DESIGN AND FPAA IMPLEMENTATION OF NOVEL CHAOTIC SYSTEM

Hamsa A. ABDULLAH[1], Hikmat N. ABDULLAH[2]

Due to characteristic of chaotic systems in terms of nonlinearity, sensitivity to initial values, and non-periodicity, they are used in many applications like security and multiuser transmission. Nahrain chaotic map is an example of such systems that are recently proposed with excellent features for the use in multimedia security applications. Although the implementation of chaotic systems is easy using low cost analogue ICs, this approach does not provide the flexibility that the reconfigurable analogue devices have in design possibilities such as reducing the complexity of design, real-time modification, software control and adjustment within the system. This paper presents a description to Nahrain chaotic system and its hardware implementation using field programmable analogue array (FPAA) device. AN231E04 dpASP board is used as a target device for the implementation. The simulation results verified the chaotic behavior of Nahrain chaotic system while the experimental results proved the successful real time system operation and match the simulation results.

Keywords: FPAA. Nonlinear. Discrete System. Nahrain Chaotic System

1. Introduction

Chaotic system of simple structure can demonstrate complex dynamical properties in infinite mathematical world, such as sensitivity to initial conditions, topological transitivity and mixing, expansiveness, and decaying autocorrelation function. Due to their wideband nature, the modulation schemes that use chaotic basis functions are potentially more resistant to multipath propagation than those based on sinusoidal functions [1]. So, designing chaos-based transmission schemes emerged a new research direction to reinforce information security of data sent through the internet.

For many years, the signal processing is implemented through digital devices such as programmable logic devices like FPGA (Field Programmable Gate Arrays), CPLDs, microcontrollers, etc., that kept analog signal processing out of modern trends in programmable devices. Recently, a number of researches have been done in the field of reconfigurable analog signal processing using

[1] Department of System Eng., Al-Nahrain University, Iraq, e-mail: hamsa.abdulkareem@coie-nahrain.edu.iq
[2] Department of Information and Communication Eng., Al-Nahrain University, Iraq, e-mail: hikmat.abdullah@coie-nahrain.edu.iq

Anadigm dpASP, and PsoCs devices. An FPAA is an analog programmable technology equivalent to FPGA. With this technology the complexity and time effort of the analog circuit design are minimized [2].

In 2014, a new dual entropy core true random number generator TRNG capable of producing high levels of randomness using hardware redundancy is proposed. Comparative analysis of the statistical and randomness properties has been performed for developed traditional and proposed TRNG architectures. FPAA is used for design and hardware implementation of the proposed model [3]. Analog programmable electronic circuit-based Lorenz chaotic system is introduced in [4]. The design and hardware implementation of the system was achieved using FPAA device. The experimental results demonstrated that the circuit exhibits pre-chaotic transient and chaotic Lorenz attractor. In 2016, a random number generation method based on a piecewise linear one dimensional (PL1D) discrete time chaotic maps for applications in cryptography and steganography is proposed. The proposed system is practically implemented by using FPAA-FPGA devices [5]. In 2017, linear synchronization and circuit implementation of chaotic system with complete amplitude control based on FPAA is proposed [6]. Later in the same year, a performance comparison study of FPAA and FPGA platforms implementation of Chaos On/Off Keying (COOK) communication system is given in [7].

In 2018, we have proposed a new dynamical system called Nahrain chaotic system [8]. Nahrain chaotic system proved that it has excellent performance for multimedia encryption and secure transmission applications [9]. However, in [8] we have presented only a part of standard randomness tests to prove the system randomness behavior. In this paper, we will review Nahrain chaotic system and complete the presentation of its FIPS 140-2 randomness tests. Then we will introduce the hardware implementation of the system. The hardware implementation is based on analog programmable hardware which allows the system dynamics, reconfigurable, rapid experimental setup, and low cost.

2.□□ Programmable Analog Array (FPAA)

FPAA is an inserted device containing configurable analog blocks (CAB) and interconnects between the blocks [10] various of their digital counterpart (FPGA). They are used for application driven rather than general purpose as they may be current mode or voltage mode devices. There are two types of system that FPAAs usually works with it. These are continuous time and discrete time systems. FPAAs help in the algorithmic implementation of the analogue circuit creation policies and provide very proper environment in which the design and implementation of analog system and circuit take short time. The ultimate goal is

to define a generic FPAA which would be capable of implementing almost any type of the analog function.

A FPAA, based on CMOS technology, contains switches, operational amplifiers, and programmable switched capacitors (S/C). The FPAA architecture have four CABs and contain seven configurable input/output structures each can be used as input or output. Four of the seven configurable input/output structures have integrated differential amplifiers as shown in Fig. 1. There is also a single chopper stabilized amplifier that can be used by three of the seven output cells. The FPAA circuits can be programmed in many different ways such as with the help of a series E^2PROM or with a connected microcontroller through the I2c line created as an inner structure [11].

The FPAA technology is convenient for many engineering applications like signal processing, control systems, and signal generation. One of the most important reasons that make FPAA suitable for dynamic reconfiguration is that it can be reconfigured "on the fly" to implement different parameter device settings [12].

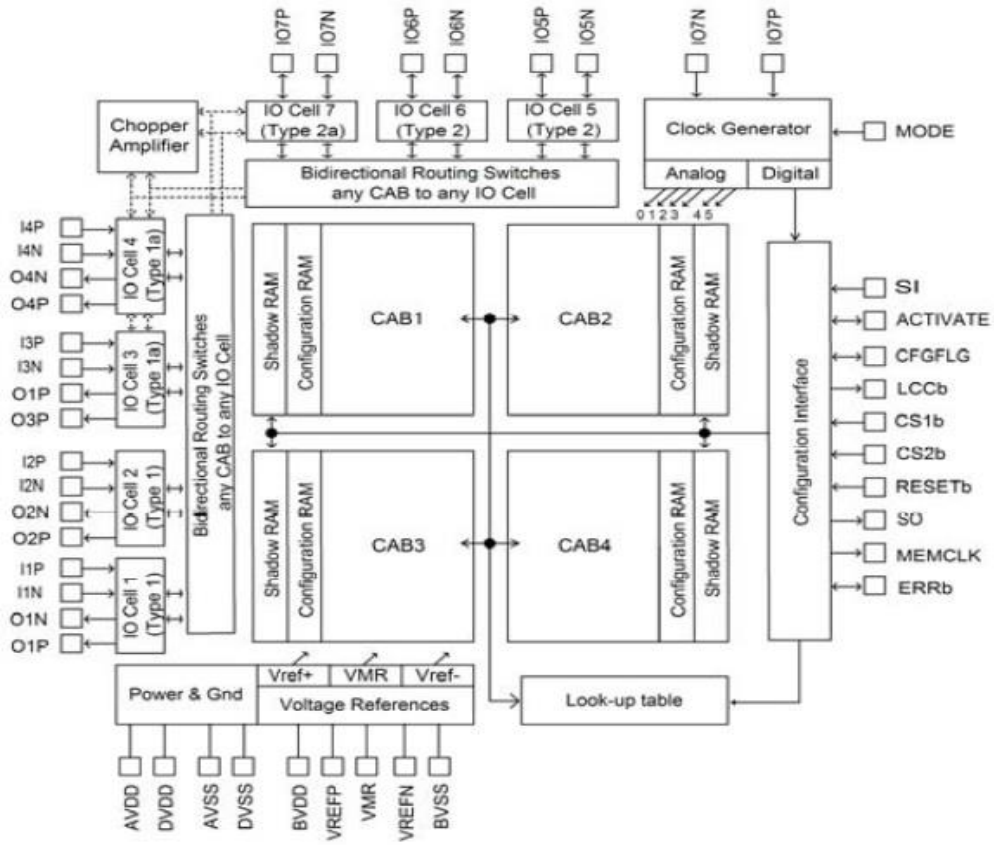


Fig. 1. FPAA Architecture

3.□□ Nahrain Chaotic System

The nonlinear equations that describe Nahrain chaotic system are [9]:

$$X_{n+1} = 1 - aX_nY_n - X_n^2 - Y_n^2$$
$$Y_{n+1} = X_n \quad (1)$$
$$Z_{n+1} = Y_n - bZ_n$$

The system consists of state variables: X, Y and Z and two parameters: a and b. Through a series of numerical modeling and simulation associated with MATLAB, the phase portraits of chaotic behavior have been acquired using system parameter values: a=1.52 and b=0.05. The schematic block diagram of Nahrain chaotic generator is shown in Fig. 2. Fig. 3 shows the phase portraits of the system when its initial conditions are: X(0)=0.3, Y(0)=0.2 and Z(0)=0.1. It is clear from this figure that the attractors have strange shape which meets the well-known properties of chaotic behavior. The other numerical and statistical tests required to confirm this behavior will be presented for Nahrain system in the next two sections, respectively.

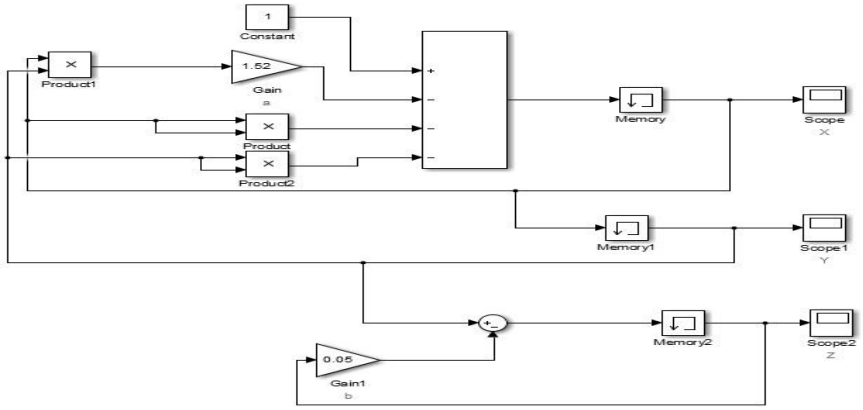


Fig. 2. MATLAB-Simulink implementation of Nahrain chaotic map.

3.1 Performance Analysis Tools for Nahrain Chaotic System

The behavior chaotic system is very useful in security applications to dis-organize the communication data in order to increase security requirements. To prove the behavior of proposed system, there are a number of system's statistical analysis that presented and discussed. These analyses are categorized into two groups. The first group includes the tests that verify whether the system is chaotic or not. The second group includes the tests that are used to verify the randomness properties of the system according to the key that is created from the system.

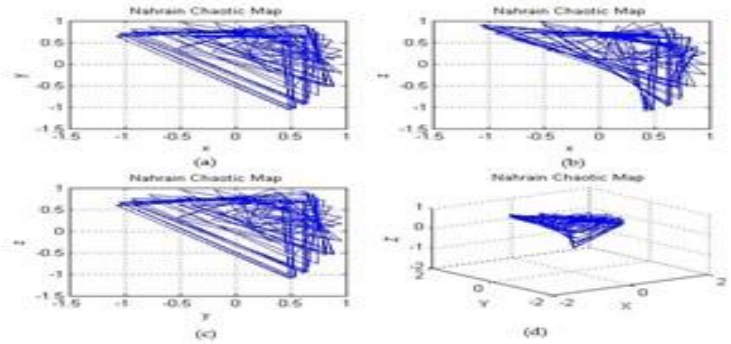


Fig. 3. Phase portraits of the proposed chaotic system: (a) X-Y, (b) X-Z, (c) Y-Z, (d) X-Y-Z

*3.1.1.**Chaotic Behavior of Dynamic System Tests***

Lyapunov exponent and 0-1 tests of any dynamical system are mathematical quantities used to measure the system behavior whether it is chaotic or not. 0-1 test is presented by Gottwald and Melbourne [12]. The input numbers used in the tests are the keys generated from the dynamic system in time domain and the output is a number between 0 to1. The algorithm of the 0-1 test could be explained as follows:

1. Assume a set of data f(n) sampled in time n, where n =1,2,3 …N, which represent a one dimensional data.
2. Choose a positive real constant number r.
3. Compute p(n) and s(n) as using the following equations:

$$p(n) = \sum_{j=1}^{n} f(j)\cos(jr) \quad (2)$$

$$s(n) = \sum_{j=1}^{n} f(j)\sin(jr) \quad (3)$$

4. Calculate the mean square displacement M(n) as follows

$$M(n) = \lim_{N\to\infty} \frac{1}{N}\sum_{j=1}^{n}[p(j+n) - p(j)]^2 + [s(j+n) - s(j)]^2 \quad (4)$$

5. The asymptotic growth rate is defined as:

$$K = \frac{logM(n)}{\log n} \quad (5)$$

The value of K for continuous system defines the system whether it is chaotic or not. K ≈ 0 denotes that, the system is not chaotic (ordinary), while K ≈ 1 denotes that, the system is chaotic.

*3.1.2.**The Randomness Tests***

The randomness tests are used to prove the randomness of chaotic random bits sequence CRBS. The standard randomness test FIPS 140-2 are well known test standard [13]. If any CRBS passes the specified tests can be pretended as a good CRBS. The following tests are implemented on sequence of 15,000 bits of output from the generator [13]:

1. Frequency (Monobit) Test: This test interests in the ratio of ones and zeroes for the whole sequence.

2. Frequency Test within a Block: This test interests in the ratio of ones in a block with M-bits size.
3. Runs Test: This test interests in the overall number of runs in the sequence (run is a continuous sequence of congruous bits).
4. Longest Run of Ones in a Block Test: This test interests in the longest run of ones within M-bits blocks.
5. Binary Matrix Rank Test: This test interests in the rank of separated sub-matrices of the complete sequence.
6. The Discrete Fourier Transform (Spectral) Test: This test interests in the peak heights in the discrete fourier transform of the sequence.
7. Maurer's (Universal Statistical) Test: This test interests in the number of bits between matching patterns.
8. Approximate Entropy Test: This test interests in the frequency of all possible overlapping M-bits patterns across the whole sequence.
9. Cumulative Sum Test: This test interests in determine whether the cumulative sum of the partial sequences is too large or too small compare to the predicted behavior of that cumulative sum for random sequences.
10. Random Excursions Test: This test interests in the number of cycles having exactly *K* visits in a cumulative sum random walk.
11. Random Excursions Variant Test: This test interests in the total number of times that a specific state is appeared in a cumulative sum random walk.

In all above tests, P-value is calculated to define the strength of the evidence against the null hypothesis. For these tests, each P-value is the probability that an ideal random number generator would generate a less random sequence than the sequence that has been tested, given the type of non-randomness estimated by the test. If a P-value of the test is equal to 1, this means the sequence has ideal randomness while if P-value is equal to zero this means the sequence is totally non-random. A threshold value (α) can be chosen for the tests. If P-value $\geq\alpha$, the sequence is random. If P-value$<\alpha$, the sequence is non-random. Typically, α is in the range [0.001, 0.01].

4.□□ Implementation of Chaos System using Embedded System

The AN231K04 development board shown in Fig. 4 is used as hardware device for implementing Nahrain chaotic system. The AN231K04 development board is one of the latest production of Anadigm’s dpASP.

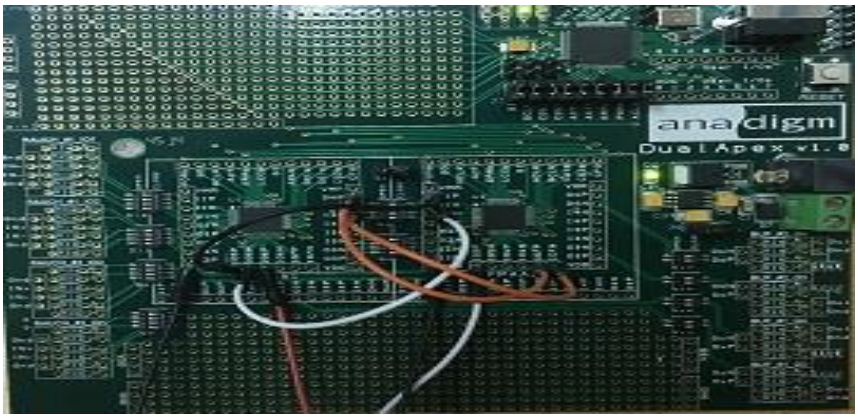


Fig. 4. AN231K04 FPAA development board

The flow chart of a model FPAA implementation is shown in Fig. 5. The diagram shows the system is firstly tested numerically simulation before implementing it on an FPAA. Then the mathematical system can be modeled by Anadigm designer®2 software. After that, the model of the system can be downloaded to FPAA board using Anadigm designer®2 software. Then the results obtained from programmed hardware are compared with simulation results. If there is different between hardware and software results, it is discarded by modulating the system model using Anadigm designer®2 software. The implementation is completed when all the different are discarded. According to the Simulink model that presented in Fig. 2, Nahrain discrete chaotic system can be built using configurable analog modules (CAMs) in Anadigm designer®2 as shown in Fig. 6 and downloaded to the development board. CAM values for FPAA1 and FPAA2 are given in table 1.

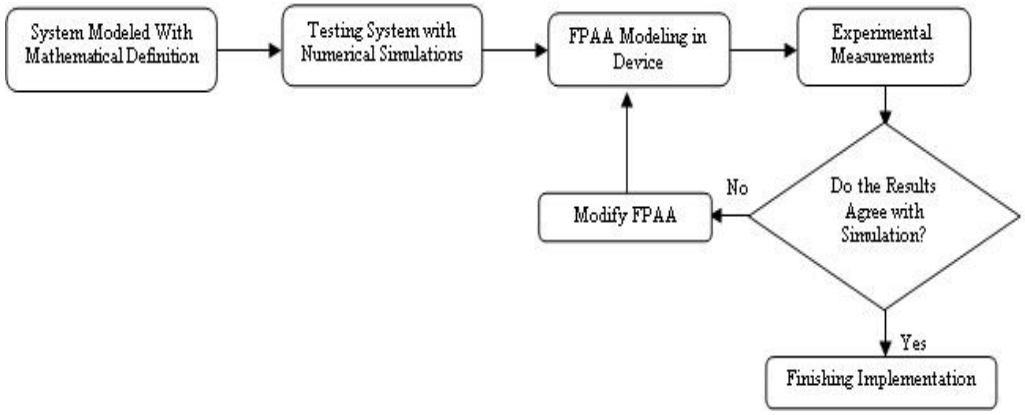


Fig. 5. The flow diagram of a typical FPAA implementation

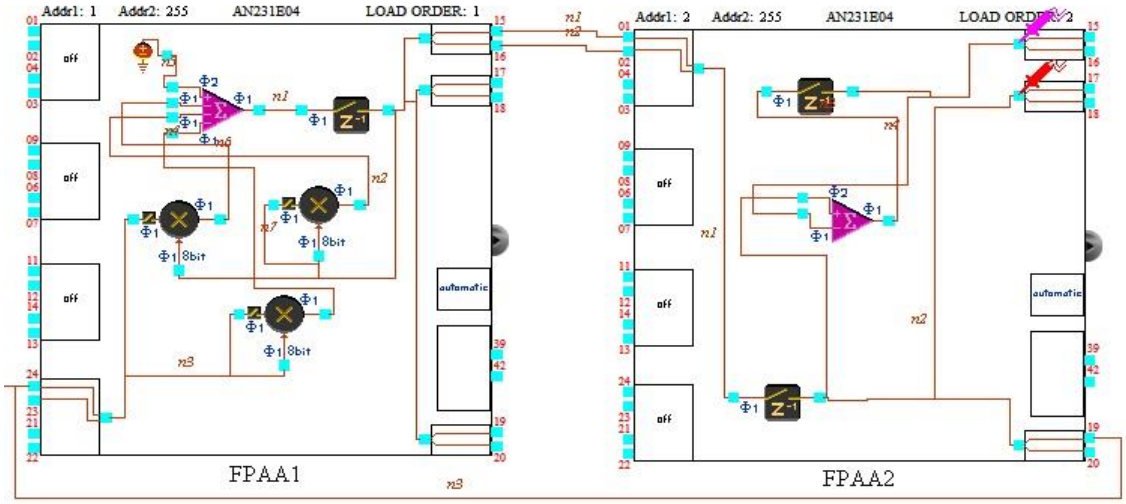


Fig. 6. The circuit of Nahrain Discrete Chaotic system Using FPAA

Table 1.

Configurable Analog Model of FPAA

FPAA1				FPAA2			
Name	**Options**	**Parameters**	**Clocks**	**Name**	**Options**	**Parameters**	**clocks**
SumDiff1 (SumDiff v1.0.1)	**Output Phase :** *Phase 1* **Input 1:** *Non-inverting* **Input 2:** *Inverting* **Input 3:** *Inverting* **Input 4:** *Inverting*	**Gain 1:** 0..5 **Gain 2:** 1.52 **Gain 3:** 1.0 **Gain 4:** 1.0	**Clock A:** *250 kHz*	SumDiff2 (SumDiff v1.0.1)	**Output Phase :** *Phase 1* **Input 1:** *Non-inverting* **Input 2:** *Inverting* **Input 3:** *Off* **Input 4:** *Off*	**Gain 1:** 1.0 **Gain 2:** 0.05	**Clock A:** *250 kHz*
Hold1 (Hold v1.0.2)	**Input Sampling Phase:** *Phase 1*		**Clock A:** *250 kHz*	**Hold1 (Hold v1.0.2)**	**Input Sampling Phase:** *Phase 1*		**Clock A:** *250 kHz*
Voltage1 (Voltage v1.0.1)	**Polarity:** *Positive (+2V)*			Hold2 (Hold v1.0.2)	**Input Sampling Phase:** *Phase 1*		**Clock A:** *250 kHz*
Multiplier1 (Multiplier v1.0.2)	**Sample and Hold:** *Input X*	**Multiplication Factor:** *1.00*	**Clock A:** *250 kHz* **Clock B:** *4 MHz*				
Multiplier2 (Multiplier v1.0.2)	**Sample and Hold:** *Input X*	**Multiplication Factor:** *1.00*	**Clock A:** *250 kHz*				

Multiplier3 (Multiplier v1.0.3) 	**Sample and Hold:** *Input X*	**Multiplication Factor:** *1.00*	**Clock B:** *4 MHz*				

5. Experimental Measurements Results

The experimental results of Nahrain chaotic system consist of two parts: the simulation results and hardware test results. These results are presented in the next sections.

5.1. Simulation Results

To verify the chaotic behavior and randomness properties of Nahrain system, a simulation model for the system using MATLAB is implemented. The numerical and statistical tests mentioned in the section 3 are applied accordingly. This section presents first the results of chaotic behavior test, then the results of randomness tests.

5.1.1. Results of Chaotic Behavior Tests

After implementing the 0-1 test to the Nahrain system, the following results of asymptotic growth rate K for different system variables are obtained: Kx = 0.9864, Ky = 0.9866, Kz = 0.9856. According to the results of this test, since all system variables produces numbers very closed to 1 then it is a chaotic system and the chaotic behavior can be obtained from anyone of its outputs.

5.1.2. Results of Randomness Test

This work gives details on implementing a method to convert chaotic sequences into binary ones as shown Fig. 7. The conversion is based on comparing the outputs of two identical Nahrain chaotic maps running simultaneously with the same parameters (a=1.52 and b=0.05) but with different initial conditions. The initial conditions for the first map are X1(0)=0.3, Y1(0)=0.2 and Z1(0)=0.1 while for the second map they are X2(0)=0.2, Y2(0)=0.1 and Z2(0)=0.2. The output binary sequences g1, g2 and g3 are generated by comparing the outputs of the two maps on sample by sample basis according to the following equations:

$$g1(X1,X2) = \begin{Bmatrix} 1 \; if \; X1 > X2 \\ 0 \; if \; X1 \leq X2 \end{Bmatrix} \; where \; X_1(0) \neq X_2(0) \tag{6}$$

$$g2(Y1,Y2) = \begin{Bmatrix} 1 \; if \; Y1 > Y2 \\ 0 \; if \; Y1 \leq Y2 \end{Bmatrix} \; where \; Y_1(0) \neq Y_2(0) \tag{7}$$

$$g3(Z1,Z2) = \begin{Bmatrix} 1 \; if \; Z1 > Z2 \\ 0 \; if \; Z1 \leq Z2 \end{Bmatrix} \; where \; Z_1(0) \neq Z_2(0) \tag{8}$$

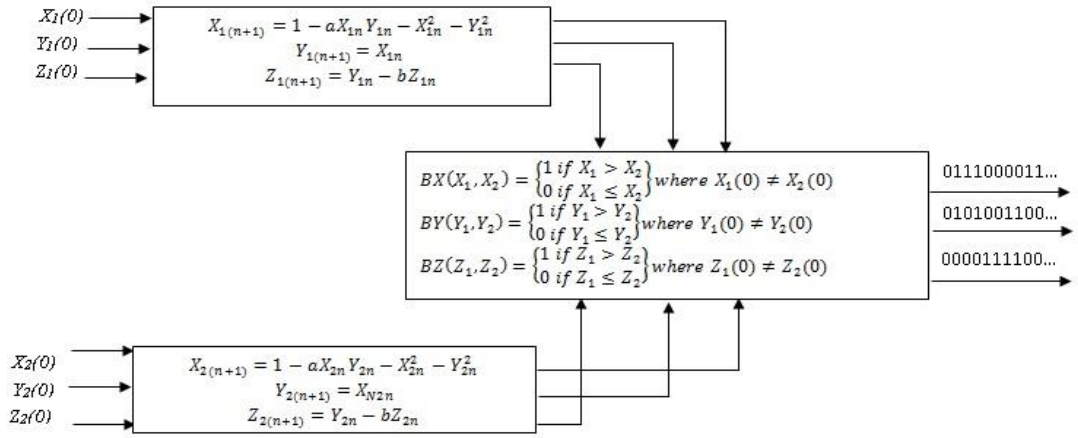


Fig. 7. Random Bit Generator

Next a sequence of 15,000 consecutive bits of each output from the system is subjected to the tests mentioned in section 3.1.2 individually. The tests results are given in Table 2. From the results in this table, we can see that the P-value of all the generated binary sequences are much higher than 0.01 which means the system is random. It can also be seen that the randomness level of output X is the best among other outputs of the system.

Table 2.

The Results of the Randomness

Test	X	Y	Z	P-value ≥ (0.01-0.001)
Frequency (MonoBit) Test	0.5787	0.5787	0.2739	accept
Frequency (Block =1000) Test	0.5031	0.5168	0.8993	accept
Run Test	0.5917	0.5917	0.2855	accept
Longest Run of Ones in a Block (128)	0.9931	0.9997	0.9606	accept
Binary Matrix Rank Test	0.2030	0.2030	0.0433	accept
DFT Test	0.4118	0.3049	0.4118	accept
Maurer's Test	0.8604	0.8744	0.8670	accept
Approximate Entropy Test	0.4002	0.4002	0.5458	accept
Cumulative Sum Test	0.9767	0.9767	0.5458	accept
Random Excursions Test	0.1085	0.1085	0.0253	accept
Random Excursions Variant Test	0.8808	0.8814	0.9042	accept

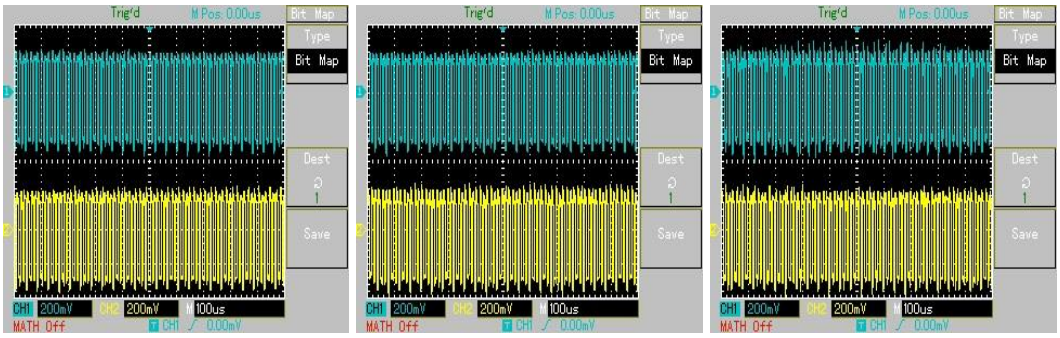
5.2. **Hardware Test Results**

To observe the behavior of the Nahrain chaotic map, the FPAA model is downloaded to the development board by setting the parameters in Eq.1. as follows: a=1.52 and b=0.05. The experimental results of the FPAA implementation are measured via an oscilloscope in time domain of the state-variables of the system namely *X*, *Y* and *Z*. Fig. 8 presents the chaotic attractor produced by the experimental implementation of the system. Table 3 illustrates the power consumptions and CAB usage capacity of these implementations. Figs.

8 and 9 show that the chaotic attractors are strange with good state space, so they can be used for generating secure key for multimedia encryption and can be used as carrier wave for secure multimedia transmission.

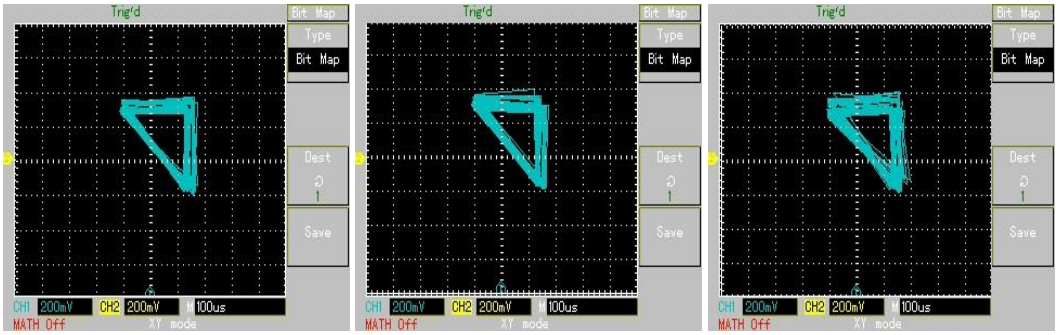
The power consumptions and CAB usage capacity of the FPAA

	FPAA1	FPAA2
Power consumption	165 ± 50 mW	74 ± 22 mW
CAB1(used/total capacity)	7/8	5/8
CAB2(used/total capacity)	6/8	2/8
CAB3(used/total capacity)	6/8	0/8
CAB4(used/total capacity)	6/8	0/8



a. b. c.

Fig. 8. Experimental implementation of state-variables a. X and Y b. X and Z c. Y and Z



a. b. c.

Fig. 9. Experimental implementation of Chaotic Attractor: a. X-Y Attractor, b. X-Z c. Attractor Z-Y Attractor

6.□□ Conclusions

The hardware implementation of Nahrain chaotic system is done using FPAA board. The three variables of Nahrain chaotic system has been generated by using programmable hardware device. And the phase portrait of Nahrain chaotic system also generated, which is matching to phase portrait of simulation results. The implementation of a chaotic system based on FPAA programmable

hardware is very convenient for reconfigurable design based in its nonlinear structure. This system used efficiently as a programmable chaos generator in plentiful chaos-based applications.

The implementation results of Nahrain chaotic system show that the ability of FPAA hardware device to implement analog circuit with low cost and short time. Since a FPAA device can be used in state of roughly all electronic hardware for implementations of discrete chaotic system, this programmable and reconfigurable implementation offers more dynamic, modest and economic solutions. Because this type of implementations provide the potential of resilient and reconfigurable design of many analog chaotic systems based on mathematical design without requirement to complex electronic hardware, FPAA-based chaos added a significant reliability to the proposed secure transmission system.

R E F E R E N C E

[1] *Georges Kaddoum, "*Wireless Chaos-Based Communication Systems: A Comprehensive Survey". IEEE Access, Vol. 4, Pp. 2621-2648, 2016.

[2] *Adam Piłat, "*Semi-automatic design and code generation for FPAA devices, Computer Methods and Systems, Kraków, Poland. Pp. 375–378, 2009.

[3] *Ihsan C., Ali E. P., Gunhan D.,"*A new dual entropy core true random number generator, Analog Integrated Circuits and Signal Processing, Springer, Vol.79, No.3, 2014.

[4] *Fadhil, R., Ramzy S. Ali, L. F.,* "Analog Programmable Electronic Circuit-Based Chaotic Lorenz System", Basrah Journal for Engineering Sciences, Vol.14, No. 1, 2014.

[5] *Fatma Y. D.:* Simple Chaotic Hyperjerk System, International Journal of Bifurcation and Chaos, Vol.26, No. 11, 2016.

[6] *Osman, B. , Ahmet, C.: uneyd Tantu* , "A Random Number Generation Method Based on Discrete Time Chaotic Maps, 60th International Midwest Symposium on Circuits and Systems (MWSCAS), Pp.1212-1215, 2017,

[7] *Enis, G., Kenan, A.:* A Performance Comparison Study of Programmable Platforms: FPAA and FPGA Implementation of COOK Communication System, European Conference on Circuit Theory and Design (ECCTD) IEEE, 2017.

[8] *Hamsa A. Abdullah, Hikmat N. Abdullah"* A New Chaotic Map for Secure Transmission, TELKOMNIKA, Vol.16, No.3, 2018.

[9] *Hikmat N. Abdullah., Hamsa, A. Abdullah.:* Two-level Secure Colored Image Transmission Using Novel Chaotic Map, Second Al-Sadiq International Conference on Multidisciplinary in IT and Communication Science and Applications, Pp.121-125, 2017.

[10] *Dipti, B.V.R. Reddy*.: Field Programmable Analog Array: A Boon for Analog World, 3rd International Conference on Computing for Sustainable Global Development (INDIACom) IEEE, Pp.2975- 2980, 2016.

[11] *Fathima, J. A., Dr M.Y.Sanavullah* Autonomus Reconfiguration using FPAA for Bandwitdh Recovery in Satellite Subsystems, IJCSNS International Journal of Computer Science and Network Security, Vol.8, No.7, 2008.

[12] *Andrzej Malcher and Piotr Falkowski*, "Analog Reconfigurable Circuits", Intl Journal of Electronics and Telecommunications, Vol.60, No.1, Pp.15–2, 2014.

[13] *Georg A G, Ian M.*: The 0-1 Test for Chaos: A Review. In : Charalampos S,Georg A G, Jacques L (ed) Chaos Detection and Predictability, Lecture Notes in Physics, Springer, Berlin, Heidelberg. Pp.221-247, 2016.