International Journal of Electrical and Computer Engineering (IJECE)
Vol. 9, No. 4, August 2021, pp. xx~xx
ISSN: 2088-8708, DOI: 10.11591/ijece.v9i4.ppxx-xx

FPGA Design of Image Encryption and Decryption Using Chua's Chaotic Masking

Wisal A. Al-Musawi [1], W.A. Wali [2], Mohammed A. Al-Ibadi [3]
Department of Computer Engineering, College of Engineering, Basrah University, Iraq

Article Info

Article history:

Received Feb 9, 2021
Revised Jun 20, 2021
Accepted July 11, 2021

Keywords:

Chua's circuit
synchronization
masking
Image encryption and decryption
XSG
Hardware co-simulation

ABSTRACT

This paper proposed the FPGA implementation of effective image encryption and decryption approach using Chua's chaotic generator. The proposed system using the Xilinx System Generator's (XSG) synchronizing and, masking technique. Pecora-Carroll identical cascading synchronization approach used to achieve synchronization. The behavior of the response system depends on the behavior of the drive system and after a short time; there is no error between the master and, the slave. The original image is successfully recovered for secure communications in real-time, the transmitted signal should be mixed or masked with a chaotic carrier and can be processed by the receiver without any distortion or loss. The proposed system will be analyzed via a histogram, correlation coefficient, and, entropy information, differential attack (NPCR and UACI). In addition, FPGA Hardware Co-Simulation over Xilinx Artix7 xc7a100t-1csg324 was used to check the reality of the Encryption and decryption of images process. The results show that the cryptosystem is feasible and, efficient.

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

1. INTRODUCTION

Communication systems such as mobile and internet networks have increasingly developed in recent years, and the area of information transmission has been expanded. This region, however, faces additional challenges in the saving and exchange of media messages by means of illegal eavesdropping. Multimedia communications such as photographs and videos should also be encrypted to avoid unauthorized attacks to ensure secure transmission over the Internet. Traditional forms of encryption have some disadvantages in high stream data encryption and are less efficient in securing photos using encryption schemes. To guarantee secure Internet data transmission, Images must be encrypted with high protection and low complexity in an efficient way [1]. The chaos system has many properties, including an ergodic, unstable signal and a deterministic system, that are very sensitive to initial conditions and parameters. Due to the significant chaotic properties, chaotic for secure communication used. Several works and studies done to apply chaos to secure communication. Li and Ou proposed a new, chaos-based 3-D structure [2]. Comfort and et al. build a simple circuit of chaotic masking using the Chua Diode [3]. A Lorenz System-based signal masking technique is introduced in [4]. The chaotic masking scheme based on embedded message synchronization is introduced in [5]. An effective and high-security communication system based on two levels of encryption based on chaotic systems was proposed in [6]. Applying chaos to cryptography did not gain much attention until the discovery of chaotic synchronization, which contributed to a turning point in the application of chaos dynamics to information security. Since Pecora and Carroll's work [7], a wide range of research efforts has focused on the study of chaos synchronization. It is applied in a variety of fields, including secure communication, biological

systems, ecological systems, physical systems, etc. [8]. Much attention was given to the control and synchronization of Chua systems by researchers [9]. Chua oscillators have recently been synchronized with active control [10], adaptive control [11], sliding control [12], fuzzy control [13], impulsive control [14], and backstepping control [15] methods, etc. The Pecora-Carroll technique shows that if a state variable of a chaotic system is passed as an input into a replica of the original system part, it is also transmitted as an input to the replica subsystem (receiver) synchronizes to the original system (transmitter). This discovery connects the theory of chaos and communications to a new field of communication study that uses chaos. Synchronization requires the same chaotic systems as the transmitter (master) and the receiver (slave), which means a synchronization problem is caused by the misaligned parameters between receiver and transmitter [16]. Digital implementation on the FPGA system is the perfect way to implement this system since it removes component drift problems and has high power and throughput capacity [17]. FPGA was the main tool for implementing high-performance systems, especially in applications for image processing, in digital signal processing systems. FPGA also can provide high efficiency of signal processing [18]. The Xilinx Device Generator(XSG) enhances the power of the FPGA and provides essential tools to make image encryption models simple to develop. The architecture of the synchronized Chua chaotic system and FPGA hardware Co-Simulation for image encryption and decryption will be discussed in this paper.

2. CHUA'S CIRCUIT DESIGN

The Circuit of Chua has a simple structure and easily generates chaotic dynamics with sufficient parameters. Thus, several researchers have been interested in this circuit. For the implementation of the chaotic system Chua, we use the Xilinx System Generator (XSG) method in this section. A 3D system of non-linear, ordinary differential equations can be used to model the Chua circuit:

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

Where f(x)

$$\mathrm{f}\,(x) = m1x + 1/2(m0 - m1)\,(|x + b1| - |x - b1\,|) \qquad (2)$$

F(x) defines the nonlinear resistor electrical response, α and β are determined by the unique value of the circuit components. Where m0, m1 is a slope that must have negative values and bi-break point values. Function f(x) is provided to control the number of scrolls created. Figure 1, shows the XSG configuration of the Chua equation system (1) and f(x) in equation (2) with each x, y, and z integrator consisting of a dt multiplied register/adder using a 32-bit fixed-point with a 16-bit fraction and a 0.01(dt) clock step size. The parameters of the system are set as follows: α =10, β = 15, m0= -2.5 and m1 = -0.3. The initial conditions are randomly selected as follows: x_0= -0.1, y_0= 0, and z_0= 0.2. The system has long-term chaotic behaviors and uneventfulness with these parameters and is sensitive to the initial parameters. The Chua XSG system's distinct phase portrait and time series are shown in Figure 2 and Figure 3 respectively.

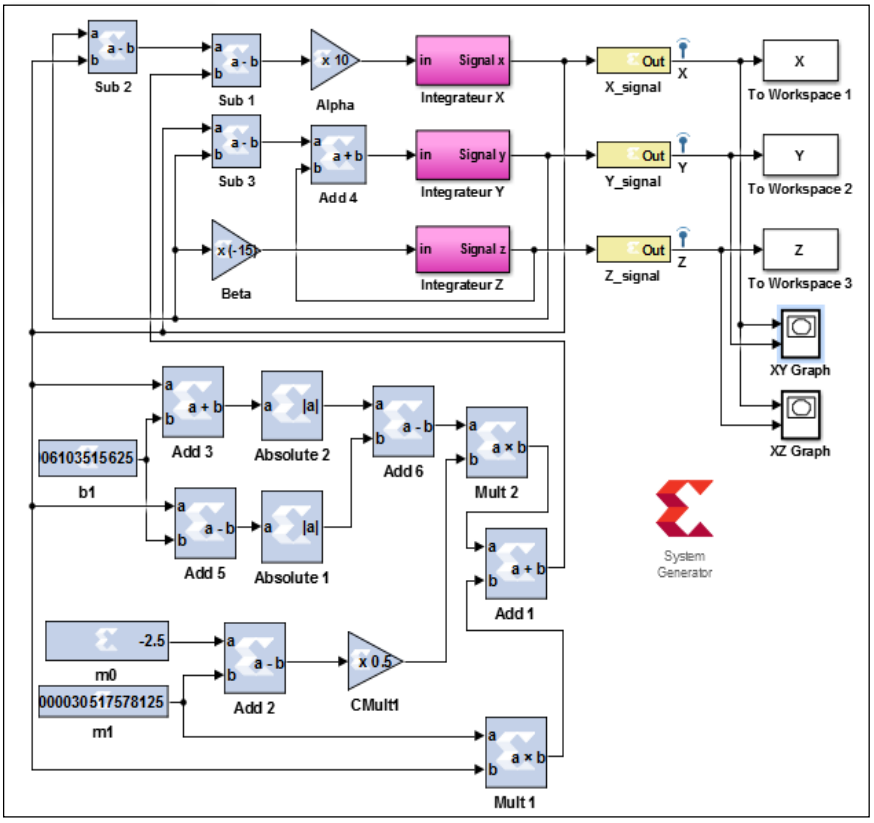


Figure.1 XSG design of Chua's circuit

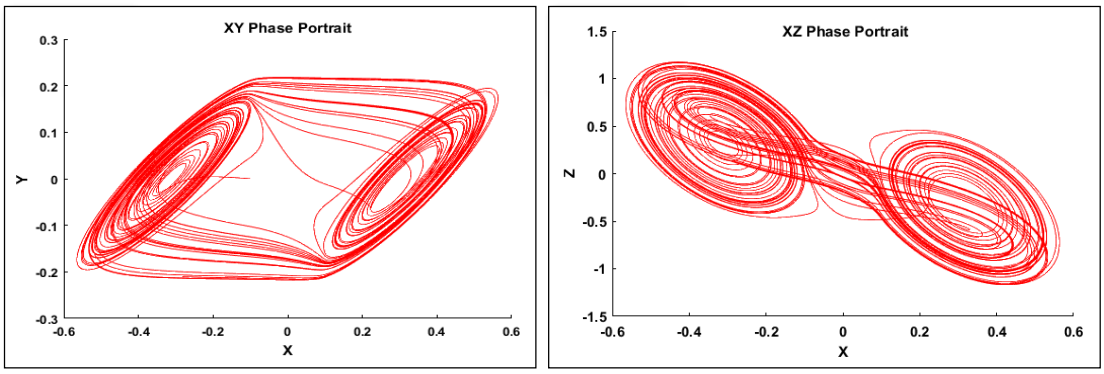


Figure.2 XY and XZ Phase Portrait Plot

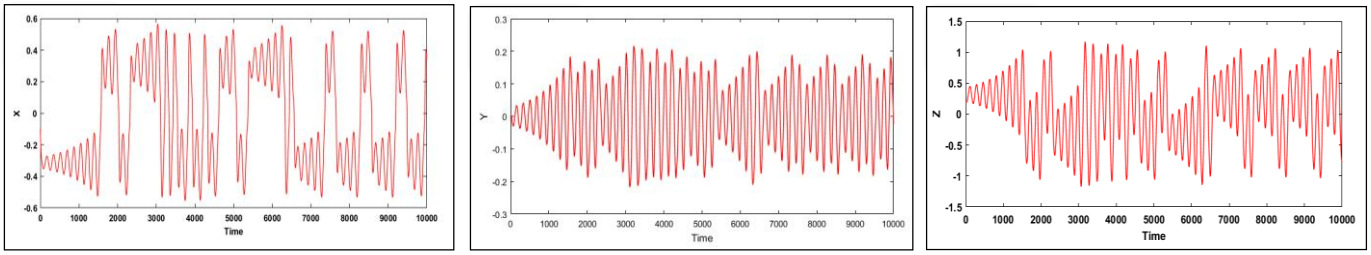


Figure.3 Time Series Plot for X, Y, and Z Signals

3. PC CASCADED SYNCHRONIZATION OF CHUA'S CHAOTIC SYSTEM

This method describes the two systems with type chaotic dynamics coupled to each other, one of them is the transmitter system also called the drive (master) and the two receivers named the response (slave). The response subsystems used here are the YZ response subsystem and XZ response subsystems. Figure 4 shows the block scheme of cascading synchronization system. The Chua cascaded synchronization system implemented using Xilinx System Generator model shown in Figure.5 where the master subsystem is implemented as in Figure 1.

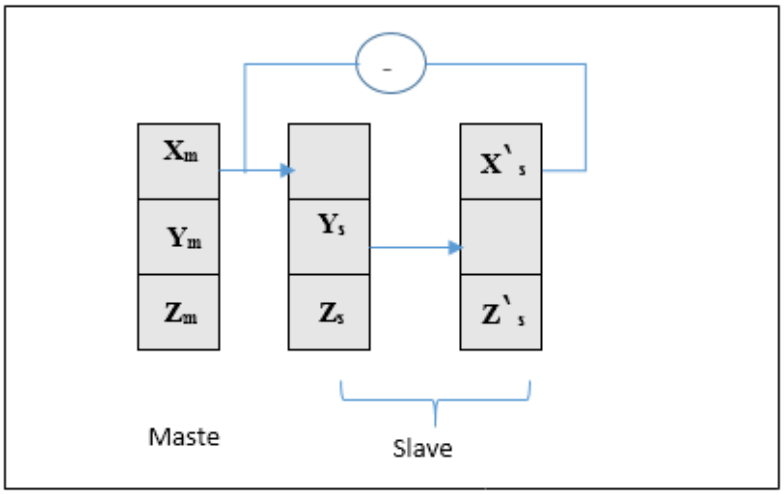


Figure.4 Block diagram of a cascaded synchronization system

The master equations

$$\begin{aligned} xm^{\cdot} &= \alpha\,(ym - xm - f\,(x)) \\ ym^{\cdot} &= xm - ym + zm \\ zm^{\cdot} &= -\beta ym \end{aligned} \tag{3}$$

YZ response subsystem equations

$$\begin{aligned} ys^{\cdot} &= xm - ys + zs \\ zs^{\cdot} &= -\beta ys \end{aligned} \tag{4}$$

XZ response subsystem equations

$$\begin{aligned} x's^{\cdot} &= \alpha\,(ys - x's - f\,(x)) \\ z's^{\cdot} &= -\beta ys \end{aligned} \tag{5}$$

The differences between master and slave are known as the synchronizing errors and the errors must converge to zero when the synchronization occurs.

$$\begin{aligned} ex &= x's - xm \\ ey &= ys - ym \\ ez &= z's - zm \end{aligned} \tag{6}$$

The chaotic signal before synchronization and the non-synchronized case are shown in Figure 6. Here, the value of α and β of the drive system and the response systems are different. Figure 7 shows the chaotic signal of the drive and response system after synchronization and the synchronization between the drive and the response system. In this case, the initial value of the two subsystems is different, but the value of α and β is the same for both drive and response systems. The system parameters as defined in Table 1. Simulation results show that the two subsystems are well synchronized. The design was implemented in Artix7 xc7a100t-1csg324 FPGA device and the resource utilization was estimated as shown in Table 2.

Table.1 cascaded synchronization system Parameters

		Synchronization		Unsynchronized		Slops & breakpoint
		Initial value	α & β	Initial value	α & β	
Drive system		x_0=0.3 y_0=0 z_0=0.1	α=10 β=15	x_0=0.3 y_0=0 z_0=0.1	α=10 β=15	m0= -2.5 m1= -0.3 b1=0.1
Response systems	YZ Response	y_0=0.1 z_0=0.4			α=9 β=100/7	
	XZ Response	x_0= 1 z_0=0.4				

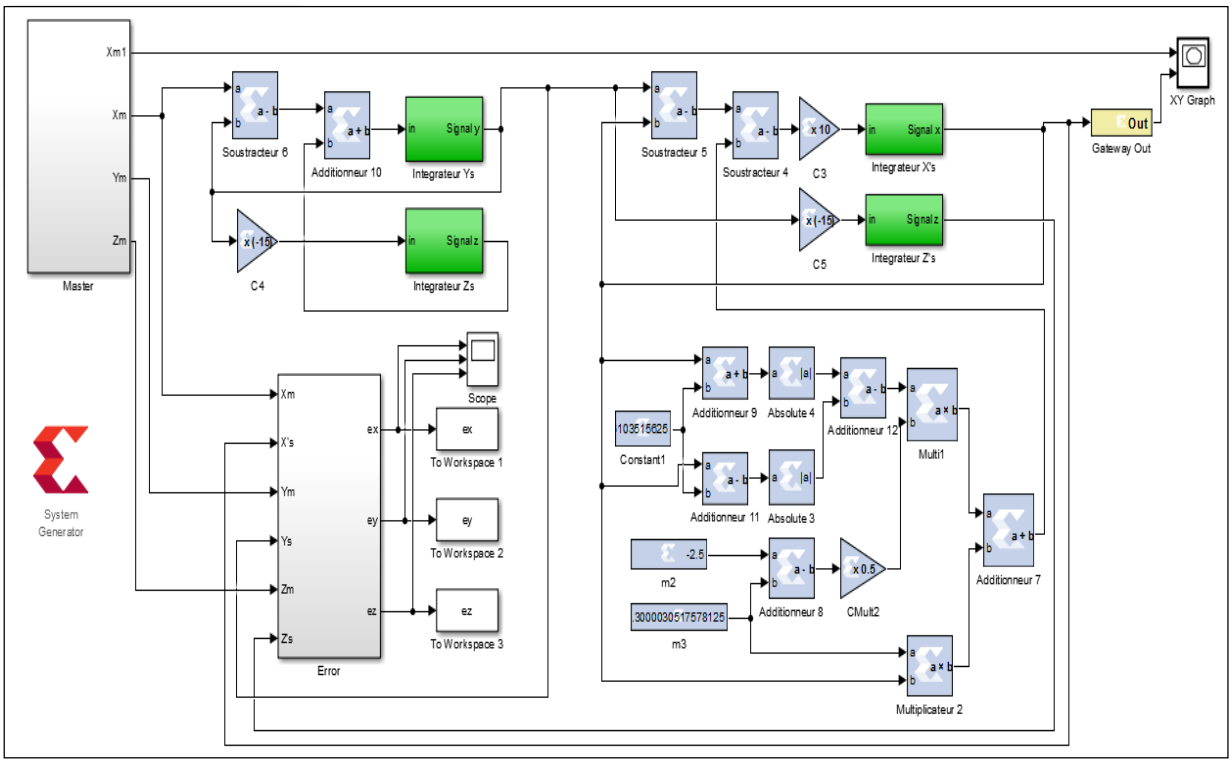
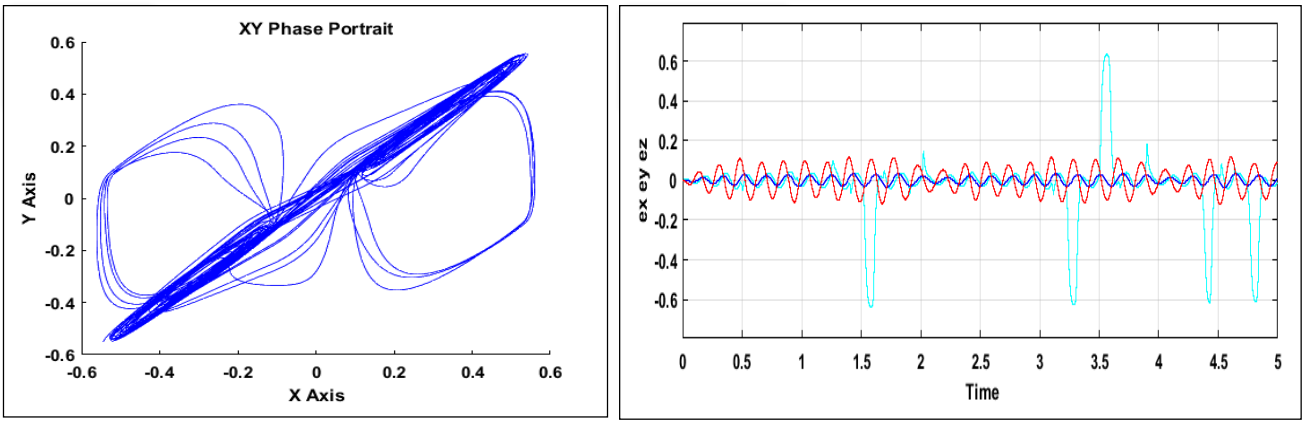
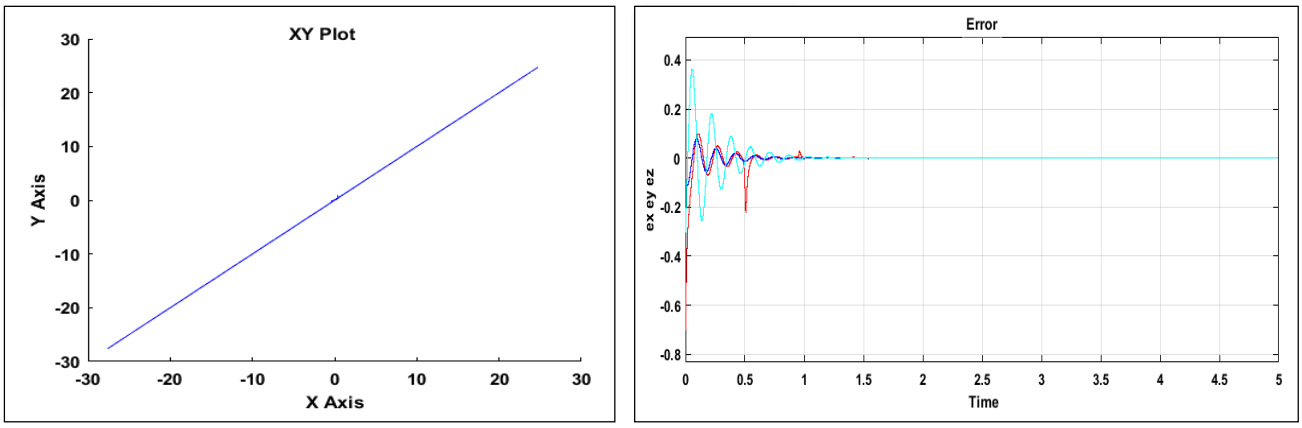


Figure.5 Chua cascaded synchronization system using XSG



(a) (b)

Figure.6 (a) Unsynchronised case (b) Error signal before chaotic synchronization



(a) (b)

Figure.7 (a) synchronization between drive and response system (b) Error signal after chaotic synchronization

Table 2: Device utilization summary of PC Cascaded Synchronization

Resource type	Available	Utilization
LUT	634000	1446
Slice Registers(FF)	126800	224
Bonded IOB(IO)	210	161
BUFGCTRL(BUFG)	32	1
DSP	240	40
Minimum period Ts (ns)	40	
Worst negative slack(WNS)	0.060	
Maximum Frequency(MHz)	25.04	
Power(W)	0.153	

4. CHAOTIC MASKING WITH FEEDBACK

The Chaotic Masking block diagram is shown in Figure 8. The image m (t) is added to the Chua chaotic Xm(t) signal generator, which also serves as a driving signal for synchronization purposes. The image is precisely retrieved from the receiver by subtracting the regenerated signal of the receiver from the obtained signal. To successfully remove the mask, both master and slave chaotic signals need to be synchronized, Pecora-Carroll (PC) Synchronization is one of the most powerful synchronization schemes to do this [6]. This device sends a signal from a chaotical generator called the master to the chaotic generator called the slave. The receiver constructs vectors for state errors that explain the difference between the variables master and slave state. In Figure 8, the received signal is

$s(t) = Xm(t) + m(t)$

And the recovered image is:

$\hat{m}(t) = s(t) - Xs(t) = [Xm(t) + m(t)] - Xs(t) = m(t) + ex(t)$

Where $ex(t) = Xm(t) - Xs(t)$

e(t) It is triggered by the fact that the presence of an information signal causes the xm(t) does not to have the same reply at the receiver. Therefore, ex (t) causes the synchronization mechanism to be disrupted. To ignore the effect of the signal information sent to the receiver on the synchronization process, the information signal is the feedback to the chaotic transmitter [19] as shown in Figure 9.

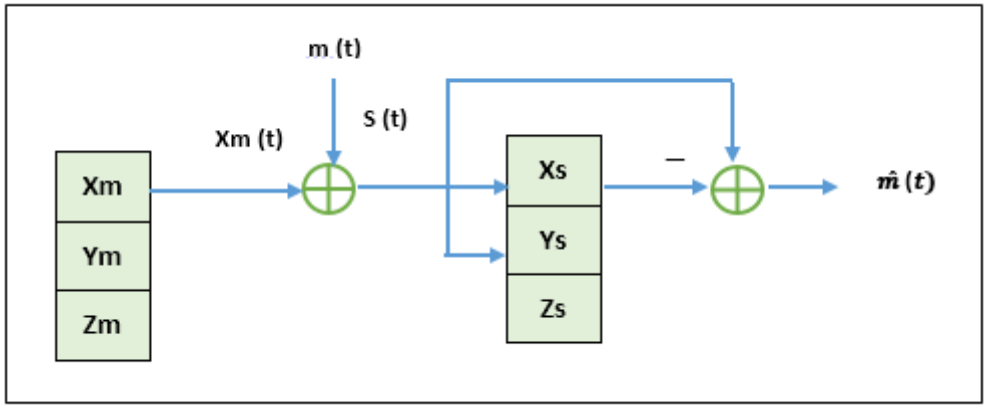


Figure.8 Chaotic masking and recovering information based on the Chua system

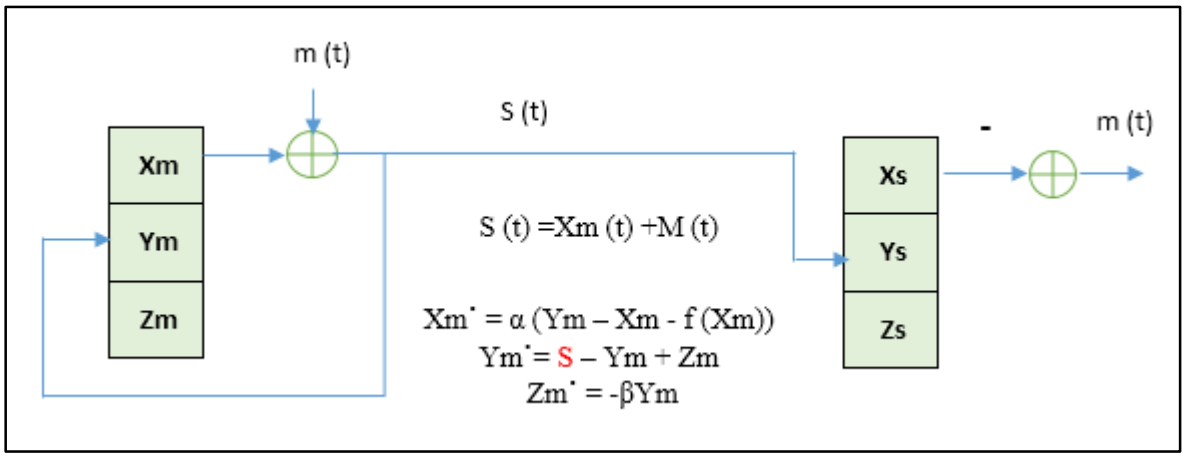


Figure.9 Chaotic masking with feedback using Chua system

5. XSG DESIGN OF IMAGE ENCRYPTION AND DECRYPTION

The XSG block diagram for encrypting and decrypting the image is shown in Figure 10. XSG input and output gateway functions are used to convert between the blocks of Simulink/Matlab and XSG. The source color image is divided into three channels (red, green, and, blue) of images. The data type is the Unint8 format for this image. In the first step of encryption, a pre-processing block is used to transform the original images I (Lr * Lc) dimension (where Lr is row numbers and Lc is column numbers) into serial samples. Pre-processing block used to transform matrix I to 8-bit serial samples (Unit8). Figure 11 displays the Pre-processing blocks. The gateway is used for transforming the sample serial format into the unsigned fixed-point format with WL=8, FL=0 and, sample period 0.01. Then masked with the Xm(t) signal produced by the Chua chaotic system to produce the ciphered image. In the decryption process, the Xs(t) response signal is subtracted from the masked signal S(t). The pre-processing and post-processing block are used to transform your serial sample into the original size (Lr×Lc) to recover the original image of the same dimension. Figure 12 displays the Post-processing blocks. For all chaotic structures, like master and slave, a fixed-point representation of WL=32 bits and FL=16 bits is used. The initial values for the master system is (α= 9 β= 100/7, m0= -3, m1= -0.3, b1=0.1, x0= -0.2, y0= 0, z0= 0.2) and slave system is (α= 9 β= 100/7, m0= -3, m1= -0.3, b1=0.1, x0= 0.7, y0= 0.1, z0= 0.6). After 700ns (simulation time), the original image is recovered and the results are shown as shown in Figure 13.

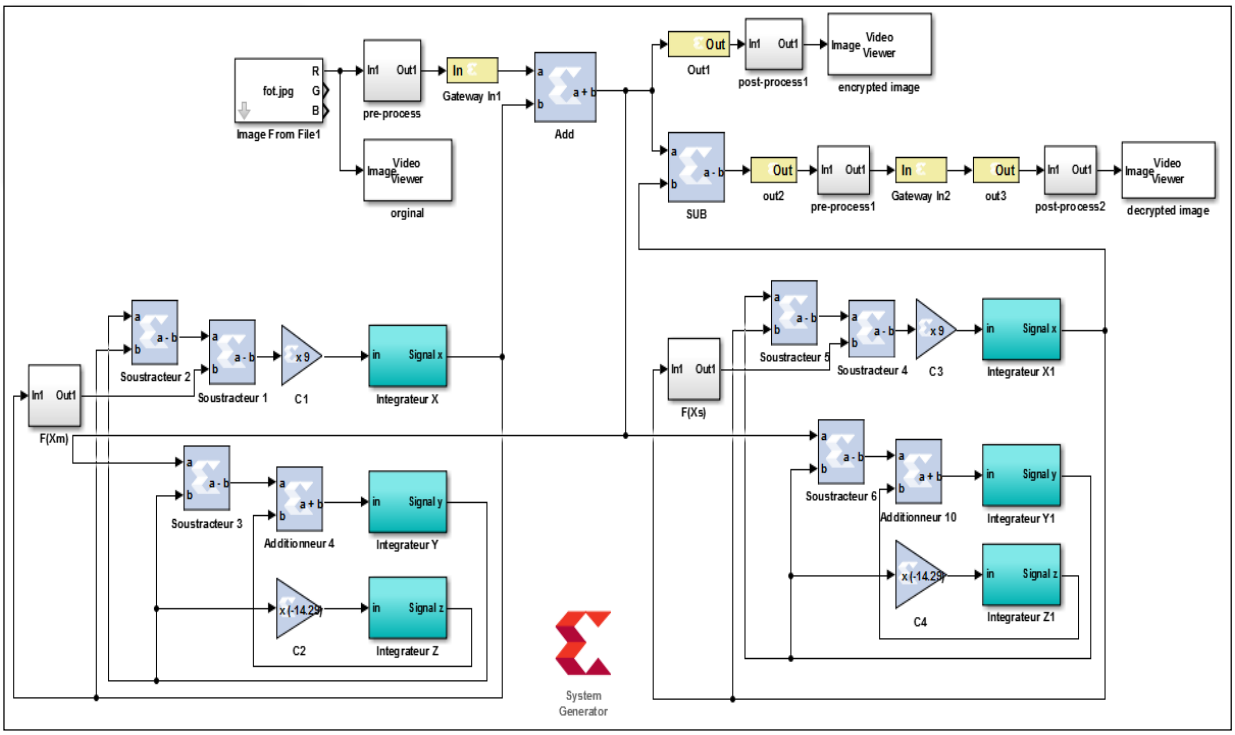


Figure.10 XSG of mage encryption and decryption

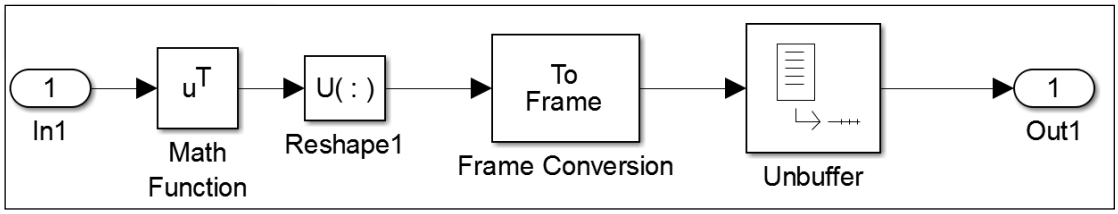


Figure.11 Pre-processing blocks

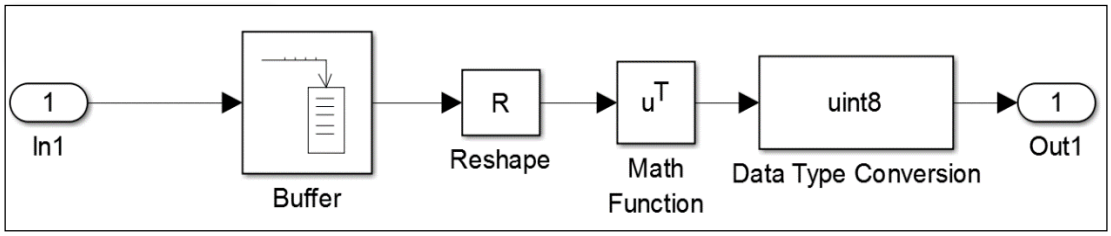
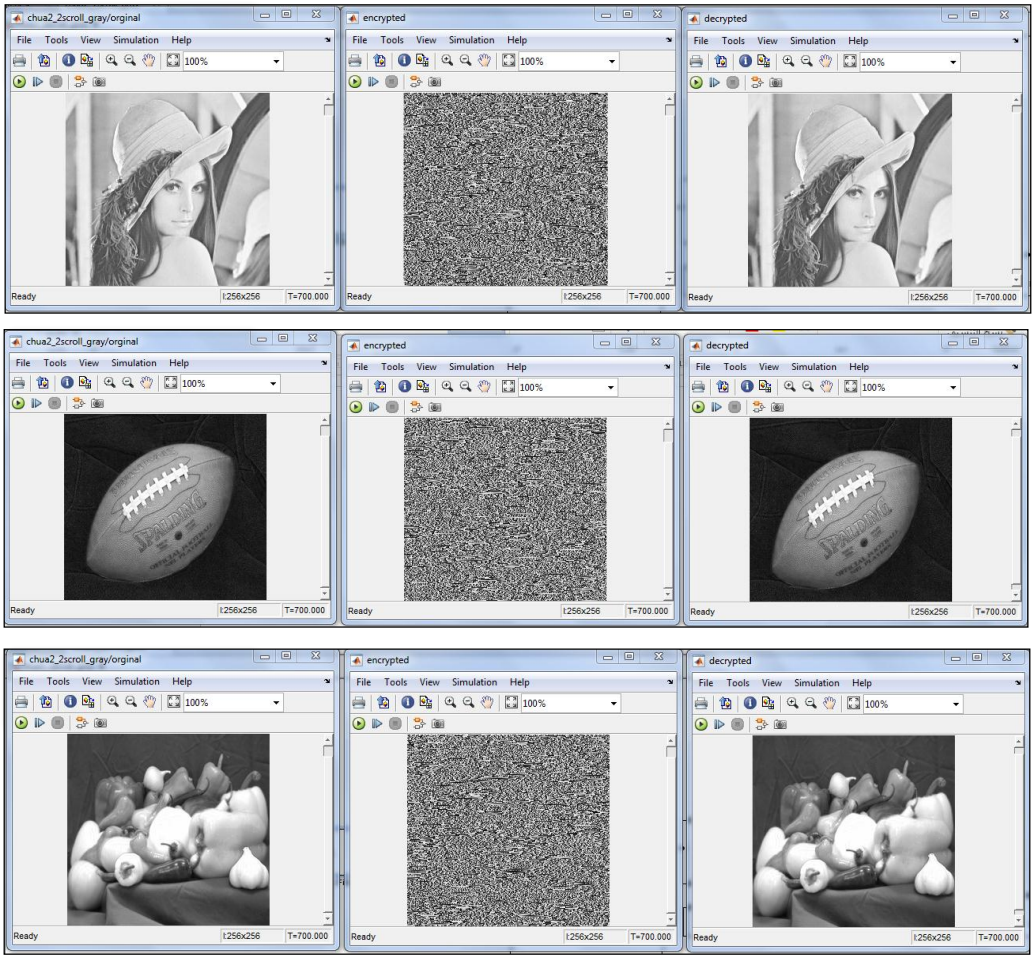


Figure.12 Post-processing blocks



(a) (b) (c)

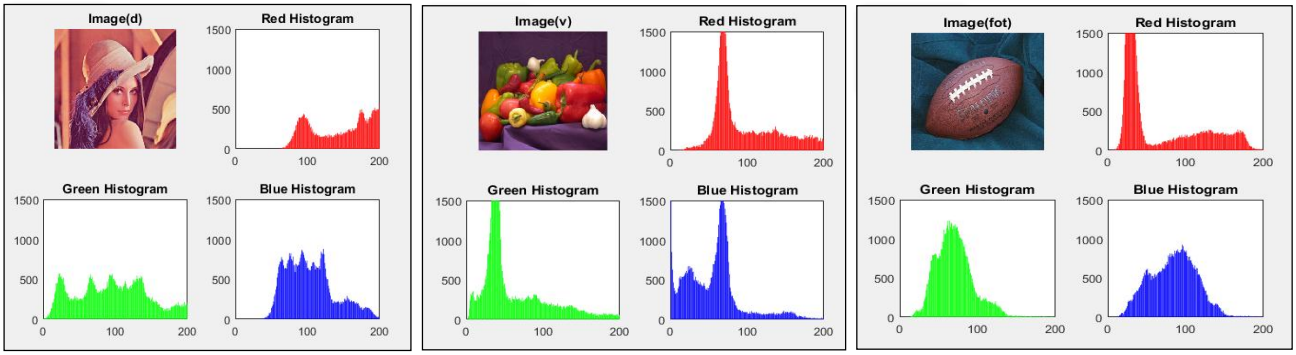
Figure.13 (a) original images (b) encrypted images (c) decrypted images

6. STATISTICAL ANALYSIS

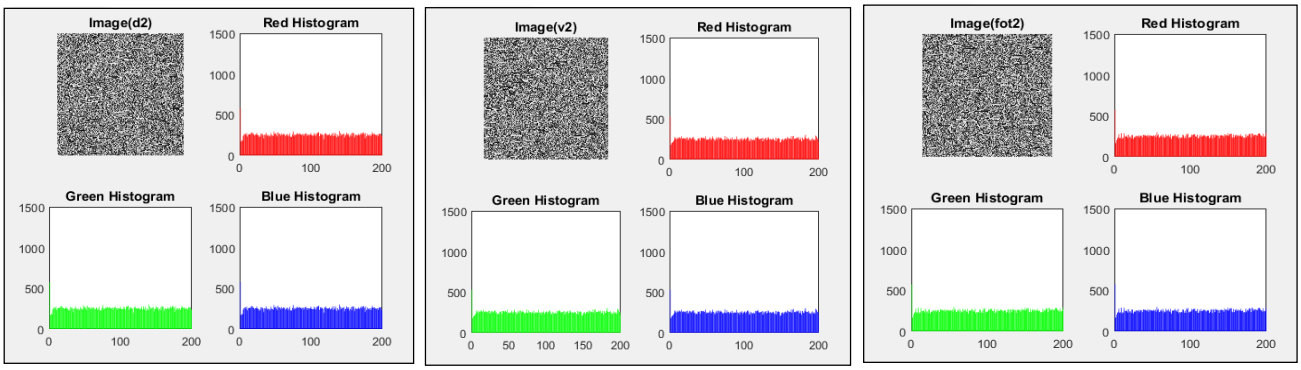
There are several analyzes of the design's efficiency and security, including histogram, CCA, the entropy of information, keyspace and, an attack on differential analysis. A different color image is used for analysis. Experiments are performed and data is analyzed using Matlab environments.

A. Analysis of histogram

The image histogram shows the distribution of pixels by graphing the number of pixels on each color intensity level [20]. A comparison of the distribution histogram before and after the encryption algorithm is shown in Figure14. It appears that the compression and encrypted image histograms (for R, G, B-channels) are greatly different from the original image histograms (for R, G, B-channels) and do not include any clues that could be used for any statistical analysis of the encrypted image. So; the algorithm can effectively resist statistical attacks. The original and cipher images have completely different pixel distribution at each level of intensity [21].



(a)



(b)

Figure.14 (a) Histogram of three-channel original images (b) Histogram of three channel-ciphered images

B. 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 out if all its attributes are hidden and the encrypted image is entirely unrelated and random. If the coefficient of correlation is =1, the two images are the same. Therefore, the encryption failed in these cases. When the value =-1, the encrypted image is opposite to the plain image The equations. (7-9) is used to measure the correlation coefficient of any two-pixel color values at the same position in the original and cipher images [22].

$$CorCoef = \frac{Covar(x,y)}{\sqrt{Vari(x)} \times \sqrt{Vari(y)}} \quad (7)$$

$$Vari(x) = \frac{1}{N}\sum_{i=1}^{N}[xi - E(x))^2] \quad (8)$$

$$Covar(x,y) = \frac{1}{N}\sum_{i=1}^{N}[xi - E(x)) \times (yi - E(y))] \quad (9)$$

Where CorCef is the x-y correlation coefficient, Vari(x) is the original image variance x, Covar (x, y) is the covariance between x and y, E(x) is the predicted value of the operator, and N is the total number of pixels in the image matrix[23]. Table 3 displays experimental correlation pixels for pictures of Lena, football, and peppers with sizes 256*256.

Table 3: correlation coefficient calculation of encrypted image with different channels

Image name	channel		
	Red	**Green**	**Blue**
Lena	0.0054	$5.2733*10^{-4}$	-0.0020
peppers	$-7.6527*10^{-4}$	-0.0020	0.0050
football	0.0013	0.0015	$-7.3397*10^{-4}$

C. Entropy Analysis

The content of an information signal is called entropy. It determines the redundancies of the characteristic randomness [24]. The entropy of the Signal Information expressed as:

$$Entrp(s) = \sum_{n=0}^{2^N-1} P(si) \times \log_2 \left(\frac{1}{P(si)}\right) bits \quad (10)$$

Where (si) the probability that a pixel occurs in an image, N is the length of the binary number of a pixel (usually N = 8 for a gray image). An important property of the cryptosystem is it is sufficient to resist entropy attacks; the ideal entropy value of the encrypted images is 8 bits/pixel [25]. Tables 4 show the Information Entropy results of Lena, football, and peppers Image with the size of 256 × 256 for different channels.

Table 4: entropy calculation of ciphered images

Image name	channel		
	Red	**Green**	**Blue**
Lena	7.9893	7.9901	7.9906
peppers	7.9906	7.9903	7.9908
football	7.9896	7.9905	7.9898

7. DIFFERENTIAL ATTACK ANALYSIS

It is the analysis of how variations in the input information will affect the resulting output variation to obtain the secret key. The sensitivity of a cipher picture should be high before the original image or secret key is slightly changed. As in Equations 11 and 12, UACI and NPCR measures are used to determine the effect on the cipher image of the change of 1 bit/pixel in the original image [26].

$$UACI(C1, C2) = \frac{1}{W \times H}\left[\sum_{i,j} \frac{|c1(i,j) - c2(i,j)|}{255}\right] \times 100\% \quad (11)$$

Where
W and, H are the width and, height of the image, respectively.

And
C1 and, C2 are encrypted representations of a plain image and, a modified image.

$$NPCR(1, C2) = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\% \quad (12)$$

Where

$$D(i,j) = \begin{cases} 0, & if\ c1(i,j) = c2(i,j) \\ 1, & otherwise \end{cases} \quad (13)$$

Table 5: NPCR test calculation for different channels

Image name	channel		
	Red	Green	Blue
Lena	99.596	99.603	99.614
peppers	99.608	99.600	99.585
football	99.621	99.612	99.633

Table 6: UACI test calculation for different channels

Image name	channel		
	Red	Green	Blue
Lena	30.28	30.42	30.44
peppers	34.10	33.98	33.90
football	32.31	32.28	32.45

8. HARDWARE CO-SIMULATION OF IMAGE ENCRYPTION AND DECRYPTION

The proposed model is formulated using the FPGA board Artix7 xc7a100t-1csg324. The summary of system utilization for the proposed Chua chaotic masking is shown in Table 7. The image encryption and, decryption process are co-simulated with FPGA hardware as in Fig.14. When JTAG is connected, serial image signal data are transmitted via a USB JTAG port to FPGA. Then serial samples were returned to PC using the Simulink / Matlab Viewer to test the image, as shown. Figure 15. In Figure 16, the images at the top represent the results of the proposed system using the system generator, and, at the bottom represent the results of FPGA hardware co-simulation. The encrypted image has proved to be the same for system generators and, co-simulation, demonstrating that the actual time for the proposed encrypted image works correctly and, is compatible with the configuration expected.

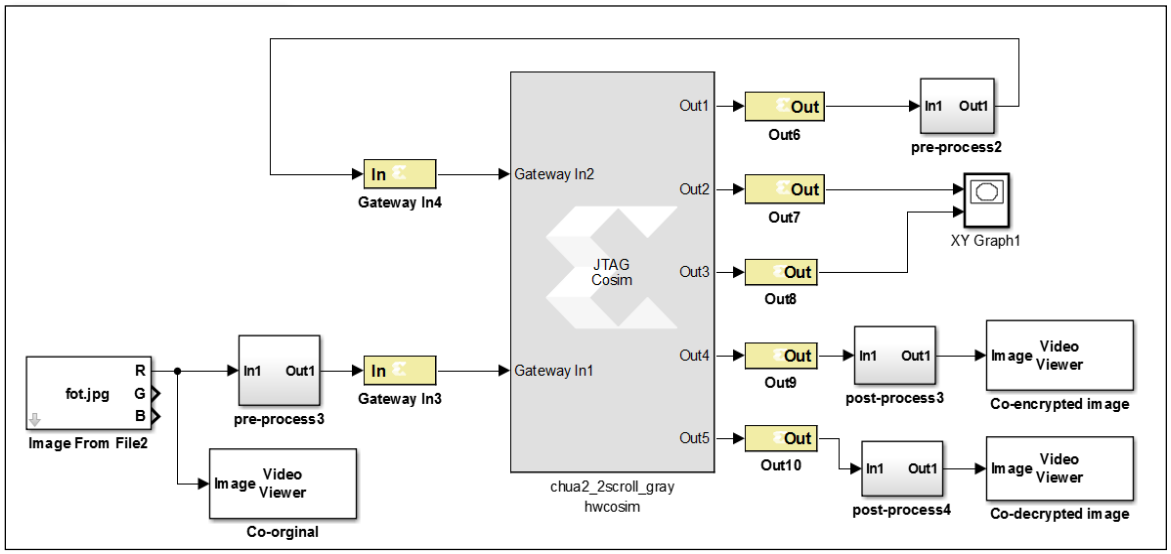


Fig.15: hardware Co-Simulation block diagram

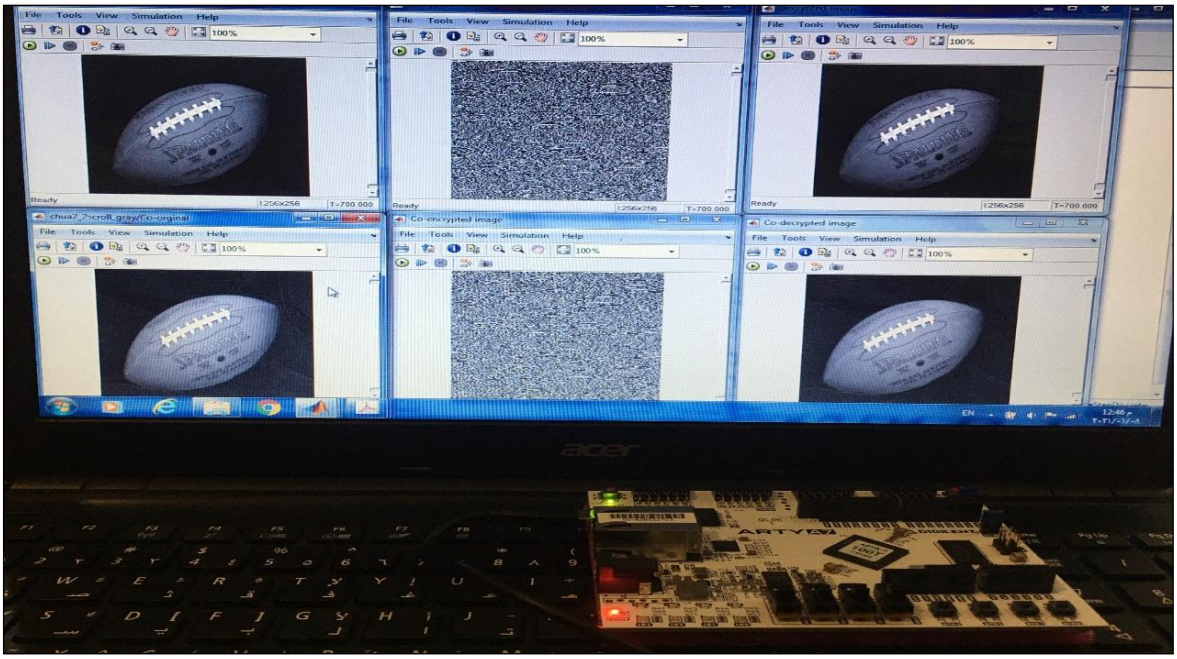


Fig.16: results with Xilinx Artix7 xc7a100t-1csg324 kit

Table 7: device utilization summary for image encryption and decryption

Resource type	Available	Utilization
LUT	634000	1563
Slice Registers(FF)	126800	192
Bonded IOB(IO)	210	89
BUFGCTRL(BUFG)	32	1
DSP	240	36
Minimum period Ts (ns)	41	
Worst negative slack(WNS)	0.444	
Maximum Frequency(MHz)	24.66	
Power(W)	0.128	

9. CONCLUSION

This research attempted to synchronize the chaotic attractor of Chua and, its use of insecure communication. The approach of synchronization uses the identical cascading method for Pecora-Carroll. Such a chaotic synchronization phenomenon can serve as a basis for secure communication. Secure communication can be accomplished by adding a message signal to the chaotic signal and, receiving it to the receiver without any distortion or loss. Communication between the transmitter and, the receiver is therefore secure only when they are synchronized. Chaotic masking with feedback algorithm used to implement a color image encryption and, decryption. The design has been implemented using XSG and, resource utilization has been measured. Security analysis is calculated for different images, including histogram, correlation coefficient and, entropy. The results of the synthesis of the proposed system have a maximum frequency of approximately 24.66 MHz. In conclusion, the real time evaluation of the system proposed was co-simulated using the FPGA Xilinx Artix7 xc7a100t-1csg324 kit.

REFERENCES

[1] F. S. Hasan and M. A. Saffo, "FPGA Hardware Co-Simulation of Image Encryption Using Stream Cipher Based on Chaotic Maps," *Sens. Imaging*, vol. 21, no. 1, pp. 1–22, 2020.

[2] X. Li and Q. Ou, "Dynamical properties and simulation of a new Lorenz-like chaotic system," *Nonlinear Dyn.*, vol. 65, no. 3, pp. 255–270, 2011.

[3] C. R. Comfort, "Simple Analog Signal Chaotic Masking and Recovery," 2012.

[4] R. Ekhande and S. Deshmukh, "Chaotic signal for signal masking in digital communications," *Int. Organ. Sci. Res. J. Eng.*, vol. 4, no. 2, pp. 29–33, 2014.

[5] S. Čelikovský and V. Lynnyk, "Message embedded chaotic masking synchronization scheme based on the generalized Lorenz system and its security analysis," *Int. J. Bifurc. Chaos*, vol. 26, no. 08, p. 1650140, 2016.

[6] S. S. Hreshee, H. N. Abdullah, and A. K. Jawad, "A High Security Communication System Based on Chaotic Scrambling and Chaotic Masking," 2018.

[7] L. M. Pecora and T. L. Carroll, "Synchronization in chaotic systems," *Phys. Rev. Lett.*, vol. 64, no. 8, p. 821, 1990.

[8] R. Karthikeyan, S. A. Kumar, R. Babu, and D. Mathew, "FPGA implementation of novel synchronization methodology for a new chaotic system," *Editor. Board*, p. 48, 2015.

[9] Y. Uyaroğlu and U. E. Kocamaz, "SYNCHRONIZATION BETWEEN CHUA AND MODIFIED CHUA OSCILLATORS WITH PASSIVE CONTROL."

[10] L. Guo-Hui, "An active control synchronization for two modified Chua circuits," *Chinese Phys.*, vol. 14, no. 3, p. 472, 2005.

[11] H. N. Agiza and A. E. Matouk, "Adaptive synchronization of Chua's circuits with fully unknown parameters," *Chaos, Solitons & Fractals*, vol. 28, no. 1, pp. 219–227, 2006.

[12] M. Feki, "Sliding mode control and synchronization of chaotic systems with parametric uncertainties," *Chaos, Solitons & Fractals*, vol. 41, no. 3, pp. 1390–1400, 2009.

[13] T.-C. Lin, M.-C. Chen, and M. Roopaei, "Synchronization of uncertain chaotic systems based on adaptive type-2 fuzzy sliding mode control," *Eng. Appl. Artif. Intell.*, vol. 24, no. 1, pp. 39–49, 2011.

[14] J. Sun and Y. Zhang, "Impulsive control and synchronization of Chua's oscillators," *Math. Comput. Simul.*, vol. 66, no. 6, pp. 499–508, 2004.

[15] S. Vaidyanathan and S. Rasappan, "Global chaos synchronization of n-scroll Chua circuit and Lur'e system using backstepping control design with recursive feedback," *Arab. J. Sci. Eng.*, vol. 39, no. 4, pp. 3351–3364, 2014.

[16] ARYALEKSHMI.B.N, "FPGA Implementation of Lorenz's Chaotic Generator," vol. VIII, no. III, 2019.

[17] J. Schmitz and L. Zhang, "Rössler-based chaotic communication system implemented on FPGA," in *2017 IEEE 30th Canadian Conference on Electrical and Computer Engineering (CCECE)*, 2017, pp. 1–4.

[18] B. Lakshmi, E. Kirubakaran, and T. N. Prabakar, "Design and Implementation of FPGA Based Dual Key Encryption," *Int. J. Comput. Appl.*, vol. 3, no. 3, 2010.

[19] H. N. Abdullah, S. S. Hreshee, and A. K. Jawad, "Noise Reduction of Chaotic Masking System using Repetition Method."

[20] H. R. Hatem, "Color Image Compression and Encryption Based on Compressive Sensing," *J. Eng. Sustain. Dev.*, vol. 22, no. 1, pp. 149–161, 2018.

[21] M. Alsaedi, "Colored image encryption and decryption using chaotic lorenz system and DCT2," *arXiv Prepr. arXiv1701.02896*, 2017.

[22] M. Ahmad, M. N. Doja, and M. M. S. Beg, "Security analysis and enhancements of an image cryptosystem based on hyperchaotic system," *J. King Saud Univ. Inf. Sci.*, 2018.

[23] 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," *Secur. Commun. Networks*, vol. 2018, 2018.

[24] E. Rodríguez-Orozco *et al.*, "FPGA-based chaotic cryptosystem by using voice recognition as access key," *Electronics*, vol. 7, no. 12, p. 414, 2018.

[25] B. Baruah and M. Saikia, "An FPGA Implementation of Chaos based Image Encryption and its Performance Analysis," *IJCSN-International J. Comput. Sci. Netw.*, vol. 5, no. 5, 2016.

[26] I. A. Taqi and S. M. Hameed, "A new Color image Encryption based on multi Chaotic Maps," *Iraqi J. Sci.*, vol. 59, no. 4B, pp. 2117–2127, 2018.