Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 05, May-2018

Highly Chaotic Random Number Generator Based on Logistic Map

Srishti Gupta
Indira Gandhi Delhi Technical University for Women
New Delhi- 110006

Utkarsha Goswami
Indira Gandhi Delhi Technical University for Women
New Delhi- 110006

Mentor: Neeraj Kohli,
Assistant Professor (Guest),
Indira Gandhi Delhi Technical University For Women
New Delhi- 110006

Abstract: **The uses and applications of random numbers are infinite. Thus it becomes imperative to have good quality random Number Generator (RNG). This paper proposes one such RNG. The simple logistic equation has been used as a basis for the proposed RNG. It has been modified to come up with a generator by adding an extra parameter that produces random numbers which pass the chi-squared test with a good value.**

Index Terms: Random number; Chaos; Security; PRNG; Chi-squared test

I. INTRODUCTION

Random number generators(RNGs) are tools that generate a string, a series of numbers or bits which are random. Any sequence of numbers is said to be random if it satisfies two conditions, first being that each number in the series is equally probable of getting selected and second that it be impossible to predict the next number in the sequence from the previous iterations/previous numbers generated.

RNGs can either be Pseudo Random Number Generator(PRNG) or True Random Number Generator(TRNG). The former uses a predefined formula and an initial seed value to generate random numbers. A change in the seed value will change the series generated, While, the latter taps various naturally occurring physical phenomenon, i.e entropy, to obtain the desired numbers. The advantage of TRNG being non-periodicity, unpredictability, high level of security and no dependencies. The use of TRNG in any security application would be ideal but we still need to use PRNGs because TRNGs are slow and inefficient, cumbersome to install and run, not reproducible, costly and have a possibility of manipulation. PRNGs on the other hand are easy to install and run, aren't as costly as TRNGs and provide a uniform set of values in the domain at a greater speed. PRNGs are designed to have long periods and since the numbers are generated using an algorithm, they are easily reproducible. PRNGs aren't as good as TRNG when it comes to security but still good enough to be used to be used in security applications wherein critical information is involved.

The aim of our paper is to modify the logistic equation given by $X_{n+1} = R * X_n * (1 - X_n)$, where 'R' is initial parameter, such as to generate a series of random numbers for use in applications that do not require very high level of security but need fastly generated random numbers. The problem with chaotic random number generators is that their periods are small for them to be used in any application involving floating points(decimal values). This brings us to the need of introduction of a parameter in the logistic map so as to increase the period length and make it usable in applications.

The desired attributes in an random number generator are uniformity in the domain, independence from previously generated value(s), efficiency to generate numbers as fast the application requires it to be, easily replicable for testing purposes especially with a long cycle length to avoid any repetitions. The evaluation of any random number generator involves the use of many tests defined and improved over time. The tests are designed such that they test for these properties. Any series cannot be surely called a random, just be denied of randomness.

The standard first test being the chi squared test. The aim of the test is to assess the independence of the values generated in the series. It basically checks how well does the actual data fit the expected data. The chi squared value and degree of freedom for the test data are considered to get the p-value for the data. The closer is this value to 1, the better does actual data fit expected data.

II. RANDOM NUMBERS AND CHAOS THEORY

Random numbers and chaos theory have one thing in common, them having high entropy. Chaos theory is the study of nonlinear systems which are dynamical in nature and have high sensitivity to initial conditions. Chaotic phenomena like stock market or our brain states are impossible to be effectively predicted unlike phenomena like gravity or chemical reactions which have a definite and fixed outcome.

Chaos works on principles of butterfly effect which states that a tiny change in initial condition can bring huge change in result, unpredictability such that only knowing of exact initial state can help know the result, feedback, mixing and fractals.

Randomness is the inherent property of chaos. The results are all mixed and chaos ensures that two adjacent points will end up in very different positions after certain time has elapsed but no one knows here. This makes chaos useful in random number generation.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 05, May-2018

III. IMPORTANCE OF RNG

One of the major applications and most important use of random numbers is in the field of secure communication or cryptography. More random be the number generated more better and more secure be the key and thus more be the chances of a safe communication. It therefore becomes essential to develop a good random number generator. Other areas where random numbers are put to use include simulation, modelling, gaming, gambling etc.

Random numbers in simulation help in giving a feeling of reality. Simulation could involve nuclear collision which happens at random space, time and angle. For such an application, a RNG can be required.

Games like Ludo or those involving cards require the rolling of dice and shuffling of cards. RNG of not very great accuracy as also be used at such a place. Random sampling of population or data set to understand it also uses RNG to decide which all data points are to be picked.

Apart from all this, random number generators are used in aesthetic applications like music applications for the shuffle feature or for art or poetry.

IV. CHI-SQUARED TEST

As stated initially, a necessary test for a set of numbers to pass before they are called random is the chi-squared test. It is a simple statistical tool that helps us judge the randomness of the numbers generated by any RNG. This assess the independence in the data produced with respect to the previously generated number(s). After this test is passed, further tests can be applied onto the series generated to understand it and ensure there are no visible patterns.

The χ^2 test first calculates a χ^2 statistic using the formula:

$$X^2 = \sum_{i=1}^{r} \sum_{j=1}^{c} \frac{(O_{i,j} - E_{i,j})^2}{E_{i,j}}.$$

Where:

O_{ij} = actual frequency in the i-th row, j^{th} column

E_{ij} = expected frequency in the i-th row, j^{th} column

r = number or rows

c = number of columns

As can be seen from the formula, χ^2 is always positive or 0, and is 0 only if $O_{ij} = E_{ij}$ for every i,j. A low value of χ^2 is an indicator of independence. CHITEST returns the probability that a value of the χ^2 statistic at least as high as the value calculated by the above formula could have happened by chance.

V. BASIS OF OUR RNG

The simple logistic equation and its modification as proposed by authors Rakesh Kumar Rai and Rakesh Prajapati in their paper titled "Creation of New Chaotic Super RNG for Improving the Security of Chaotic Cryptography" formed the basis for developing our RNG.

The authors, in this paper, modified their RNG by adding an extra parameter to make the previously given logistic map random number generation process more secure. This also helped in passing more tests and getting a better cycle length so that now the chaotic RNG can be used in applications. Simply put, they added an extra parameter named 'b' to the existing logistic map equation to come up with a better RNG. For this, they set the value of parameter 'b' to be 0.5 and computed values for different seeds like 0.1 and 0.2. The initial Logistic Equation is as follows :

$$X_{n+1} = R * X_n * (1 - X_n)$$

(where 'R' is initial parameter)

The modified equation is as follows:

$$f(x_n) = f(x_{n-1}) * b + (x_n - 1) * b$$

(where x_n is the nth number
b is the extra parameter)

We worked on similar lines as this modified equation keeping the format of RNG same as that of a standard logistic equation as mentioned above to develop a new RNG capable of producing random numbers with better cycle length and strong enough to pass the tests.

VI. HIGHLY CHAOTIC RNG

Many modifications to the logistic equation produced series that became stable over time. Some produced output of two numbers alternatively too. All theses were rejected. After many modifications, we came onto a random number generator that when tested against chi squared test produced value of the order of 10^{-7}. This was not sufficient and barely considerable. Further improvement onto the equations led to further improvement of p-value leading us to the order of 10^{-6}. The p-value should be beyond 0.5 to be considered for further tests. With more modifications, the final RNG with a p-value of greater than 0.5 was obtained. The equation for the same is:

$$X_{n+1} = x_n * (1+ x_n) * (1-x_n) * b + x_n * b$$

The above is the mathematical formula used by our RNG to generate random numbers. Here, X_{n+1} is the next number in the series, b is the extra parameter added and X_n is the previously generated number in the series. When the value of b is set to 0.5 and that of X_0 as 0.196, the output is as follows:

0.192235, 0.188683, 0.185325, 0.182142, 0.179121, 0.176247, 0.17351, 0.170898, 0.168402, 0.166015, 0.163727, 0.161532, 0.159425, 0.157399, 0.155449, 0.153571, 0.15176, 0.150012, 0.148325, 0.146693, 0.145115, 0.143587, 0.142107, 0.140672, 0.13928, 0.137929, 0.136617…….

The p-value calculated is 0.894201 which is much greater than 0.5 and thus can be used for applications.

VII. CONCLUSION

There exist various PRNGs that are used in various fields these days. Chaos Theory can be used as a Pseudo Random Number Generator as it provides unpredictability, extreme sensitivity to initial states and good pseudo-randomness. The logistic map forms a basis for many RNG because of its chaotic behavior at value of R>3.5.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 05, May-2018

In our case too, the basic logistic map has been used as equation has been modified to come up with a RNG. The random numbers generated by the proposed RNG perform brilliantly when it comes to chi-squared test. They when tested result in a p-value of 0.894201. The generated numbers satisfy all the parameters that a random number should and thus can be put to use in various applications.

The series is generated using a simple algorithm thus is fast and does not require a very fast processor either. The generator can be written in several different languages because of its simple nature. The values generated can be scaled as per the requirement of the application. The numbers generated are independent of one another and can be reproduced for testing, evaluation and analysis for the strength of the RNG.

VIII. FUTURE WORK

The work can further be enhanced by trying the modified RNGs for various values of input parameters. Testing the same using other tests such as those defined by NIST and die-hard is another extension. Further, the final RNG can be put to use in various applications such as image encryption by understanding certain hyper chaotic systems, Wifis and other security related applications.

REFERENCES

[1] Rakesh Kumar Rai and Rakesh Kumar Prajapati. “Creation of new chaotic super random number generators for improving the security of chaotic cryptography.” International Journal of Engineering Research and Technology, Vol 2, Issue 11 (2013)

[2] Stojanovski, Toni, and Ljupco Kocarev. "Chaos-based random number generators-part I: analysis [cryptography]." IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications 48.3 (2001): 281-288.

[3] Kocarev, Ljupco. "Chaos-based cryptography: a brief overview." IEEE Circuits and Systems Magazine 1.3 (2001): 6-21.

[4] Wong, Wai-kit, Lap-piu Lee, and Kwok-wo Wong. "A modified chaotic cryptographic method." Communications and Multimedia Security Issues of the New Century. Springer US, 2001. 123-126.

[5] Lawande, Q. V., B. R. Ivan, and S. D. Dhodapkar. "Chaos based cryptography: a new approach to secure communications." BARC newsletter 258.258 (2005).

[6] Patidar, Vinod, Krishan K. Sud, and Narendra K. Pareek. "A pseudo random bit generator based on chaotic logistic map and its statistical testing." Informatica 33.4 (2009).

[7] Guyeux, Christophe, Qianxue Wang, and Jacques M. Bahi. "A Pseudo Random Numbers Generator Based on Chaotic Iterations: Application to Watermarking." WISM. 2010.