Journal of Engineering and Applied Sciences 14 (11): 3741-3745, 2019
ISSN: 1816-949X

A Parallel Programming for Robust Chaotic Map Generation Based on Two Dimensional Equation System

Khalid Ali Hussein and Sawsen Abdulhadi Mahmood
Department of Computer Science, College of Education, Al Mustansiriyah University, Baghdad, Iraq

Abstract: In the last two decades, cryptography systems based on chaos methods have been developed due to the interesting shared properties between cryptography and chaos systems such as sensitivity to the initial conditions along with the effects of confusion, diffusion techniques. In this study, a seven term new two Dimensional (2D) chaotic system based on two quadratic nonlinear equations has been derived and analyzed. The experimental results and performance evaluations exhibit that the proposed system is capable to generate abundant 2D chaotic maps with expansive chaotic ranges and chaotic manner. The validated chaotic behavior of the proposed system was investigated using maximum Lyapunov exponents, Kaplan-Yorke dimension, phase portraits and sensitivity to initial condition. Furthermore, the generation of chaotic random sequences can be accomplished simultaneously with parallel manner based on two threads which reinforce the speedup performance of the proposed chaotic map generation algorithm. The parallel implementation of the proposed chaotic system using parallel computing library offered by MATLAB equips highly performance than the pipeline ones and would be helpful to utilize in image encryption/decryption with large size.

Key words: Chaotic map, parallel programming, Lyapunov exponents, MATLAB, implementation, performance

INRODUCTION

Lately, significant research of chaotic system were presented by scientists due to its critical issue in cryptography systems. They realize that some nonlinear dynamic systems have a chaotic behavior. Chaotic systems have been used and applied in many scientific, cryptography and engineering environments. According to this consideration, many characteristics of chaotic systems including: periodicity, sensitivity to initial conditions, mixing and spreading, dynamics estimation property and structural intricacy can be considered to get the confusion, diffusion, pseudo number generation in cryptography systems (Alvarez and Li, 2006; Amigo *et al*., 2007). The main salience properties of Chaotic system are represented by its wide dynamic behaviors and sensitivity to initial condition in order to fit the encryption methods requirements (Alvarez and Li, 2006). One dimensional chaotic map systems have been studied and introduced by many research. These type of chaotic systems have some disadvantage such as the restricted and discontinuous domain of the based chaotic system action (Li *et al*., 2009; Arroyo *et al*., 2013) the allergy to the basic analysis functions such as iteration and correlation tools (Sobhy and Shehata, 2001), the non-regular data distribution of chaotic systems production. Subsequently, improving new chaotic systems with performance upgrading is required. Two dimensional chaos system was presented by the researchers by Andrecut and Ali (2001) they designed a 2-D Model maps for powerful chaos system using a transformation of a critical point into an unstable fixed point. The researcher by Perez (2004) has also presented a linear interpolation relationship between the chaotic logistic map and quartic maps offered by other research and exhibits the bifurcation diagram with no periodic window. Another research conducted by Elhadj and Sprott (2012) he presented a specific 2D consolidated refined map that consist of Henon and Lozi maps. The dynamic system concept was analyzed by Elhadj and Sprott (2010), they present a mathematical model based on multi-function in term of unified chaotic map has the ability of producing hyperbolic, Lorenz map in addition to quasi attractors. To address the main disadvantages of one dimensional chaotic system mentioned above, this study presents a new chaotic system based on two dimensional nonlinear equations.

MATERIALS AND METHODS

The proposed chaotic system structure: The new two-dimensional chaotic system is described and characterized by three quadratic nonlinearities terms, given by the following two first order differential equations:

Corresponding Author: Khalid Ali Hussein, Department of Computer Science, College of Education, Al Mustansiriyah University, Baghdad, Iraq

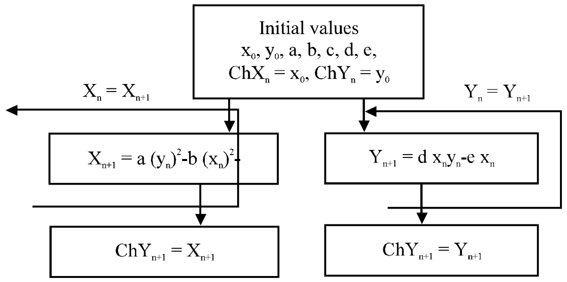
Initial values
x_0, y_0, a, b, c, d, e,
$ChX_n = x_0$, $ChY_n = y_0$
$X_n = X_{n+1}$
$Y_n = Y_{n+1}$
$X_{n+1} = a (y_n)^2\text{-}b (x_n)^2\text{-}$
$Y_{n+1} = d\, x_n y_n\text{-}e\, x_n$
$ChY_{n+1} = X_{n+1}$
$ChY_{n+1} = Y_{n+1}$

Fig. 1: The structure of the proposed two dimensional chaotic system

$$\begin{aligned}\frac{dx}{dt} &= ay^2 - bx^2 - c \\ \frac{dy}{dt} &= dxy - ex\end{aligned} \tag{1}$$

where, x, y are real numbers called the states variables and a-e are positive parameters of the proposed system. The initial values of the proposed chaotic system are: x_0 = 1.2 and y_0 = 0.8 in addition to the typical parameters chosen as: a = 4, b = 1.1, c = 4.4, d = 0.1, e = 8. Figure 1 describes the main structure of the proposed two-dimensional chaotic system with n iteration number.

Lyapunov exponents and Lyapunov dimensions: The Lyapunov exponents dimension determine an attractors dynamics in information theoretic terms (Wolf *et al*.,1985). According to the nonlinear dynamical theory, the quantitative measure of the sensitivity dependence on the initial conditions and Lyapunov exponents magnitude. An n dimensional system have n Lyapunov exponents LEI (Wolf *et al*., 1985). The negative value of Lyapunov exponents refers to the stable state of the chaotic system while positive value represents the unstable state of the chaotic system. It is the average rate of divergence (or convergence) of two neighboring trajectories. The numerical calculation of the two Lyapunov exponents (LE1 and LE2) of the proposed nonlinear dynamical system (1) is performed with parameter values; a = 4, b = 1.1, c = 4.4, d = 0.1 and e = 8. In this study, the related Lyapunov exponents acquired are LE1 = 0.0529592 and LE2 = - 0.061395. Remarkably, it can be seen that the largest Lyapunov exponent is positive indicating that the system have chaotic characteristics. Since, the LE1 is a positive Lyapunov exponent and the rest Lyapunov exponents is negative. Thus, the system is chaotic. The fractal dimension is another typical characteristic of chaotic behavior calculated by Kaplan-Yorke dimension DKY. Equation 2 refers to DKY dimension and expressed by:

$$DKY = j+\frac{1}{|Lj+1|}\sum_{i=1}^{j} L_i \tag{2}$$

where, j is identified and satisfied by the following conditions:

$$\sum_{i=1}^{j} L_i > 0 \text{ and } \sum_{i=1}^{j+1} L_i < 0 \tag{3}$$

This means that the first Lyapunov exponent is nonnegative and j is the maximum value of i value. L_i is in descending order of the sequence according to the sequence of Lyapunov exponents. DKY is the upper bound of the dimension in information theory term. It is worth mentioning, we determine that the value of j is one and then the Kaplan-Yorke dimension can be expressed from the above equation due to LE1>0 and LE2<0. Thus, the Kaplan-Yorke KY dimension of the proposed chaotic system is given by:

$$D_{KY} = j+\frac{1}{|L_j+1|}\sum_{i=1}^{j} L_i \tag{4}$$

$$D_{KY} = 1+\frac{1}{|L_j+1|}\sum_{i=1}^{j} L_i = 1+\frac{LE_1}{LE_2} \tag{5}$$

$$1+\frac{0.052952}{0.0613954} = 1.86259$$

which means that the Lyapunov dimension of system (Eq. 1) is fractional. Because of the fractal nature, the new system have non-periodic orbits and nearby trajectories diverge. Therefore, the proposed nonlinear system shows a chaotic behavior.

Phase portraits: The initial value of the proposed chaotic system were taken as x_0 = 1.2, y_0 = 0.8 with typical values of the system parameters: a = 4, b = 1.1, c = 4.4, d = 0.1 and e = 8. Essentially, the Lyapunov exponent is a mathematical tool to analyze and examine the nonlinearity of the dynamic systems. One positive value of Lyapunov exponents refers to chaotic behavior of the system. Based on the experiment results, the corresponding values of Lyapunov exponents of the proposed system (Eq. 1) are determined to be LE1 = 0.0529592 and LE2 = -0.0613954. There is one positive Lyapunov exponents which proved that the proposed system have a chaotic behavior. The simulation of the phase portraits for the proposed chaotic system is performed using Mathematica Program which exhibits complex and abundant chaotic dynamics behaviors with strange attractors in two-dimensions (x-y), (y-x) as shown in Fig. 2. The phase portraits of the new chaotic system are illustrated in Fig. 1a and b in (x-y) and

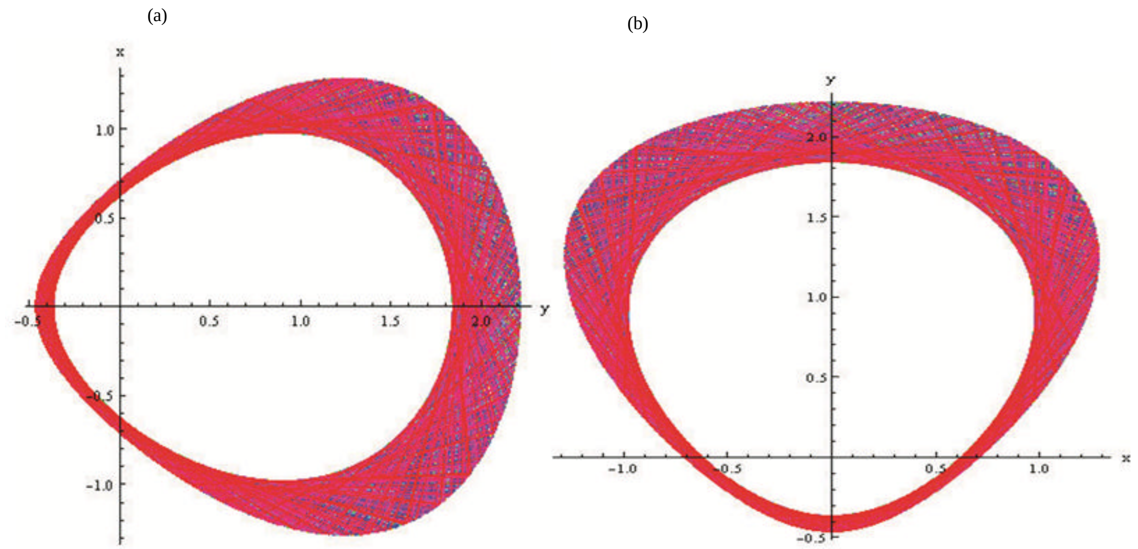

Fig. 2: Chaotic attractors: a) Two-dimensional view (x-y) and b) Two-dimensional view (y-x)

(y-x) plans, respectively. It appears that the new chaotic attractor exhibits a very interesting, complex and chaotic dynamical behavior.

Waveform analysis of the proposed chaotic system: In order to investigate the chaotic behavior of the proposed system, the waveform of a chaotic system should be periodic. The waveforms of (x(t), y(t)) in time domain are shown in Fig. 3.

Obviously, the waveforms of (x(t), y(t)) are periodic, multiple periodic motions with complicated and chaotic behavior. Furthermore, we can observed that the time domain waveform has a bounded periodic length random number sequences with abundant shorter seed.

Sensitivity to initial conditions: The most characteristics of a chaotic system represented by its long-term unpredictability (Riecke *et al*., 2007). Significantly, the chaotic system sensitivity dependence on its initial conditions. Sensitivity to initial conditions signify that a little disturbance in the incipient state of the system causes a far conduct of the future state of the chaotic system.

Two different initial conditions, no matter how close, will eventually become widely separated and leads to hurdle estimation of the chaotic system future state. Figure 4 shows that the evolution of the chaos trajectories is very sensitive to initial conditions. The initial values of the system are set to: x (0) = 1.2 , y (0) = 0.8 for the solid line and x (0) = 1.2 , y (0) = 0.8000001 for dotted line.

Parallelism implementation: The most critical issue in chaotic system based cryptography methods is their high

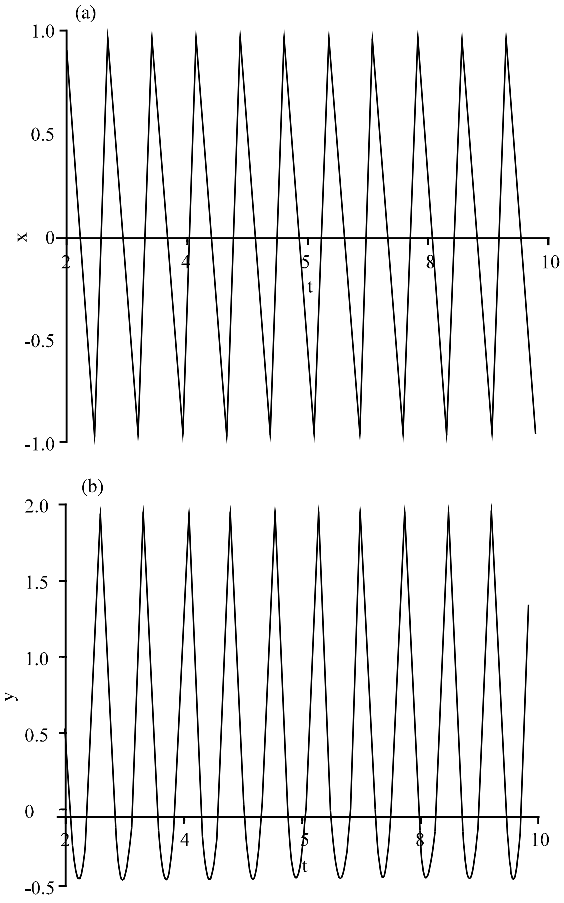

Fig. 3: Time series of variable: a) x with initial conditions (1.2, 0.8) and b) y with initial conditions (1.2, 0.8)

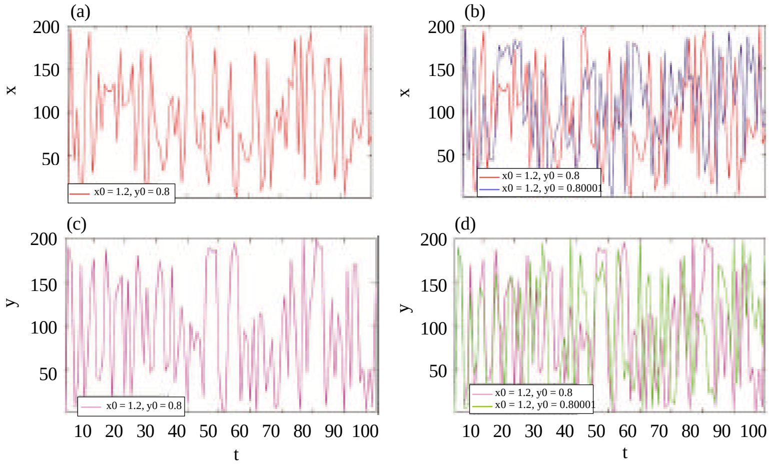

Fig. 4: Sensitivity simulation of: a) x- time series with initial conditions (1.2, 0.8) in solid line and initial conditions (1.2, 0.8000001) in dotted line and b) y-time series with initial conditions (1.2, 0.8) in solid line and initial conditions (1.2, 0.8000001) in dotted line

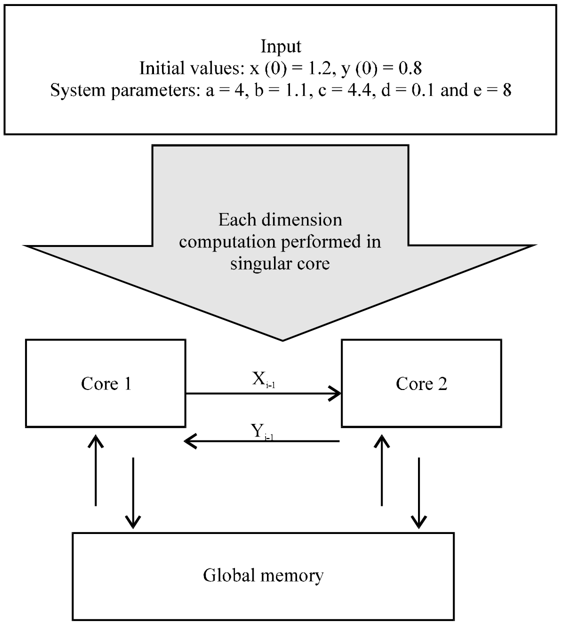
Input
Initial values: x (0) = 1.2, y (0) = 0.8
System parameters: a = 4, b = 1.1, c = 4.4, d = 0.1 and e = 8
Each dimension computation performed in singular core
Core 1
Core 2
X_{i-1}
Y_{i-1}
Global memory

Fig. 5: The parallelism implementation scheme process

implementation time. In the parallel processing manner, the random chaotic map generation is not as modest as the serial case. In this study, a parallel implementation of the proposed chaotic map generation demands different seeds to guaranty reach of variant sequence numbers for each core. The run time of chaotic map generation based on the proposed two dimensional chaotic system is minimized and improved using the parallelism potential of CPU. In order to exploit the parallelism property of CPU, the parallel computing toolbox in MATLAB offer a functional methods to perform the parallel processing of specific task using parallel data processing method (SPMD). As illustrated above the proposed chaotic system generate two instances or two 1D vector (X and Y), therefore, a single program with two different input values on two threads is conducted to manage the parallelism implementation procedure. The labSend() and labReceive() function are also adopted to achieve the values passing process between two workers (threads), since, each value of X and Y is dependent on the previous value represented by Xo and Yo. An illustration of parallelism implementation process is described in Fig. 5.

RESULTS AND DISCUSSION

In this study, a seven term new two-dimensional nonlinear chaotic system is introduced. The dynamical characteristics of the proposed system were analyzed and investigated based on several tools such as maximum Lyapunov exponents, Kaplan-York dimension, time series waveform, phase portraits, sensitivity to initial conditions. The numerical calculations were conducted and simulated in MATLAB 2017. Based on the results, the proposed system is able to produce a wide range of chaotic map numbers x(t), y(t) with precision 10-15. Moreover, a parallel implementation of chaotic map generation process is performed in this study in order to minimize the computation time and programming efforts required for chaotic map generation. We have investigate the speed up of the proposed chaotic system on HB Laptop Intel Core i7, 2.20 GHz with 6.0 GB Ram Running on Microsoft Window 8 using MATLAB 2015 platform. In order to analyze and compare the computation time of the

Table 1: The serial and paralle implemetation time resultes

Cores No.	Iteration	Speedup	Execution time (sec)	Efficiency (%)
1	4,096	1.00	0.007	100
	16,384	1.00	0.020	100
	65,536	1.00	0.054	100
	262144	1.00	0.185	100
2	4,096	1.75	0.004	87.5
	16,384	2.00	0.010	100
	65,536	1.58	0.034	79
	262144	1.83	0.101	91.5

proposed chaotic map generation in serial and parallel manner, the implementation time of serial and parallel manner is stated in Table 1. In addition, the speedup factor and efficiency are calculated for different iterations. The speedup factor represents the ratio between the implementation time required for specific task with one processor and the implementation time required for the same task using N processors:

$$\text{Speedup} = \text{IT}\ (1)/\text{IT}\ (\text{N}) \tag{6}$$

$$\text{Efficiency} = \text{Speedup}*100/\text{N} \tag{7}$$

Where:

IT (1) = The Implementation Time of specific task using one processor

IT (N) = The Implementation Time of the same task using N processor

CONCLUSION

It's worth mentioned and from Table 1, the speedup and efficiency are increased and improved when the parallel implementation scheme is carried out to perform the proposed chaotic map generation. In this way, we can adopt this research to perform image encryption with high speed based on the proposed chaotic map generation.

ACKNOWLEDGMENTS

This researcger was fully confirmed and supported by Al Mustansiriyah University and Computer Science, Department at Collage of Education. The researchers would like to render their thanks for the head of Computer Science Department.

REFERENCES

Alvarez, G. and S. Li, 2006. Some basic cryptographic requirements for chaos-based cryptosystems. Int. J. Bifurcation Chaos, 16: 2129-2151.

Amigo, J.M., L. Kocarev and J. Szczepanski, 2007. Theory and practice of chaotic cryptography. Phys. Lett. A., 366: 211-216.

Andrecut, M. and M.K. Ali, 2001. Robust chaos in a smooth system. Intl. J. Mod. Phys. B., 15: 177-189.

Arroyo, D., J. Diaz and F.B. Rodriguez, 2013. Cryptanalysis of a one round chaos-based substitution permutation network. Signal Process., 93: 1358-1364.

Elhadj, Z. and C.J. Sprott, 2010. The unified chaotic system describing the Lorenz and Chua systems. Electron. Energetics, 23: 345-355.

Elhadj, Z. and J.C. Sprott, 2012. A unified piecewise smooth chaotic mapping that contains the Henon and the Lozi systems. Annu. Rev. Chaos Theor, Bifurcations Dyn. Syst., 1: 50-60.

Li, C., S. Li, M. Asim, J. Nunez and G. Alvarez *et al*., 2009. On the security defects of an image encryption scheme. Image Vision Comput., 27: 1371-1381.

Perez, G., 2004. Robust chaos in polynomial unimodal maps. Intl. J. Bifurcation Chaos, 14: 2431-2437.

Riecke, H., A. Roxin, S. Madruga and S.A. Solla, 2007. Multiple attractors, long chaotic transients and failure in small-world networks of excitable neurons. An Interdiscip. J. Nonlinear Sci., 17: 026110-026110.

Sobhy, M.I. and A.E. Shehata, 2001. Methods of attacking chaotic encryption and countermeasures. Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing (Cat. No.01CH37221), May 7-11, 2001, IEEE, Salt Lake City, UT, USA, ISBN:0-7803-7041-4, pp: 1001-1004.

Wolf, A., J.B. Swift, H.L. Swinney and J.A. Vastano, 1985. Determining lyapunov exponents from a time series. Phys. D. Nonlinear Phenom., 16: 285-317.