Artificial intelligence techniques for encrypt images based on the chaotic system implemented on field-programmable gate array

Wisal Adnan Al-Musawi, Mohammed Abd Ali Al-Ibadi, Wasan A. Wali
Department of Computer Engineering, Collage of Engineering, University of Basrah, Basrah, Iraq

Article Info

Article history:

Received Dec 21, 2021
Revised Aug 8, 2022
Accepted Sep 6, 2022

Keywords:

Artificial neural networks
Chua chaotic systems
Field programmable gate array
Image encryption and decryption
Xilinx system generator

ABSTRACT

Image encryption is an important issue in protecting the content of images and in the area of information security. This article proposes a novel method for image encryption and decryption using the structure of the artificial neural network (ANN)-based chua chaotic system (CCS). This structure was efficiently designed on a field-programmable gate array (FPGA) chip utilizing the xilinx system generator (XSG) tool with the IEEE-754-1985 32-bit floating-point number format. For ANN-based CCS design, a multilayer feed forward neural network (FFNN) structure with three inputs and three outputs was created. This structure consists of one hidden layer with four neurons, each of which has a Tangent Sigmoid activation function. The training of ANN-based CCS yielded a 3.602e-13 mean square error (MSE) value. After successfully training the ANN-based CCS, the design was carried out on FPGA, utilizing the ANN structure's bias and weight values as a reference. The xilinx vivado (2017.4) design suite was used to synthesis and test the ANN-based CCS on the FPGA. The histogram, correlation coefficient, and entropy are used to perform security analysis on various images. Finally, FPGA hardware co-simulation using a Xilinx Artix7 xc7a100t-1csg324 chip was utilized to verify that the encryption and decryption of the images were successful.

Corresponding Author:

Wisal Adnan Al-Musawi
Department of Computer Engineering, University of Basrah
Basrah, Iraq
Email: wisal.eng@gmail.com

1. INTRODUCTION

In recent years, image encryption, being a significant area of information security, has attracted a large number of researchers and scientists. Numerous studies using various methodologies have been implemented, and novel and useful algorithms have been proposed to improve secure image encryption schemes. Digital image encryption approaches based on chaotic systems are novel techniques. This technology encrypts images using random chaos sequences and is a very secure and fast method of image encryption [1]. The use of chaotic systems in cryptography to encrypt images has been proposed as a possible solution to a variety of security problems due to their numerous advantages over random characteristics such as sensitive dependency on initial conditions and parameter settings, simplicity of design, and aperiodic signal, which makes them an ideal option for cryptography systems [2].

This work aims to build a secure cryptographic algorithm that conforms to the following criteria: It is highly resistant to common cryptographic attacks, has a strong key, has a high throughput to meet the demands of large multimedia data volumes, and is simple to implement and consumes little power. The method used, which is artificial neural network (ANN)-based chua chaotic system (CCS), was simpler, more effective, and produced good results as compared to other complex methods of image hiding, such as chaotic block image permutation and XOR operations are performed to achieve image encryption in [3]. Čelikovský and Lynnyk [4], introduced the chaotic masking scheme based on embedded message synchronization. An effective and high-security communication system based on two levels of encryption based on chaotic systems was proposed [5].

Artificial intelligence techniques have gained significant importance in modeling because of their ability to reason and learn in an environment of uncertainty, approximation, and imprecision. These techniques comprise a collection of new technologies that offer an alternate approach to mathematical modeling for nonlinear dynamics, an issue that permeates all fields of science. Fuzzy logic, neural networks, and genetic algorithms are considered the principal constituents of artificial intelligence techniques. In the area of prediction, nonlinear prediction of chaotic time series is a big challenge [6]. ANN models are considered a subject of interest due to their many practical applications in modeling complex nonlinear systems and in chaotic time-series predictions [7]. One of the most efficient and general modeling methods is ANN, developed and inspired by actual biological neural brain structures as an artificial intelligence approach, non-parametric and non-linear, which can model complex systems such as chaotic systems [8].

This work contributed to implementing an ANN model by xilinx system generator (XSG)capable of predicting time series generated by a double scroll Chua circuit directly after training it instead of using the solution of differential equations. It is used as a novel cryptographic technique in secure communications for encrypting images. Numerous studies and research based on the prediction of chaotic systems using neural networks have been established [8]–[10].

For many reasons, ANN implementations on field-programmable gate arrays (FPGAs) proved useful. FPGAs can offer higher speeds because they can be completely exploited by the parallel design of ANNs. Moreover, FPGAs are easily reconfigurable and FPGAs have a relatively small design time compared to ASIC design [11].

The following is the organization of the paper: section 2 is an overview of chaotic systems, including the Chua Chaotic System. In section 3, the design and implementation of ANN-based CCS on FPGA are introduced. Section 4 shows image encryption using ANN-based-CCS. In section 5, Performance and Security Analysis is investigated. FPGA hardware Co-simulation testing was conducted in section 6. Finally, conclusions are stated in section 7.

2. CHAOTIC SYSTEMS

Chaos systems exhibit distinctive qualities such as noise-like behavior, sensitivity to initial conditions, and non-periodic features [12]. Chaotic systems' dynamics are entirely influenced by their initial conditions and parameters. That is why even a small change in the initial conditions has a significant effect on how the system behaves. Due to these characteristics, chaotic systems provide excellent candidates for secure communication, information technology, and cryptography [13]. Today, chaos and chaotic systems are widely used in a variety of technical applications, including biomedicine, cryptology, signal and image processing, artificial neural networks, random number generators, industrial control, and power electronics [14].

The Chua chaotic system has an easy structure and creates chaotic dynamics with sufficient parameters, showing chaos and several known phenomena of bifurcation. Therefore, several researchers have been interested in this method. In 1983, Leon Chua developed a nonlinear circuit that is capable of demonstrating a rich collection of dynamical phenomena, ranging from fixed points to cycle points, standard bifurcations (period-doubling), other standard routes to chaos, and chaos itself. The relevance of the Chua circuit has recently made possible the birth of a large family of multi-scroll oscillators and techniques to control chaos [15]. Chua circuit has found many applications in physics, communication, and control, mechanics, as well as chemistry, economics, and medicine [16]. Chua circuit has also been employed as a chaotic noise generator. Because of this feature, it has found several applications in cryptography and steganography [17]. The following nonlinear equations describe this chaotic system:

$$\begin{aligned} x &= \alpha(y - x - f(x) \\ y &= x - y + z \\ z &= -\beta y \end{aligned} \tag{1}$$

where α and β are the parameters of the system and f(x) Piece-Wise Linear (PWL) function known as Chua's diode and defined by**:**

$$f(x) = m_1 x + 1/2(m_0 - m_1)(|x + b_1| - |x - b_1|) \quad (2)$$

In this equation, m_0, m_1 is a slope that must have negative values and bi-break point values.

3. DESIGN OF ANN-BASED CHUA CHAOTIC SYSTEM ON FPGA

In this section, an ANN-based CCS is implemented on an FPGA based on the biases and weights obtained from the (FFNN) model. As illustrated in Figure 1, the implementation of an ANN-based CCS can be divided into two stages: offline training and hardware design using XSG. The Matlab Neural Network Processing Toolbox was used for the offline training stage. Following the training phase, the appropriate network parameters (weights and biases) were determined and then deployed on the FPGA [9]. Throughout the design process, several architectural types were examined. Finally, the (FFNN) (3×4×3) architecture was selected because this architecture has given better results than other architectures available. Increases in the number of hidden neurons affect not only response time but also the network's processing speed. The 10,000 training samples have been generated by using the Dormand-Prince (Ode5) algorithm. The generated samples have been divided into three subsets: 70% of the samples are used for training, 15% for validation, and 15% for testing. The trained network's weights and biases have been measured in MATLAB and then saved in Xilinx blocks. The MATLAB neuron network toolbox includes three training algorithms: Levenberg-Marquardt (the default), Scaled Conjugate Gradient (a faster training algorithm), and Bayesian Regulation (slower but with better convergence). The experimental results showed that an FFNN, trained with the Bayesian Regulation back-propagation algorithm, was found to be the suitable network structure. The performance function achieves a 3.602e-13 mean square error (MSE) value at the end of training when four neurons are utilized for the hidden layer, as shown in Table 1. It is possible to reduce the MSE value by increasing the number of neurons in the hidden layer, but this results in slower performance and greater size, both of which are undesirable for real-time ANN implementations. Furthermore, there is a trade-off between the number of hidden neurons used in the FFNN model structure and the FPGA resources. As a result, an acceptable value of MSE can be utilized for the implementation of the ANN-based CCS.

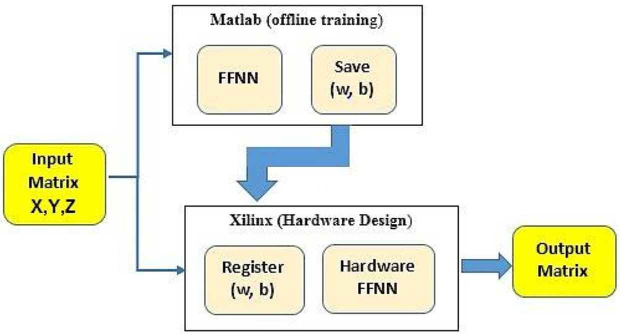


Figure 1. General block diagram of the ANN implement work

Table 1. FFNN structure and parameters

Parameters	Details
Network structure	3×4×3
Activation function	Hidden Layer: TanSig Output Layer: Purelin
Training functions	TrainBR
Performance function	MSE: 3.602e-13
Number of inputs/signals	10,000
Number of epochs	150.000
Fault tolerance	1E-13

An FPGA implementation not only provides the option of parallelism, but it also lowers design costs and increases flexibility, making it particularly suitable for ANN applications [9]. That is why an ANN-based CCS was built using FPGA. The ANN-based Chua chaotic system design model, which is a hardware design using the XSG (XSG) stage shown in Figure 2, contains Chua circuit implemented directly based on their definitions represented by a unique group of ordinary differential equations (ODEs). One hidden layer with four neurons. Each neuron has a hyperbolic tangent sigmoid activation function is implemented directly, as shown in Figure 3. One output layer has three neurons. The Tangent Sigmoid (TanSig) activation function has been used for the hidden layer due to its success in modeling nonlinear dynamic systems with chaotic behavior. The linear (PureLin) function has also been used for the activation function of the output layer. Figure 4 displays the phase portrait generated by the ANN-based CCS. Figure 5 displays the comparison between the 2-scroll generated from ANN and that generated from equations and the synchronization between them. The system parameters and initial values are as: α=10, β= 14.87, m0= -1.27, m1= -0.68, b=1 (x0= -0.4, y0= 0.1, z0= 0).

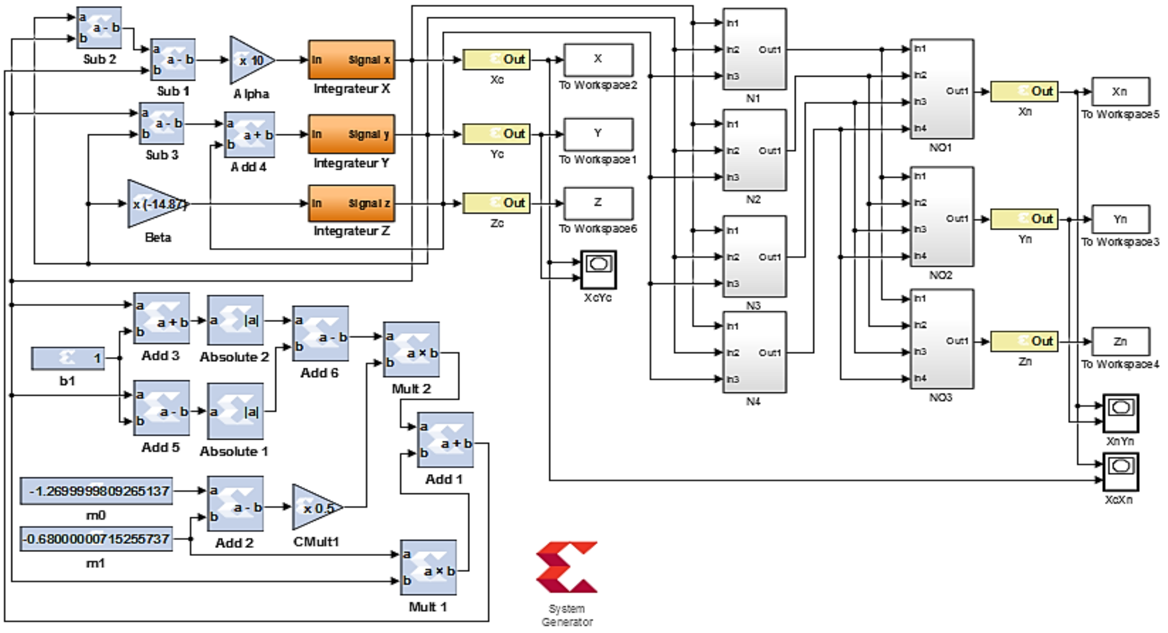


Figure 2. ANN based Chua chaotic system design using XSG

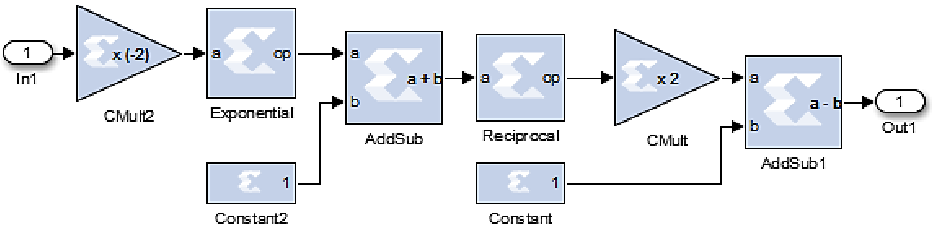


Figure 3. Tan-sigmoid activation function

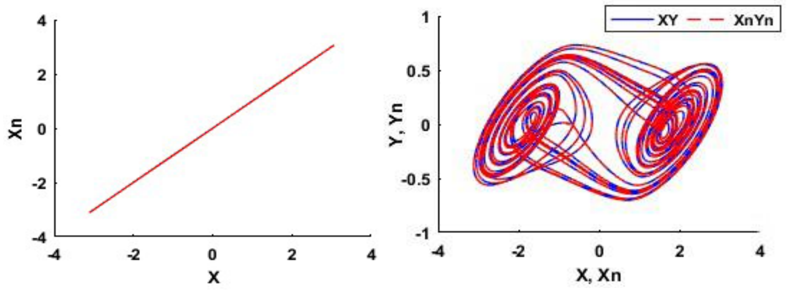


Figure 4. Comparison between 2-scroll generated from ANN (dotted lines) and from equations (solid lines) and synchronization state

3.1. Image encryption using ann based-chua chaotic system

The XSG design of image encryption using the ANN-based Chua Chaotic System is displayed in Figure 5. The first step is to produce chaotic signals X, Y, and Z using ANN. Then, 32 bits from each of the three signals are passed through a slicing function to extract the least significant bits, and then passed through a concatenation function to generate a new 32-bit sequence. Where Lx is equal to 12 bits, Ly is equal to 10 bits, and Lz is equal to 10 bits. The reason for selecting the least significant bits (LSBs) is that these bits provide a greater amount of randomness than the most significant bits (MSBs). The second step is to XOR the 8 bits (LSB) from this sequence with the 8 bits from the image to produce the ciphered image. As illustrated in Figure 6, the system is composed of encryption and decryption processes. The original color image is divided into red, green, and blue images, and its data type is Unint8. The original image, I (Lr * Lc), is converted to serial samples during the encryption stage using a preprocessing block as shown in Figure 7. The gateway-in converts the serial sample format to an unsigned fixed-point format with a (width length) WL=8 and a (fractional length) FL=0. The same key is used in the decryption stage to recover the original image by XORing it with the ciphered image and returning it to Matlab/Simulink via the gateway-out. To restore the original image at its original size, a post-processing block is utilized to convert the serial sample to its original size (Lr * Lc), as illustrated in Figure 8. The results are displayed in Figure 9. Optimizing ANN architectures is critical for enhancing the performance of hardware implementations [10]. After making an optimization by adding delay to the longest path to improve timing performance, system outputs are produced once per 80-clock cycle. The minimum clock period of the ANN-based CCS on FPGA is (Ts-WNS) (80-0.221)=79.779 ns and the maximum frequency is (1/79.779)=12.53 MHz. The chip statistics for the image encryption using ANN-based CCS on FPGA are given in Table 2.

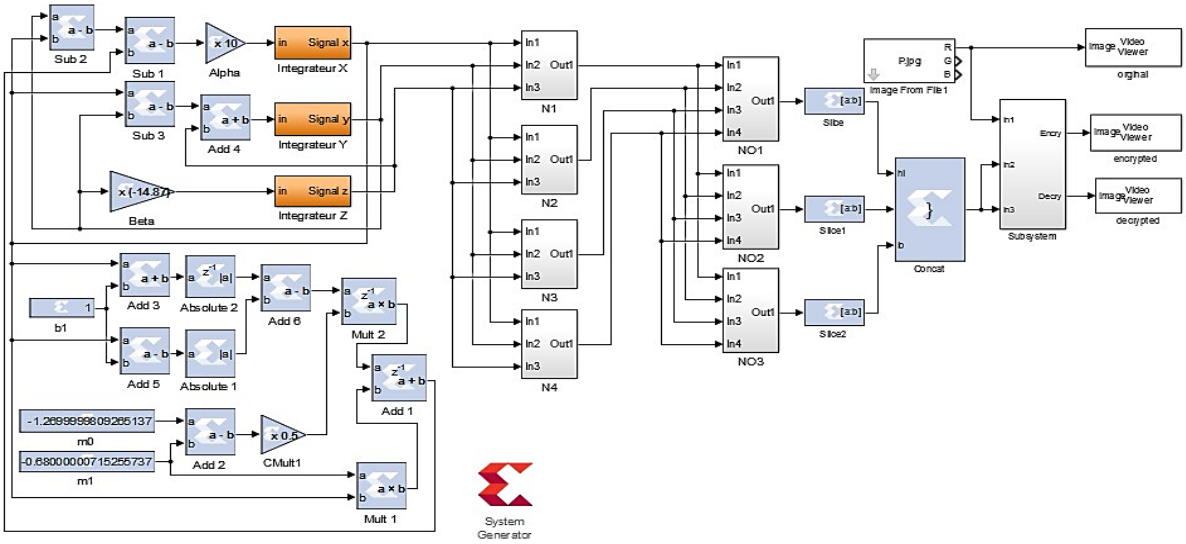


Figure 5. XSG design for cryptography used ANN

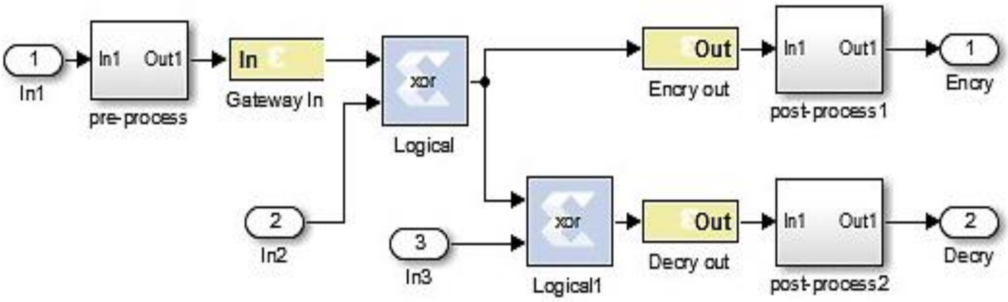


Figure 6. Subsystem for image encrypted and decrypted

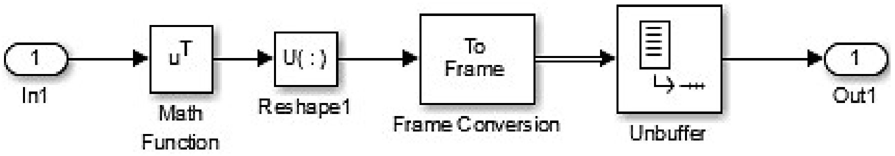


Figure 7. Pre-processing blocks

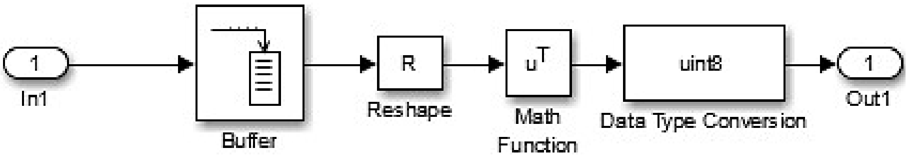


Figure 8. Post-processing blocks

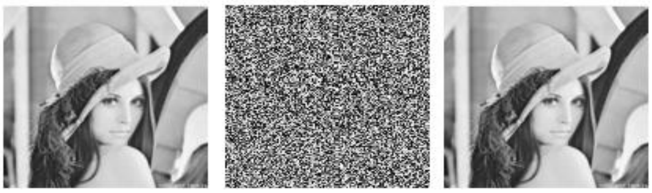


Figure 9. Image encryption and decryption result using ANN

Table 2. FPGA utilization summary for image encryption and decryption

Resource Type	Available	Utilization
LUT	63400	20589
Slice Registers (FF)	126800	240
Bonded IOB(IO)	210	73
BUFGCTRL(BUFG)	32	1
DSP	240	158
Minimum Period Ts (ns)	80	
Worst Negative Slack (WNS)	0.221	
Maximum Frequency (MHz)	12.53	
Throughput (MB/sec)	400.96	
Power(W)	0.181	

4. PERFORMANCE AND SECURITY ANALYSIS

Numerous analysis are presented to evaluate the proposed algorithms' efficiency and security, including histograms, correlation coefficients, information entropy, key space, and differential attack analysis. This section applies the study to an image of 512*512 size. Experiments are conducted and data analysis is performed using a Matlab environment.

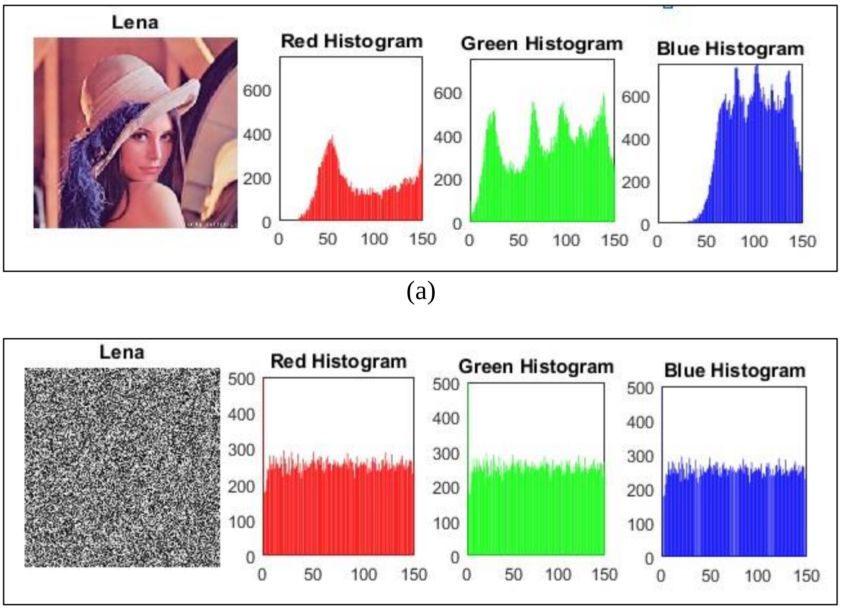
4.1. Histogram analysis

The histogram is a useful statistical function that illustrates the distribution of pixel values by graphing the number of pixels at each color intensity level [18]. It is commonly used to test image encryption algorithms' accuracy. A successful encryption algorithm should produce encrypted images with uniformly distributed histograms. Figures 10(a) and 10(b) illustrate a comparison of the distribution histograms before and after the encryption algorithm. As can be observed, our histograms are highly uniform in distribution, and the histograms generated by the ANN-based-CCS encryption process are extremely robust.

4.2. Correlation coefficient analysis (CCA)

A correlation factor is another significant factor in the study of the cryptosystem. The correlation between the pixels of the original image is strong, while the correlation between the pixels of the encrypted image is very low. An algorithm for image encryption would have succeeded if all its attributes were hidden and the encrypted image was entirely unrelated and random. If the coefficient of correlation is equal to 1, the two images are the same. Therefore, the encryption failed in these cases. When the value is 1, the encrypted image is the opposite of the plain image. The (3) is used to measure the correlation coefficient of any two-pixel color values at the same position in the original and cipher images [19]. where μx and μy represent mean values of x and y, σx and σy are the standard deviations of x and y, and $E[\cdot]$ is the expectation function [20]. Table 3 displays experimental correlation pixels for pictures of Lena with sizes 512*512.

$$Corr(x, y) = \frac{E[(x-\mu_x)(y-\mu_y)]}{\sigma_x\sigma_y} \quad (3)$$



(a)

(b)

Figure 10. Histogram of three-channel; (a) original images and (b) ciphered images

Table 3. Correlation coefficient comparison between proposed algorithm and other approach

Image name		Proposed Algorithm			Ref [20]		
	Channel	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
	R	0.0012	2.4824-e-04	8.6752e-04	0.0033	0.0155	0.0158
Lena	G	-0.0012	-0.0014	-0.0022	0.0294	0.0146	0.0102
	B	5.0191e-04	6.1836e-04	-1.9552e-04	0.0086	− 0.0229	− 0.0366

4.3. The information entropy

The entropy of information can be used to express randomness. At (4) can be used to compute the information entropy [21]. Where si is the pixel value, P(si) is the probability of symbol si, 2L is the total state of the information source, and log2P (si) is used to convert si to bit form. In general, a higher entropy value indicates a more secure encryption technique [21]. Table 4 summarizes the results of the entropy calculation. As can be observed, all of the entropy values are close to 8. As a result, the technique that is used is more efficient and secure.

$$Entrp(s) = \sum_{n=0}^{2^N-1} P(si) \times \log_2\left(\frac{1}{P(si)}\right) bits \quad (4)$$

Table 4. Information entropy comparison between suggested techniques and other ways

Image name	Channel	Original	Ciphered	Ref [22]	Ref [2]
	R	7.598	7.993	7.9974	7.9993
Lena	G	7.663	7.992	7.9969	7.9992
	B	7.221	7.992	7.9884	7.9993

4.4. NPCR and UACI analysis

The two most widely used metrics to calculate this requirement are the Number of Pixel Change Rate (NPCR) and the Unified Averaged Changed Intensity (UACI), which are used to assess the strength of image encryption algorithms against brute force attacks [2]. The NPCR and UACI metrics can be expressed as:

$$UACI = \frac{1}{W \times H}\left[\sum_{i,j}\frac{|C_1(i,j)-C_2(i,j)|}{255}\right] \times 100\% \tag{5}$$

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\% \tag{6}$$

Where W and H denote the width and height, respectively, of the ciphered image, C_1 is the encrypted image, while C_2 is the ciphered image created by randomly changing one pixel in C_1. D (i, j) is given by (7) [23]. The UACI and NPCR measures as shown in Table 5 are used to determine the effect on the cipher image of the change of 1 bit/pixel in the original image [24], [25].

$$D(i,j) = \begin{cases} 0, \; if \; C_1(i,j) = C_2(i,j) \\ 1, \; otherwise \end{cases} \tag{7}$$

Table 5. NPCR and UACI test calculation for ciphered images

Image name	channel	NPCR	UACI
Lena	R	99.61	30.49
	G	99.61	30.53
	B	99.61	30.50

5. FPGA HARDWARE CO-SIMULATION TEST

The proposed model is formulated using the FPGA board Artix7 xc7a100t-1csg324. The image encryption and decryption processes are co-simulated with FPGA hardware. When a Joint Test Action Group connection (JTAG) is connected, serial image signal data is transmitted via a USB JTAG port to the FPGA. Then, serial samples were returned to the PC using the Simulink/Matlab Viewer to test the image. In Figure 11, the images at the top represent the results of FPGA hardware co-simulation, and the images at the bottom represent the results of the proposed system using XSG. The encrypted image has proved to be the same for system generators and for co-simulation, demonstrating that the actual time for the proposed encrypted image works correctly and is compatible with the expected configuration.

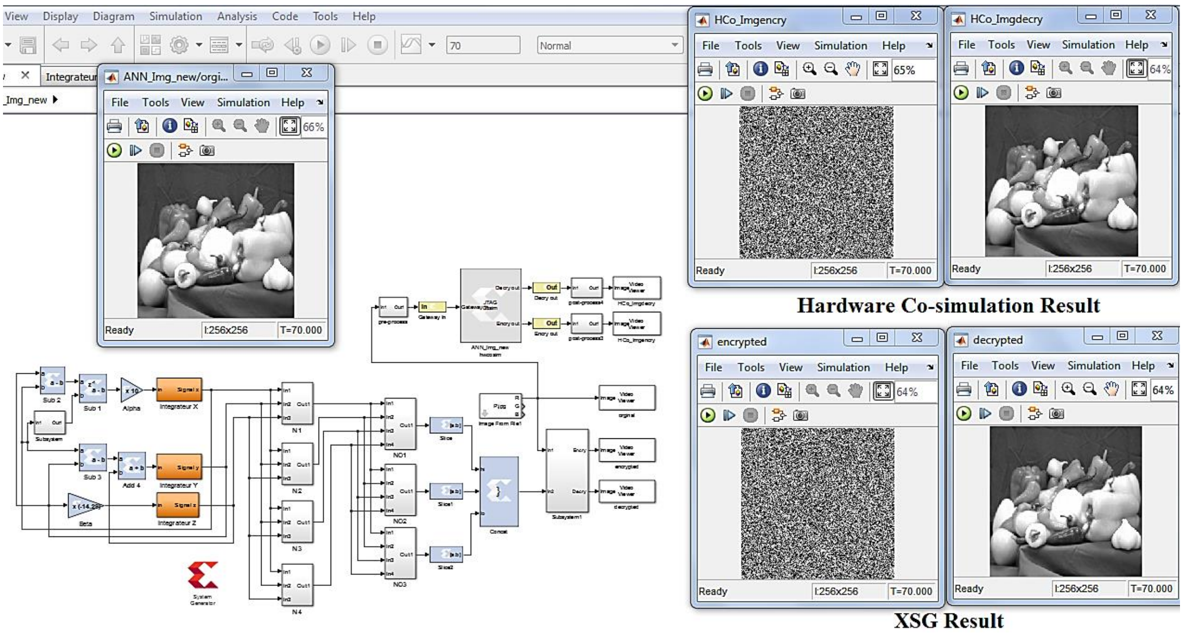


Figure 11. Hardware Co-simulation test results of the image encryption and decryption

6. CONCLUSION

The FFNN (3×4×3) architecture was chosen because of its better results with respect to the number of hidden neurons. At the end of the training, the performance function reached 3.602e-13 MSE. After successfully training the ANN-based CCS, the system on FPGA has been designed in XSG with the 32-bit IEEE-754-1985 floating-point number standard by taking the network structure, bias, and weight values as reference. The implementation of the proposed system on FPGA has been tested by synthesizing it with the Xilinx Vivado program. Securing transmitted images is important, as the transmission channel is open and susceptible to attack. To protect this channel, this paper implements an image encryption algorithm using a novel cryptographic technique called an ANN-based CCS. Numerous statistical tests such as histograms, entropy, correlations, NPCR, and UACI were used, and the results indicate that the proposed mechanism generates an optimal analysis result that is resistant to various attacks. Resource utilization has been measured and the proposed system has a maximum frequency of approximately 12.53 MHz. Finally, the real-time evaluation of the system proposed was co-simulated using the FPGA Xilinx Artix7 xc7a100t-1csg324 chip.

REFERENCES

[1] Y. Pourasad, R. Ranjbarzadeh, and A. Mardani, “A new algorithm for digital image encryption based on chaos theory,” *Entropy*, vol. 23, no. 3, p. 341, Mar. 2021, doi: 10.3390/e23030341.

[2] F. S. Hasan and M. A. Saffo, “FPGA hardware co-simulation of image encryption using stream cipher based on chaotic maps,” *Sensing and Imaging*, vol. 21, no. 1, p. 35, Dec. 2020, doi: 10.1007/s11220-020-00301-7.

[3] R. A. Aboughalia and O. A. S. Alkishriwo, “Color image encryption based on chaotic block permutation and XOR operation,” *arXiv preprint arXiv:1808.10198*, Aug. 2018, [Online]. Available: http://arxiv.org/abs/1808.10198.

[4] S. Čelikovský and V. Lynnyk, “Message embedded chaotic masking synchronization scheme based on the generalized Lorenz system and its security analysis,” *International Journal of Bifurcation and Chaos*, vol. 26, no. 8, p. 1650140, Jul. 2016, doi: 10.1142/S0218127416501406.

[5] S. S. Hreshee, H. N. Abdullah, and A. K. Jawad, “A high security communication system based on chaotic scrambling and chaotic masking,” *International Journal on Communications Antenna and Propagation (IRECAP)*, vol. 8, no. 3, p. 257, Jun. 2018, doi: 10.15866/irecap.v8i3.13541.

[6] W. A. Wali, “Application of particle swarm optimization with ANFIS model for double scroll chaotic system,” *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 11, no. 1, pp. 328–335, Feb. 2021, doi: 10.11591/ijece.v11i1.pp328-335.

[7] A. D. Pano-Azucena, E. Tlelo-Cuautle, and S. X. D. Tan, “Prediction of chaotic time series by using ANNs, ANFIS and SVMs,” in *2018 7th International Conference on Modern Circuits and Systems Technologies (MOCAST)*, May 2018, pp. 1–4, doi: 10.1109/MOCAST.2018.8376560.

[8] M. Alçın, İ. Pehlivan, and İ. Koyuncu, “Hardware design and implementation of a novel ANN-based chaotic generator in FPGA,” *Optik*, vol. 127, no. 13, pp. 5500–5505, Jul. 2016, doi: 10.1016/j.ijleo.2016.03.042.

[9] I. Koyuncu, M. Alcin, P. Erdogmus, and M. Tuna, “Artificial neural network-based 4-D hyper-chaotic system on field programmable gate array,” *International Journal of Intelligent Systems and Applications in Engineering*, vol. 8, no. 2, pp. 102–108, 2020.

[10] L. Zhang, “Multilayer artificial neural network design and architecture optimization for the pattern recognition and prediction of EEG signals based on henon map chaotic system,” in *2017 International Conference on Computational Science and Computational Intelligence (CSCI)*, Dec. 2017, pp. 345–350, doi: 10.1109/CSCI.2017.58.

[11] P. Dondon, J. Carvalho, R. Gardere, P. Lahalle, G. Tsenov, and V. Mladenov, “Implementation of a feed-forward artificial neural network in VHDL on FPGA,” in *12th Symposium on Neural Network Applications in Electrical Engineering (NEUREL)*, Nov. 2014, pp. 37–40, doi: 10.1109/NEUREL.2014.7011454.

[12] M. Tuna, M. Alçın, İ. Koyuncu, C. B. Fidan, and İ. Pehlivan, “High speed FPGA-based chaotic oscillator design,” *Microprocessors and Microsystems*, vol. 66, pp. 72–80, Apr. 2019, doi: 10.1016/j.micpro.2019.02.012.

[13] M. Zhou and C. Wang, “A novel image encryption scheme based on conservative hyperchaotic system and closed-loop diffusion between blocks,” *Signal Processing*, vol. 171, p. 107484, Jun. 2020, doi: 10.1016/j.sigpro.2020.107484.

[14] M. Alcin, I. Koyuncu, M. Tuna, M. Varan, and I. Pehlivan, “A novel high speed artificial neural network–based chaotic true random number generator on field programmable gate array,” *International Journal of Circuit Theory and Applications*, vol. 47, no. 3, pp. 365–378, Mar. 2019, doi: 10.1002/cta.2581.

[15] A. Byagowi and W. Kinsner, “Implementation of a Chua circuit to demonstrate bifurcations and strange attractors in a class,” *Proceedings of the Canadian Engineering Education Association (CEEA)*, Jun. 2012, doi: 10.24908/pceea.v0i0.4706.

[16] A. S. Andreatos and A. P. Leros, “Secure image encryption based on a chua chaotic noise generator,” *Journal of Engineering Science and Technology Review*, vol. 6, no. 4, pp. 90–103, Oct. 2013, doi: 10.25103/jestr.064.11.

[17] L. Merah, A. Ali-Pacha, N. H. Said, and M. Mamat, “A pseudo random number generator based on the chaotic system of Chua’s circuit, and its real time FPGA implementation,” *Applied Mathematical Sciences*, vol. 7, no. 53–56, pp. 2719–2734, 2013, doi: 10.12988/ams.2013.13242.

[18] H. Raheem Hatem, “Color image compression and encryption based on compressive sensing,” *Journal of Engineering and Sustainable Development*, vol. 2018, no. 01, pp. 149–161, Jan. 2018, doi: 10.31272/jeasd.2018.1.12.

[19] M. Ahmad, M. N. Doja, and M. M. S. Beg, “Security analysis and enhancements of an image cryptosystem based on hyperchaotic system,” *Journal of King Saud University - Computer and Information Sciences*, vol. 33, no. 1, pp. 77–85, Jan. 2021, doi: 10.1016/j.jksuci.2018.02.002.

[20] C. Fu, G. Zhang, M. Zhu, Z. Chen, and W. Lei, “A new chaos-based color image encryption scheme with an efficient substitution keystream generation strategy,” *Security and Communication Networks*, vol. 2018, pp. 1–13, 2018, doi: 10.1155/2018/2708532.

[21] Z. Tang, Y. Yang, S. Xu, C. Yu, and X. Zhang, “Image encryption with double spiral scans and chaotic maps,” *Security and Communication Networks*, vol. 2019, pp. 1–15, Jan. 2019, doi: 10.1155/2019/8694678.

[22] W. Wang *et al.*, “An encryption algorithm based on combined chaos in body area networks,” *Computers & Electrical Engineering*, vol. 65, pp. 282–291, Jan. 2018, doi: 10.1016/j.compeleceng.2017.07.026.

[23] M. Tuna, "A novel secure chaos-based pseudo random number generator based on ANN-based chaotic and ring oscillator: design and its FPGA implementation," *Analog Integrated Circuits and Signal Processing*, vol. 105, no. 2, pp. 167–181, Nov. 2020, doi: 10.1007/s10470-020-01703-z.

[24] I. A. Taqi and S. M. Hameed, "A new color image encryption based on multi chaotic maps," *Iraqi Journal of Science*, vol. 59, no. 4B, pp. 2117–2127, Dec. 2018, doi: 10.24996/ijs.2018.59.4B.17.

[25] H. A. Abdullah and H. N. Abdullah, "FPGA implementation of color image encryption using a new chaotic map," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 13, no. 1, pp. 129–137, Jan. 2019, doi: 10.11591/ijeecs.v13.i1.pp129-137.

BIOGRAPHIES OF AUTHORS

Wisal Adnan Al-Musawi Holds the M.Sc. degree in computer engineering from University of Basrah, Iraq, in 2021 and the B.Sc. degree in computer engineering from University of Basrah, Iraq, in 2012. Her research includes cryptography, prediction, modular neural networks, chaotic systems, and FPGA. She can be contacted at email: wisal.eng@gmail.com.

Mohammed Abd Ali Al-Ibadi Holds a PhD in Computer Engineering from University of Basrah, Iraq. He is currently Head of Compuer Engineering Department at Collage of Engineering, University of Basrah. His interest area of work is the Parallel and Distributed Systems, PFGA based systems, and ASIC. He has many projects implemented in the field of internet of things and computer vision systems. In addition, he is a member of IEEE and a reviewer for many local and international journals and conferences. He can contact at email: mohammed.joudah@uobasrah.edu.iq.

Wasan A. Wali Holds a PhD in Automation and Control Engineering, Built Environment and Sustainable Technologies Institute (BEST), Faculty of Technology and Environment, Livepool John Moores University, UK. MSc, BSc in Electrical Engineering, Electrical Engineering Department, College of Engineering, University of Basrah, Iraq. 1996, 1992 respectively. She is currently a lecturer in Computer Engineering Department, College of Engineering- University of Basrah, Iraq. Research interests: automation and control engineering, artificial intelligent control, microwave and microwave plasma control technologies, renewable energy, and chaotic systems. She can be contacted at email: wasan.wali@uobasrah.edu.iq.