Al-Mustansiriyah Journal of Science
ISSN: 1814-635X (print), ISSN:2521-3520 (online) Volume 31, Issue 1, 2020 DOI: http://doi.org/10.23851/mjs.v31i1.734

Research Article Open Access

Key Generation Based on Henon Map and Lorenz System

Ansam Sabah*, Shaymaa Hameed, Maisa'a Abid Ali K.

Department of Computer Science, University of Technology Baghdad, IRAQ.
*Correspondent author ansamsabah357@gmail.com

ArticleInfo

Received
03/09/2019

Accepted
03/11/2019

Published
01/03/2020

ABSTRACT

Securing information has been the most significant process for communication and data store. Orderly to secure information such as data authentication, data integrity, and confidentiality must be verified based on algorithms of cryptography. Where, the most important part of any encryption algorithms is the key which specifies if the system is strong enough or not. The proposal of this paper is a new method to generate keys based on two kinds of chaos theory in order to improve the security of cryptographic algorithms. The base of this proposal is to investigate a new method for generating random numbers by using the 3D Lorenz system and 2D Henon map. The newly generated keys have successfully passed the National Institute of Standards and Technology (NIST) statistical test suite.

KEYWORDS: 2D Henon map; 3D Lorenz system; NIST test suite.

الخلاصة

يعتبر تأمين المعلومات العملية الاكثر أهمية لغرض اتمام التواصل وتخزين المعلومات.من اجل تأمين المعلومات كالتحقق من صحة البيانات وتكامل البيانات وسريتها يتم استخدام خوارزميات التشفير الجزء الاكثر أهمية في أي خوارزمية تشفير هو المفتاح والذي يحدد ما اذا كان النظام قويا كفاية ام لا. نقترح في هذه الورقة طريقة جديدة لإنشاء المفاتيح بالاعتماد على نوعين من نظريات الفوضى من اجل تحسين امن خوارزميات التشفير. اساس هذا الاقتراح هو اكتشاف طريقة جديدة لإنشاء ارقام عشوائية باستخدام خريطة لورنز ثلاثية الابعاد وخريطة هينون ثنائية الابعاد .اجتازت المفاتيح التي تم انشاؤها حديثا بنجاح مجموعة الاختبارات الاحصائية للمعهد الوطني للمعايير والتقنية.

INTRODUCTION

The quantum of information exchanged through the network was increased with the development of communication networks, and the dependence of organizations on these new communication channels has grown dynamically. At the same time, the risks are incremented significantly, so, many technologies like cryptography were developed to overcome these threats[1]. The cryptography uses to secure data, which means a mechanism to protect the data over communication network [2]. In cryptography, there are two kinds of cryptographic algorithms: symmetric and asymmetric cryptography [3]. In symmetric cryptography, the same key is shared between the sender and receiver e.g. Data Encryption Standard (DES) and Advanced Encryption Standards (AES)[4]. While in asymmetric cryptography sender and receiver used different keys to encrypt and decrypt data [3]. the first key, which is called the private key, is kept secret and another one known as the public key is revealed and this removes the need for the sender and the receiver to share key. The only request is that public keys are shared with the users who are authenticated [5]. RSA (Ron Rivest, Adi Shamir, and Leonard Adleman) which is considered as a base to the e-commerce revolution [6], is one of the public key algorithms which is widely used in this context [4].

For a lot of reasons, all these an encryption algorithm typically uses a pseudo-random encryption key generated by a key generation process[7]. Chaotic signal has been much interesting in the past few decades for used it vastly in cryptography. The popularity of chaotic systems depends on the non-predictable behavior and randomness of these systems [8]. The most important feature of the chaotic system is sensitivity to the initial condition; Edward Lorenz is the first researcher who clarifies this property. During a search, he finds out that if the initial conditions in the system of differential equations bit changed that would

completely after the short time change the resulting, and many researchers have been confirming this special feature of chaos[9]. In this paper, a new key generator will be presented based on the 2D Henon map and 3D Lorenz system.

The paper topics can be illustrated as shown below: the chaotic map was briefly introduced in section II. the related work implemented in section III, In the following two sections proposed work, results and discussions were explained. and finally, the conclusions.

CHAOSE SYSTEMS

Chaos is irregular long-term behavior in a deterministic system that exhibits sensible dependence on initial states[10].

Henon Map

the famous two-dimensional Henon map was proposed by H'enon in 1978, as a diminutive approach to study the dynamics of the Lorenz system[11]. The study of the Henon map shows a simple two-dimensional map with quadratic nonlinearity equation. The map gives a first example of the exotic attractor with a fractal structure[12]. which is described as following:

$$x = 1 - ax^2 + by \quad (1)$$

$$y = x \quad (2)$$

Here, the dynamic behavior of the system depends on the values of the parameters, a and b. The system is chaotic when the value of a and b are 1.4 and 0.3 as shown by Figure 1, while x and y are variables [8].

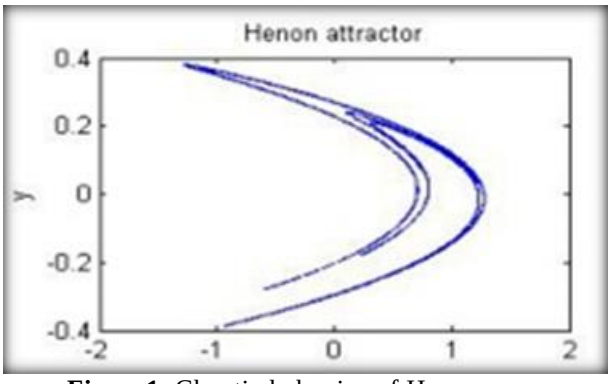

Figure1. Chaotic behavior of Henon map.

Lorenz System

About 1960, Edward Lorenz invented the Lorenz system which is a dynamical system characterized by a nonlinear system of, simple differential equations[14].

$$x' = \sigma(y - x) \quad (3)$$

$$y' = rx - y - xz \quad (4)$$

$$z' = xy - bz \quad (5)$$

σ, **b** and **r** are parameters. the system enters a chaotic scope when Choosing **σ =10**, **r=28**, **b=8/3**. So, given initial values $\mathbf{x_o}$, $\mathbf{y_o}$, and $\mathbf{z_o}$, the system will speedily spread and generate values widely different from a system given only little different values for $\mathbf{x_o}$, $\mathbf{y_o}$, or $\mathbf{z_o}$ [13].

RELATED WORK

In 2018, Ali Kashmar proposed a new method for key stream generator Based on Chebyshev Maps to meet the requirement of image encryption. The output is tested in different measurements; outcomes show that our proposed method is resistant versus security analysis and has good cryptographic strength[9].

In 2017, Ronald Marsh, Scott Kerlin proposed a 'many-key approach' for images using the Lorenz System that combines bit by bit diagonal and anti-diagonal mix of the pixels in an image, using a large key space of 2808 bits for 24-bit color images and 936 bits for gray scale images. However, as shown, a large key length is not sufficient .some form of diffusion can be used to provide high security which provides very secure image encryption [13].

In 2017, Ekhlas Abbas Albahrani, Tayseer Karam proposed a new schema based on a combination of two types of chaotic maps which is 3D Cat map and 3D Henon map to generate keystream .the first step in this method is using 3D Henon map to generating random numbers and converted these numbers to a binary sequence. Then, in the final step permuted and XOR the generated sequence positions by using the 3D Cat map. The outcome of this schema is the goodness of the produced keystream, and a high degree of security versus different attacks, sensibility to the initial values [15].

In 2016, G. Madhuri, I.M.V. Krishna proposed schema to provide efficient and secure key generation uses a non-linear chaos theory approach. The secret keys K1 and K2 have many potential choices that give the image the highest level of security. the master key is with a length of 64 bits binary string. The two-session keys

Al-Mustansiriyah Journal of Science
ISSN: 1814-635X (print), ISSN:2521-3520 (online) Volume 31, Issue 1, 2020 DOI: http://doi.org/10.23851/mjs.v31i1.734

generated from the master key are each 64 bit long, and are processed against versus the input image turned into bit blocks of 64 bits each[16].
In 2013, N. S. Raghava, Ashish Kumar Henon's map with byte sequences and a new approach of pixel shuffling was used to suggest a new symmetric encryption algorithm for image encryption. the suggested method resulting in effective encryption of images[8].

Proposed Key Generation System

In the proposed system, two of chaotic maps are used 2D Henon map and 3D Lorenz system, it will generate a sequence of random numbers between zero and one, these numbers will be processed according to a specific mechanism and generate keys as illustrate in the steps bellow. Figure 2 indicates the generation system method.

Step1: Apply 2D Henon map and 3D Lorenz chaotic system.

For i=1 to 1000

$$\left.\begin{aligned} x &= 1 - ax^2 + y \\ y &= bx \end{aligned}\right\}$$ Henon map

$$\left.\begin{aligned} x' &= \sigma(y - x) \\ y' &= rx - y - xz \\ z' &= xy - bz \end{aligned}\right\}$$ Lorenz system

Step 2: Set the numbers produced by x in string 1, y in string 2, x′ in string 3, y′ in string 4, z′ in string 5.

Step 3: Remove the negative sign.

Step 4: Cut number s after the comma.

Step 5: Convert number to hexadecimal

Step 6: cut substrings of length 4 from each string.

Step 7: scatter numbers by taking the first two digits from each string then the second two digits.

Step 8: divide the result of step6 to sub string of length 32

Step 9: convert result of step7 to binary of length 4.

Step 10: Present key of 128 bit.

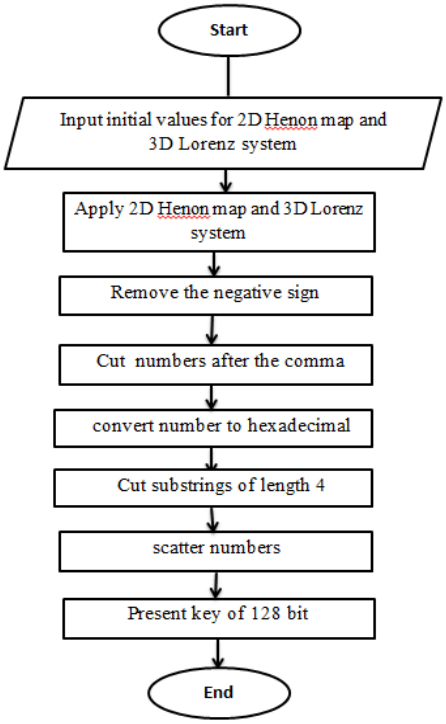

Figure2. Block diagram illustrate Steps of key generation.

Step1: Apply 2D Henon map and 3D Lorenz chaotic system.

Input the initial values and the control parameters values which are a =1.76 and b =0.1 to the Henon map equations and σ =10, r=28, b =8/3 to the Lorenz system equations. The initial values for the Henon map (x0,y0) and Lorenz system ($x0$,$y0$,$z0$) are floating-point numbers with a range of [0-1].

The output of this step is floating numbers. In **step2** set, the numbers produced by x in string 1, y in string 2, x′ in string 3, y′ in string 4, z′ in string 5. and **step 3** remove the negative sign, Figure 3 represents a sample of 20 iterations, the first three columns are for the Lorenz system and the second two-column is for the Henon map.

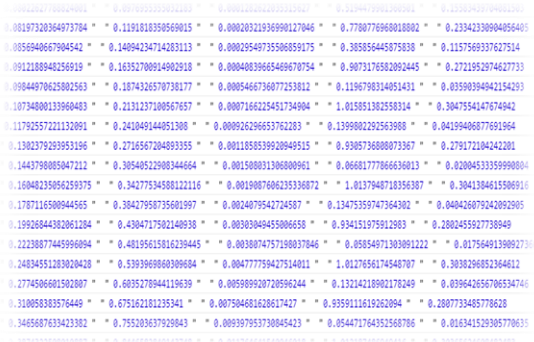

Figure3. The output of Henon map and Lorenz system.

Step 4: Cut number s after the comma.
Cut numbers after the comma and take only float numbers, as shown in Figure 4 then convert numbers to hexadecimal in **step 5** while, In **step 6** take only substrings of length 4 from each string to obtain high randomness, as shown in Figure 4 and Figure 5.

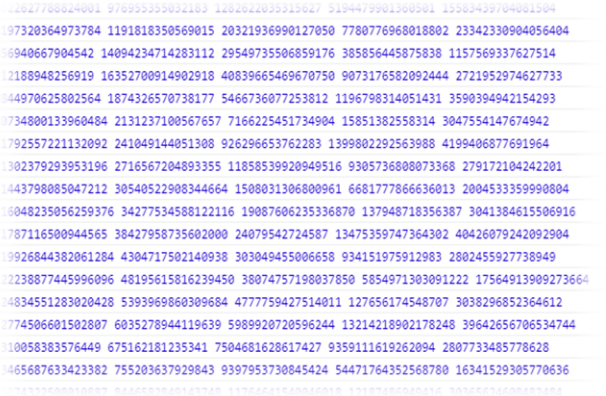

Figure4. The float numbers.

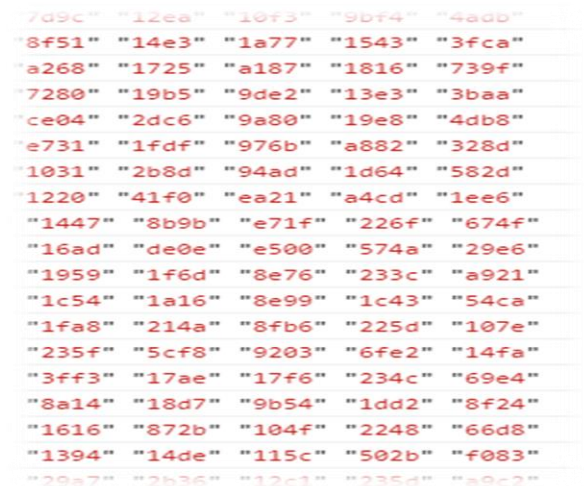

Figure5. The four digits random numbers.

Step 7: Scatter Numbers
This step is worked for scattered the numbers to arrive high randomness for key generated by cutting the first two digits from x0, y0, z0 (Lorenz system) and x0, y0 (Henon map) save the result in array. Then, considering the second two digits are proposed and so on until the end of iterations, as shown in Figure 6.

Step 8: divide the result of step6 to sub string of length 32
Each substring then will convert to binary in **step 9.**

Performance and Security Analysis

In order to analyze the performance and measure the degree of security of our proposal, some cryptographic tests must be applied such as randomness tests.

Figure6. Scattered the numbers.

Statistical Analysis

The output should offer a high degree of randomness, whatever the initial values. So, statistical analysis should be assortment to show the nature and quality of the binary sequences.

Randomness test

Randomness test is done on binary sequences and applied through statistical tests suite NIST [8]. The result from step 3 was converted to binary sequences. 1000 of various binary sequences each of which has length 128bits was passed through the NIST test. NIST consists of 5 tests which are frequency-test, run-test, poker-test, serial-test, auto-correlation test. Each test has a p-value which is compared to fixed significance level α. If the p-value ≤ α, the test is passed otherwise it is failing. The result of a statistical test is illustrated in Table 1.

Table 1: Five test's result of(128 bits) key space

Tests		Freedom Degree	State
Frequency Test		<= 3.84	Pass =1.531
Run Test	T0	<=13.784	Pass =12.938
	T1	<= 7.531	Pass = 4.188
Poker Test		<=11.1	Pass =4.725
Serial Test		<=7.81	Pass =2.875
Auto Correlation Test	1st Shift	<= 3.84	Pass= 0.638
	2nd Shift		Pass= 3.175
	3rd Shift		Pass= 0.392
	4th Shift		Pass=0.806
	5th Shift		Pass=0.984
	6th Shift		Pass=1.180
	7th Shift		Pass=0.008
	8th Shift		Pass=0.133
	9th Shift		Pass=0.008
	10th Shift		pass=0.034

Al-Mustansiriyah Journal of Science
ISSN: 1814-635X (print), ISSN:2521-3520 (online) Volume 31, Issue 1, 2020 DOI: http://doi.org/10.23851/mjs.v31i1.734

Key space analysis

It's simple: if you want to avoid brute-force attacks and want cipher to be secure, then the proposed system should have enough possible keys (a large enough key space) that an attacker cannot simply try every one of them. Cryptographers are conservative, so they usually specify key space to be more than 2^{128} possible keys (128-bit security). In the proposed system the key space is consist of the Lorenz system parameters(x0, y0, z0) and Henon map parameters(x0, y0). If each of these parameters has a precision of 10^{-16}, the key space size for the Lorenz system will be 2^{192} $((10^{16})^3)$ for initial values. And the key space size for initial values to the Henon map is 2^{128} $((10^{16})^2)$. Finally, the full space of keys is $2^{192}+2^{128}=2^{320}$.

Key sensitivity analyses

To warranty the sensitivity of keys Correlation test is used which is to check the correlation between the generated sequences of keys. Correlation test involves two ways:

The Pearson's correlation coefficient which means calculating the correlation coefficient among each pair of created keys sequences to analyzes the correlation between them. In a sample, it is denoted by $R_{(str,\ str1)}$ and Hence, The formula described below is used to find the Pearson R correlation [15]:

$$R_{(str,str1)} = \frac{\sum_{i=0}^{n-1}(x_i - \bar{x}).(y_i - \bar{y})}{[\sum_{i=0}^{n-1}(x_i - \bar{x})^2]^{1/2} . [\sum_{i=0}^{n-1}(y_i - \bar{y})^2]^{1/2}} \quad (6)$$

str, str1 represent two sequences specified by Str = [x1, . . , xn] and Str1 = [y1, . . , yn].

Where:

$\bar{x} = \sum_{i=0}^{n-1} x_i/n$, $\bar{y} = \sum_{i=0}^{n-1} y_i/n$ represents the mean values of Str and Str1.

Hamming distance is the second method of correlation test to warranty the sensitivity of keys, this way of correlation based on analyzing directly the bits of sequences.by finding the number of different bits between two binary sequences that have the same length M. Thus, for two binary sequences, the Hamming distance is given by:

$$d(s_1^b s_2^b) = \sum_{j=0}^{m-1} (x_j \oplus y_j) \quad (7)$$

where xj , yj are the elements of S_1^b, s_2^b. The binary sequences are truly random when the normal distance is about M/2, who gives an attribution of around 0.50 [17].

With the pseudo-random generator, the sensitivity of keys is an essential element. That's mean, the output must be uncorrelated if a little different happened on initial values. Correlation tests (Pearson's correlation and Hamming distance) are performed to warranty the sensitivity of the key on four binary key sequences K1, K2, K3, K4, which are generated from a little various in initial values. Table 2 illustrates the results of Pearson's correlation coefficients and Hamming distance which explain that the correlation between the generated sequences is little.

Table 2: The results of Pearson's correlation coefficients and Hamming distance.

	Tests	
	Correlation Analysis	**Correlation Analysis**
K1vs k2	0.316395	0.316395
K1vs k3	0.031362	0.031362
K1vs k4	-0.24205	-0.24205
K2vs k3	0.110193	0.110193
K2vs k4	0.317937	0.317937
K3vs k4	0.150229	0.4765625

Speed analysis

The analysis of speed performance is done on a personal computer which characterized by Intel(R) Core(TM) i7 CPU M620@ 2.67 GHz 2.67 GHz. The algorithm is implemented using JavaScript on the Komodo editor. In this analysis, binary sequences of 128-bit lengths are generated and its execution time is calculated. Table 3 shows the performance time in milliseconds.

Table 3: Performance analysis.

Length in Bit	Speed in milliseconds
128 bit	631

CONCLUSIONS

A chaotic keys generator was proposed in this paper based on the 2D Henon map and 3D Lorenz system. The initial conditions (x0,y0) are the input to the 2D Henon chaotic map and (x0, y0, z0) are the input to the 3D Lorenz chaotic system. float numbers are only taken and used only four digits from it. Scattered is used to obtain high randomness by taking the first two digits from these four digits and then the second two digits until the end of numbers.

The proposed system has the ability to generate a large number of key sequences that can be useful in many applications in cryptography. The system has the sensitivity to the initial values (keys), the quality of the produced key sequences and the degree of security versus several attacks.

REFERENCES

[1] Omer K. Jasim Mohammad, Safia Abbas, El-Sayed M. El-Horbaty, Abdel-Badeeh M. Salem," Innovative Method for enhancing Key generation and management in the AES-algorithm", Apr 2015. [CrossRef]

[2] Nikita Somani, Dharmendra Mangal," An Improved RSA Cryptographic System ",International Journal of Computer Applications , Volume 105 – No. 16, November 2014.

[3] Rajan.S.Jamgekar, Geeta Shantanu Joshi," File Encryption and Decryption Using Secure RSA " , International Journal of Emerging Science and Engineering (IJESE), Volume-1, Issue-4, February 2013.

[4] Aayush Chhabra, Srushti Mathur ," Modified RSA Algorithm ",IEEE,2011.

[5] Ravi Shankar Dhakar, Prashant Sharma, Amit Kumar Gupta," Modified RSA Encryption Algorithm (MREA)", IEEE, 2012. [CrossRef]

[6] Avi Kak , "Public-Key Cryptography and the RSA Algorithm", Avinash Kak, Purdue University, February 20, 2019.

[7] Gutha Jaya Krishna, Ravi Vadlamani, Nagesh Bhattu," Key Generation for Plain Text in Stream Cipher via Bi-Objective Evolutionar Computing", Applied Soft Computing, May 2018. [CrossRef]

[8] N. S. Raghava & Ashish Kumar,"Image Encryption Using Henon Chaotic Map With Byte Sequence", International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR), Vol. 3, Issue 5, Dec 2013, pp 11-18.

[9] Ali Kashmar,"Key Generator to Encryption Images Based on Chaotic Maps" November 2018.

[10] "The Lorenz Equations", online, https://www2.physics.ox.ac.uk/sites/default/files/profiles/read/lect6-43147.pdf

[11] Haoran Wen, "A review of the H´enon map and its physical interpretations", Georgia Tech PHYS ,2014.

[12] Zhiliang Zhu, Zhe Lin, Beilei Wang, Hongjuan Liu, Huiyan Jiang ," An encryption algorithm based Logistic and Henon mapping for agricultural images in remote transmission", Proceedings of SPIE - The International Society for Optical Engineering, 2016.

[13] Ronald Marsh and Scott Kerlin," A Many-key Image Encryption Method Using the Lorenz System",2013.

[14] Obaida M. Al-hazaimeh, Mohammad Fawaz Al-Jamal," Image encryption algorithm based on Lorenz chaotic map with dynamic secret keys ", Neural Computing and Applications ,August 2017. [CrossRef]

[15] Ekhlas Abbas Albahrani, Tayseer Karam," A New Key Stream Generator Based on 3D Henon map and 3D Cat map", International Journal of Scientific & Engineering Research, Volume 8, Issue 1, January-2017.

[16] G.Madhuri, (M.Tech), I.M.V.Krishna, M.Tech," Chaotic Maps for Key Generation in Block Cipher for Multimedia Encryption/Decryption" International Journal of Computer Science and Information Technologies, Vol. 7 (6) , 2016, 2476-2480.

[17] M. FRANCOIS, D. DEFOUR," A Pseudo-Random Bit Generator Using Three Chaotic Logistic Maps", hal.archives-ouvertes,February 6, 2013.., How to write Results, NY: Wiesly company, 2003, p. 55.