FPGA-BASED ADCSK MODULATION TECHNIQUE

Hamsa A ABDULLAH[1]

The use of a chaotic system to construct an efficient modulation approach is introduced in this paper. The proposed system of this paper consists of two stages of security. In the first stage of security, a new chaotic modulation method (ADCSK) is proposed, the chaotic signal is used as a carrier for message signal. While in the second stage of security, the controller of synchronization is employed in the receiver side to produce the matching signal. The modulated signal is transmitted over AWGN and Rayleigh channel. The BER performance shows that, the ADCSK over AWGN and Rayleigh channel has better performance than CSK and DCSK modulation where the signal recovered with error free at 4 dB. The hardware resources that used to implement the proposed system are IO blocks, FF, LUT, and DSP. The proposed system's LUT utilization percentage is 0.14 percent. Furthermore, the Bounded IO that was employed is 46%. The intended signal has been successfully recreated at the receiver, according to the MATLAB simulation and FPGA hardware findings.

Keywords: Chaotic, ADCSK, Synchronization, FPGA

1. Introduction

Security methods are necessary to block unwanted access and use the information that transmitted via an unprotected channel [1]. The wideband noise-like signal is produces via chaotic system. The chaotic signal possesses statistical features that are reliable and repeatable. The chaotic system's wideband nature makes it an excellent carrier of signal in a modulation platform, making it more resistant to fading channels propagation than a sinusoid-based system [2]. The first class of chaotic cryptosystem is secure communication founded by analog chaos. Another type of security can be provided by synchronizing chaotic systems between transmitter and receiver. One or more analog chaotic signals can be driven and broadcast across the physical channel to achieve synchronization [3]. There have been many different types of analog chaos-based communication systems established. The first generations of analog chaos-based communication were chaotic masking and Chaotic Shift Keying (CSK) [4]. Different methods for transmitting digital data based on chaotic systems

[1] College of Information Engineering, Al-Nahrain University, Iraq, E-mail: hamsa.abdulkareem@coie-nahrain.edu.iq

have been developed in communication systems, including CSK, Differential Chaotic Shift Keying (DCSK), and Frequency-Modulated Differential Chaos Shift Keying (FM-DCSK). In these modulation methods, the digital signal at the transmitter is replaced by a chaotic signal. The chaotic subsystem at the receiver, which is equivalent to the chaotic subsystem at the transmitter, is built using one of the received signals [5].

Many chaotic systems have been studied in recent years for use in secure data transmission and other applications. Some academics are working on developing dependable chaotic systems with embedded system implementation and synchronization algorithms, as well as introducing practical chaotic modulation techniques [6]. In 2017, Two-level Secure Colored Image Transmission Using Novel Chaotic Map is introduced. The chaotic system is utilized as a key in the first level to encrypt the secure color image. The chaotic system is utilized as a carrier signal for digital data modulation at the second level. In addition, the study introduces two new chaotic modulation approaches, each of which is tailored for various types of testing. The first approach is based on one bit modulation and has seven kinds. The second approach is based on two bits modulation and has three variants. Bit Error Rate (BER) and Peak Signal to Noise Ratio (PSNR) over Additive White Gaussian Noise (AWGN) channel are used to evaluate the proposed approaches' performance. NCM performed better than Henon and Logistics chaotic systems [1]. In 2019, Design Chaotic Security Communication System based on FPGA Technology is presented. This study describes a communication system that employs the chaos approach, in which data is added to a chaotic signal before being sent across the channel. It will synchronize signals at the receiver, decreasing travel confusion and allowing the information to be retrieved. Because the characteristics of chaotic communications resemble noise to an eavesdropper, this technique improves the system's security. The FPGA-based communication technology that has been examined was designed and implemented [7]. In 2020, Hardware Implementation of DCSK Communication System Using Xilinx System Generator (XSG) is presented. The use of XSG to construct the noncoherent DCSK system across an AWGN channel with a variable spread factor is proposed in this research. The DCSK system is hardware co-simulated on the SP605 xc6slx45t-3fgg484 evaluation board with a clock frequency of 27 MHZ. The results of the hardware simulation show that the system is functioning properly. The system was successfully routed in using the ISE 14.5 program, with maximum modulation and demodulation frequencies of 39.587 and 41.592 MHZ, respectively. The XSG is the most user-friendly, adaptable, and dependable tool for creating FPGA designs [8] .

This work aims to offer a secure image transmission system with a strong encryption algorithm and great resilience to channel degradations. The results are split

into two sections in this paper: MATLAB simulation results using package (R2014b), and FPGA implementation results using Vivado System Generator and Genesys2–Kintex7 FPGA.

2. The Proposed System

The proposed system of this paper consists of two stages of security as shown in Fig. 1 where the Lorenz chaotic system used as main security key for these two levels of security. In the first stage of security, a new modulation method is proposed as described in section 2.1. In this level of security, the binary sequences are modulated based on the chaotic signal. The chaotic signal is used as a carrier for original signal. The modulated signal is transmitted over AWGN and Rayleigh Channel. While in the second stage of security, the controller of synchronization is utilized in the receiver to produce the matching signal. The chaotic system that was formed at the receiver is then used to demodulate the received signal. Finally, using the same key that was used on the transmitter, the desired binary data is recovered.

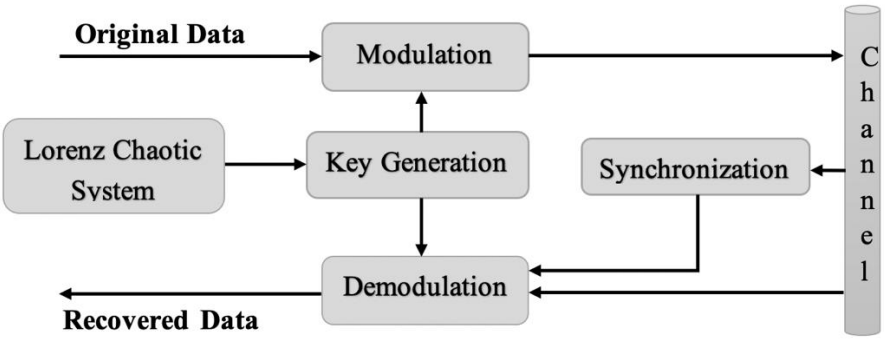


Fig. 1. Block Diagram of Proposed System

2.1 Adaptive Differential Chaotic Shift Keying (ADCSK)

Fig. 2 shows the proposed ADCSK technique. When binary data is “1”, the chaotic signal X(t) is transmitted in the period of data duration T. when binary data is “0”, the chaotic signal X(t) is transmitted in the first half the period of data duration T, while negative value of X(t) is transmitted in the second half the period of data duration T. The transmitted signal S(t) can be represented by:

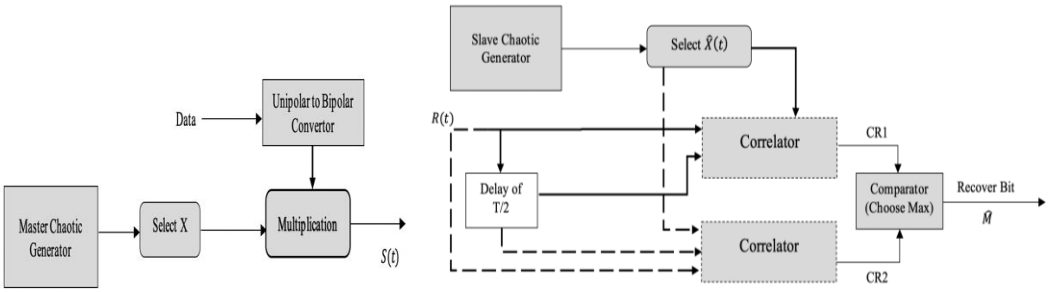
$$S(t) = \begin{cases} X(t) & when\ data = 1 \quad 0 \le t < T \\ X(t) & when\ data = 0 \quad 0 \le t < \frac{T}{2} \\ -X(t) & \quad \frac{T}{2} \le t < T \end{cases} \tag{1}$$

On the receiving end, the slave signal generated that exactly match with the signal at transmitter based on synchronization system. To gain the decision variable for producing the output binary stream, the received signal is delayed by half a bit period and correlated with the created signal and its negative value. Fig. 3 show the proposed ADCSK signal representation and comparison with DCSK. The CR1 and CR2 are correlator between the received and the slave signal. The correlator system can be represented as:

$$CR1 = \sum_{t=0}^{T} R(t) * \hat{X}(t)$$
$$CR2 = \sum_{t=0}^{T/2} R(t) * \hat{X}(t) - \sum_{t=\frac{T}{2}+1}^{T} R(t) * \hat{X}(t) \tag{2}$$

The recovered binary data can be represented as:

$$M(t) = \begin{cases} 1 & if\ CR1 \ge CR2 \\ 0 & if\ CR1 < CR2 \end{cases} \tag{3}$$



a. b.

Fig. 2. Block Diagram of ADCSK System, a. ADCSK Modulation, b. ADCSK Demodulation

Data Stream									
1		0		1		0		1	
Chaotic Stream									
C1	C2	C3	C4	C5	C6	C7	C8	C9	C10
DCSK									
C1	C1	C3	-C3	C5	C5	C7	-C7	C9	C9
ADCSK									
C1	C2	C3	-C4	C5	C6	C7	-C8	C9	C10

Fig. 3. Signal Representation

2.2 Synchronization

The synchronization of Lorenz chaotic map ability is tested based on nonlinear control laws. The master system of Lorenz is:

$$X = XY - Z$$
$$Y = X$$
$$Z = Y \quad (4)$$

While the Slave system is:

$$\hat{X} = \hat{X}\hat{Y} - \hat{Z} + u_1$$
$$\hat{Y} = \hat{X} + u_2$$
$$\hat{Z} = \hat{Y} + u_3 \quad (5)$$

The phase error can be defined by:

$$e_1 = \hat{X} - X$$
$$e_2 = \hat{Y} - Y$$
$$e_3 = \hat{Z} - Z \quad (6)$$

The substitution of eq. (4) and eq. (5) in eq. (6):

$$e_1 = \hat{X}\hat{Y} - \hat{Z} + u_1 - XY - Z$$
$$0 = \hat{X}\hat{Y} - \hat{Z} + u_1 - XY - Z$$

In Ref. [9], equation identities are employed to simplify equations, and these equations are as follows:

$$\hat{X}\hat{Y} - XY = Ye_1 + \hat{X}e_2$$

So,

$$0 = Ye_1 + \hat{X}e_2 - e_3 + u_1$$

The control law u_1 is:

$$u_1 = -Ye_1 - \hat{X}e_2 + e_3 \quad (7)$$
$$e_2 = \hat{X} + u_2 - X$$
$$0 = \hat{X} + u_2 - X$$
$$0 = e_1 + u_2$$

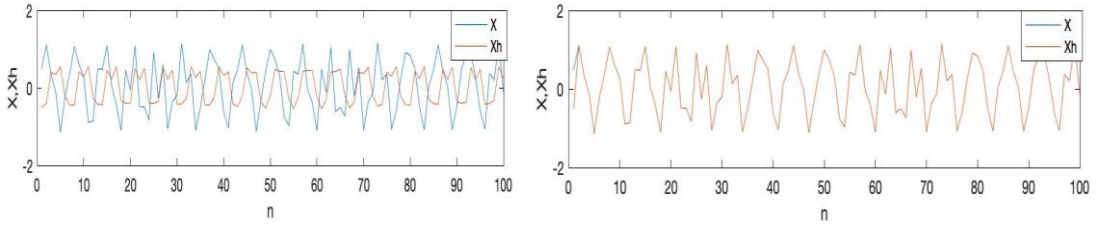
The control law u_2 is:

$$u_2 = -e_1 \quad (8)$$
$$e_3 = \hat{Y} + u_3 - Y$$
$$0 = \hat{Y} + u_3 - Y$$
$$0 = e_2 + u_3$$

The control law u_3 is:

$$u_3 = -e_2 \quad (9)$$

The initial values of master system are $X(0) = 0.5, Y(0) = 0.2\ and\ Z(0) = -1$, while the slave system's initial values are $\hat{X}(0) = -0.5, \hat{Y}(0) = -0.2\ and\ \hat{Z}(0) = 0.5$. Fig. 4.a depicts the master-slave signals without and with control laws applied. Fig. 4.b shows that master-slave signal synchronization can be accomplished in as little as 0.3 milliseconds.



a. b.

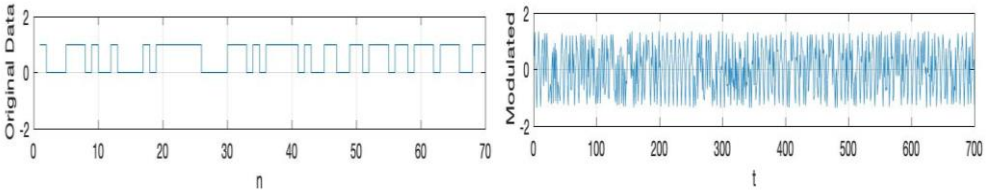
Fig. 4. Chaotic Signal Synchronization a. Without Controller b. With Controller

3. The Performance Measurements

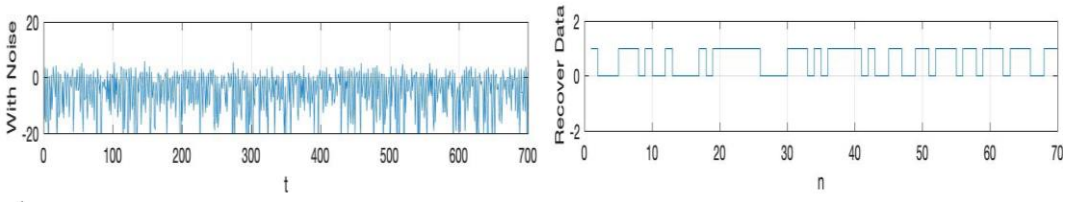
The performance of the suggested system is modeled in MATLAB and built on FPGA board. So, the performance measurements are security and hardware measurements.

3.1 Security Measurements

To measure the efficiency of the suggested communication system, the performance of demodulated information should be examined by using BER. Fig. 5 shows the input digital data waveforms that symbolize by the binary bits, the modulated chaotic carrier using the ADCSK modulation, transmitted signal over AWGN and Rayleigh channel, and the recovered data (with synchronization). Figs. 6.a and b show the BER curves obtained for ADCSK and traditional CSK, DCSK respectively over AWCN and Rayleigh channel. It is clear in these figures that the ADCSK has better performance than CSK and DCSK. This is an excellent outcome since it enables the user to employ a new modulation method as a secret key without compromising quality.

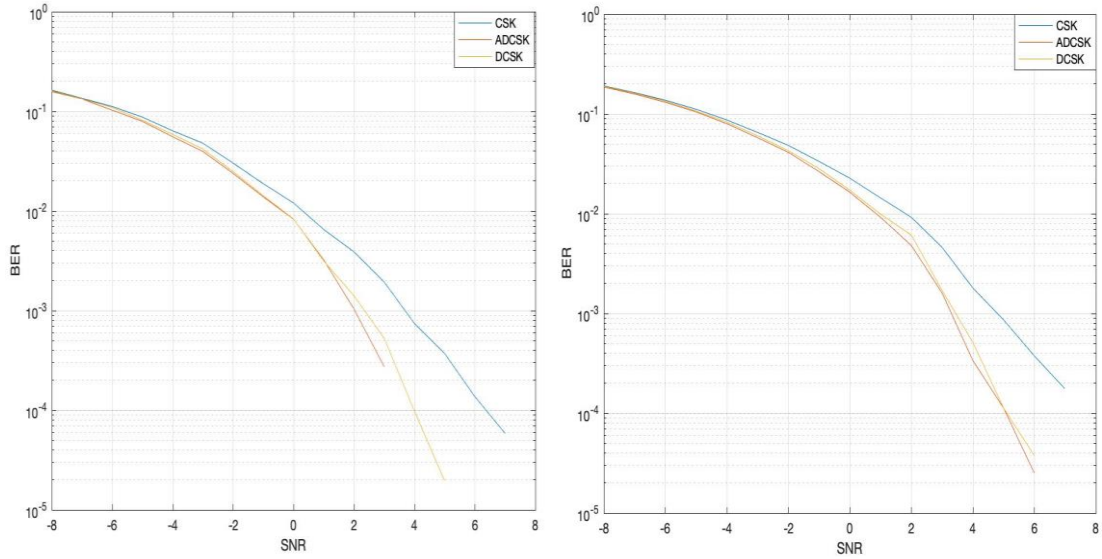


a. b.



c. d.

Fig. 5. Waveform Signal a. Original Binary Signal b. Modulated Signal Using ADCSK c. Transmitted Signal over AWGN Channel d. Recovered binary Signal



a. b.

Fig. 6. BER of ADCSK modulation a. AWGN Channel b. Rayleigh Channel

3.2 Hardware Measurements

The hardware implementation of the proposed system is shown in Figs. 7 and 9. Fig. 7 illustrates the transmitter system, which contains two main blocks: Master chaotic system, ADCSK Modulation. While figure 9 illustrates the receiver system, which contains three main blocks: Synchronization, Slave chaotic system and ADCSK Demodulation.

A. The Master Chaotic System

Based on (4), the master chaotic system consists of three signals: X, Y and Z. The main blocks that were used to generate these three chaotic signals are: pulse generator, delay, multiplexer, multiplier, adder, IN/OUT gateway. The system shown in figure 7.b.

B. ADCSK Modulation System

The ADCSK modulation system is implemented based on (1 and 2) as shown in Fig. 7.c. The main blocks that were used to generate this system are: pulse generator, multiplexer, multiplier, constant, IN gateway. Fig. 8 illustrate the modulation signal of the proposed system.

C. The Slave Chaotic System

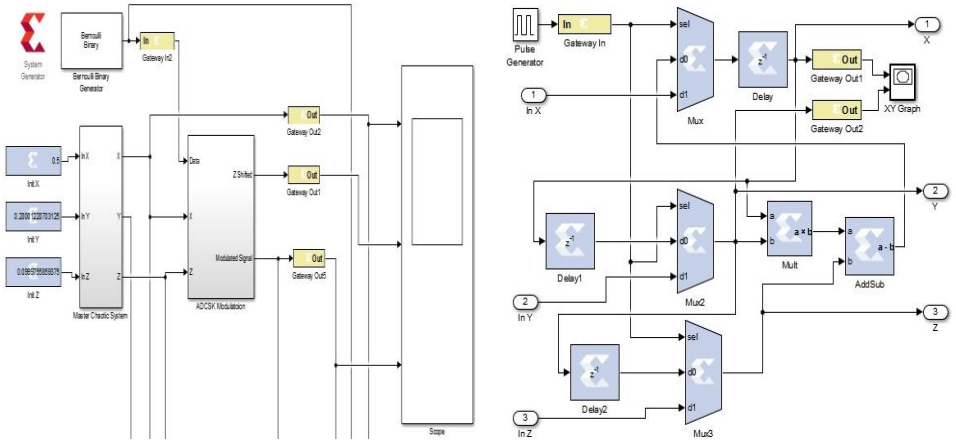
Based on (5), the slave chaotic system consists of three signals: $\hat{X}$, $\hat{Y}$ and $\hat{Z}$. The main blocks that were used to generate these three chaotic signals are: pulse generator, delay, multiplexer, multiplier, adder, IN/OUT gateway. The system shown in Fig. 9.b.

D. Synchronization System

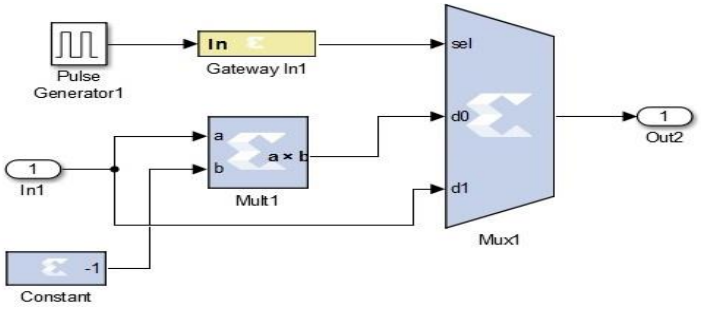
The synchronization system is implemented based on (5, 6 and 7, 8, 9) as shown in Fig. 9.c. The main blocks that were used to generate this system are: multiplier, adder, OUT gateway.

E. ADCSK Demodulation System

The ADCSK demodulation system is implemented based on (3) as shown in Fig. 9.d. The main blocks that were used to generate this system is rational block. Fig. 10 illustrate the recovered signal.



a. b.



c.

Fig. 7. Hardware Implementation of Proposed Transmitter System a. Transmitter System b. Master Chaotic System c. ADCSK Modulation

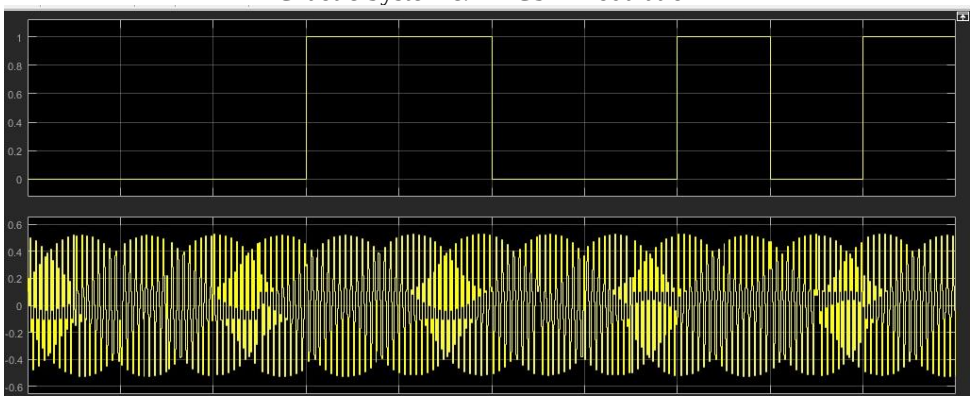
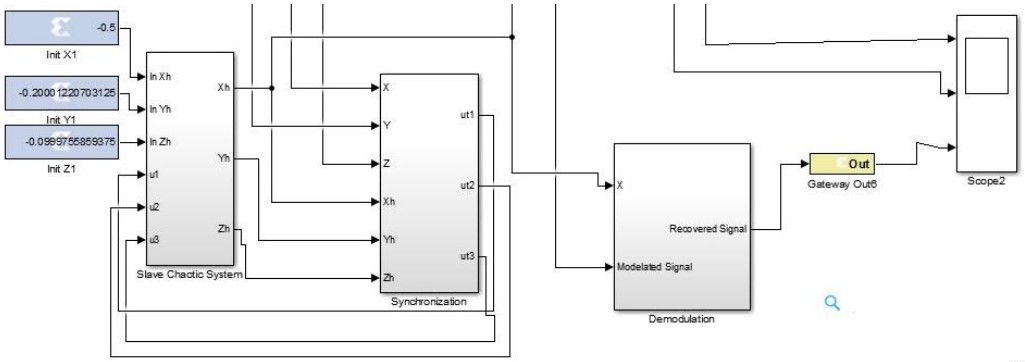
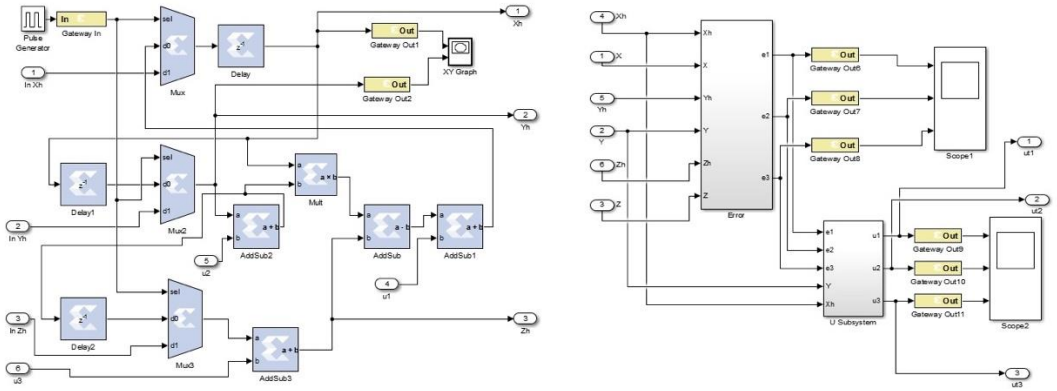
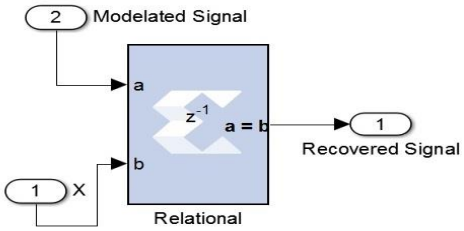


Fig. 8. Transmitter Signals: a. Input Signal, b. Modulated Signal



a.





d.

Fig. 9. Hardware Implementation of Proposed Reciver System a. Receiver System b. Slave Chaotic System c. Synchronization system d. ADCSK Demodulation

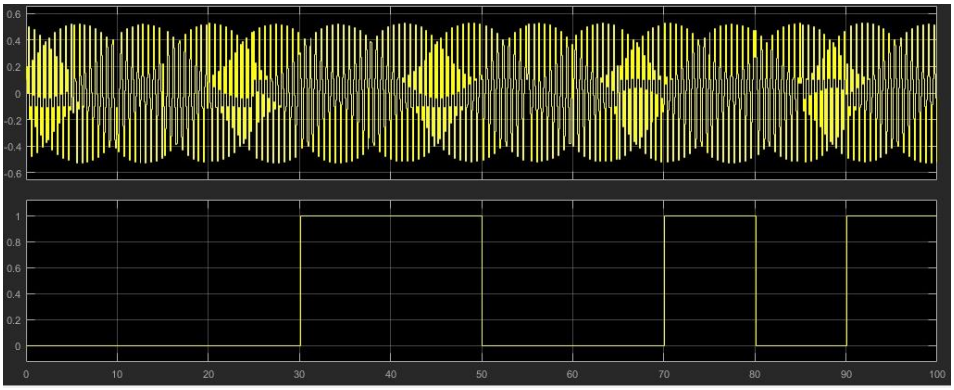


Fig. 10. Receiver Signals: a. Modulated Signal, b. Recovered Signal

With the target board of FPGA and its clock specifications chosen, the proposed system was converted to VHDL code using HDL netlist transformation in an XSG. Then, for the converted VHDL project, the Vivado software is being utilized to synthesize, implement, generate bitstreams, and program the targeted hardware. Table

1 shows an outline of the implemented system's utilization. Slice LUTs, Slice Registers, Slice, DSP, BUFGCTRL, and IO blocks are one of the resources available. The amount of IO required is 46%. Fig. 11 shows the proposed system's power consumption. As shown, the I/O consumes approximately 87 percent of the overall power.

Table 1

Outline of Design Systems Usage

Resource	Usage	Obtainable	Usage Percentage
Slice LUT	289	203800	0.14 %
Slice registers	161	407600	0.04 %
Slice	137	50950	0.27 %
BUFGCTRL	1	32	3.13 %
DSP	7	840	0.83 %
IO	320	500	46 %

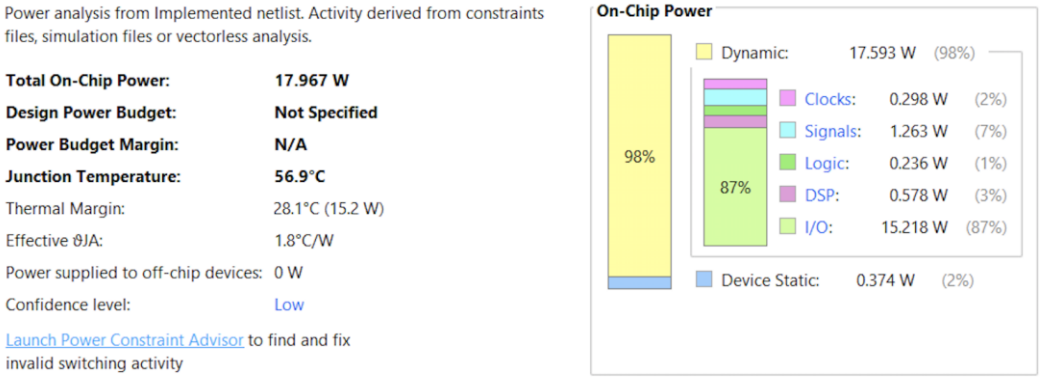


Fig. 11. The power consumption

4. Conclusion

In this paper, a new method of chaotic modulation is introduced to improve the secure communication based on chaotic synchronization. Due to the behavior of Lorenz chaotic map in terms of randomize, wide range of initial value and three dimension is used to provide more security and robustness to image transmission using the proposed system. The proposed system is simulated firstly using MATLAB then implemented using FPGA hardware. To evaluate the performance of the proposed system, a BER performance evaluation is implemented. The BER performance illustrate that the proposed modulation method (ADCSK) over AWGN and Rayleigh channel has better performance than CSK and DCSK modulation where the signal recovered with error free at 4 dB. The hardware resources that used to implement the

proposed system are Slice LUTs, Slice Registers, Slice, DSP, BUFGCTRL, and IO blocks. The amount of IO required is 46% while the LUT usage percentage is 0.14%. The intended signal has been successfully recreated at the receiver, according to the MATLAB simulation and FPGA hardware findings.

R E F E R E N C E S

[1] H. N. Abdullah, H. A. Abdullah, "Two-level Secure Colored Image Transmission Using Novel Chaotic Map," in *2nd -AL-Sadiq International Science Conference on Multidisciplinary in IT and Communication Science and Technologies -2nd- AIC – MITC*, Baghdad – IRAQ, 2017.

[2] H. A. Abdullah, H. N. Abdullah, "FPAA Implementation of Chaotic Modulation Based on Nahrain Map," *raqi Journal of Information and Communications Technology(IJICT)*, vol. 1, no. 3, pp. 17-30, 2018.

[3] W. Chang, S. Shih, and C. Chen, "Chaotic Secure Communication Systems with an Adaptive State Observer," *Journal of Control Science and Engineering*, vol. 2015, no. 15, pp. 1-7, 2015.

[4] K. Georges, "Wireless Chaos-Based Communication Systems: A Comprehensive Survey," *IEEE Access*, vol. 4, pp. 1-28, 2016.

[5] X. Gao, M. Cheng, L. Deng, M. Zhang, S. Fu, and D. Liu, "Robust chaotic-shift-keying scheme based on electro-optical hybrid feedback system," *Optics Express*, vol. 28, no. 8, pp. 10847-10858, 2020.

[6] H. A. Abdullah, H. N. Abdullah, "Embedded Hardware Implementation for Image Security Using Chaotic Maps," in *Multimedia Security Using Chaotic Maps: Principles and Methodologies*, Warsaw, Poland, Springer, 2020, pp. 231-263.

[7] H. V. Tran, V. T. Nguyen, and T. H. Nguyen, "Design Chaotic Security Communication System based on FPGA Technology," *International Journal of Engineering Research & Technology (IJERT)*, vol. 8, no. 4, pp. 173-176, 2019.

[8] D. S. Ibrahim, F. S. Hassan, "Hardware Implementation Of Dcsk Communication System Using Xilinx System Generator," in *First Online Scientific Conference for Graduate Engineering Students*, 2020.

[9] B. Jovic, "Chaotic Synchronization of Maps," in *Synchronization Techniques for Chaotic Communication Systems*, Berlin, Springer, 2011, pp. 79-102.