International Journal of New Technology and Research (IJNTR)
ISSN: 2454-4116, Volume-5, Issue-7, July 2019 Pages 82-85

Hybrid Keys Generated Based on Arnold cat Map and Henon Map

Shaimaa H. Shaker, Noor M. Jaafar

***Abstract*—In encrypted systems with public key, if someone reach to the ability of break the public key, can fully decrypted the message, so the key in any security system is important part to determine the weakness and the strength of the system, this paper aimed to proposed a new way to generate key stream based on a integration between 2D Henon map and 2D Cat map, which also in this paper the main goal after generated was to test the threshold of the hybrid technique.**

***Index Terms*— Hybrid, 2D, Henon, Arnold, Cat map, chaotic, Key.**

I. INTRODUCTION

In technology of electronic communication with increasing the development and the complexity, the cryptography has been needed as vital requirement, the security in the most of system specialties in crypto is depend on generate random key that not guessable highly, one of most famous systems that generate the pseudo- random keys is the chaotic system which has many models types inside it with many type of dimensions, Henon map and Arnold cat map is one of types of the chaos system [1].

2D Henon Map

Random numbers are critical in every aspect of cryptography, we need such numbers to encrypt important data depend on type of systems, Henon map is simplified model of chaotic systems, that has been introduced to be used in cryptology by Michel Hénon [2]. Henon map is a two dimensional discrete-time nonlinear dynamical system. There two fundamental properties in chaotic map that can be done well in Henon map first one is called sensitive dependence on the initial conditions and the second is ergodicity. The two dimensional Henon maps is given in the following equation: [3].

$$x_{k+1} = -\alpha x^2_k + y_k + 1 \quad \ldots.1$$

$$y_{k+1} = \beta x_k \quad \ldots.2$$

Represented by the state equations (x, y) pair is the two dimensional state of the system. The initial point is (x_0, y_0). The variables in state equation are for $\alpha = 1.4$ and $\beta = 0.3$ and where k = 0, 1 ... is the discrete time [4].

Shaimaa H. Shaker, Department of Computer Science, University of Technology, Baghdad, Iraq.

Noor M. Jaafar, Department of Computer Science, Iraqi Commission for Computers and Informatics/ Informatics Institute for postgraduate studies, Baghdad, Iraq

2D Arnold Cat Map

Randomness means being unknown with any certainty. And random numbers are unpredictability in cryptography and no correlation between the samples of numbers in statistics. Arnold cat map is special from chaotic map. That has been discovered by Arnold and Avez which is named after Vladimir Arnold. It is possible to generate a large number of number streams easily by simply changing the initial conditions [5]. This system can be represented like this:

$$(x\ ;\ y) \longrightarrow (x + y;\ x + 2y) \bmod n \quad \ldots.. 3$$

$$x_m = (2x_m + y_m) \bmod n \quad \ldots.. 4$$

$$y_m = (x_m + y_m) \bmod n \quad \ldots.. 5$$

Where (x, y) is pair of two-dimension state, and the initial point is (x_0, y_0). The variables in state equation, where k = 0, 1 ... is the discrete time [6].

Performance Analysis

To measure degree of the security there are a cryptographic test must be implemented and randomization for the output sequences from chaotic system which is called statistical analysis [6].

Statistical Analysis

The output from chaotic system as binary sequence type must have a high degree of randomization and decorrelated from each other even whatever were the initial values. Statistical analysis measures the quality of randomization, and have many types [7].

- **Frequency of occurrence Test (Monobit –Chi Square)**

This test used for calculate if the number of 0's and 1's in s are approximately the same, as would be expected for a random sequence. This test give evaluates for accuracy which one and zero in a string should be the same. All other subsequent tests depend on the report of this test [8].

$$X1=(n_0 - n_1)^2/n \quad \ldots.. 6$$

The chi square statistic, along with the chi square distribution, allow to determine if the data is distributed as right. If the chi square statistic is large enough to reject [9].

- **Serial test (two-bit test)**

The goal of this type of test is to compute the frequency of occurrence for each form of two bits in the whole string. Almost the occurrences of the four forms (00, 01, 10, and 11) of two bits is the same number should be expected for original random string. Let n0 denote the number of 0's, and n1 is 1's in string that have it from frequency test, let n_{00}, n_{01}, n_{10}, n_{11} refer the number of occurrences of 00, 01, 10, 11 in string, respectively, and at end n is total size of string. [10].

The statistic used is

$$X2 = 4/n\text{-}1(n^2_{00}+n^2_{01}+n^2_{10}+n^2_{11}) - 2/n\ (n^2_0+n^2_1) +1 \quad \ldots. 7$$

- **Poker frequency Test**

Which it is used to test three bit where certain digits are repeated in certain sequence of numbers. The steps of poker are the same steps of serial test but with different in number of digit tested. The result is compared with the maximum passing threshold 14.0671.

$$Ps = (d-(d-1) \dots (d-r+1)/ dk) * (k/r) \quad \dots. 8$$

Where p is probability of obsevation , k window = 16, d = number of bit in each pattern category = 3, and r is the three-bit pattern [9].

- **Run Frequency Test**

The objective of this test is to compute the number of sequences of bits that are uninterrupted [10].

$$\Pi = \frac{\sum_j \varepsilon_j}{n} \dots.9$$

Where j number of 1 in the bit stream, and n = the length of bit stream,

$$\Gamma = \frac{2}{\sqrt{n}} \quad \dots.10$$

Where $r(k)$=0, if $\varepsilon_k = \varepsilon_{k+1}$ and r (k) =1 otherwise using this equation

$$v_n(\text{obs}) = \sum_{k=1}^{n-1} r(k) + 1 \qquad \dots. 11$$

At end compute the probability value and compare it with threshold using this equation

$$P - value = erfc\left(\frac{|v_n(obs) - 2n\pi(1-\pi)|}{2\sqrt{2n\pi}\,(1-\pi)}\right) \quad \dots. 12$$

II. RELATED WORK

- **Ekhlas Abbas Albahrani, Tayseer Karam [2017]** proposed a new way for generated key based on Arnold cat map and Henon map, where this method generate random keys, these keys are convert to shape of binary sequences. Which all sequence numbers are pass the NIST statistical test, they are used in security system [6].
- **Erdin c AVARO GLU [2017]:** Generate a random bit stream based on chaotic system for pseudo random generator, where these bits are sensitive for initial conditions, the statistical of randomization is obtain by verified NIST [5].
- **Behrouz Fathi Vajargah, Rahim Asghari [2015]:** In cryptography application the generation of pseudo numbers are required, and chaotic Henon map and other types are helpful and satisfied the requirements, to test the randomization there are two well-known tests are used to approve that the keys are proper in applications of cryptography [2].

III. PROPOSED METHOD

In this proposed method will illustrated the way to generated random keys from hybrid way based on integrated two model of chaotic system (2D Henon map and 2D Arnold Cat map), using equations (1, 2, 3, 4, 5) sequentially which generate a group of highly randomized numbers that unpredictable, with initial values that (0.01, 0.01) for both models and then using logic operation to combine the both results, which are describe in details below as steps,

The Proposed Random Chaotic Key Generator (CKSG)

Step1: Input all initial values for each Henon and Arnold cat maps are X_0 and Y_0, where $X_0[0] = 0.01$ and $Y_0[0] = 0.01$.

Step2: Compute X_n for each Henon and Arnold cat maps, as follow

$X_{n+1} = (2 * X_n + Y_n) \bmod 1$ and $X_{n+1} = 1-(1.4)\, X^2_n + Y_n \bmod 1$ respectively, the results as a double arrays between 0 and 1.

Step3: Compute Y_n for each Henon and Arnold cat maps by using $Y_{n+1} = (Xn + Y_n) \bmod 1$ and $Y_{n+1} = (0.3)\, X_n \bmod 1$ respectively which are double arrays type, the results as double arrays are between 0 and 1.

Step4: Convert double array to byte array for each X and Y that resulted from previous steps to obtain array consist of 1's and 0's.

Step5: reversed the sequence of Y arrays only that resulted from Henon map and Arnold cat map.

Step6: apply XOR operator between X and Y of Arnold cat map and apply also XOR operator between X and Y that resulted from Henon to obtain one Key sequence1 from Arnold cat map and Key sequence2 from Henon map in each iteration.

Step7: Finally, XOR between the two keys, Key sequence1 that resulted from Arnold cat map and Key sequence2 that resulted from Henon map to have Key sequence3 with high randomization.

After generated the proposed key based on hybrid method Arnold cat map and Henon map, which Arnold Cat map model integrates with Henon map model to at end obtains one high random key sequence at a time, the process of testing the randomization is necessity, the testing of key has been entered into four type of statistical test, first test is the frequency test which checks the total numbers of ones in the key stream of bits and also the zeros in the same stream to check if the count number of ones and zeros are approximately the same and finally check it with static threshold to pass or fail the frequency test using equation (6), While the second type was the serial test , which is taken every two bit in each key stream bits and check it if it equal to one of these (00, 01, 10, 11) shapes and compare the result with static threshold to obtain pass or fail as a result for the serial test using equation (7), The third type is the poker test, which has been taken every two bits in key stream bits and check it if it equal to one of these (000, 001, 010, 011,100,101,110,111) shapes and compare the result with static threshold to obtain pass or fail as a result for poker test using equation (8), And the final type is the run frequency, where it divide to three equations which are work sequentially to find a single number compare it with threshold to test the random if it pass or fail the randomization using equations (9,10,11,12). The proposed method that have been mentioned above and all types of test are illustrate in figure (1).

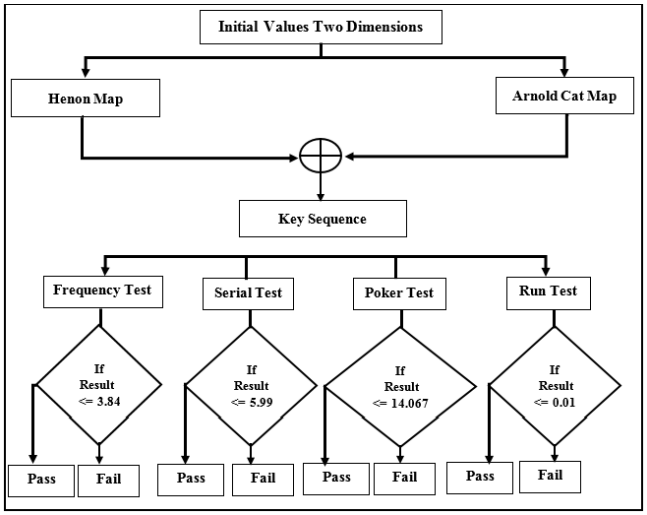
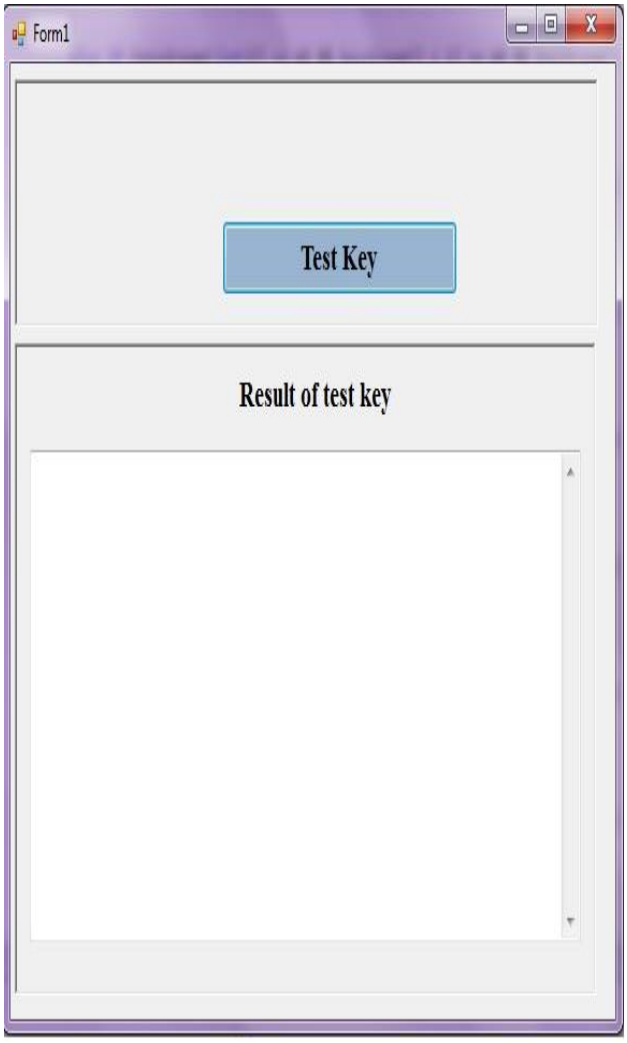
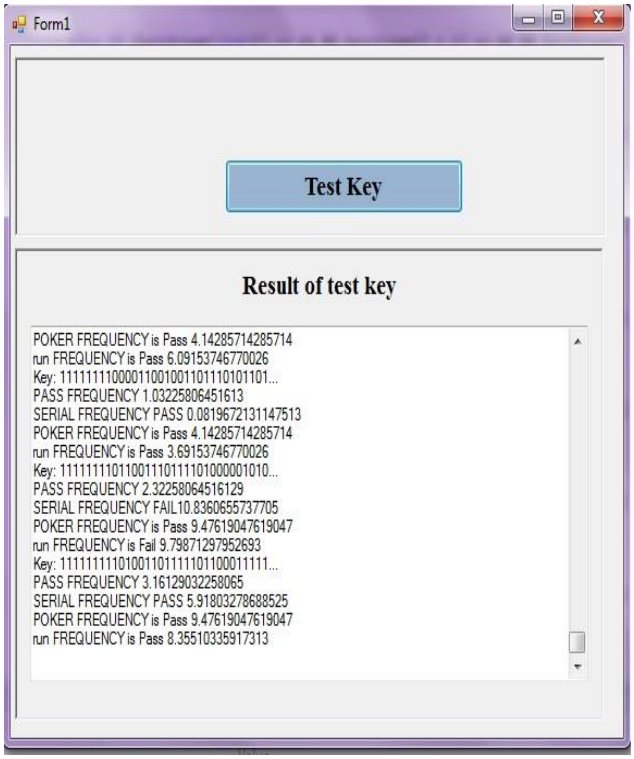


Figure 1: Proposed Method

IV. RESULTS

Here in this section the results of proposed integrate algorithm is illustrating and that for appreciate the efficiency of the proposed algorithm. The test of generated key of proposed are shown in figure (2), with initial parameters X=0.01, Y=0.01 for both models (Arnold cat map, Henon map) and a=1.4 m b=0.3 as initial value also for Henon map





Which all the 1000 keys that have been generated using the proposed algorithm have been passed the four types of statistical test by comparing with the threshold for each type.

V. CONCLUSION

In this paper the initial values and parameters for chaotic system cause very high sensitive to the system that relies on unpredictable and secret key, we used Henon map and Arnold cat map models as hybrid key with unknown way for attacker in integrated, this process helps to made the data more secure from unauthorized people. Which ready to use these key in any encrypted and decrypted algorithms.

REFERENCES

[1] S. Khatarkar, and Rachana Kamble. "A survey and performance analysis of various RSA based encryption techniques." International Journal of Computer Applications, vol. 114, no. 7, 2015.

[2] Vajargah, Behrouz Fathi, and Rahim Asghari. "A pseudo random number generator based on chaotic henon map (CHCG)." International Journal of Mechatronics, Electrical and Computer Technology (IJMEC), vol. 5, no. 15, pp: 2026-37, 2015.

[3] Sun, Fuyan, and Shutang Liu. "Cryptographic pseudo-random sequence from the spatial chaotic map." *Chaos, Solitons & Fractals*, vol. 41, no. 5, pp: 2216-2219, 2009.

[4] *Pranjali Sankhe, Shruti Pimple, Surabhi Singh, Anita Lahane, "An Image Cryptography using Henon Map and Arnold Cat Map", International Research Journal of Engineering and Technology (IRJET), vol. 5, no. 4, 2018.*

[5] Avaroğlu, Erdinc. "Pseudorandom number generator based on Arnold cat map and statistical analysis." *Turkish Journal of Electrical Engineering & Computer Sciences*, vol. 25, no. 1, pp: 633-643, 2017.

[6] Albhrany, Dr EA, and TayseerKaram Alshekly. "A New Key Stream Generator Based on 3D Henon map and 3D Cat map." *International Journal of Scientific & Engineering Research*, vol. 8, no. 1, 2017.

[7] Meligy, Ali M., Hossam Diab, and Marwa S. El-Danaf. "Chaos encryption algorithm using key generation from biometric images." *International Journal of Computer Applications, vol.* 149, no. 11, 2016.

[8] Dragomir, Ioana Roxana. "Statistical assessment of binary sequences generated by cryptographic algoithms." *DEZBATERI SOCIAL ECONOMICE, vol*, 5, no. 2, pp: 23-31, 2016.

[9] Bassham III, Lawrence E., Andrew L. Rukhin, Juan Soto, James R. Nechvatal, Miles E. Smid, Elaine B. Barker, Stefan D. Leigh et al. " a statistical test suite for random and pseudorandom number generators for cryptographic applications.", NIST Special Publication 800-22 Revision 1a (2010).

[10] Abdel-Rehim, Wael MF, Ismail A. Ismail, and Ehab Morsy. "Testing randomness: Implementing poker approaches with hands of four numbers." *International Journal of Computer Science Issues (IJCSI)*, vol. 9, no. 4, pp: 59, 2012.