المجلّة الدولية للعلوم والتقنية
International Science and Technology Journal
ISTJ

عدد خاص
بالمؤتمر الليبي الدولي للعلوم التطبيقية
و الهندسية
27-28- سبتمبر 2022

LICASE
المؤتمر الليبي الدولي للعلوم التطبيقية و الهندسية

Improving Information Transmission Security by Using Intelligent Chaos

Salema Younus[1], **Ibrahim Ighneiwa**[2], **Salwa Almoshity**[3]
[1,3] College of Electrical and Electronics Technology-Benghazi, Libya
[2]University of Benghazi, Benghazi, Libya
salema_younus@ceet.edu.ly

الملخص:

أصبح الاتصال عبر الشبكات ضرورة عالمية للأفراد والشركات والهيئات الحكومية والخاصة والمشكلة هي أن هناك متطفلين ومتسللين على كافة مستويات الأعمال والحكومات يهاجمون أنظمة المعلومات ويسرقونها لأسباب عدة سواء كانت اقتصادية أو سياسية، المعلومات في مجملها معرضة لخطر السرقة واستخدامها لأغراض مختلفة نتيجة لتأثيرها الذي لا يطال الافراد فقط وانما حتى الدول والحكومات ،حيث أصبحت سرقة المعلومات واستخدامها في صالح اللصوص جزءًا من حروب التدمير محليًا وعالميًا، كل هذا يعني أن حماية المعلومات بالطرق التقليدية ليست كافية لضمان وصول المعلومات المنقولة إلى وجهتها بأمان وهناك حاجة لتقنيات ذكية يمكنها هزيمة المتسللين والمتطفلين الذين ينفذون تقنيات متقدمة لسرقة المعلومات، في هذا العمل، تم الجمع بين الفوضى والذكاء الاصطناعي لإنشاء ما يسمى بالفوضى الذكية التي من شأنها حماية المعلومات حتى لا يتم إساءة استخدامها حتى لو وجدت طريقها إلى الأيدي الخطأ، تم استخدام خوارزميات التشفير التي تنفذ الذكاء الاصطناعي بالتحديد الشبكات العصبية الاصطناعية وتغذيتها بدوائر فوضوية للحصول على أوزان متولدة ديناميكيًا والتي من شأنها أن تتغير مع الظروف الأولية وتضمن بدورها توليد المفتاح السري اللازم لتشفير الصور وفك تشفيرها، تم التنفيذ باستخدام برنامج ماتلاب لتفاعله مع الشبكات العصبية و الفوضى ولضمان كفاءة التدريب والتحقق من صحة واختبار آلية التشفير القائمة على الشبكات العصبية الفوضوية .

الكلمات الرئيسية: التشفير ، الفوضى، الشبكات العصبية الاصطناعية، دائرة تشوا.

Abstract

Network communication has become a worldwide necessity for individuals, businesses and private and government entities. The problem is that there are hackers, and intruders both at the business and governments level who attack information systems and steal information for economical and political reasons. Information is in danger of being stolen and used for various purposes that affect not only individuals and companies but even nations. Stealing information and used in the advantage of the thieves has become part of the wars ravaging both locally and globally. all that mean that conventional information protection is not enough to guarantee that transmitted information reach its destination safe and secure and there is a need for intelligent techniques that can defeat hackers and intruders who implement advanced techniques to steal information.

In this work chaos and artificial intelligence is combined to create what is called intelligent chaos that would protect information so it will not be misused even if it has found its way to

the wrong hands. Has been used encryption algorithms that implement artificial intelligence (AI), specifically artificial neural networks (ANN) and fed them with chaotic circuits to obtain dynamically generated weights that would changes with the initial conditions and in turn ensure the generation of secret key needed for image encryption and decryption. Matlab is implemented to interface chaos with ANN and guarantee that training, validation and testing the chaotic ANN based encryption mechanism is efficient.

Keywords: Cryptography, Chaos, ANN, Chua's Circuit.

1. Introduction

Information security (IS) is a phenomenon that protects the information from being unauthorized access and use in anyway such as for the purpose of misuse, disrupt, disclosure, modification etc and it is a It is a generic phrase that is typically applied to both physical and electronic forms of information [1]. This concept has become more ever more enmeshed in many aspects of our society In our everyday life, Where many of us work on computers, buy goods from merchants on the Internet and check our e-mail,We use our phones to check our bank balances, and so on [2].

Although this technology enables us to be more productive and allows us to access a host of information with only a click of the mouse, it also carries with it a host of security issues. If the information on the systems used by employers or banks becomes exposed to an attacker, the consequences can be dire indeed. People could suddenly find themelves out of funds, as the contents of their bank account are transferred to a bank in another. Employer could lose millions of dollars (Figure 1), face legal prosecution, and suffer damage to their reputation because of a system configuration issue allowing an attacker to gain access to a database containing personally identifiable information (PII) or proprietary information. Such issues appear in media with disturbing regularity [2].

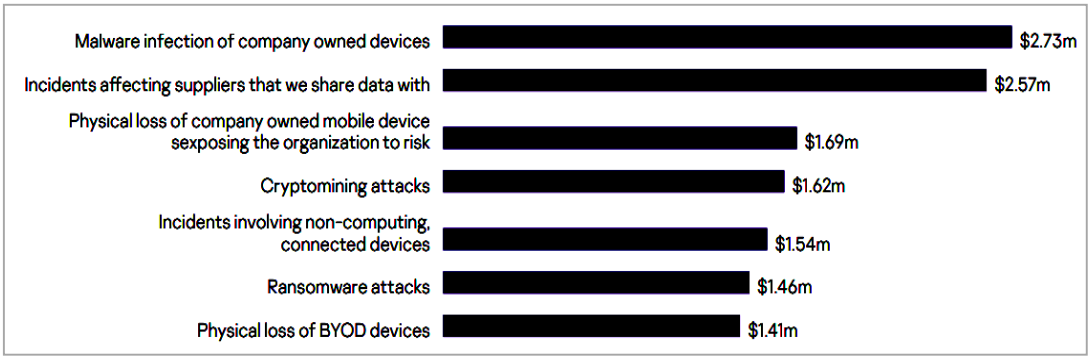

Figure 1. The average financial impact of data breaches by type for enterprises [3].

Transmission security is the capability to send a message electronically from one computer system to another computer system so that only the intended recipient receives and reads the message and the message received is identical to the message sent. The message would not be identical if it was altered in any way, whether transmitted over faulty channels or intercepted by an eavesdropper. Transmission security translates into secure networks. Although many people regard networks as computers connected by wires, this definition of a

network, while technically correct, misses the point. Rather, networks are transmitting data, the data flowing over wires [4].

Cryptography is one of the aim techniques used in information security to protect information from unauthorized or accidental disclosure while the information is in transit and while information is in storage. Information security uses cryptography to transform usable information into a form that renders it unusable by anyone other than an authorized user, this process is called encryption. The original message is referred to as plaintext and the message that is sent through the channel is referred to as the cipher text. Information that has been encrypted can be transformed back into its original usable form by an authorized user, who possesses the cryptographic key, through the process of decryption [5][6].

In the literature, some studies focused on encryption of information; in one study, Bhamarea and Sawarkarb [7] used backpropagation technique with the use of 'trainlm' function in Matlab. The system has been divided into four modules encryption, decryption, interface module, and the authentication module. The sender provided the image to be sent to the encryption module each time he wants to send an image. In the encryption module, the image data is encrypted before being sent to the interface module in encrypted form. The image data is encrypted in the encryption module and the encrypted data is fed to the interface module. This module sends the remote system the encrypted image data. By feeding the received data to the decryption module at the receiving end, the user in the distant system decrypts the image data. ANN are used for decryption.

Blackledge and Bezobrazov [8] used NNs and evolutionary computing to produce encryption algorithms based on the application of natural noise sources obtained from data, which can include atmospheric noise (caused by radio emissions due to lightning, for example), radioactive decay, electronic noise, and input noise approximation with the aim of generating a nonlinear output function. This output was used as a repeater and put through number of tests to determine its potential coding strength using measurements like positive large Lyapunov exponent.

AlSabti and Hashim [9] approach used RSA Cryptosystem is a public key cryptosystem that is provided to be applied over gray and color images with the aid of a Matlab program, used Matlab to apply this cryptosystem over gray and color images. Two algorithms were designed for the encryption and decryption processes, applied over the plain image and cipher image after reading them in the matrices forms, the image is partitioned into blocks that are n x m matrices.

Hussein el al [10] used three different encryption methods rivest cipher 5 (RC5), chaotic and permutation and measure their quality using the peek signal to noise ratio (PSNR), correlation, entropy, number of pixels changes rate (NPCR) and unified average changing intensity (UACI), The results of these tests were then fed into a fuzzy logic system, which was then used to determine which technique was the most effective.

2. The Proposed Model

The structure of the proposed methodology includes the main stages, based on the intelligent chaos approach, which means combining chaotic algorithms with artificial intelligence, namely ANN. The dynamics of the Chua circuit is designed combine it with an artificial neural network which is trained by diversifying its structure, using different

educational algorithms and integrating them with chaos to encode and decode information. Combining the two techniques and implementing the combination is the reason for calling it "intelligent chaos", The main methodology of this work is illustrated in Figure. 2.

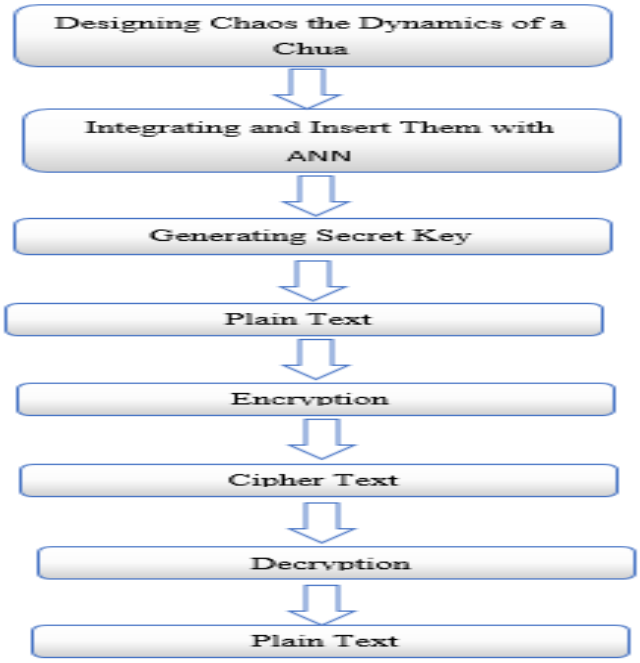

Figure.2 . Proposed of Intelligent Chaos (Chaos+ANN) Model.

2.1. Chaos

A chaos is deterministic, but it has a pseudorandom behavior. It is a nonlinear system that has a large sensitivity to the initial conditions and control parameters [11]. Chaotic maps show complex and dynamic behaviors that occur in nonlinear systems and in determining system states. Logistics chaotic map is a dynamic system with discrete time. The logistic map is one-dimensional and nonlinear as in the following equation [12].

$$X_n + 1 = aX_n\,(1 - X_n) \qquad (1)$$

Attractors called a self-excited attractor if its basin of attraction intersects any arbitrarily small open neighborhood of an equilibrium, otherwise it is called a hidden attractor. Hidden attractors are attractors in systems without equilibria or with only one stable equilibrium (a special case of multistability and coexistence of attractors). The self-excited and hidden classification of attractors was introduced by Leonov and Kuznetsov in connection with the discovery of hidden chaotic attractor in the Chua system of equation (2) [13].

$$\begin{aligned} \dot{x} &= \alpha\,(y - x\,(m_1+1) - \alpha\psi(x)) \\ \dot{y} &= x - y + z \\ \dot{z} &= -(\beta\, y + \gamma z) \\ \psi(x) &= (m_0-m_1)\mathrm{sat}(x) = \tfrac{1}{2}(m_0-m_1)(\,|x+1| - |x-1|) \end{aligned} \qquad (2)$$

where α, β, γ, m_0, m_1 are parameters. This system provides a mathematical model, describing the behaviour of the Chua circuit with five linear elements and saturation non-linearity (Figure 3) Self-excited chaotic attractors had been found in Chua circuits (Figure 4) [13] [14].

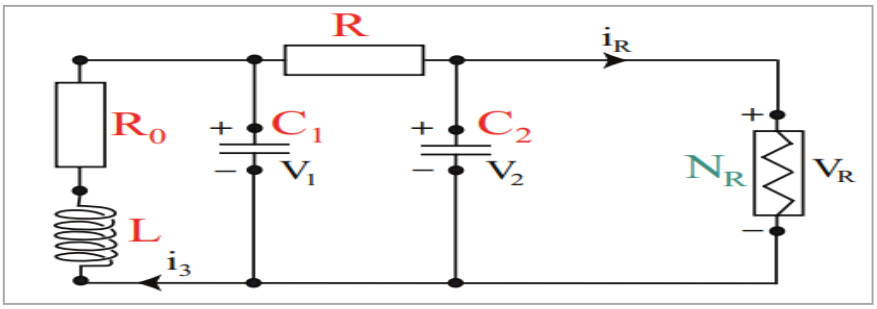

Figure 3. Chua Circuit with a Nonlinear Resistor N_R "Chua diode".

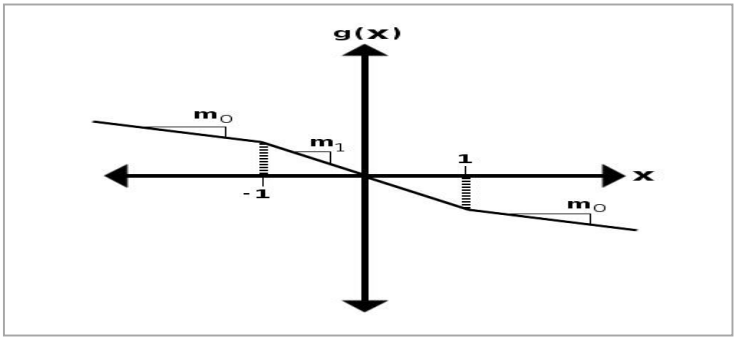

Figure 4. Chua's Nonlinear Diode Characteristics.

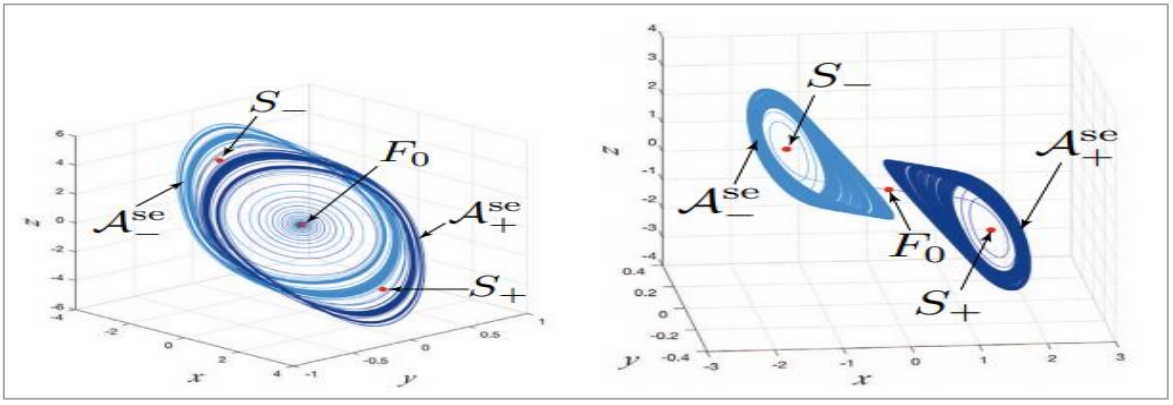

Figure 5. Two chaotic systems: Left: α = 15, β = 28; Right: α = 8.5, β = 14.28, γ = 0, m0 = −8/7, m1 = −5/7.

2.2. Artificial Neural Network

An ANN consists of large number of simple processors linked by weighted connections. By analogy, the processing nodes may be called “neurons” (Figure 6). Each node output depends only on the information that is locally available at the node, either stored internally or arriving via the weighted connections. Each unit receives inputs from many other nodes

transmits its output to yet another nodes. By itself, a single processing element is not very powerful; it generates a scalar output with single numerical value, which is a simple non-linear function of its inputs [15].

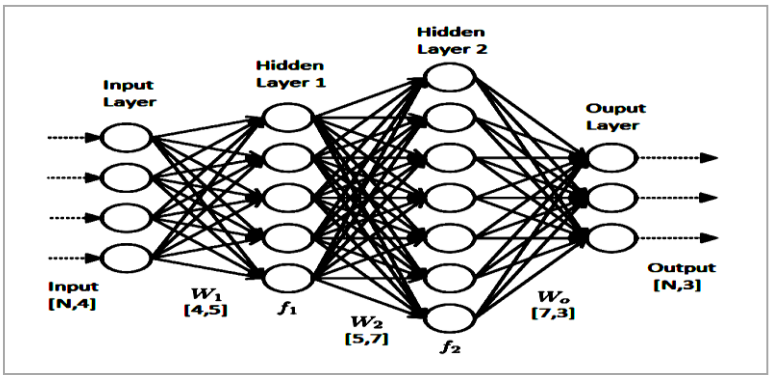

Figure. 6. A general layered of ANN.

3. Experimental Results

In this work, since chaos is used in improving security, chaos generation is first dealt with by using Matlab and implementing Chua's model, where the initial values are entered into the dynamic chaotic system model and they are: x=1, y=0, z=0,t=[0 150] and running the Matlab code.

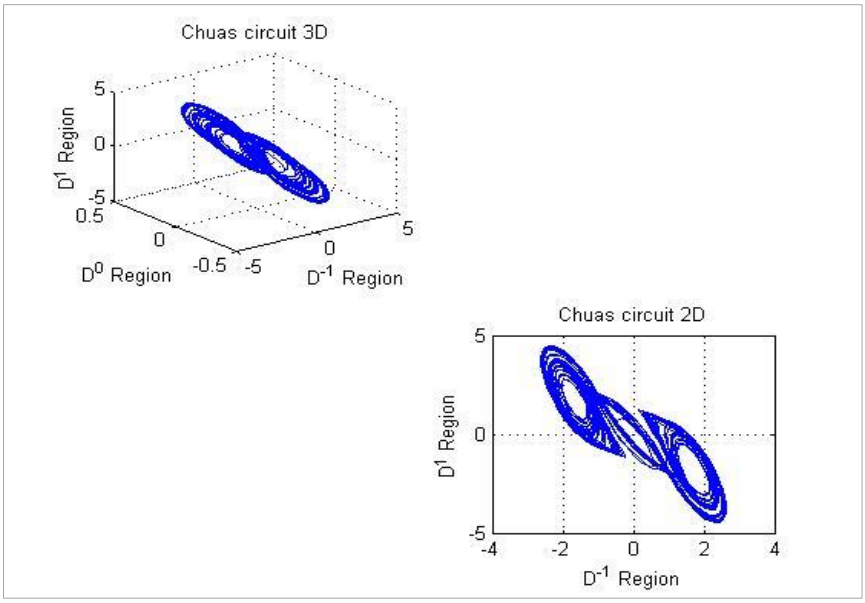

Figure. 7. Chaotic Attractors Generated Using x=1, y=0, z=0 ,t=[0 150].

While when entering the following values: x=1,y=1 ,z=0, t=[0 140], different results appear, and this confirms the sensitivity of chaos to initial conditions.

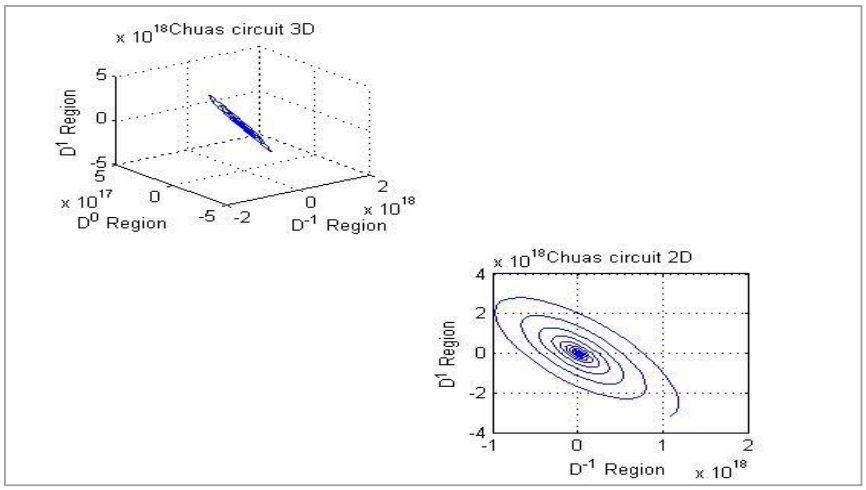

Figure .8 Chaotic Attractors Generated Using x=1, y=1, z=0, t=[0 140].

Since intelligent chaos is considered in this work, artificial intelligence is used, by implementing the artificial neural networks (ANNs) techniques in which the system is trained using Levenberg Marquardt algorithm by inputting the initial dynamics obtained from Chua circuit above, where the number of input data records considered is 3,987. The training and testing were done using an ANN with a 1x20x17x1 parameter is designed, with one input, 20 neurons first hidden layer, 17 neurons second hidden layer and one output, is shown on Figure 9. The secret key for encryption is generated by the dynamics weight updating generated by the ANN system.

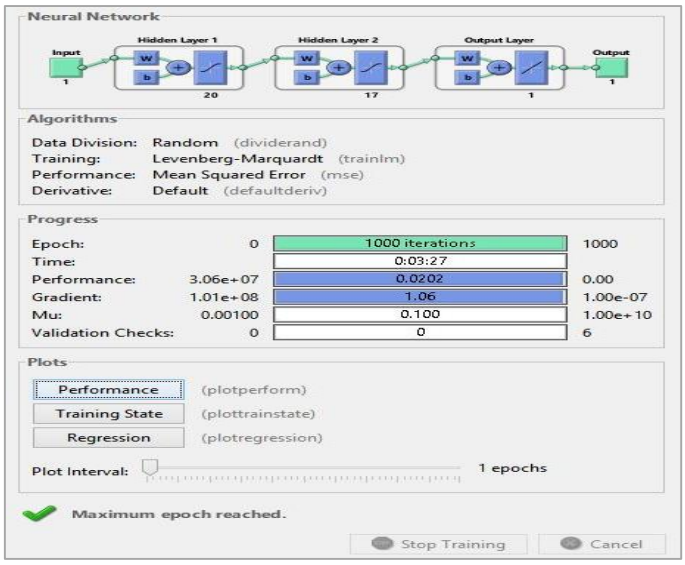

Figure 9. ANN and Performance Measures

Training, validation and test compared with the target value is shown in Figure 10.

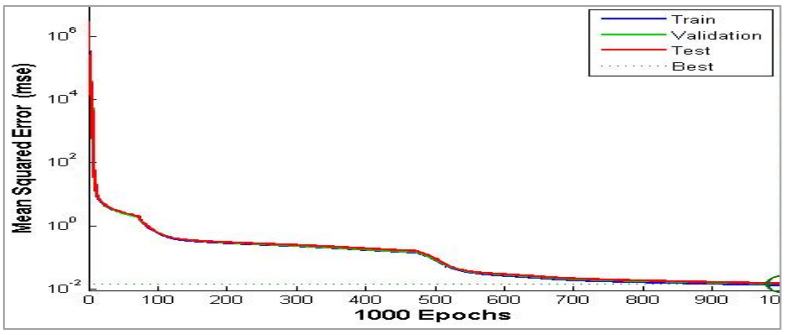

Figure 10. Training, Validation, Test and Target (1000 epochs).

Using different ANN algorithm, namely conjugate gradient other than the default Levenberg-Marquardt algorithm used in the previous examples, lead to much improvent in processing time and reaching closer values to the target in lesser time (Figure 11). As an example, image in Figure 12 is encrypted as shown in Figure 13 and its decrypted version is shown in Figure 14. The encryption and decryption were done in the same way for the second image in Figures 15, 16, and 17.

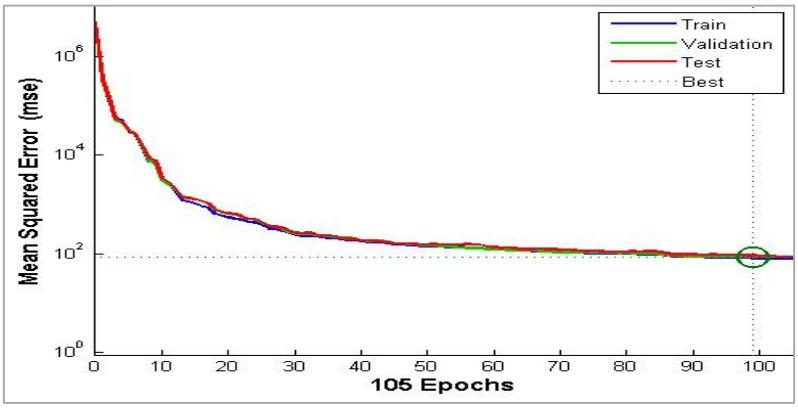

Figure 11. Training, Validation, Test and Target (105 epochs).

Figure 12. Orignal Image.

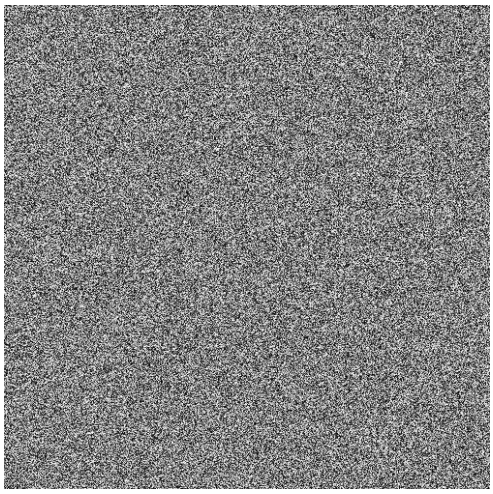

Figure 13. Encrypted Image.

Figure 14. Decrypted Image.

Figure 15. Orignal Image.

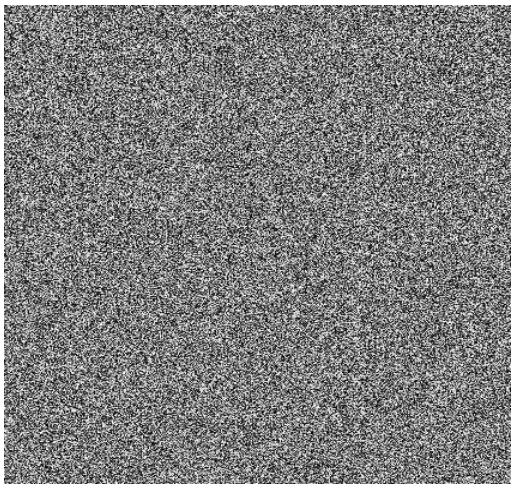

Figure 16. Encrypted Image.

Figure 17. Decrypted Image.

All values generated from different algorithms of the ANN for secret keys of the encryption process were less than one and consisting of five bits. They yield a mean squared error (MSE) which is very small (0.00001) and a peak signal to noise ratio (PSNR) of 98.13 , It was determined using the following equation.

$$PSNR = 10 \log_{10} (Max_i^2/MSE) \quad (3)$$

where Max_i is the maximum possible pixel value of the image (= 255 for 8 bits).

7. Conclusions

In this work chaos and artificial intelligence, specifically artificial neural networks (ANN), are combined for creating chaotic ANN based and named intelligent chaos to protect information and guarantee that sent information reaches its destination safe and secure. Secret keys for information encryption has been generated by using the ANN's dynamic change of weights to guarantee the change of chaotic circuits initial condition that would guarantee the

dynamic change of chaos and hence the continuous change of information encryption secret access keys and in turn prevent hackers and intruders and even enemy's electronic armies from attacking the system from viewing information sent.

Matlab simulation results with the use of known images proved that the chaotic ANN based encryption algorithm to be highly efficient and reliable. Training, validation and test results showed that they deviate very little from the target outcome and moreover the PSNR of 98.13% was found to be very high compared with other algorithms results both conventional and advanced.

The algorithm used in this work could be improved if more than one artificial neural network is used, for example in the case of very close values in the ANN problem may be solved by using fuzzy logic control (FLC) to take care of the minute change values.

References

[1] S. Dhawan, Information and Data Security Concepts, Integrations, Limitations and Future, International Journal of Advanced Information Science and Technology (IJAIST), October (2014), PP. 2319-2682.

[2] J. Andress, The basics of information security: understanding the fundamentals of InfoSec in theory and practice. Syngress, (2014).

[3] Kaspersky Daily, IT Security Economics in 2019. Retrieved from https://media.kasperskydaily.com/wpcontent/uploads/sites/92/2019/10/01041217/. (2019).

[4] Blacksheepnetworks, Security: Secure Internet Data Transmission. retrieved from http://www.blacksheepnetworks.com/security/info/misc/inun/ch16.htm. (2021).

[5] A.Singh, A.Vaish, and P. K.KeserwaniInformation security: Components and techniques. International Journal of Advanced Research in Computer Science and Software Engineering, 4 (2014).

[6] A. Gupta , P. Tiwari, and D. Nagaria, Cryptography Using Artificial Intelligence, Journal of Emerging Technologies and Innovative Research (JETIR), (2020),PP.2349-5162.

[7] S. Bhamarea , S. Sawarkarb, Image/Data Encryption-Decryption using Neural Network, 3 rd International Conference on Recent Trends in Engineering and Technology,(2014).

[8] J . Blackledge, and S. Bezobrazov, Cryptography using Artificial Intelligence , IEEE ,(2015), pp.1-6.

[9] K. AlSabti and H. Hashim , A New Approach for Image Encryption in the Modified RSA Cryptosystem Using MATLAB, Global Journal of Pure and Applied Mathematics,(2016), pp. 3631-3640.

[10] M.Hussein, K. Hassan, and H.Al-Mashhadi, The quality of image encryption techniques by reasoned logic, TELKOMNIKA Telecommunication, Computing, Electronics and Control, (2020), pp. 2992-2998.

[11] M. Farajallah, Chaos-based crypto and joint crypto-compression systems for images and videos (Doctoral dissertation, Universite de Nantes), (2015).

[12] Z. Garip, M. E Cimen, D. Karayel, and A. F. Boz, The chaos-based whale optimization algorithms global optimization. Chaos Theory and Applications, (2019), pp.51-63.

[13] N.V. Kuznetsov, O. A. Kuznetsova, G. A Leonov, T. N. Mokaev, and N.V. Stankevich, Localization of hidden Chua attractors by the describing function method, (2017), pp. 1705-02311.

[14] A. S.Mhetras, and N. N. Charniya, Cryptography based on artificial neural networks and chaos theory, International Journal of Computer Applications, (2016),pp.975, 8887.

[15]A. D. Dongare, R. R. Kharde, and A. D. Kachare, Introduction to artificial neural network. International Journal of Engineering and Innovative, (2012).