryption process are seen in figure 3.

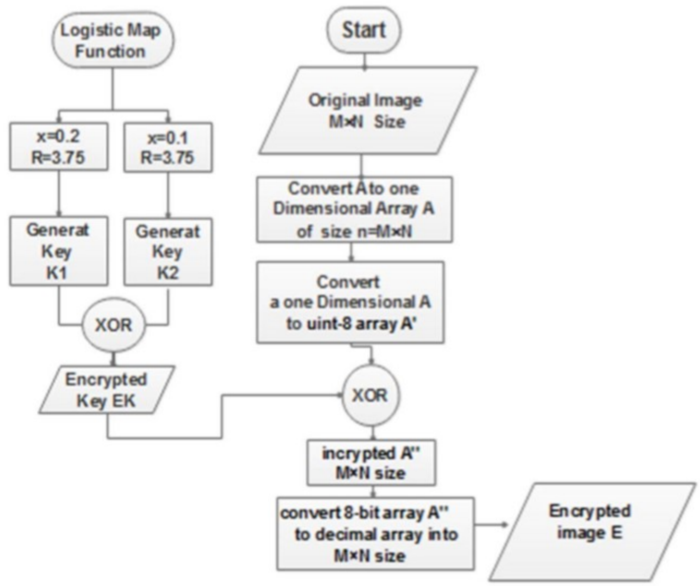

Figure 3: Architecture of the encryption algorithm

The process for encryption starts with entering an original photo of any size. Transform the original photo into a gray scaled photo if the entered photo is a color photo. Now hold the values of gray scaled photo into a 1-D array. Create two sets of private keys a_1 and $a_2$can be obtained from the map for any two different conditions in the early stage, i.e., the value of r and x_i. Now two different stages are required for cryptography using this method from the different keys created. Now to create a private key both the keys are EX-ORed with each other. Further this newly created private key is again EX-ORed with the original photo. Finally, an encrypted photo is obtained.For decryption of the image, similar measures are taken, only difference is that this time in place of original image, encrypted image is used and, in the end, the original image is obtained.

For implementation of chaotic neural network, The weights and external effects of an ANN are obtained by a sequence which has a chaos nature. Such type of method are called CNN. Thus for every iterative process, the weights and external efeects of the units in an ANN are adjusted according to the binary set of sequence created using chaos based random sequence. Following steps are followed for encrypting process using CNN:

iJETRM
International Journal of Engineering Technology Research & Management

1) For any input in an unit one must first know the size of the input. Such size is being hold in a variable. Let that variable be X.
2) Set the values of early conditions in the map.
3) From this create a chaos based sequence.
4) Now let us start a loop using a looping variable i, from 0 to X-1.

Let $s(i) = \sum_{k=0}^{7} d_i \text{ X } 2^k$……………………………1

for k= 0 to 7

l ϵ (0,1,2,3,4,5,6,7)

$$\theta_k = \begin{cases} -\frac{1}{2}\ if b(8i+k)=0, \\ \frac{1}{2}\ if b(8i+k)=1, \end{cases} \text{…………………...2}$$

end

for k= 0 to 7

$d'_k = f(\sum_{k=0}^{7} w_{kl} * d_k + \theta_k)$…………3

end

To obtain the decrypted output, the similar sets of procedure can be followed. Only difference is that yield obtained in equation 3 is given as input in s(i).

RESULTS AND DISCUSSION

Following are the results obtained after the implementation of sequential machine:

Using sequential machine, the serial adder was created as an example. Training is done by giving the number of inputs, number of outputs, number of states, input values, state values and the expected output values in different cases. Then, an error function graph was plotted by giving random inputs and observing the deviation from expected outputs.

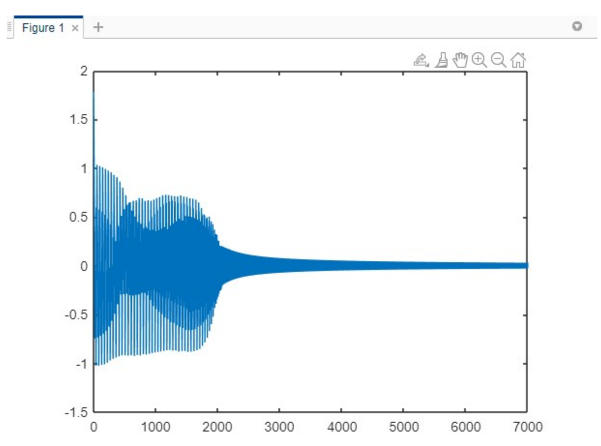

Figure 4: The error function graph plotted after learning is completed

iJETRM
International Journal of Engineering Technology Research & Management

In this graph (figure 4), the x axis represents the number of iterations and the y axis represents the mean error (deviation from the expected output). It can be observed that the error value decreases as the number of iterations increases.

Following are the results obtained after the implementation of sequential machine:

A comparative analysis is conducted between the architectures of type 1 and type 2 and the neural network size needed for the design.

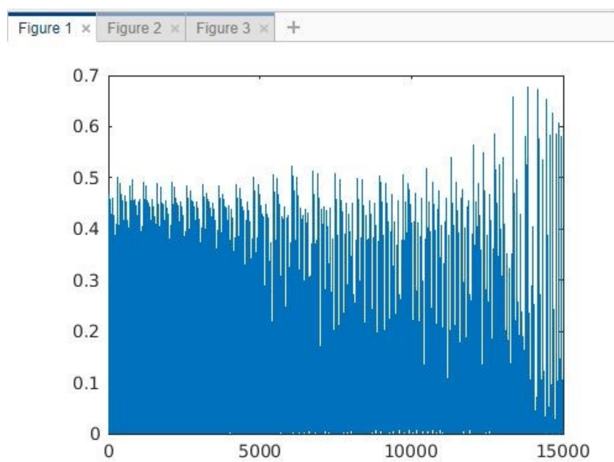

Figure 5: Neural network (fully connected) Type-1 MSE

In figures 5 and 6, x axis represents the number of iterations and y axis represents mean square error (MSE) of the ANN of types 1 and 2.

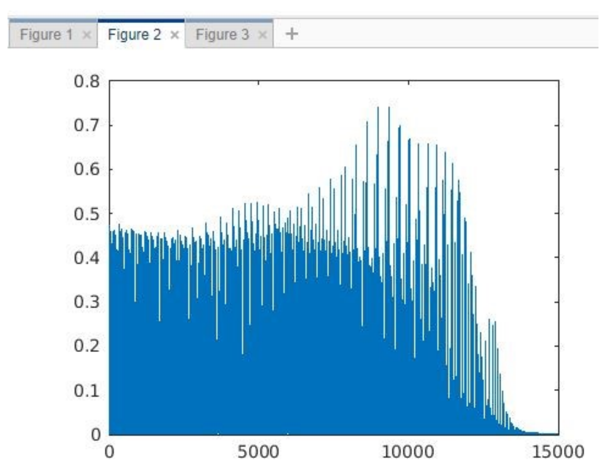

Figure 6: One output per network Type-2 MSE

iJETRM
International Journal of Engineering Technology Research & Management

From figure 6 it can be clearly seen that the neural network of type 2 looks for a lesser number of patterns and thus reduces both the number of neurons and the training time.

It can be seen from figure 5 that the neural network when fully connected (type 1) has a goal of combining training of all output bits and thereby using fewer neurons and weights. Hence, a trade-off between training time and weights is made when choosing the network type-1 and network type-2.

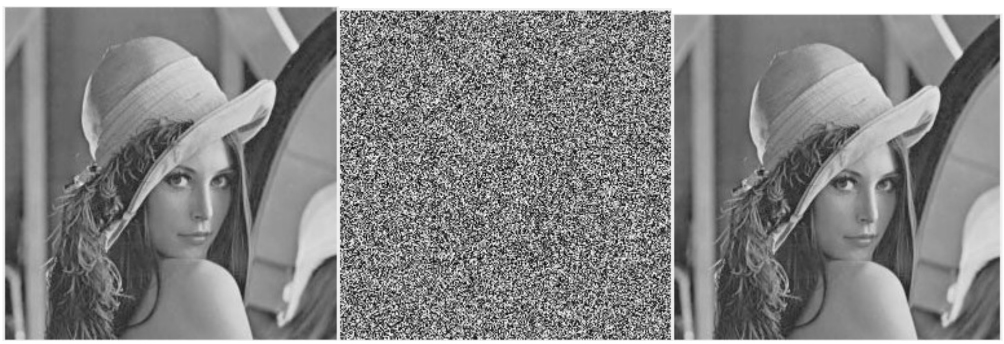

Figure 7 (a) **Figure 4 (b)** **Figure 4 (c)**

Figure 4: (a) Image before encryption, (b) Image after encryption, (c) Image after decryption

The image shown in figure 7 (c) is the decrypted image formed by the keys K1 & K2 from the double key logistic map. The original image cannot be produced if the wrong key is used. The original image of is shown in Figure 7 (a). While the image displayed in figure 7 (b) is the encrypted image with no relation to each other. Also, it is proved that the original image has no connection with the encrypted one.

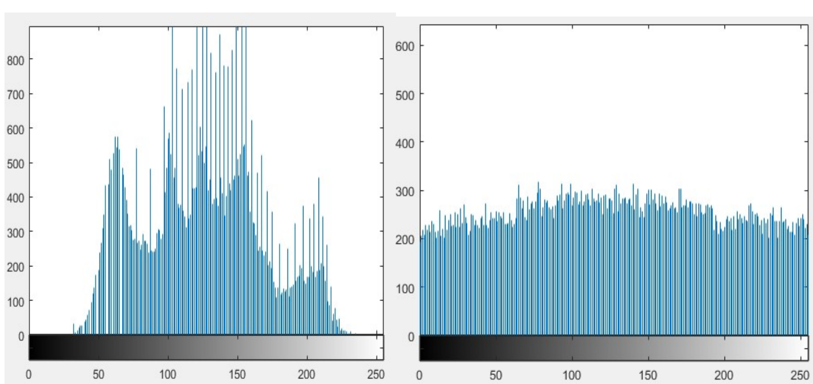

Figure 8 (a) **Figure 8 (b)**

Figure 8: (a) Histogram of the original image (b) Histogram of the encrypted image

Figure 8 displays the histogram in general. X axis represents the pixel values and Y axis represents the frequency values. The original image is shown in figure 8 (a), whereas in figure 8 (b) it is the encrypted image obtained after the proposed algorithm. After observing the histograms in figures 8 (a)

iJETRM
International Journal of Engineering Technology Research & Management

and figure 8 (b), it was observed that the second plot proves to be a more uniform and flatter graph than the first plot. Thus, it is concluded that the method proposed is secure. The correlation measure is important for finding out the relationship in the image between adjacent pixels that shows the quality of the algorithm proposed. The original images which are highly correlated have correlation coefficient values nearly equal to 1 whereas for the encrypted images it is nearly 0.

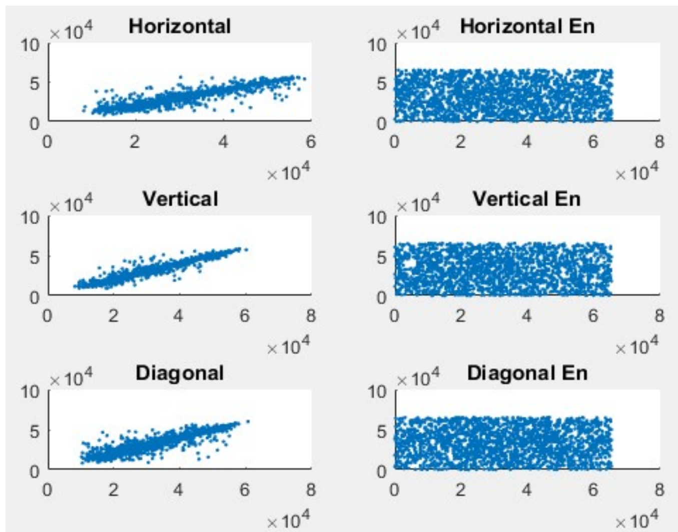

Figure 9: Pixel correlations for original and encrypted image

In figure 9, scatter plots are used in which pixel values of one band are displayed along x axis and pixel values of another band are displayed along y axis. 'Horizontal' is the horizontal pixel correlations for original image and 'Horizontal En' is the horizontal pixel correlations of encrypted image. From figure 9, it can be seen that the linking between pixels of original image is higher than that of encrypted ones which means there is no correspondence at all between the original and the encrypted image.

Following are the results obtained after the implementation of CNN Based Cryptography:

A chaos network is a certain neural network, the weights of which rely on a chaotic pattern. The chaos sequence relies heavily on the initial conditions, the parameters are set as $\mu = 3.9$ and $x(0) = 0.75$. When making an extensive search, it is very tough to decrypt the encrypted data accurately, without knowing μ and $x(0)$. A sequence of 10 numbers (1 2 3 4 5 6 7 8 9 0) is given as input for encryption, and the input variables for the chaotic network (μ and $x(0)$) are used as indicated. The output is obtained (155 151 157 136 168 109 215 8 106 211) and can clearly be seen in a chaos state. Then, the output obtained after encryption is used for decryption.

iJETRM
International Journal of Engineering Technology Research & Management

ACKNOWLEDGEMENT

We thank the staff and our colleagues from R.V. College of Engineering, and our guide, H.V. Kumaraswamy, who provided insight and expertise that greatly assisted the research. We are expressing our gratitude to our families for being an inspiration. Above all, to God.

CONCLUSION

A technique is being implemented in this paper to construct plain and quick sequential and combinational machine with the use of back propagation algorithm. ANN is a simple yet effective method capable of emulating computing machines that are massively complicated. An analysis was conducted between two distinct network topologies of the neural network, and their advantages and disadvantages are listed. Different sequential and combinational logics which are complicated in its own sense, is also being implemented with ANN.

It also examines encryption and decryption of photos two separate keys generated from chaotic dual-map. Two different stages are required for cryptography using this method from the different keys created and to create a private key both the keys are exclusive OR with each other. Further this newly created private key is again exclusive OR with the original photo to obtain encrypted photo. Computing MSE, spread of pixels and correlation by analyzing the performance of the proposed method. The results depict a more consistent and flatter spread of pixels' plot, with large MSE values. The nearby pixel correlation is about zero and therefore there is no link between the two editions of the photo obtained.

Chaos-based systems are highly responsive to variable of the system, and starting conditions also for those unauthorized users without any access to keys these properties are also notable. Distortion-like actions of these structures are the principal explanation for using these structures. However, several features of chaos-based systems including less variables, coordination, and so forth cause considerable cryptographic difficulties

In order to address the demerits of chaos-based system, it is proposed to combine methods of ANN and chaotic cryptosystem where CNN combines the advantages of both systems which are criteria such as key responsiveness and also to hide the connection between original message and encrypted message in the reference to encryption/decryption can be satisfied by the properties of chaos-based cryptography. The ability the greater level of architectural concurrency, to gather results from primary diagnosis to unexpected circumstances, efficiency, and reliability are some of the perks achieved through ANN. In a system it can be implement to identify the connection between the input and output.

REFERENCES

[1] Shital Daulat Jagtap, Mr. P. BalaRamudu, and Mr. Manoj Kumar Singh, "Cryptography Based on Artificial Neural Network", International Journal of Advanced Research in Electronics and Communication Engineering Volume 4, Issue 11, November 2015.

[2] Sarita Kumari, "A research Paper on Cryptography Encryption and Compression Techniques",

iJETRM
International Journal of Engineering Technology Research & Management

International Journal of Engineering and Computer Science, 2017.

[3] Minal Chauhan and Rashmin Prajapati, "Image Encryption Using Chaotic Based Artificial Neural Network", International Journal of Scientific & Engineering Research, Volume 5, Issue 6, 2015.

[4] Jacques M. Bahi, Jean-François Couchot, Christophe Guyeux and Michel Salomon, "Neural Networks and Chaos: Construction, Evaluation of Chaotic Networks, and Prediction of Chaos with Multilayer Feedforward Networks",2016.

[5] Md.Billal Hossain, Md.Toufikur Rahman, A B M Saadmaan Rahman, Sayeed Islam, "A New Approach of Image Encryption Using 3D Chaotic Map to Enhance Security of Multimedia Component", International Conference on Informatics, Electronics & Vision (ICIEV), 2015.

[6] Thomas H¨utter, Mario Preishuber, Jutta H¨ammerle-Uhl, and Andreas Uhl(B), "Weaknesses in Security Considerations Related to Chaos-Based Image Encryption", International Conference on Information and Communications Security, 2016

[7] Alpa Agath, Chintan Sidpara, Darshan Upadhyay, "Critical Analysis of Cryptography and Steganography", National Conference on Advanced Research Trends in Information and Computing Technologies, 2018.

[8] Akif Akgula, Shafqat Hussainb, Ihsan Pehlivanc, "A new three-dimensional chaotic system, its dynamical analysis and electronic circuit applications", International Journal for Light and Electron Optics, 2016.

[9] Dilip Roy Chowdhury, Deepanjan Sen, "Artificial Neural Network Based Trend Analysis and Forecasting Model for Course Selection", International Journal of Computer Sciences and Engineering, 2017.

[10] Amir Anees, Iqtadar Hussain, "A Novel Method to Identify Initial Values of Chaotic Maps in Cybersecurity," Symmetry, 2019.

[11] Mina Mishra, Vijay H. Mankar, "Chaotic Encryption Scheme Using 1-D Chaotic Map", International Journal Communications, Network and System Sciences, 4, 452-455, 2011.

[12] Safwan El Assad, Mousa Farajallah, "A new chaos-based image encryption", Signal Processing-Image Communication, 2015.

[13] Ilker Dalkiran, Kenan Danisman, "Artificial neural network based chaotic generator for cryptology", Turkish Journal of Electrical Engineering & Computer Science, Volume 18, Number 2, 2010.

[14] Charu Gupt, "Implementation of cryptography using Jordan network," International Journal of Advance Engineering and Research Development, Volume 4, Issue 12, 2017.

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

[16] X. Wang, K. Guo, "A new image alternate encryption algorithm based on chaotic map" Nonlinear Dynamics, 2014.

iJETRM
International Journal of Engineering Technology Research & Management

[17] M. Mishra, V. Mankar, "Review on chaotic sequences based cryptography and cryptanalysis", International Journal of Electronics Engineering , 189–194, 2011.

[18] Kuldeep Singh, Komalpreet Kaur, "Image Encryption using Chaotic Maps and DNA Addition Operation and Noise Effects on it", International Journal of Computer Applications, Volume 23, Number 6, June 2011.

[19] William Stallings, "Cryptography and Network Security: Principles and Practices", Seventh edition, 2017.

[20] 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, Volume 3, Number 2, March 2011.

[21] Maddodi G, Awad A, Awad D, Awad M, Lee B, "A new image encryption algorithm based on heterogeneous chaotic neural network generator and dna encoding", Multimedia Tools and Applications, 2018.