Pseudo Random Bits Generation Using Chaotic Functions

Mr. Said Juma Said Juma Al Sulti[a], Ms. Ajitha Sajan [b]

The telecommunication development technologies especially mobile and internet networks had extended the demand of information transmission. This results as a challenge to protect the information from the attackers. These require advanced encryption systems to protect the information during transmission. Cryptography is a basic information security measure that encodes messages to make them non-readable. During last two and a half decades, several studies of chaos based on cryptosystems had been developed. An application of discrete chaotic dynamical systems in pseudo random bit generation (PRBG) has been widely studied recently. In each study, proposed a separate pseudo random generation for a particular map running side-by-side in one of them or proposing a hybrid chaotic system used two different maps. The PRBG is generated by combining then comparing the output of both chaotic maps. This report will show the previous studies done in the different ways to generate pseudo random bit. Methods will be discussed in details for the algorithmic formula done for each system and what logical operations done for combination and comparing the output for each.The generated chaotic sequence is implemented for encrypting and decrypting the image and text message

Keywords: PRNG; Logistic Map; Henon Map; Encryption; Decryption; Cryptosystem; and Chaos.

[a] Info Tech & Telecom Security, Al Burkan Engineering LLC – ITTS, Muscat, Sultanate of Oman, said.sulti@gmail.com

[b] Dept. of Electronics and Communication Middle East College, Knowledge Oasis, Muscat, Sultanate of Oman, ajitha@mec.edu.om

I. Introduction

Chaos are important in secured cryptography because of the attractive features of chaotic systems. These systems are consisting of mixing property, structural complexity, deterministic dynamics, diffusion, sensitivity, traditional cryptosystem, algorithmic complexity, multiple access capability, low cross-correlation value, and resistance to jamming (Admin,2016), .

During last three decades; the chaotic systems had many researches to become as an essential topic in communication security/cryptography.

Chaotic systems are considered as a very high secured transmission in communications. The degree of randomness is the main standard for a unique Pseudo Random Bit Generation (PRBG). This paper discusses the following:

- Generate multiple maps with Pseudo Random Bit Generator (PRBG)
- Analyze the suitability between maps used by highlighting statistical properties
- Using the generated chaotic sequence successfully encrypted and decrypted an image and text.

Internet and telecommunication networks became the most common tools every day in everybody's life. Each data transmission if it simple or high sensitive data requires continuous development to improve the transaction of security methods. These require data randomness while transferring from point to point to enhance the security. The researcher came with different results to generate pseudo random numbers in each transaction to achieve the required security in last three decades. The research came with a common study call a Pseudo Random Number Generator (PRNG) as an algorithm operation which generates a sequence numbers with randomness properties.

There are many applications to enable generating or designing chaotic systems. There is an interesting relationship between the existing chaos and the cryptography. The different chaotic systems are designed for the high sensitivity to their conditions and some properties like random behaviors and ergodicity. This sensitivity conditions makes chaotic systems very important for the developments of pseudo-random number/bit generator and cryptographic applications. A rigorous mathematical analysis is necessary to evaluate the level of randomness and the efficiency of the generator while presenting sequences of numbers properties of randomness production.

II. Chaotic random bit generation

Two researchers finalized that to implement PRNG is difficult to be aperiodic or infinite with a precision computer system. The bit depth allocated to each numerical representation inherently limits the quantity of unique numbers. However, this numerical representation limits the seed space for any implementation in PRNG. In the context of finite precision implementations, an ideal PRNG will repeat itself after all seed space element (V. Patidar 2008), .

A new research made for PRNG using algorithm with two chaotic maps to generate multiple key sequences. This uses permutations positions computed based on linear congruence. The functional used with two chaotic maps is XOR to enlarge the complexity of the system and increase difficulty of attackers to extract the secured information as below formulas (R. Kumar 2013), .

A proposed PRBG based on build block of standard maps to run side-by-side to increase the complexity in random bit generation to become difficult for intruder to extract the information (B. Fathi 2015), .

A new PRBG proposed by using two different chaotic functions (Logistic Map & Chebyshev Map). Those used with their mathematical formulas for the randomness enhancement. The NIST testing methods used in the generated sequences with sixteen statistical. It results that the proposed PRBS is random and highly secured (Vimala 2014), .

Algorithm deterministic properties to generate application in pseudo random sequence numbers. It used congruential generator of henon map to generate the cryptographic sequence. It could evaluate independence of number sequences which generated by PRNG in randomness (R. K. J. Persohn 2011), . The main parameters used to implement cryptography are:

- Using unpredictable bits generation
- Bits sequence generation practical and easy
- Large period of key generation

The statistical tests results used correlation test and chi-square goodness-of-fit test. It shows that this implementation has high level of security properties in cryptographic applications (V. Patidar 2009), .

Features used for chaos in deterministic non-linear systems to get randomness behavioral. Also, three types of properties as:

- Density of periodic points
- Topological transitivity
- Sensitive to initial conditions

It used image encryption algorithm based on henon map. The henon map is xored with original pixel value (encryption process). Then, it will be xored again with henon map (decryption process) to get the original image before encryption step (Vimala 2014), .

ASCII stands for American Standard Code for Information Interchange. Due to computers and devices understand the binary or decimal numbers only. It helps to read various types of characters in decimal or binary numbers. Means that, it will convert the characters from their forms to decimal or binary numbers [9].

In ASCII table, can see values of decimal, binary, octal, hexadecimal for each character. It includes all characters used in windows systems exactly in Microsoft word.

III. The Cryptosystem Proposed

By generating a pseudo random bit generation using different ways. Some of them used the same method/map to generate PRNG/PRBG/PRBS and got new stream ciphers. Here will use a hybrid chaotic maps by using Logistic Map and Henon Map to combining them together arithmetically to get the required output. A Lyapunov exponent calculation will be taken to quantify the sensitivity of the system, where 1. Lorenz Attractor System may be used within implementation if found it possible or good to enhance the randomness of the generated bits/numbers.

1) Logistic Map:

It is a polynomial mapping of second order. Its equation is $L_{n+1} = AL_n(1 - L_n)$, where n=0,1,2,… ,$0 \le L \le 1$, and $0 \le A \le 4$

Example to propose PRBG sequence with 2 Logistic Maps, can be generated by comparing the outputs of both maps as the following:
$X_{n+1} = \lambda_1 X_n(1 - X_n)$ and $Y_{n+1} = \lambda_2 Y(1 - Y_n)$

$$g(X_{n+1}, Y_{n+1}) = \begin{cases} 1, if X_{n+1} > Y_{n+1} \\ 0, if X_{n+1} \le Y_{n+1} \end{cases}$$

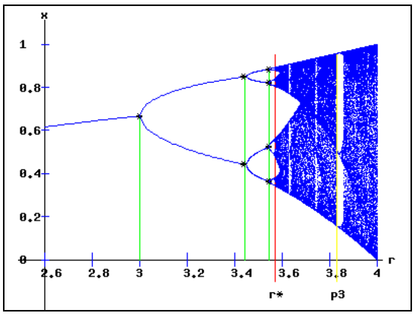


Figure 1 – Bifurcation Diagram for Logistic Map

2) Henon Map:

It is a 2-D iterated map with its equation $\begin{cases} X_{n+1} = 1 - aX_n^2 + Y_n \\ Y_{n+1} = \beta X_n \end{cases}$, where X and Y are the two dimensional state of the system. The plane diagram for a=1.4, and for $\beta = 0.3$.

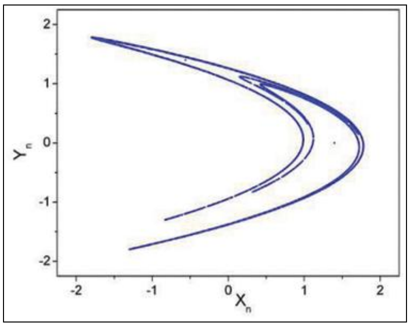


Figure 2 – Chaotic Iteration for Henon Map

An example to generate PRBS for two Henon Maps, it requires mapping functions to state the sequence to (0,1). Initially can consider to bits of b_x and b_y as follows:

$$b_x = \begin{cases} 1 \; if \; x > \tau_x \\ 0 \; if \; x \leq \tau_x \end{cases}$$

$$b_y = \begin{cases} 1 \; if \; y > \tau_y \\ 0 \; if \; y \leq \tau_y \end{cases}$$

IV. System Simulation

Here will show the simulation of image process to be shown as output in MATLAB to do the converting part from decimal to binary as from MSB to LSB to show eight outputs.

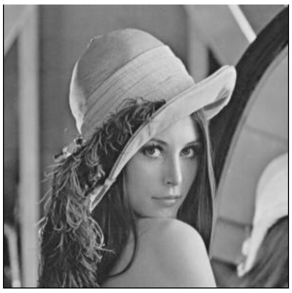


Figure 3 – Original Image1

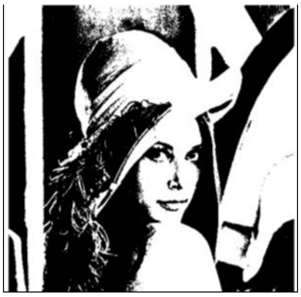


Figure 4 – B1

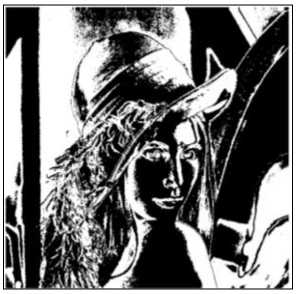


Figure 5 – B2

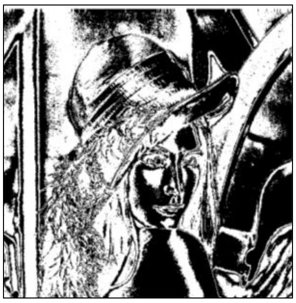


Figure 6 – B3

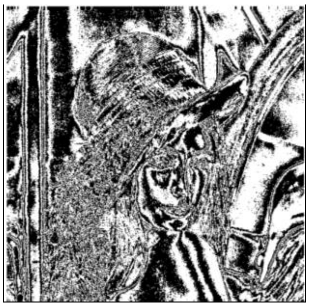


Figure 7 – B4

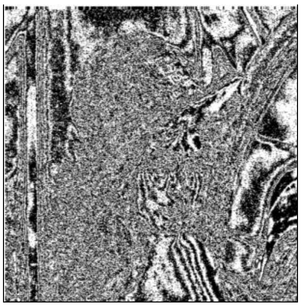


Figure 8 – B5

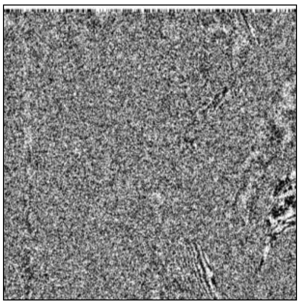


Figure 9 – B6

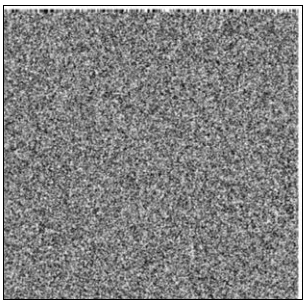


Figure 10 – B7

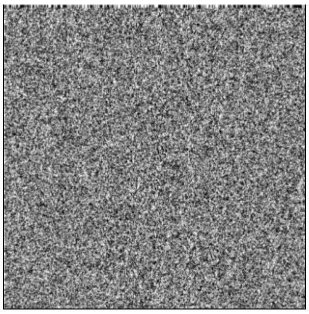
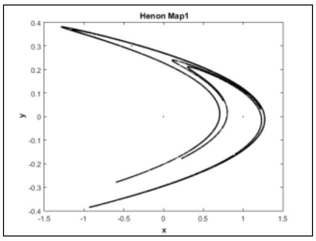


Figure 11 – B8

Meanwhile, here is trying to implement Henon map with the same at same script. Will use two iterations with 10000 and 1000 to see the difference in output.



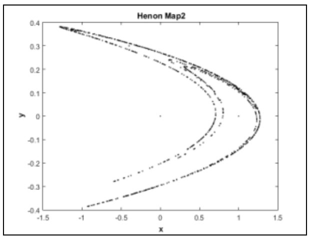
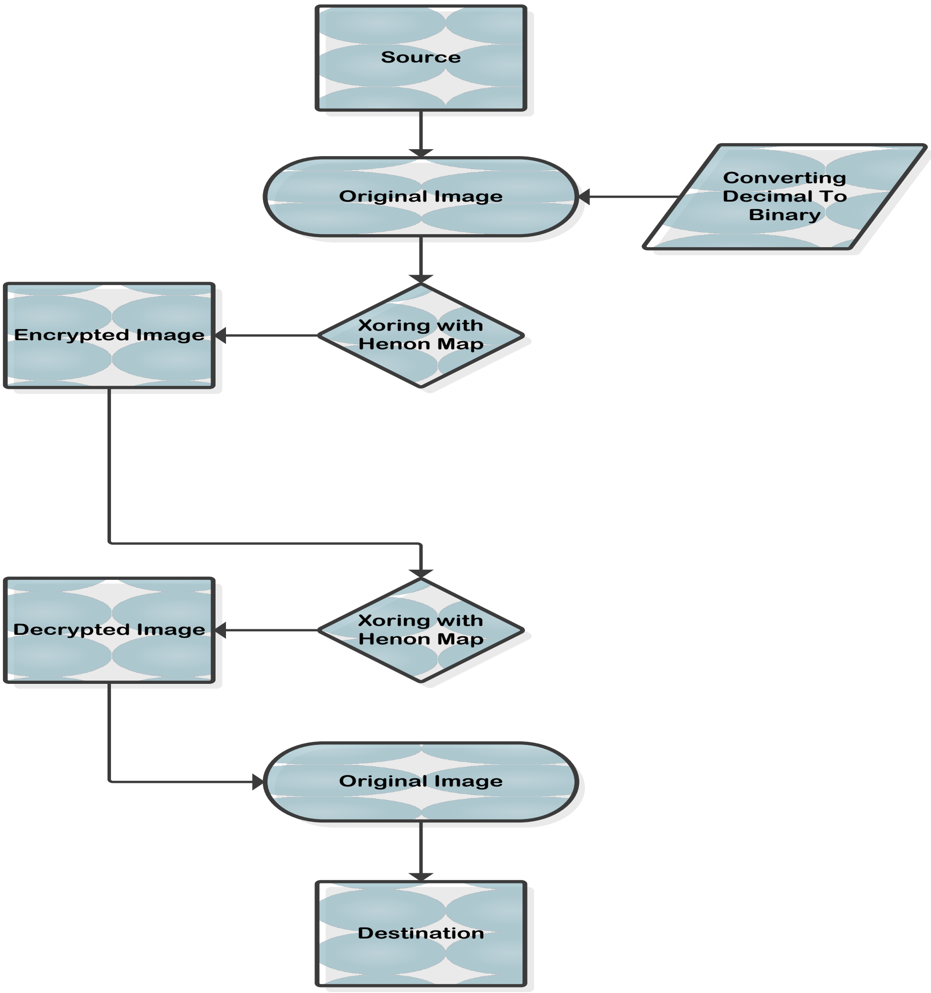


Figure 12 – 10000 Iteration Output

Figure 13 – 1000 Iteration Output

After that, will make the image process with converting from decimal to binary with the henon map. That to be done by combining the image process to be XORED with Henon Map.



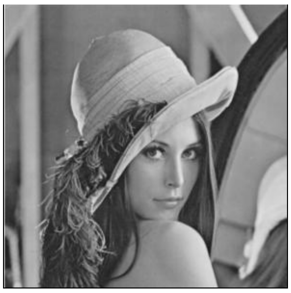


Figure 14 – Original Image2

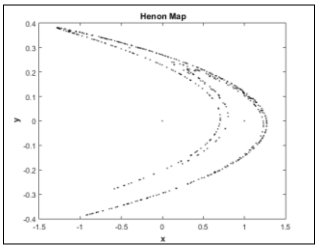


Figure 15 – Iteration Output

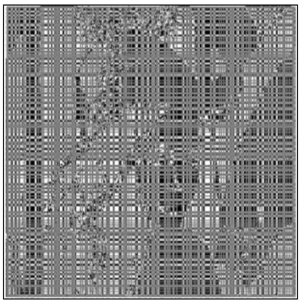


Figure 16 – Encrypted Image

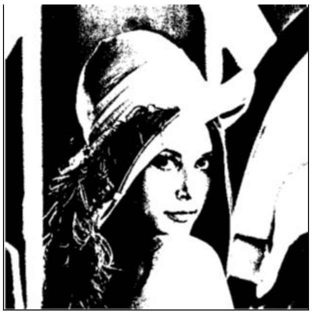
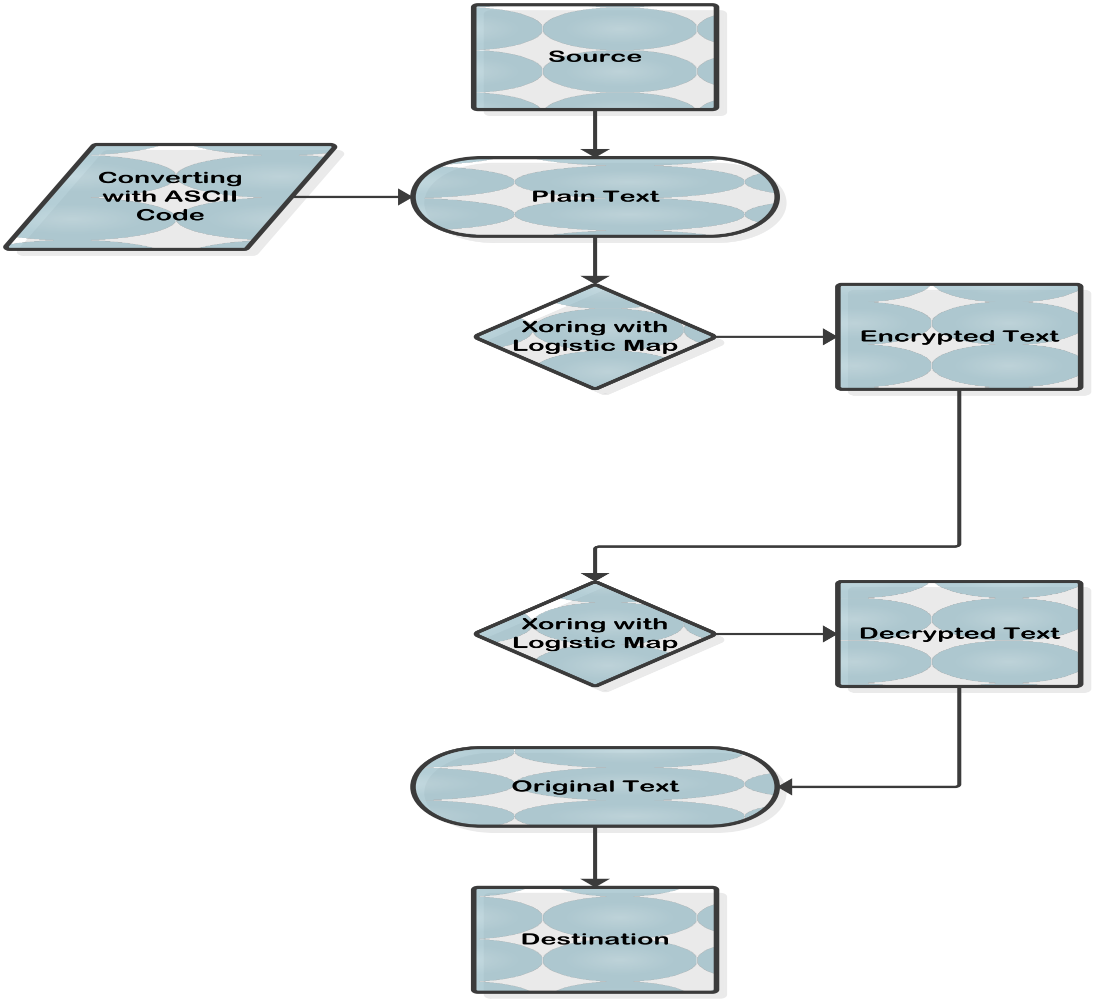


Figure 17 – Decrypted Image

Text process in MATLAB:

In this part, will show the simulation of text process to be shown as output in MATLAB according to the script given.

ASCII chart has values with decimal, hexadecimal, binary, oct, and character. Here, will do the combining of of converting the plain text with ASCII code to be XORED with Logistic Map.



V. System Testing

This paper based in 100% MATLAB works. All algorithms, coding, and converting had done in MATLAB. The strategy followed is to test each step separately and accordance to the output can go to the next process in coding by MATLAB. First trying to complete and get the output required by each map. Then, implement the encryption and decryption of image and text each alone.

Finally, combine the image process with Henon map and text conversion with Logistic map. The test for images has taken much time from test to another. Due to the image process or converting from decimal to binary should take 512 rows into 512 columns. That is why test was taking much time. It caused some delay in project implementation plan, but after giving more effort, could to get it done.

VI. CONCLUSIONS

Here done a study on generation of different chaotic maps to do the encryption and decryption of data, to improve the security sector for sensitive organization.

In this paper, proposed two different chaotic sequences using Logistic Map and Henon Map. The generated sequence is passed for statistical tests for confirming the randomness. With this generated chaotic sequence, successfully implemented encryption and decryption for an image and text data.

The randomness of the chaotic sequence generated in this paper can be enhanced by using scrambling techniques to ensure more security.

Acknowledgment

I would like to express my very great appreciation to my supervisor Miss. Ajitha Sajan for supplying the source of information and resources for this work.

The assistance provided by Miss. Ajitha Sajan for reading and checking the format of this report and guiding throughout the semester was greatly appreciated.

References

Admin (2016), "Matrix Lab," Retrived 22 Dec 2016 from http://www.matrixlab-examples.com/ascii-chart.html. .

B. Fathi(2015), "A Pseudo Random Number Generator Based on Chaotic Henon Map (CHCG)," International Journal of Mechatrinics, vol. 5, p. 10, .

FRANCOIS, (2012) "A New Pseudo-Random Number Generator Based on Two Chaotic Maps,".

R. K. J. Persohn (2011), "Analyzing Logistic Map Pseudorandom Number Generators for Periodicity Induced by Finite Precision Floating-Point Representation," vol. 1, p. 6.

R. Kumar (2013), "New Approach of Color Image Encryption Based on Henon," Journal of Information Engineering and Applications, vol. 3, no. 6, p. 7.

V. Patidar(2008), "Pseudo Random Bit Generator Based on Chaotic Logistic Map and its Statistical Testing,"

V. Patidar 2009), "Novel Pseudo Random Bit Generator Based on Chaotic Standard Map and its Testing," Electronic Journal of Theoretical Physics, no. 20, p. 18.

Vimala (2014), "A New Pseudo Random Bit Generation Based on Hybrid Chaotic Maps," in The 2nd International Conference on Applied Information and Communications Technology, Muscat.