International Journal of Electrical and Computer Engineering (IJECE)
Vol. 12, No. 3, June 2022, pp. 2414~2424
ISSN: 2088-8708, DOI: 10.11591/ijece.v12i3.pp2414-2424

Field-programmable gate array design of image encryption and decryption using Chua's chaotic masking

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

Article Info

Article history:

Received Feb 1, 2021
Revised Dec 24, 2021
Accepted Jan 5, 2022

Keywords:

Chua's circuit
Hardware co-simulation
Image encryption and decryption
Masking
Synchronization
XSG

ABSTRACT

This article presents a simple and efficient masking technique based on Chua chaotic system synchronization. It includes feeding the masked signal back to the master system and using it to drive the slave system for synchronization purposes. The proposed system is implemented in a field programmable gate array (FPGA) device using the Xilinx system generator tool. To achieve synchronization, the Pecora-Carroll identical cascading synchronization approach was used. The transmitted signal should be mixed or masked with a chaotic carrier and can be processed by the receiver without any distortion or loss. For different images, the security analysis is performed using the histogram, correlation coefficient, and entropy. In addition, FPGA hardware co-simulation based Xilinx Artix7 xc7a100t-1csg324 was used to check the reality of the encryption and decryption of the images.

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 application of chaotic cryptographic to the security of images has been proposed as a way to resolve a variety of security issues, as chaotic systems have a number of advantages over random systems, including their sensitivity to initial conditions and parameter settings, and their aperiodic signal nature makes them an excellent choice for encryption systems [2].

This article contributed to the use of chaotic systems in the process of information security, rather than conventional methods of encryption, and the approach used was simpler, more effective, and produced good results as compared to other complex methods of image hiding such as. In the paper [3], a chaotic block image permutation and XOR operation are performed to achieve image encryption. The chaotic masking scheme based on embedded message synchronization is introduced in [4]. An effective and high security communication system based on two levels of encryption based on chaotic systems was proposed in [5]. Merah *et al.* [6] present a novel stream cipher based on chaotic synchronization. Suggest an image encryption model that combines chaotic maps such as logistic, sine, and tent chaotic systems [7].

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. From Pecora and Carroll's work [8], 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, and physical systems [9]. Much attention was given to the control and synchronization of Chua systems by researchers. Chua system have recently been synchronized with active control [10], adaptive control [11], sliding control [12], fuzzy control [13], and backstepping control methods [14].

The digital implementation of this system on an field programmable gate array (FPGA) system is ideal because it eliminates part drift and has high power and throughput capability [15]. FPGAs are the primary tool for implementing high-performance systems, especially in image processing applications and digital signal processing systems. Additionally, FPGAs can perform signal processing at a high rate of efficiency [16]. The Xilinx system generator (XSG) extends the capabilities of the FPGA and offers important tools for developing image encryption models.

This paper is arranged as follows. In section 2, a Chua circuit design using XSG was illustrated; the concept of the Pecora-Carroll (PC) cascaded synchronization method and its implementation using XSG is given in section 3. In section 4, we explain the chaotic masking with feedback and the purpose of this procedure. In section 5, the FPGA platform of image encryption using chaotic masking with feedback is performed. Section 6 shows the randomness measures of the system proposed. The efficiency and security review of the proposed model is presented in section 7. Next, section 8, which co-simulates image encryption by FPGA hardware. Finally, section 9 presents the conclusion of 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. The relevance of the Chua circuit has recently made possible the birth of a big family of multi-scroll oscillators and techniques to control the chaos [17]. Chua's circuit has found many applications in physics, communication, and control, mechanics, as well as chemistry, economics, and medicine [18]. Chua's circuit has also been used as a chaotic noise generator. Because of this property, it has found many applications in cryptography and steganography [19]. The as nonlinear (1), (2) describe this chaotic system:

$$\mathrm{X}^{\cdot} = \mathrm{A}\,(\mathrm{Y} - \mathrm{X} - \mathrm{F}(\mathrm{X})$$

$$\mathrm{y}^{\cdot} = \mathrm{x} - \mathrm{y} + \mathrm{z}$$

$$\mathrm{Z}^{\cdot} = -\mathrm{BY} \tag{1}$$

where $f(x)$

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

where α and β are the parameters of the system and $f(x)$ piecewise linear (PWL) function, m_0 and m_1 are the negative slopes, and b1 is the breakpoint. Figure 1 shows XY phase portrait and 3D plot of the Chua attractor using fixed-point data format (Fix 32_16). The initial values x_0=-0.3, y_0= 0.1, and z_0= 0.2, and system parameters are α =9, β = 100/7, m_0=-3 and m_1 =-0.3, b1=0.1, with step size dt = 0.01**.**

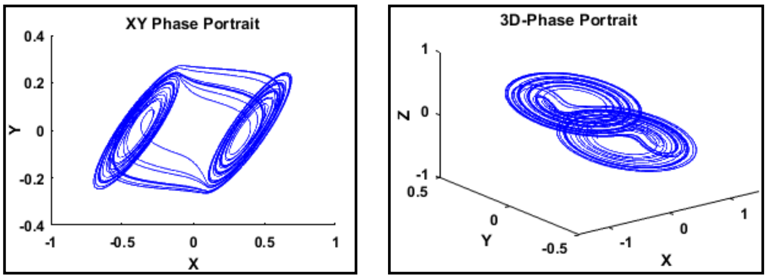


Figure 1. XY and XYZ phase portrait plot

3. PC CASCADED SYNCHRONIZATION OF CHUA'S CHAOTIC SYSTEM

This method describes the two systems with 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. The Chua cascaded synchronization system is implemented using the Xilinx system generator model shown in Figure 2.

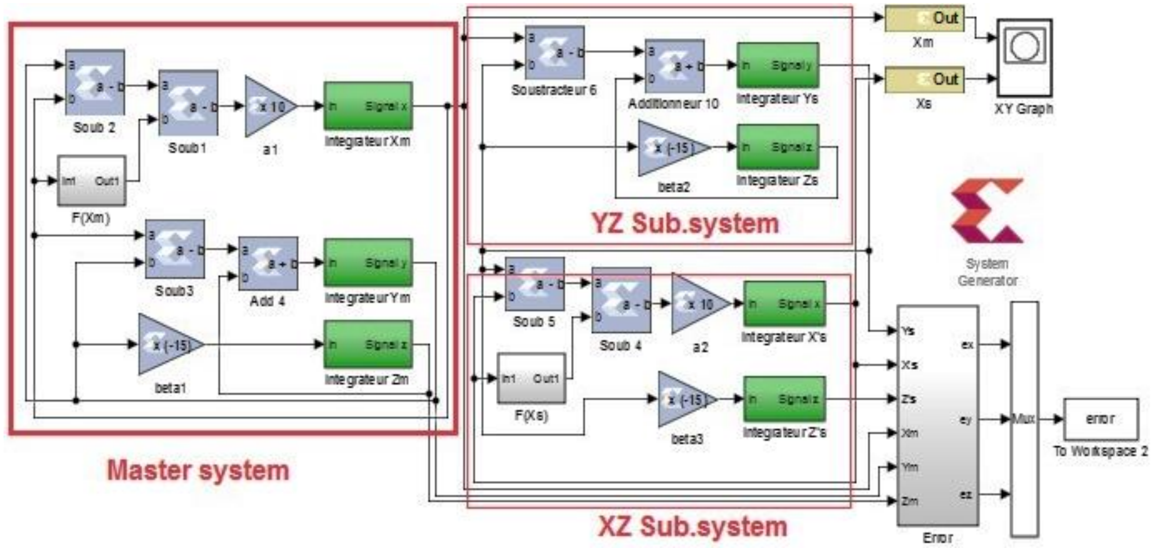


Figure 2. PC cascaded synchronization of chua system using XSG

The master as (3)

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

YZ response subsystem (4)

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

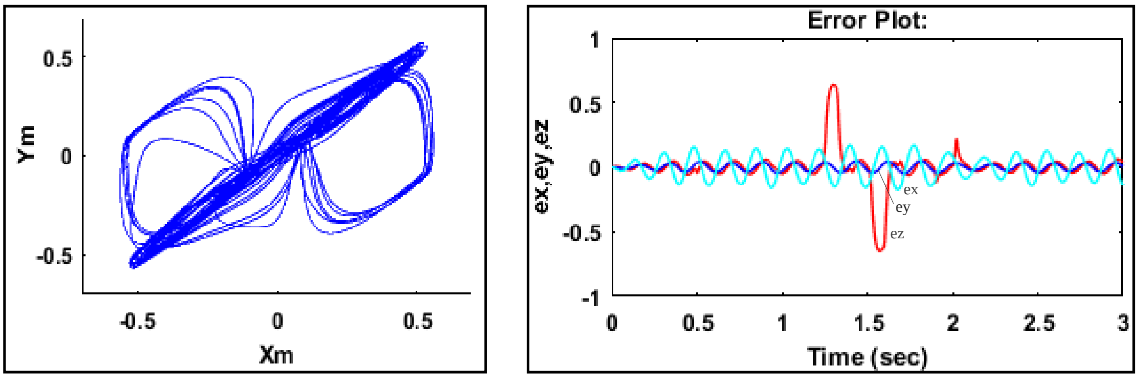
XZ response subsystem (5)

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

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

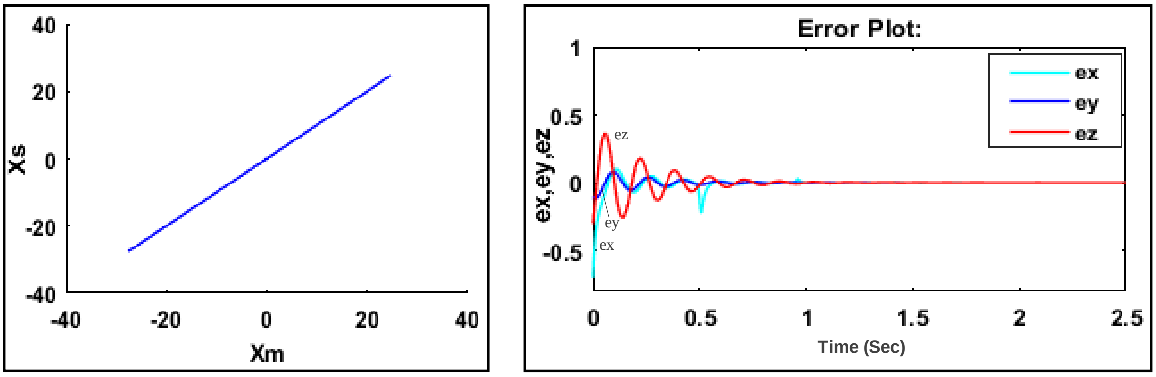
$$\begin{aligned} ex &= x's - xm \\ ey &= ys - ym \\ ez &= z's - zm \end{aligned} \tag{6}$$

The phase portrait and error signal in case of unsynchronized are shown in Figures 3(a) and 3(b) respectively, here, the value of α and β of the drive system and the response systems are different. Figures 4(a) and 4(b) show the phase portrait and error signal in case of 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 are defined in Table 1. Simulation results show that the two subsystems are well synchronized. The design was implemented on an Artix7 xc7a100t-1csg324 FPGA device and the resource utilization was estimated as shown in Table 2.



(a) (b)

Figure 3. PC synchronization in the case of mismatched parameters (a) phase portrait and (b) error signal in case of unsynchronized



(a) (b)

Figure 4. PC synchronization in the case of matched parameters (a) phase portrait describes the xm versus xs and (b) error signal in case of synchronization

Table 1. Cascaded synchronization system parameters

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

Table 2. FPGA utilization summary of PC cascaded synchronization

Resource type	Available	Utilization
LUT	63400	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

There are different techniques for uses the chaotic signal in secure communications: chaotic parameter modulation, chaotic shift keying, on-off key, and chaotic masking. The chaotic masking can be viewed as one of the earliest and easiest techniques in chaotic secure communications, which is based on the PC synchronization concept and mostly used for analog signal transmission. Additionally, it is quickly implemented in electronic circuits, which is why it is used in this proposed scheme [20]. As shown in Figure 5 the general block diagram of chaotic masking, the information signal $m(t)$ is added to the wideband chaotic signal $Xm(t)$, followed by transmitting the combined (masked) signal $s(t)$.

$$s(t) = Xm(t) + m(t) \tag{7}$$

To successfully remove the mask, both master and slave chaotic signals need to be synchronized, PC synchronization is one of the most powerful synchronization schemes to do this [5]. The image $m(t)$ is precisely retrieved on the receiver side by subtracting the regenerated signal *Xs(t)* from the received signal $s(t)$ with the assumption that the system is free of noise. The recovered signal (image) is.

$$\hat{m}(t) = s(t) - Xs\,(t) = [Xm(t) + m(t)] - Xs(t) = m(t) + ex\,(t) \tag{8}$$

where

$$e_x(t) = Xm(t) - Xs(t) \tag{9}$$

$e_x(t)$ 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, $e_x(t)$ 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 [21].

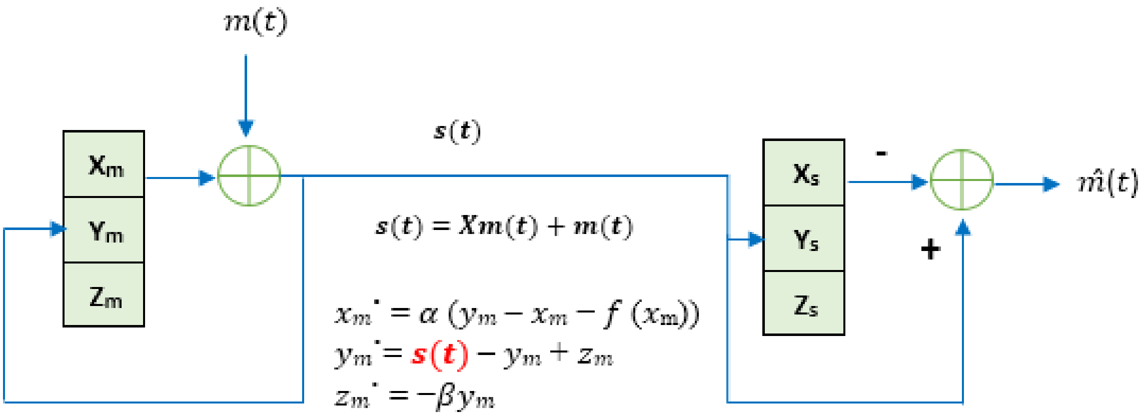

$m(t)$
$s(t)$
Xm
Ym
Zm
Xs
Ys
Zs
-
+
$\hat{m}(t)$
$s(t) = Xm(t) + m(t)$
$x_m^{\cdot} = \alpha\,(y_m - x_m - f\,(x_m))$
$y_m^{\cdot} = s(t) - y_m + z_m$
$z_m^{\cdot} = -\beta y_m$

Figure 5. Chaotic masking with feedback and recovering information based on the Chua system

5. XSG DESIGN OF IMAGE ENCRYPTION AND DECRYPTION

The XSG block diagram for encrypting and decrypting the image is shown in Figure 6. XSG input and output gateway functions are used to convert between the blocks of MATLAB/Simulink and XSG. The original color image is divided into different red, green, and blue images. This image's data type is unint8. 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. The Pre-processing block is used to transform matrix I to 8-bit serial samples (Unit8). Figure 7 displays the pre-processing blocks. The gateway-in transforms the serial sample format to an unsigned fixed point format with WL=8 and FL=0 with sample period 0.001. Then masked with the $Xm(t)$ signal produced by the Chua chaotic system to obtain the encrypted image. In the decryption process, the $Xs(t)$ response signal is subtracted from the masked signal $S(t)$. The post-processing blocks are used to transform the serial.sample into the original size (Lr×Lc) to recover the original image of the same dimension. Figure 8 displays the post-processing blocks. For all chaotic structures, like master and slave, it is implemented using a fixed-point representation with WL=32 bits and FL=16 bits. The initial values for the master system are (α= 9, β=100/7, m0=-3, m1=-0.3, b1=0.1, x0=-0.2, y0=0, z0=0.2) and for the slave system are (α= 9, β=100/7, m0=-3, m1=-0.3, b1=0.1, x0= 0.7, y0= 0.1, z0=0.6). After 70 ns (simulation time), the original image, encrypted image, and recovered image are shown in Figures 9(a) to 9(c) respectively.

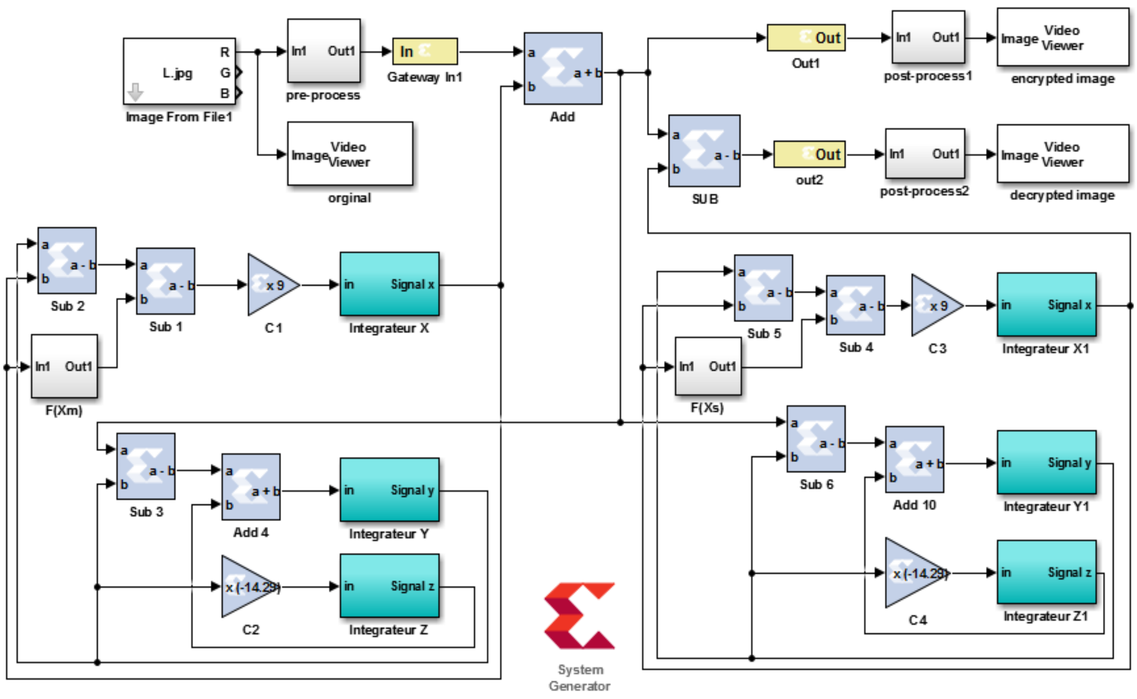


Figure 6. XSG of image encryption and decryption

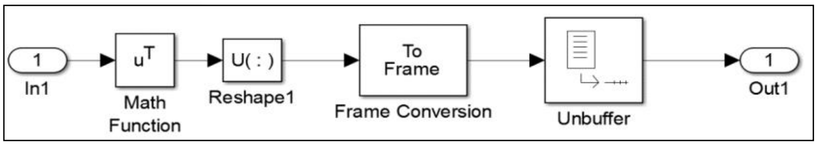


Figure 7. Pre-processing blocks

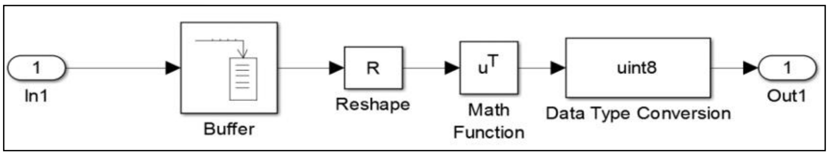


Figure 8. Post-processing blocks

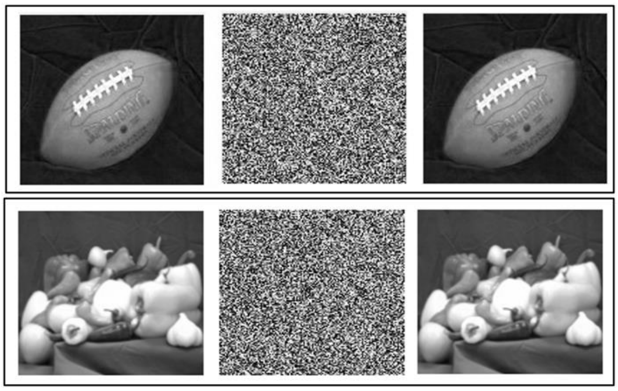

(a) (b) (c)

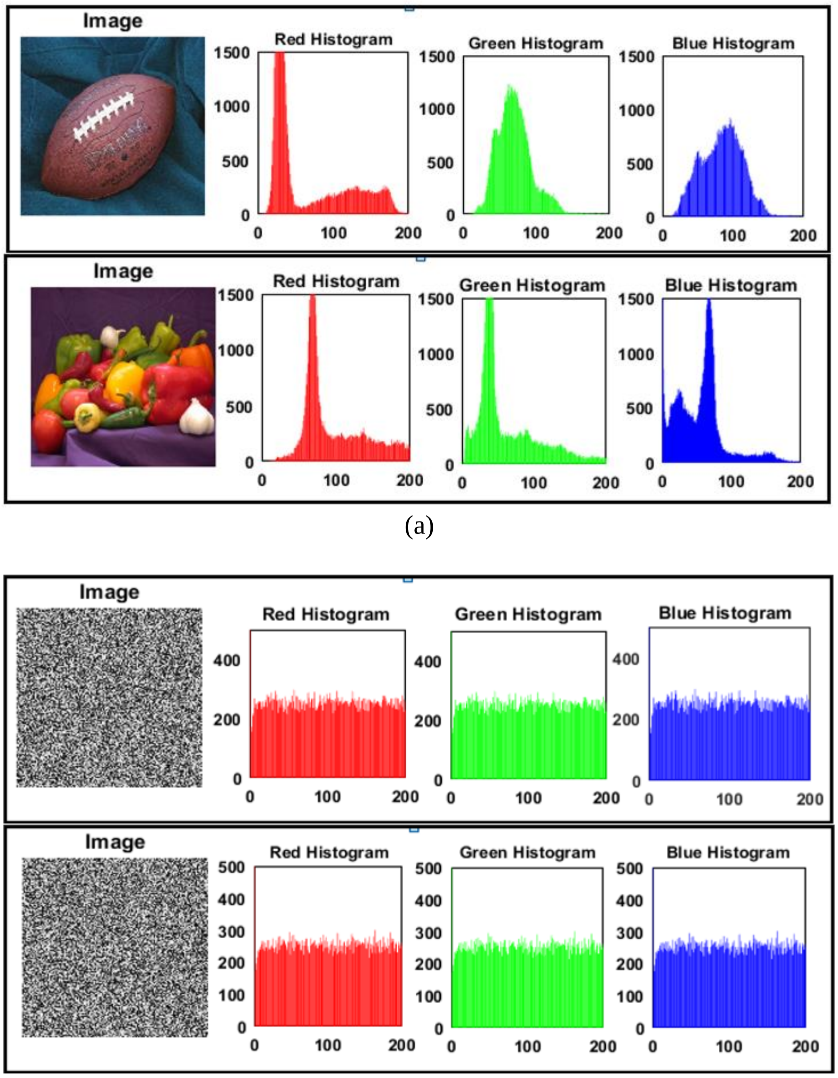
Figure 9. Results (a) original images, (b) encrypted images, and (c) decrypted images

6. STATISTICAL ANALYSIS

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

6.1. Analysis of histogram

The image histogram shows the distribution of pixels by plotting the number of pixels at each level of color intensity [22]. In Figures 10(a) and 10(b), a comparison of the distribution histograms of original images and ciphered images was shown. 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 [23].



(a)

(b)

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

6.2. 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 =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 (9) is used to measure the correlation coefficient of any two-pixel color values at the same position in the original and cipher images [24].

$$Corr(x, y) = \frac{E[(x-\mu_x)(y-\mu_y)]}{\sigma_x \sigma_y} \tag{9}$$

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 [25]. Table 3 displays experimental correlation pixels for pictures of football, and peppers with sizes 256*256.

Table 3. Correlation coefficient calculation of encrypted image with different channels

Image name	Channel		
	Red	Green	Blue
peppers	-7.6527*10^{-4}	-0.0020	0.0050
football	0.0013	0.0015	-7.3397*10^{-4}

6.3. Entropy analysis

The content of an information signal is called entropy. It determines the redundancies of the characteristic randomness [26]. The entropy of the signal information expressed as:

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

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 [27]. Table 4 show the Information Entropy results of two images with the size of 256×256 for different channels.

Table 4. Entropy calculation of ciphered images

Image name	channel		
	Red	Green	Blue
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 (11) and (12), 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 [28], [29].

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

Where W and H are the width and height of the image, respectively, C1 and C2 are encrypted representations of a plain image and a modified image.

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

Where

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

Table 5. NPCR and UACI test calculation for different channels

Image name	channel	NPCR	UACI
peppers	Red	99.608	34.10
	Green	99.600	33.98
	Blue	99.585	33.90
football	Red	99.621	32.31
	Green	99.612	32.28
	Blue	99.633	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 resource utilization for the encryption and decryption method using chaotic masking with feedback is shown in Table 6. The image encryption and decryption process are co-simulated with FPGA hardware. When JTAG is connected, serial image signal data is transmitted via a USB JTAG port to FPGA. Then serial samples were returned to the PC using the MATLAB/Simulink viewer to test the image, as shown in Figure 11. 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.

Table 6. FPGA utilization summary for image encryption and decryption

Resource type	Available	Utilization
LUT	63400	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	

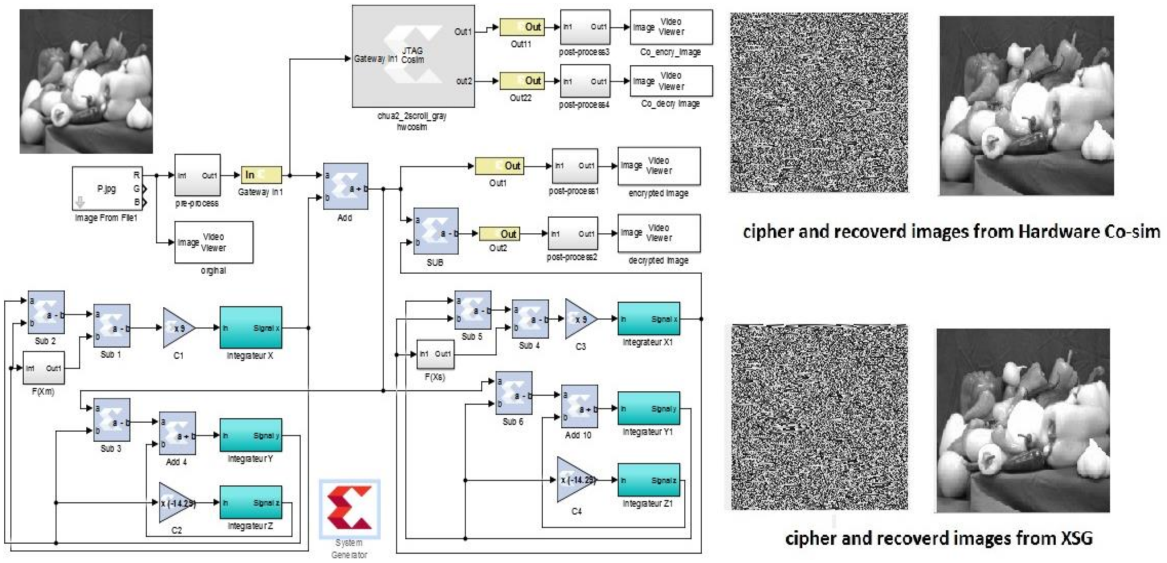


Figure 11. Hardware co-simulation results

9. CONCLUSION

In this research, Chua's chaotic attractor was synchronized based on the PC cascading method. such a chaotic synchronization phenomenon can serve as a basis for secure communication. Applying protection to transmitted images is critical, as the communication channel is open and susceptible to attack. To protect this channel, this article implements an image encryption algorithm based on chaotic masking with feedback. This method, which is based on chaotic signals, was considered the simplest in terms of secure communication because it produced an optimal analysis result that can resist various attacks and provides an extremely high level of protection that can be used to transmit images over insecure networks. The design has been implemented in an efficient way by using the XSG tool. The proposed method's synthesis results indicate that its maximum frequency is 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 and resource utilization has been measured.

REFERENCES

[1] 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, Jul. 2020, doi: 10.1007/s11220-020-00301-7.

[2] M. K. Khan, "Editorial: Chaotic cryptography and its applications in telecommunication systems," *Telecommunication Systems*, vol. 52, no. 2, pp. 513–514, May 2013, doi: 10.1007/s11235-011-9456-x.

[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*, 2018.

[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. 08, p. 1650140, 2016.

[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*, vol. 8, no. 3, pp. 257–264, Jun. 2018, doi: 10.15866/irecap.v8i3.13541.

[6] L. Merah, A. Ali-Pacha, N. Hadj-Said, B. Mecheri, and M. Dellassi, "FPGA hardware co-simulation of new chaos-based stream cipher based on lozi map," *International Journal of Engineering and Technology*, vol. 9, no. 5, pp. 420–425, Oct. 2018, doi: 10.7763/ijet.2017.v9.1010.

[7] R. Parvaz and M. Zarebnia, "A combination chaotic system and application in color image encryption," *Optics & Laser Technology*, vol. 101, pp. 30–41, 2018.

[8] L. M. Pecora and T. L. Carroll, "Synchronization in chaotic systems," *Physical Review Letters*, vol. 64, no. 8, pp. 821–824, Feb. 1990, doi: 10.1103/PhysRevLett.64.821.

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

[10] U. E. Vincent, "Chaos synchronization using active control and backstepping control: a comparative analysis," *Nonlinear Analysis: Modelling and Control*, vol. 13, no. 2, pp. 253–261, Apr. 2008, doi: 10.15388/na.2008.13.2.14583.

[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 and Fractals*, vol. 41, no. 3, pp. 1390–1400, Aug. 2009, doi: 10.1016/j.chaos.2008.05.022.

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

[14] S. Vaidyanathan and S. Rasappan, "Global Chaos synchronization of n-scroll chua circuit and lur'e system using backstepping control design with recursive feedback," *Arabian Journal for Science and Engineering*, vol. 39, no. 4, pp. 3351–3364, Jan. 2014, doi: 10.1007/s13369-013-0929-y.

[15] J. Schmitz and Lei Zhang, "Rössler-based chaotic communication system implemented on FPGA," in *2017 IEEE 30th Canadian Conference on Electrical and Computer Engineering (CCECE)*, Apr. 2017, pp. 1–4, doi: 10.1109/CCECE.2017.7946729.

[16] B. Lakshmi, E. Kirubakaran, and T. N. Prabakar, "Design and Implementation of FPGA based dual key encryption," *International Journal of Computer Applications*, vol. 3, no. 3, pp. 21–27, Jun. 2010, doi: 10.5120/714-1006.

[17] 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.

[18] 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.

[19] 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.

[20] E. A. R. Hussein, M. K. Khashan, and A. K. Jawad, "A high security and noise immunity of speech based on double chaotic masking," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 4, pp. 4270–4278, Aug. 2020, doi: 10.11591/ijece.v10i4.pp4270-4278.

[21] H. N. Abdullah, S. S. Hreshee, and A. K. Jawad, "Noise reduction of chaotic masking system using repetition method," *Unpublished*. 2015, doi: 10.13140/rg.2.1.4023.7209.

[22] H. R. Hatem, "Color image compression and encryption based on compressive sensing," *Journal of Engineering and Sustainable Development*, vol. 22, no. 1, pp. 149–161, 2018.

[23] M. Alsaedi, "Colored image encryption and decryption using chaotic lorenz system and DCT2," *arXiv preprint arXiv:1701.02896*, 2017.

[24] 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*, 2018.

[25] 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, 2018.

[26] E. Rodríguez-Orozco *et al.*, "FPGA-based chaotic cryptosystem by using voice recognition as access key," *Electronics (Switzerland)*, vol. 7, no. 12, Dec. 2018, doi: 10.3390/electronics7120414.

[27] B. B. Saikia and Monjul, "An FPGA implementation of chaos based image encryption and its performance analysis," *IJCSN - International Journal of Computer Science and Network*, vol. 5, no. 5, pp. 712–720, 2016.

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

[29] 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 (IJEECS)*, 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. Email: wisal.eng@gmail.com.

Wasan A. Wali Holds a PhD in Automation and Control Engineering, Built Environment and Sustainable Technologies Institute (BEST), Faculty of Technology and Environment, Liverpool 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. Email: wasan.wali@uobasrah.edu.iq.

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.