TELKOMNIKA, Vol.16, No.3, June 2018, pp. 1135~1142
ISSN: 1693-6930, accredited **A** by DIKTI, Decree No: 58/DIKTI/Kep/2013
DOI: 10.12928/TELKOMNIKA.v16i3.8545

A New Chaotic Map for Secure Transmission

Hamsa A. Abdullah*, Hikmat N. Abdullah
College of Information Engineering, Al-Nahrain University, Baghdad, Iraq
*Corresponding author, e-mail: hamsa.abdulkareem@coie-nahrain.edu.iq
**dr.h.abdullah@ieee.org

Abstract

The secure communication through synchronization between two identic chaotic systems have recently gained a lot of interest. To implement a robust secure system based on synchronization, there is always a need to generate new discrete dynamical systems and investigate their performances in terms of amount of randomness they have and the ability to achieve synchronization smoothly. In this work, a new chaotic system, named Nahrain, is proposed and tested for the possible use in secure transmission via chaos synchronization as well as in cryptography applications. The performance of the proposed chaotic system is tested using 0-1 test, while NIST suite tests are used to check the randomness statistical properties. The nonlinear control laws are used to verify the synchronization of master-slave parts of the proposed system. The simulation results show that Nahrain system has chaotic behavior and synchronizable, while the equivalent binary sequence of the system has excellent randomness statistical properties. The numerical results obtained using MATLAB for 0-1 test was 0.9864, and for frequency test was 0.4202, while for frequency test within a block was 0.4311. As a result, the new proposed system can be used to develop efficient encryption and synchronization algorithms for multimedia secure transmission applications.

Keywords*: secure communication; synchronization; the nonlinear control laws; randomness; multimedia*

1. Introduction

Chaos is non-linear, designable modality and most complex steady-state performance. Chaotic systems are very sensitive to initial conditions and system parameters which make them preferred in security applications [1-3]. In recent years many of cryptosystems based on chaos have been researched. Most of them are based on the classical confusion-diffusion architecture proposed by Shannon. Compared to the conventional cryptographic algorithms (DES, 3DES, AES, etc.), the chaos-based cryptosystems provide several advantages, such as: very high security level, high speed especially in stream ciphers, increased flexibility, increased modularity, low computational overheads and computational power, and easier to be performed. These features make them more convenient for encrypting a wide range of data, such as videos, voices and images. Indeed, with a fixed block size, the advanced encryption standard (AES) is not suitable for selective video encryption and stream ciphers [4]. Designing of dynamical systems, intended to be used as base of cryptosystems, must be done so as to ensure the use of a set of associated control parameters' values that leads to chaos. Moreover, the ergodic and randomness properties must be confirmed, as a certainty of high security level of the chaotic dynamical system [5].

Non-linear control laws regulate that chaotic systems can be synchronized by initiating various initial conditions. Nonlinear control laws are designed to ensure that the eigenvalues of the error system matrix always located within the unit circle in the z domain. This ensures the stability of the global estimate of error system and thus makes the master-slave system of any synchronization complexity [6]. The Synchronization of chaos systems has important applications in secure communications [7]. The famous functional application of synchronizing chaotic systems is the Pecora and Carroll (PC) [1]. In 1990, PC showed that systems of chaotic can be synchronized by using various introductory conditions. The original chaotic system introduced by PC consists of two particular sub-systems: the driver and the responder. Chaotic synchronization can be accomplished by creating a congruous responder sub-system at receiver module and driving it with the main driver, and this fact could be proved both

Received January 7, 2018; Revised April 2, 2018; Accepted April 22, 2018

practically and theoretically. Since then, the PC method used in many secure communication and synchronization.

In [1], a novel chaotic system for secure communication applications is introduced where the synchronization condition is proved by PC. In [8], a study of a new chaotic dynamical system and its usage in a novel pseudorandom bit generator is introduced. The new chaotic system was verified by using chaotic behavior test and randomness test. In [9], the dynamics, circuit design, and synchronization of a new chaotic system with closed curve equilibrium is introduced. The new system behavior have been tested by using phase portrait, and maximal Lyapunov exponents. In [10], Pseudorandom Number Generator (PRNG) based on Arnold cat map and statistical analysis is introduced where PRNG that generates bit sequences of two Arnold cat map outputs. The randomness test of bit streams obtained using this PRNG proved that the system provides high quality random bits. In [11], a novel chaos-based encryption algorithm over TCP data packet for secure communication is proposed. In this paper a new algorithm that can be used to encrypt data by using a novel chaotic random number generator. The randomness test of bit streams obtained using this PRNG proved that the system has good randomness properties. In [12], a unified chaotic map called PRBG for voice encryption in wireless communication is presented. The randomness tests of the generated bit streams proved its suitability for digital voice encryption.

Although many new chaotic systems were proposed in the literature to serve for the applications of encryption or secure transmission using synchronization, these systems have complex structures which may limit their implementation. Furthermore, they are designed and tested for one level security approach. i.e. either for encryption based or synchronization based security purposes. In this paper, a new chaotic system of simple structure has been introduced to serve for both encryption and synchronization security. Its randomness performance has been checked statistically and synchronization performance has been verified by the nonlinear control laws methods.

2. The Proposed Chaotic System

A new chaotic system, we call it Nahrain, has been proposed. The nonlinear equations that describe the system are given in equation 1:

$$\begin{aligned} X_{n+1} &= 1 - aX_nY_n - X_n^2 - Y_n^2 \\ Y_{n+1} &= X_n \\ Z_{n+1} &= Y_n - bZ_n \end{aligned} \tag{1}$$

Where a and b are the bifurcation parameters of the system. Through a series of numerical modeling and simulation associated with MATLAB, The phase portraits of chaotic behavior have been acquired by using system parameter values: a=1.52 and b=0.05. The schematic block diagram of the proposed Nahrain chaotic generator is shown in Figure 1. Figure 2 shows the phase portraits of the proposed 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 and applied for Nahrain system in the next two sections respectively.

3. Performance Analysis tools for the Proposed Chaotic System

The chaotic system behavior is very valuable and leads to confuse the communication data in order to increase security requirements. To confirm the proposed system behavior, a number of system's statistical analysis are presented and discussed. These analysis 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.

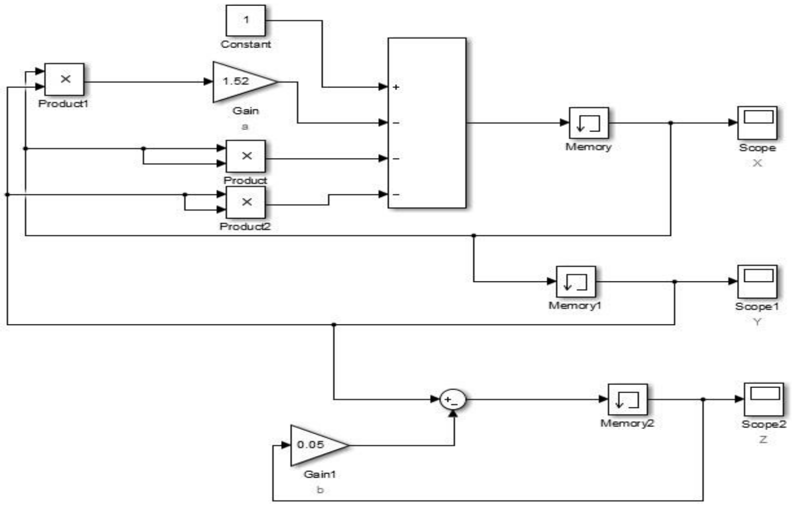

Figure 1. MATLAB-simulink implementation of Nahrain chaotic map.

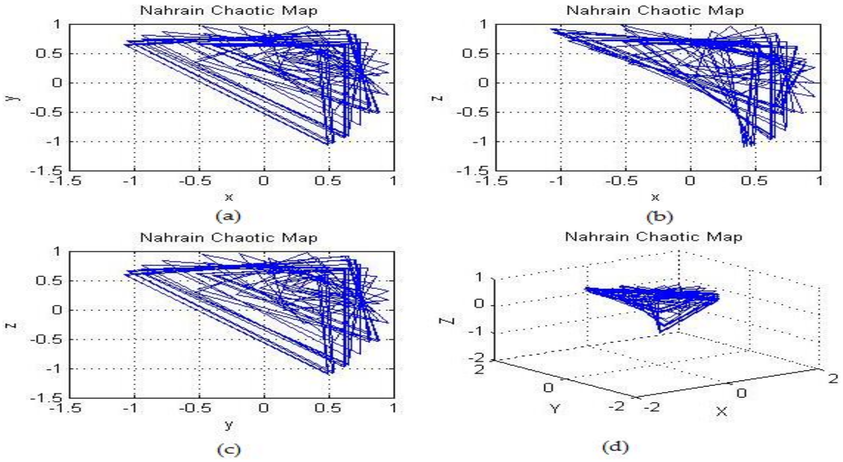

Figure 2. Phase portraits of the proposed chaotic system:
(a) X-Y, (b) X-Z, (c) Y-Z, (d) X-Y-Z

3.1. 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 [13]. 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 0-1 test is more preferred to Lyapunov exponent test due to two reasons:

a. There is no need for phase space reconstruction of the chaotic system. So, it is applied directly on the generated key from the system.

b. It could be applied on the generated key even if the system is continuous, discrete, exponential data, maps, integer or fractional order system.

The algorithm of the 0-1 test could be explained as follows:

a. Assume a set of data f(n) sampled in time n, where n=1,2,3 …N, which represent a one dimensional data.

b. Choose a positive real constant number r.

c. Compute p(n) and s(n) as using the following equations:

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

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

Calculate the mean square displacement M(n) as follows

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

The asymptotic growth rate is defined as:

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

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

3.2. 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 20,000 bits of output from the generator [13-15]:

a. Frequency (Monobit) Test: This test interest to the ratio of ones and zeroes for the whole sequence. The test objective is to evaluate the nearness of zeros to ½, which means that the ones and zeros in whole range is the same. All next tests rely on the crossing of this test [16].
b. Frequency Test within a Block: This test interest to the ratio of ones in a block with M-bit size. The test objective is to define if the frequency of ones in an M-bit block is near M/2 or not [8].
c. Runs Test: This test interest to the overall number of runs in the sequence (run is a continuous sequence of congruous bits). The goal of this test is to define if the number of runs (of ones and zeros) of different lengths is as foreseeable for a random sequence or not [17].

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 ≥α, the sequence is random. If P-value<α, the sequence is non-random. Typically, α is in the range [0.001, 0.01] [18-19].

4. 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 previous section are applied accordingly. This section presents first the results of chaotic behavior test, then the results of randomness test. Finally, it presents the model used for testing the synchronization of Nahrain system and its corresponding results.

4.1. 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.

4.2. Results of randomness test

In this paper, we used method that is proposed in [20] to convert a chaotic sequences into binary ones as shown Figure 3. 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 [20]:

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

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

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

Next a sequence of 20,000 consecutive bits of each output from the system is subjected to the tests mentioned in section 3.2 individually. The three tests results are given in Table 1. 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 proposed system is random. It can also be seen that the randomness level of output X is the best among other outputs of the proposed system and as compared with the test results other works in [8],[10-12].

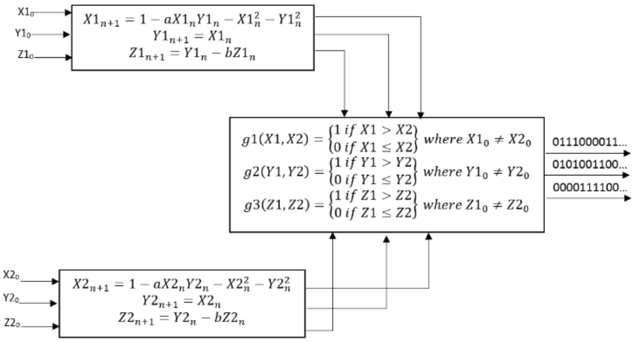
$X1_0$
$Y1_0$
$Z1_0$
$X1_{n+1} = 1 - aX1_nY1_n - X1_n^2 - Y1_n^2$
$Y1_{n+1} = X1_n$
$Z1_{n+1} = Y1_n - bZ1_n$
$g1(X1,X2) = \begin{Bmatrix} 1 \; if \; X1 > X2 \\ 0 \; if \; X1 \le X2 \end{Bmatrix} \; where \; X1_0 \neq X2_0$
$g2(Y1,Y2) = \begin{Bmatrix} 1 \; if \; Y1 > Y2 \\ 0 \; if \; Y1 \le Y2 \end{Bmatrix} \; where \; Y1_0 \neq Y2_0$
$g3(Z1,Z2) = \begin{Bmatrix} 1 \; if \; Z1 > Z2 \\ 0 \; if \; Z1 \le Z2 \end{Bmatrix} \; where \; Z1_0 \neq Z2_0$
0111000011...
0101001100...
0000111100...
$X2_0$
$Y2_0$
$Z2_0$
$X2_{n+1} = 1 - aX2_nY2_n - X2_n^2 - Y2_n^2$
$Y2_{n+1} = X2_n$
$Z2_{n+1} = Y2_n - bZ2_n$

Figure 3. Random Bit Generator

Table 1. The Results of the Randomness Tests

Method		Frequency (Mono Bit) P-value	Frequency (Block) P-value	Run Test P-value
Nahrain	X	0.4121	0.9202	0.4014
	Y	0.4041	0.9284	0.3934
	Z	0.1232	1	0.1158
[6]		0.6434	0.3628	0.3489
[8]		0.6640	0.2220	0.2410
[9]		0.5850	0.4921	0.7858
[10]	X1	0.5580	0.9994	0.0284
	X2	0.3057	0.8730	0.0161
	X3	0.8814	0.9335	0.0100

4.3. Results of synchronization test

The synchronization capability of the Nahrain three-dimensional chaotic map given in Equation 1 is tested using nonlinear control laws. Figure 4 shows the block diagram of the Nahrain master-slave system configuration. The slave system is modeled as:

$$\begin{aligned} \hat{X}_{n+1} &= 1 - a\hat{X}_n\hat{Y}_n - \hat{X}_n^2 - \hat{Y}_n^2 + u_{1n} \\ \hat{Y}_{n+1} &= \hat{X}_n + u_{2n} \\ \hat{Z}_{n+1} &= \hat{Y}_n - b\hat{Z}_n + u_{3n} \end{aligned} \tag{9}$$

The phase error associated with each output is defined by:

$$\begin{aligned} e_{1n} &= \widehat{\mathrm{X}}_{\mathrm{n}} - \mathrm{X}_{\mathrm{n}} \\ \mathrm{e}_{2\mathrm{n}} &= \widehat{\mathrm{Y}}_{\mathrm{n}} - \mathrm{Y}_{\mathrm{n}} \\ \mathrm{e}_{3\mathrm{n}} &= \hat{\mathrm{Z}}_{\mathrm{n}} - \mathrm{Z}_{\mathrm{n}} \end{aligned} \tag{10}$$

The control laws u1n, u2n and u3n are computed using the following formulas:

$$\begin{aligned} u_{1n} &= a(Y_n e_{1n} + X_n e_{2n}) + \left(\hat{X}_n + X_n\right) e_{1n} + (\hat{Y}_n + Y_n)\, e_{2n} \\ u_{2n} &= -e_{1n} \\ u_{3n} &= -e_{2n} + b e_{3n} \end{aligned} \tag{11}$$

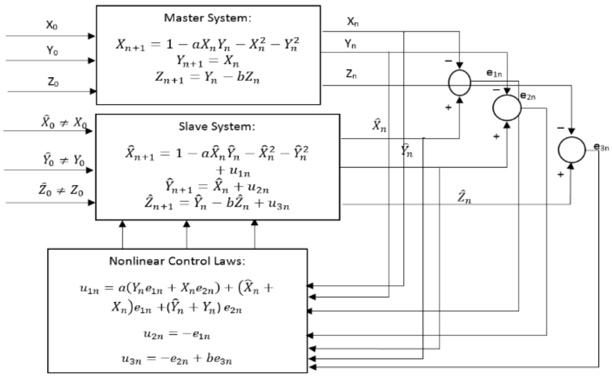
X0
Y0
Z0
Master System:
$X_{n+1} = 1 - aX_nY_n - X_n^2 - Y_n^2$
$Y_{n+1} = X_n$
$Z_{n+1} = Y_n - bZ_n$
Xn
Yn
Zn
e1n
e2n
e3n
−
+
$\hat{X}_0 \neq X_0$
$\hat{Y}_0 \neq Y_0$
$\hat{Z}_0 \neq Z_0$
Slave System:
$\hat{X}_{n+1} = 1 - a\hat{X}_n\hat{Y}_n - \hat{X}_n^2 - \hat{Y}_n^2 + u_{1n}$
$\hat{Y}_{n+1} = \hat{X}_n + u_{2n}$
$\hat{Z}_{n+1} = \hat{Y}_n - b\hat{Z}_n + u_{3n}$
$\hat{X}_n$
$\hat{Y}_n$
$\hat{Z}_n$
Nonlinear Control Laws:
$u_{1n} = a(Y_ne_{1n} + X_ne_{2n}) + (\hat{X}_n + X_n)e_{1n} + (\hat{Y}_n + Y_n)\, e_{2n}$
$u_{2n} = -e_{1n}$
$u_{3n} = -e_{2n} + be_{3n}$

Figure 4. The Nahrain three-dimensional chaotic map master-slave system.

The initial states of master system in Equation 1 are X(0)=0.3, Y(0)=0.2 and Z (0)=0.1, while the initial states of slave system are assumed to be $\hat{X}(0) = -0.1$, $\hat{Y}(0) = 0.3$, and $\hat{Z}(0) = -0.2$. Figure 5 and Figure 6 show the master-slave signals without and with using the control laws respectively. In Figure 6 it very clear that immediate synchronization of all three master-slave signals can be achieved after few number of samples. Figure 7 shows the master-slave signals with different parameters. In master system the parameters used are a=1.52 and b=0.05 while for the slave system the parameters are $\hat{a} = 0.5$ and $\hat{b} = 0.5$. This figure depicts the sensitivity of synchronization system to parameter change. Finally, Figure 8 shows the plot of synchronization errors associated with each system variable versus the sample number. This plot demonstrates that the error values become zero and perfect synchronization occurs in 0.000091 sec. which is very short time.

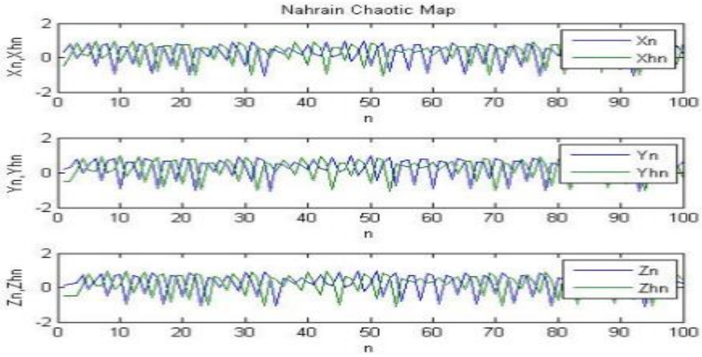

Figure 5. The master-slave Nahrain three-dimensional chaotic map without applying the synchronization control.

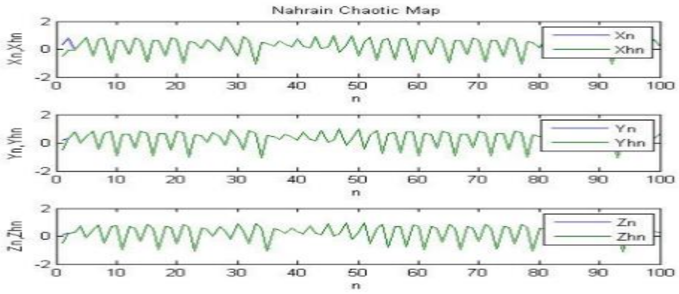

Figure 6. Synchronization of the master-slave Nahrain three-dimensional chaotic map

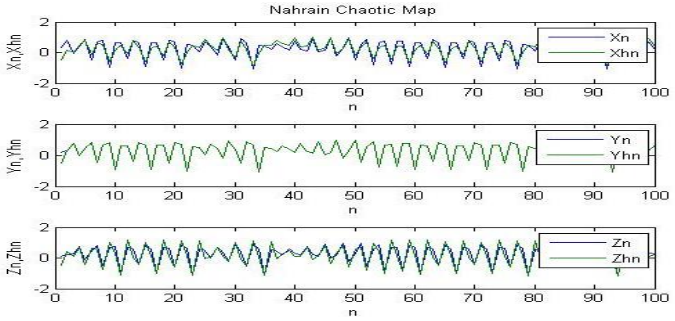

Figure 7. The master-slave Nahrain three-dimensional chaotic map
with different parameters values

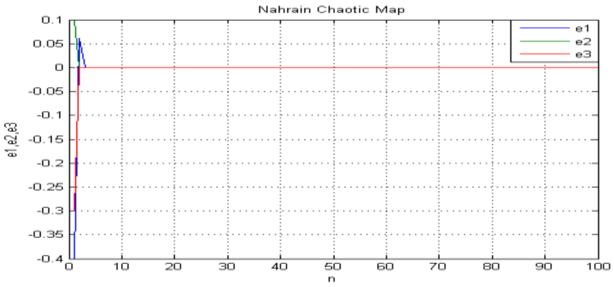

Figure 8. Time of the synchronization errors of master-slave Nahrain
three-dimensional chaotic map

5. Conclusion

In this paper, a new three dimensional discrete chaotic dynamic system, named Nahrain is proposed. The proposed system successfully passes all numerical and statistical tests and proved its good randomness properties. The synchronization test of the proposed system showed that the synchronization occurs in a very short time. The good randomness properties and fast synchronization capability offered by Nahrain system qualify it for the use in designing robust encryption algorithms and real time secure transmission systems based on chaos synchronization. Therefore, it offers the possibility of realizing multi-level security system efficiently.

References

[1] Ali D, Ahmet TÖ. A Novel Chaotic System for Secure Communication Applications. *Information Technology and Control.* 2015; 44(3):271-278.

[2] Edwin R, Arboleda Joel L, Balaba John Carlo L Espineli. Chaotic Rivest-Shamir-Adlerman Algorithm with Data Encryption Standard Scheduling. *Bulletin of Electrical Engineering and Informatics.* 2017; 6(3): 219-227.

[3] Li Feng Z. Secure Communication and Implementation for a Chaotic Autonomous System. *TELKOMNIKA Indonesian Journal of Electrical Engineering*. 2014;12:361-370.

[4] Mousa F. Chaos-based crypto and joint crypto-compression systems for images and videos. Ph.D Thesis, Engineering Sciences. Universite De Nantes, 2015.

[5] Ana-Cristina D, Radu E B, Adrian-Viorel D. Study of a New Chaotic Dynamical System and Its Usage in a Novel Pseudorandom Bit Generator. *Mathematical Problems in Engineering.* 2013.

[6] Wei-Der C, Shun-Peng S, Chih-Yung C. Chaotic Secure Communication Systems with an Adaptive State Observer. *Journal of Control Science and Engineering*. 2015.

[7] rian A, Javad R, Hamid M, Mohammad AA. Output Feedback Synchronization of A Novel Chaotic System And Its Application in Secure Communication. *International Journal of Computer Science and Network Security*. 2017.

[8] Ana C, Dascalescu RB. A New Chaotic Dynamical System and its Usage in a Novel Pseudorandom Number Generator with a Linear Feedback Register Structure. *The publishing house proceedings of the Romanian academy.* 2015; 16: 357-366,.

[9] Xiong W, Viet-Thanh P, Christos V. Dynamics, Circuit Design, and Synchronization of a New Chaotic System with Closed Curve Equilibrium, Complexity, Hindawi. 2017.

[10] Erdinc, A. Pseudorandom number generator based on Arnold cat map and statistical analysis. *Turkish Journal of Electrical Engineering & Computer Sciences*. 2017.

[11] Ünal C, Akif A, Sezgin K, İhsan P, Ahmet Z. A novel chaos-based encryption algorithm over TCP data packet for secure communication. *Security and Communication Networks*. 2016.

[12] Sattar BS, Rana SM. *Proposed random unified chaotic map as PRBG for voice encryption in wireless communication.* International Conference on Communication, Management and Information Technology. 2015; 314 – 323,.

[13] Georg AG, 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. 2016; 221-247.

[14] Andrew R, Juan S, James N, Miles S, Elaine B, Stefan L, Mark L, Mark V, David B, Alan H, James D, San V. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. National Institute of Standards and Technology, 2010.

[15] JKM Sadique UZ, Ranjan G. Review on fifteen Statistical Tests proposed by NIST. *Journal of Theoretical Physics & Cryptography*. 2012; 1.

[16] Dimo, M, Construction of Pseudorandom Binary Sequences Using Chaotic Maps. *Applied Mathematical Sciences*. 2015.

[17] Rashidah K, Mohd AM. *Randomness Analysis of Pseudorandom Bit Sequences*. International Conference on Computer Engineering and Applications. 2011; 772-774.

[18] Sýs M, Matyáš V. Randomness Testing: Result Interpretation and Speed. In: Ryan P., Naccache D., Quisquater JJ. (eds) The New Codebreakers. Lecture Notes in Computer Science, vol 9100. Springer, Berlin, Heidelberg, 2016.

[19] Suryadi MT, Eva Nurpeti, Dhian Widya, Performance of Chaos-Based Encryption Algorithm for Digital Image. *TELKOMNIKA (Telecommunication, Computing, Electronics and Control*, 2014;12(3): 675-682.

[20] Vinod P, KK Sud. A Pseudo Random Bit Generator Based on Chaotic Logistic Map and its Statistical Testing. *Informatica*. 2009.