Cryptography based on Artificial Neural Networks and Chaos Theory

Aditya S. Mhetras
PG Student M.E. (Electronics and Telecomm.)
V.E.S.I.T.,
University of Mumbai, Mumbai

Nadir N. Charniya, PhD
Professor (Electronics and Telecomm.)
V.E.S.I.T.,
University of Mumbai, Mumbai

ABSTRACT

Cryptography is a skill of sending the data in such a form that only those for whom it is intended can read it. There are number of methods to perform cryptography, one of such methods is Chaos theory which studies the behavior of a dynamical systems that are highly sensitive to initial conditions. Even slight changes in initial conditions result in extensively deviating outcomes for such dynamical systems, hence making long-standing estimate unmanageable. The limitations of applying Chaos Theory are choosing the input parameters and synchronization. The computation of these input parameters lies on the dynamics underlying the data and the highly complex analysis, not always accurate. Artificial neural networks (ANN) well known for learning and generalization are hence used to model the dynamics of Chua's circuit viz. x, y and z. The designed ANN was trained by varying its structures and using different learning algorithms. ANN was trained using 9 different sets which were formed with the initial conditions of Chua's circuit and each set consisted of about 1700 input-output data. A feed-forward Multi-Layer Perceptron (MLP) network structure, trained with Levenberg-Marquardt backpropagation algorithm, produced best outcome. Further a case study in which a plain text was first encoded and then decoded by both the chaotic dynamics obtained from the proposed ANN and the numerical solution of Chua's circuit and are compared with each other.

General Terms

Cryptography, Artificial Neural networks, Multilayer Perceptrons et.al.

Keywords

Encryption, decryption, chaos theory, chaotic dynamics.

1. INTRODUCTION

Cryptography is technique which converts a given message into an unreadable format which is seen as noise by the third parties. It is a vital part of a safe communication process [1-5]. Cryptosystem is a system which provides encryption and decryption of the data and can be designed either using hardware mechanisms or using programming. Nearly every cryptosystem algorithms are complex mathematical procedures that consume a lot of time and money.

Chaotic theory is being implemented in the field of cryptography for its noise like behavior. The theory was summarized by Edward Lorenz as [6] Chaos: When the present determines the future, but the approximate present does not approximately determine the future. The chaotic systems are known for their sensitivity to initial conditions, system parameters and non-periodic nature. Because of such properties and noise-like non-periodic dynamics they are also considered as a preferable method for cryptography.

The chaotic systems are very sensitive to initial conditions. Even a small change in the initial condition can create chaos is the whole system and diverge the final output to a vast extent. Hence it is nearly impossible to define the exact set of initial conditions and generate the desired dynamics in any another machine. But the disadvantage of this method is the fewness of its system parameters. These parameters are the keys for the chaotic cryptosystems and hence it can be seen as a threat to the security of the system.

In machine learning and cognitive science, artificial neural networks (ANNs) are a family of statistical learning models motivated by the biological neural networks (the central nervous systems of humans, principally the brain) and hence are used to estimate the functions that can depend on a large number of inputs and are commonly unknown. ANN are systems of interconnected perceptrons (neurons) which send messages to each other. The contacts consist of the numeric weights which on the basis of training can be manipulated, making ANN adaptive to the inputs and skilled for learning [7].

In this paper , a cryptography algorithm forming a chaotic generator using ANN is designed which overpowers the weaknesses of chaotic cryptosystems . The designed ANN model, was trained in MATLAB to generate chaotic dynamics $\hat{x}$, $\hat{y}$ and $\hat{z}$ which are s imilar to actual chaotic dynamics x, y and z produced by the numerical solution of Chua's circuit. For the application of the designed chaotic based cryptosystem a plain text was first encoded and then decoded by both the chaotic dynamics obtained from the proposed ANN and the numerical solution of Chua's circuit and were compared with each other.

This paper is organized as follows: In Section 2, Chua's circuit and its properties are described with suitable diagrams. The description of ANN in short and the designed ANN model is described in Section 3. In Section 4, the methodology and the experimental results of encryption and decryption processes are discussed and in Section 5 concluding remarks are projected.

2. CHUA'S CIRCUIT

Chua's circuit is a simple electronic circuit that exhibits classic chaos theory behavior. It produces distinct chaotic dynamics using given parameters. The easy experimental implementation of the circuit, combined with the existence of a simple and accurate theoretical model, makes Chua's circuit a useful system to study many fundamental and applied issues of chaos theory.

Chua's circuit is shown in Figure 1. The circuit contains of three constituents which store energy (C_1, C_2 and L), two linear resistors (R and r) and a nonlinear resistor (R_n) also called Chua's diode [8]. Kirchhoff's current and voltage laws are applied to obtain the differential equations in Equation (1).

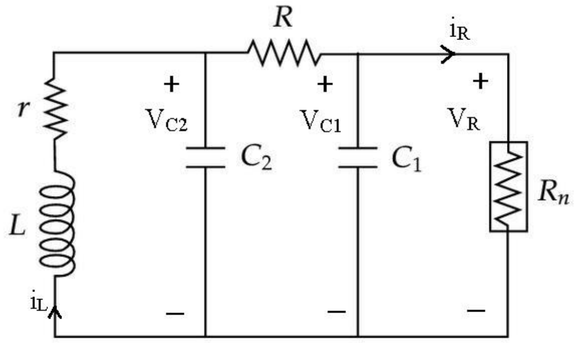

Fig 1: Chua's circuit

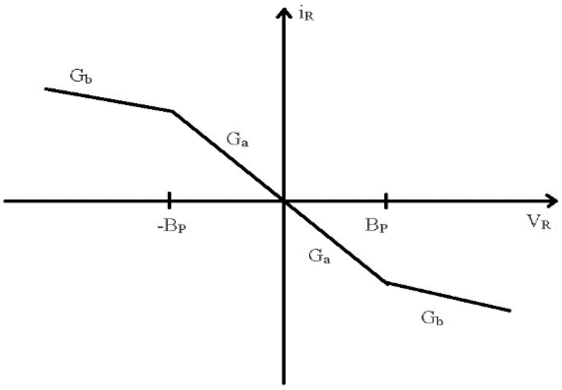

Fig 2: Characteristic of nonlinear Chua's diode

Equation (2) represents the mathematical model f (V_{C1}) and Fig 2 shows characteristic of nonlinear Chua's diode. The G_a and G_b are the inner and outer region slopes and ± B_P denote the breakpoints [9].

$$C_1\frac{dV_{C1}}{dt} = \frac{1}{R}(V_{C2} - V_{C1}) - f(V_{C1})$$

$$C_2\frac{dV_{C2}}{dt} = i_L - \frac{1}{R}(V_{C2} - V_{C1}) \qquad (1)$$

$$L\frac{di_L}{dt} = -V_{C2} - i_L.r$$

$$\begin{aligned} i_R = f(V_{C1}) = G_b.V_{C1} + \frac{1}{2}(G_a - G_b) \\ * \left(|V_{C1} + B_P|\right. \\ \left.- |V_{C1} - B_p|\right) \qquad (2) \end{aligned}$$

By introducing the following variables, Equation (1) and (2) can be transformed into dimensionless state equations (4) and (5).

$$x = \frac{V_{C1}}{B_P} \qquad y = \frac{V_{C2}}{B_P} \qquad z = \frac{Ri_L}{B_P}$$

$$\alpha = \frac{C_2}{C_1} \qquad \beta = \frac{C_2R^2}{L} \qquad \tau = \frac{t}{RC_2} \qquad (3)$$

$$a = G_aR \qquad b = G_bR \qquad c = B_P$$

The resulting three dimensionless state equations in Equation (4) were solved by MATLAB differential equation solver, named ode 45. The required parameters and initial conditions which were taken into consideration while solving the equations were: α = 10, β = 14.87, a= -1.27, b= -0.68, c= 1, x_0 = 1, y_0 = 0 and z_0 = 0. The chaotic dynamics so formed are named as x, y and z and the double scroll attractor formed by plotting x dynamic vs. y dynamic are shown in Figure 3(a) and Figure 3(b) respectively.

$$\frac{dx}{d\tau} = \alpha[y - x - f(x)]$$

$$\frac{dy}{d\tau} = x - y + z \qquad (4)$$

$$\frac{dz}{d\tau} = -\beta y$$

$$f(x) = bx + \frac{1}{2}(a - b) * (|x + c| - |x - c|) \qquad (5)$$

On solving the differential equations using ode45 we get the chaotic dynamics x, y and z where x represents V_{C1}, y representsV_{C2} and z represents i_L as shown in Figure 3(a). The relation between chaotic dynamics x and y also known as double scroll is shown in Figure 3(b).

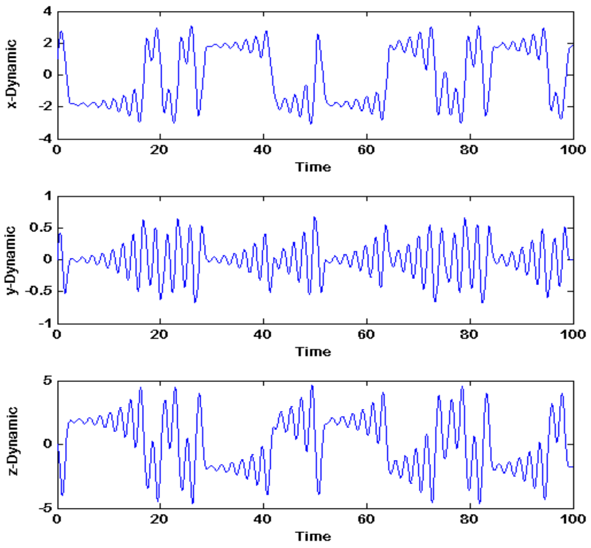

Fig 3(a): The dynamics by taking 1, 0, 0 as initial conditions

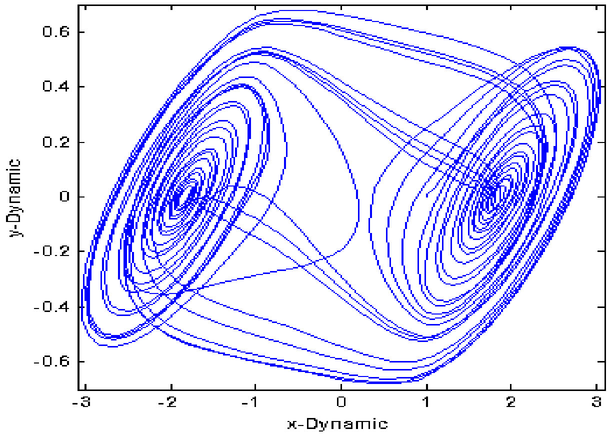

Fig 3(b): The double scroll attractor of chaotic Chua's circuit using MATLAB

3. PROPOSED MODEL BASED ON ARTIFICIAL NEURAL NETWORKS

Artificial Neural Networks (ANN) are nothing but a block of interconnected of the perceptrons arranged in a way to achieve a particular goal of learning. They are built as a replica of human nervous system and their learning mechanism follows human generalization rather than calculation. There can be a group of perceptrons at each level depending on the set goal. The optimization of an ANN can be proceeded in three ways as follows [10]:

1. Changing the number of neurons in each level,
2. Changing the number of levels of neurons and
3. Changing the activation function at each level of neurons.

The simple structure of ANNs is made up of numerous interconnected perceptrons (neurons) having weighted inputs and bias, its summation , the activation function as needed and its final output. Inputs are thus passed from one neuron, processed and then again passed to the next neuron forming an intermediate output until the final output is achieved. Every neuron in an ANN has an activation function, a non-decreasing function like hard limiting threshold function describing the output of a neuron if a given input is being applied. Neurons act as actuators which output as 1 when they are above threshold i.e., activated and a 0 when below threshold.

Figure 4 shows the block diagram of the designed ANN model. This model is inspired from the technical paper "Artificial neural network based chaotic generator for cryptology" written by Ilker Dalkiran, Kenan Danisman which projected us to the ANN based chaotic generator for encryption [11]. The four inputs, two layers of neurons and three outputs (dynamics) can be seen in the block diagram. Out of the four inputs, three were initial conditions x_0, y_0 and z_0 and time as the fourth variable , varying from 0 to 100 and three chaotic dynamics x̂ , ŷ and ẑ were the outputs of the ANN. For the training and test phases of the ANN, approximately 1700 input-output combinations of data pairs which belong to 9 different initial condition sets were obtained from Equation (4).

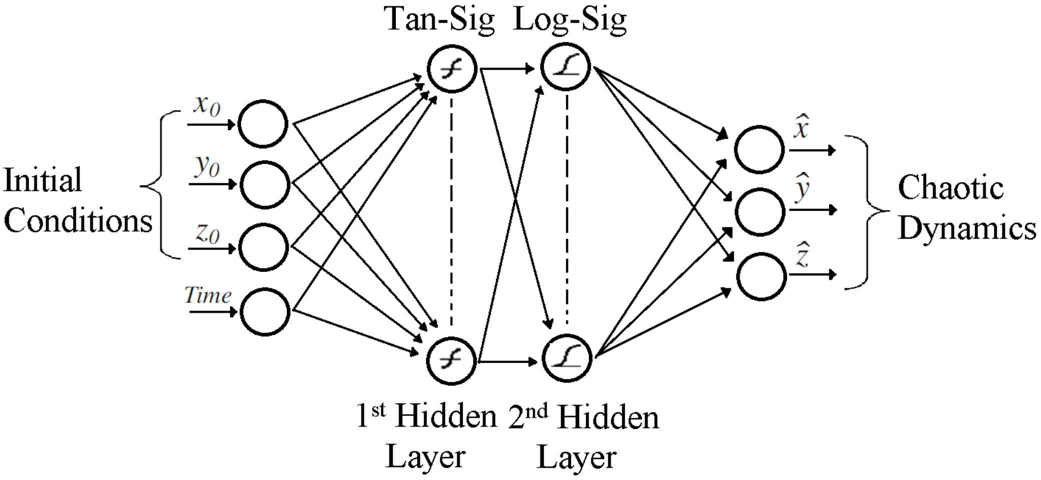

Figure 4. Block Diagram of Proposed ANN model

The ANN model was proposed to learn the exact replica of the chaotic dynamics x̂, ŷ and ẑ and to do so the ANN was to be designed to learn the dynamics to its best. Various combinations of the ANN structures were trained to give the optimal ANN structure. The number of neurons in the hidden layers were changed from 2 to 20 for each layer, the number of layers were also changed along with their activation functions.

4. METHODOLOGY AND EXPERIMENTAL RESULTS

The chaotic dynamic z obtained from the Chua's equations and $\hat{z}$ from the proposed ANN act as the key for both encryption and decryption. For the communication between transmitter and the receiver the initial conditions and the system parameters need to be known by both of them. The ANN models were trained using five training algorithms and the results showing MSE and correlation coefficient ($\hat{z}$) can be seen in Table 1.The ANN model configuration of 4x18x20x3 which indicates 4 inputs, 18 neurons in first layer, 20 neurons in second layer and 3 outputs which was trained with Levenberg–Marquardt backpropagation learning algorithm offered least MSE as seen in the table. The first and second layer neurons were trained using tan sigmoid and log sigmoid as their activation functions respectively. The blockdiagram of the encryption and decryption processes is given in Figure 5. The correlation coefficients and MSE were plotted against the number of neurons during training can be seen in figure 6.

A control unit block was designed at both transmitter and receiver side to calculate the values of the initial conditions and hence control the generated dynamics.Plain-text here was a gray scaled image. A gray scaled picture, in MATLAB, is simply a matrix of pixels having integer values varying between 0 and 255. The chaotic dynamic $\hat{z}$, in Figure 3(a), whose amplitude varies between +5 and -5 was chosen to encrypt the plain-text. The plain text i.e., gray scaled picture which was originally a 2-D matrix , after taking a note of its original dimensions was then converted into specific format of resolution. Then it was converted to a single column vector and normalized in the interval -0.01 and +0.01. In the encryption process, the normalized column vector is added with the chaotic dynamic $\hat{z}$, to obtain the cipher-text. For the decryption process, the selected initial conditions, original image dimensions and normalizationparameters were to be known,and hence a tail containing the above listedwas tied to the cipher-text by the control unit and then it was transmitteed along with the cipher-text. Fordecryption, the important information about parameters, dimensions and initial conditions were first extracted from the received tail. The extracted initial conditions were then applied to the ANN based chaotic generator to obtain the chaotic dynamic $\hat{z}$. Now, to obtain the plain-text form the ciphertext, thechaotic dynamic $\hat{z}$ *was* subtractedfrom the cipher-text. The obtained plain text gray scaled image was reshaped to its original dynamic with the help of the original resolution obtained from tail.

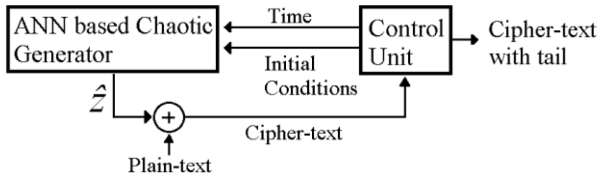

Figure 5(a). Transmitter Block Diagram

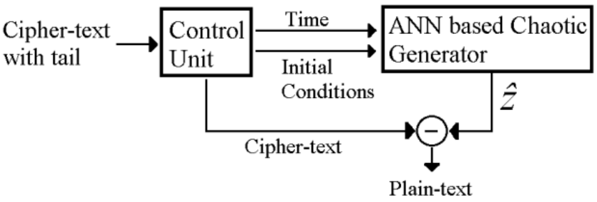

Figure 5(b). Reciver Block Diagram

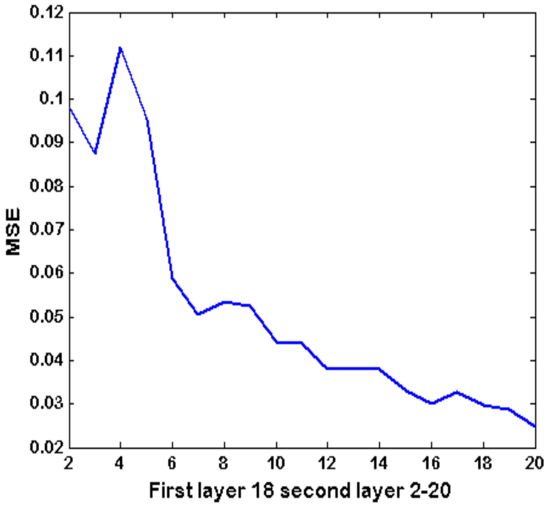

Figure 6(a). The MSE plotted against the number of neurons during training

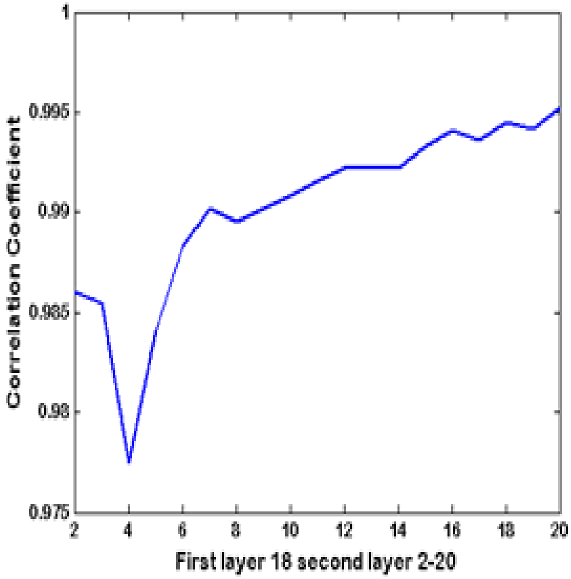

Figure 6(a). The correleation coefficients plotted against the number of neurons during training

Table 1. MSE and correlation coefficients of $\hat{z}$ produced by the five learning algorithms by the proposed ANN

Training Algorithm	First Hidden Layer	Second Hidden Layer	MSE	Correlation Coefficient
Levenberg–Marquardt (LM)	18	20	0.0249	0.9952
Bayesian Regularization (BR)	20	19	0.0252	0.9948
Broyden–Fletcher–Goldfarb–Shanno (BFGS)	20	20	0.0387	0.9918
Conjugate Gradient Backpropagation with Powell-Beale restarts (CGB)	16	15	0.0703	0.9863
Scaled Conjugate Gradient(SCG)	16	15	0.071	0.986

The plain -text grayscale image is shown in Figure 7. This plaintext image was encrypted using the chaotic dynamics $\hat{z}$ generated using ANN and z by Chua's equations, and the acquired cipher-texts were sent to receiver in the scalar vectors form are shown in Figure 8(a) and 8(b) respectively. For a cryptanalyst who somehow manages to get the image form of ciphertext and knows its dimension, and tries to converts it back into image structure, can only see the image as black blocks shown in Figure 8(c) and 8(d). At the encryption process, the image was first normalized and then encrypted using the chaotic dynamics z and $\hat{z}$. Now for an attacker who knows the normalization parameters along with the image dimensions and tries to denormalize the black image blocks, he can obtain the images shown in Figure 8(e) and 8(f) respectively. The encrypted images are then decrypted using the chaotic dynamics $\hat{z}$ and z , and are the same as grayscale image shown in Figure 8(g) and 8(h).

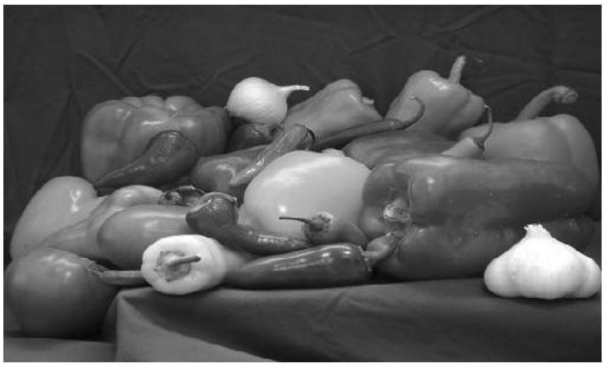

Fig 7: The plain-text grayscale image

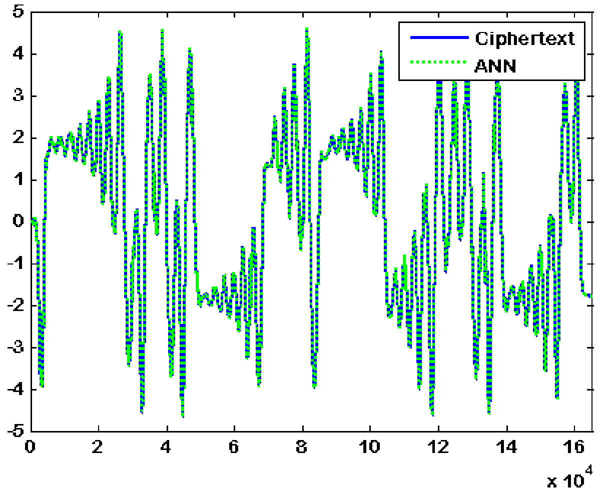

Fig 8(a): Cipher-text in the scalar vectors form using ANN

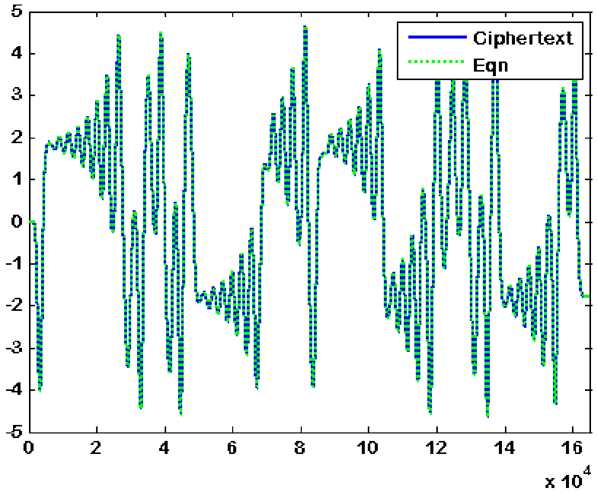

Fig 8(b): Cipher-text in the scalar vectors form using Chua's equations

Fig 8(c): Encrypted message using ANN in image form

Fig 8(d): Encrypted message using Chua's equations in image form

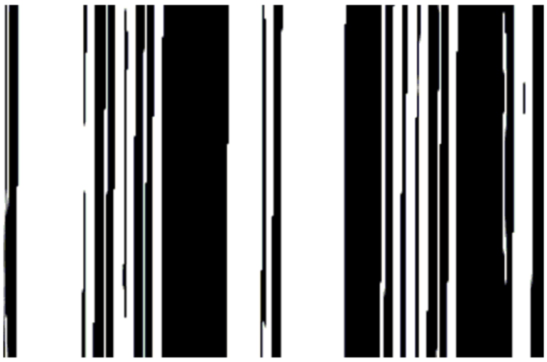

Fig 8(e): Encrypted message using ANN in image form after denormalization

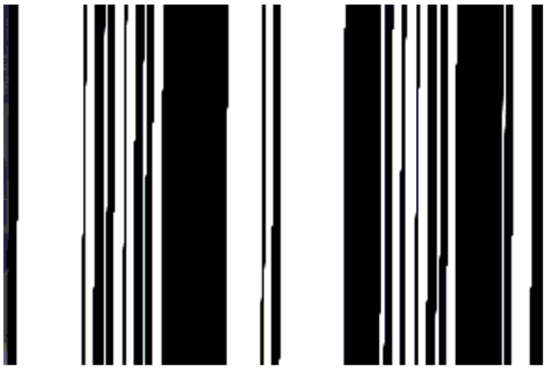

Fig 8(f): Encrypted message using Chua's image equations in image form after denormalization

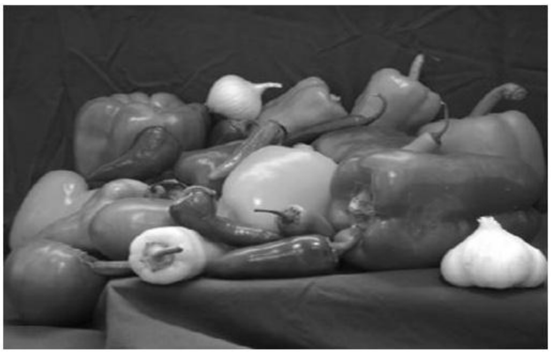

Fig 8(g): Image after decryption using the chaotic dynamic $\hat{z}$ obtained from ANN

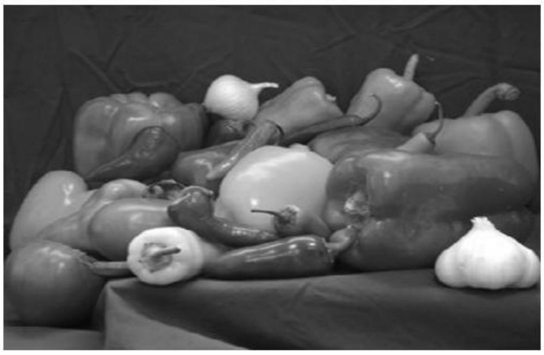

Fig 8(h): Image after decryption using the chaotic dynamic z obtained from Chua's equations

After the decryption process, the image quality was evaluated by subjecting the original image and the decrypted image to Mean Squared Error (MSE) and Peak Signal to Noise Ratio (PSNR) [12]. The decoded image was nearly as accurate as the plaintext grayscale image. The MSE and PSNR values were calculated from the plaintext image and the decrypted image for both the ANN model and Chua's encryption are tabulated in table 2.

Table 2. MSE and PSNR (dB) calculated for encryption system using Chua's equations and ANN model

Encryption technique	MSE	PSNR(dB)
Chua's equations	4.14	41.96
ANN trained using Levenberg–Marquardt (LM)	4.14	41.96

As seen from the table, the MSE values and PSNR values obtained from Chua's model and ANN model are identical with low MSE and high PSNR making the decrypted image keep its integrity to the highest possible value.

5. CONCLUSION

All the inferiorities of the chaotic encryption systems were eliminated using an ANN model. An optimum ANN model was designed and trained in MATLAB software to learn and produce the chaotic dynamics which were found closest to the chaotic dynamics generated by the Chua's circuit numerical solution. ANN model in the configuration 4x18x20x3 multilayer perceptron setup, trained with Levenberg–Marquardt (LM) learning method, created chaotic dynamics with least MSE was found optimum model. Because of the advent of ANN ,for an attacker wants to generate chaotic dynamics identical as the ANN model, the ANN structure need to be accurately known, weights and biases values must be accurately found out. In order to produce the identical chaotic dynamics one should define the exact number of neurons in each layer, activation functions for each neuron, the precise values of 492 weights and 41 biases. Thus making it very difficult for the attacker to figure out the exact decryption scheme and overcoming the disadvantages as synchronization and cons of the analogue circuit and the numerical solution of the chaotic circuit, the ANN based dynamics generator proves its importance in the field of cryptography.

6. REFERENCES

[1] A.J. Menezes, P.C. Van Oorschot, S.A. Vanstone, Handbook of Applied Cryptography, New York, CRC Press, 1996

[2] B. Schneier, Applied Cryptography, New York, John Wiley & Sons Inc., 1996.

[3] H.C.A. Van Tilborg, Fundamentals of Cryptology, New York, Kluwer Academic Publishers, 2000.

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

[5] 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.

[6] Danforth, Christopher M. (April 2013). "Chaos in an Atmosphere Hanging on a Wall", *Mathematics of Planet Earth 2013*. Retrieved 4 April 2013.

[7] S. Haykin, Neural Networks: A Comprehensive Foundation, Second Ed., New Jersey, Prentice Hall, 1999.

[8] L.O. Chua, C.W. Wu, "A universal circuit for studying and generating chaos", IEEE Trans. on Circuits and Sys.-I: Fundamental Theory and Applications, Vol. 40, pp. 732-745, 1993.

[9] Michel Kennedy, "Three Steps to Chaos-Part II: A Chua's Circuit Primer", IEEE Trans. on Circuits and Sys.-I: Fundamental Theory and Applications, Vol. 40, No. 10, October 1993.

[10] R. M. Hristev, The ANN Book, Edition-1, 1998.

[11] Ilker Dalkiran, Kenan Danisman, "Artificial neural network based chaotic generator for cryptology", Turk J Elec Eng & Comp Sci, Vol.18, No.2, 2010, © TUBITAK.

[12] Pooja Kaushik and Yuvraj Sharma, "Comparison of Different Image Enhancement Techniques Based Upon Psnr & Mse", International Journal of Applied Engineering Research, Vol.7 No.11 (2012).