Application of FPTRNG and Logistic Map in Cryptography
Hanaa Mohsin Ahmed
Pages 221 – 226
DOI: http://dx.doi.org/10.21700/ijcis.2016.126

# Application of FPTRNG and Logistic Map in Cryptography

**Hanaa Mohsin Ahmed**
Department of Computer Science
Iraq University of Technology
Baghdad, Iraq
[110113]@uotechnology.edu.iq

**Abstract:** *Recently, chaos theory has appeared as the core of many applications in cryptography, information hiding and forensics. One of these chaotic maps is the logistic map. Usually, the secret key (initial condition and control parameter), must be greater than 214 bytes to avoid any cryptographic attack. However, remembering such a long key proves impractical. An ID-based random number generator is used to generate TRNG or PRNG. In this work, I propose an FPTRNG to be used as the secret key for the logistic map. To address the design need, a symmetric logistic-map-based cryptographic system is implemented using confusion and diffusion. The design is tested with image data types. The experiment analyses the following parameters: key space, key sensitivity, sensitivity, autocorrelation, histograms, information entropy, randomness and execution speed. The results show the effectiveness of the proposed technique for secure image data and applicability to multimedia security.*

**Keywords:** *Cryptosystem Application, Chaos, Logistic Map, FPTRNG, Multimedia Security.*

***Received***: May 01, 2016 | ***Revised***: August 10, 2016 | ***Accepted***: September 10, 2016

## 1. General Introduction

The theory of chaos plays a significant role in modern security systems as a basis for developing cryptography, information hiding and forensics. The purpose of using chaos refers to its basic characteristic settings (random-behaviour, sensitivity to initial conditions and control parameters) to meet the classic Shannon provisions of confusion and diffusion [2]. Many chaotic maps [3–5], their improvements [6–8] and their mixed modes [9–11] have been previously presented, such as logistic map, cat map, uniform map and Arnold map. This work focused on the discrete-time logistic map, which functions as the mathematical core to secret-key encryption algorithms for image data.

Many chaotic cryptosystems [3–11] have been previously suggested in the research literature. These systems can generally be divided into two categories: chaotic block-ciphers and chaotic stream-ciphers. The work by Baptista [12] was one of the earliest attempts to build a block-cipher based on chaotic encryption. In early 1991, a stream-cipher, based on a chaotic map, was presented by Habutsu et al. [13]. Even though several schemes/maps were proposed in earlier work, the logistic map remains one of the simplest maps that is used in many schemes [14].

Several varieties of pseudo random number generators (PRNGs) have been proposed. They are based on different methods [15], including that of the non-linear principle [1]. Non-linear systems theory is applied to cryptography to increase the security level. For this reason, many schemes of chaotic systems are proposed to address the weaknesses of classical encryption algorithms such as DES, AES and RSA. Using the methods of PRNG in chaotic systems can produce high-quality random numbers and good cryptographic characteristics [16–18].

## 2. Contribution

This paper provides the following contributions:

1. Solve the problem of remembering the secret key (initial condition and control parameter) of the logistic map using FPTRNG.
2. Use the logistic map, as the core algorithm for TRNG.
3. Provide non-repudiation, due to the use of FPTRNG as a seed (secret key).

## 3. Logistic Map

The logistic map is one of the simplest chaotic maps, described by [3] $x_{k+1} = \mu x_k(1 - x_k)$, where $0 < \mu \leq 4$.

When $3.5699456 < \mu \leq 4$, the map is in the chaotic state: $x_0 \in (0, 1)$; $k = 0, 1, 2, \ldots l$; and $l$ is the size of the logistic map.

## 4. Proposed Design

In this work, my previously published work on FPTRNG was used to generate a secret key of size $L$, where $L = 128$. Here, we halve the value of $L$, to generate the secret key for the *first* logistic map. Next, we use a parameter such as $K_Z$ and the rest of the value of $L$, to generate the secret key for the *second* logistic map. We use previously found logistic maps as the core of confusion and diffusion, which are ultimately used as the encryption key. The design implementation steps are:

1. Secret-key generation: Apply the FPTRNG algorithm to the advice fingerprint image. Convert the generated 128-bits number into hexadecimal, such as:
   $K_A = \frac{(K_1, K_2, \ldots K_8)}{2^{32}+1}$, $K_B = \frac{(K_9, K_{10}, \ldots K_{16})}{2^{32}+1}$, $K_C \frac{(K_{17}, K_{18}, \ldots K_{24})}{2^{32}+1}$, $K_D = \frac{(K_{25}, K_{26}, \ldots K_{32})}{2^{32}+1}$.
2. Logistic map $Y$: Compute the initial condition and control parameter of logistic map $Y$, such as:
   $a_y = 3.998 + (K_A + K_B) mod (1/1000)$, $y_0 = (K_C + K_D) mod 1$.
   Logistic map $Y$ is iterated $L$ times, where $L$ = size of the input data.
   $x_i^y = \{[x_i^y] * 1000\} mod\ 1$
3. Logistic map $X$: Compute the parameter $K_Z$ such that:
   $S = \{S + [P_i * x^y_{2173-i}] + x^y_{2173-i}\} mod 1$,
   $K_Z = \frac{round(S*254)+1}{255}$.
   Compute the initial condition and control parameter of logistic map $X$, such that:
   $a_x = 3.998 + (K_A + K_B + K_Z) mod 1/1000$, $x_0 = (K_C + K_D + K_Z) mod 1$,
   $3.998 < a_{x,y} < 4$, $0 < x_0, y_0 < 1$.
4. Confusion Process: Compute:
   $Q_i = round(x^x_{2928+i} * 2071) + 1$.
5. Diffusion Process: Compute:
   $F_i = \{(x^x_{2928+i} * 1000) + K_Z\} mod\ 1$.
6. Encryption: Compute the parameters:
   $Y_i = round(M_i \times 255)$,
   $E_i = (P(Q_i) + Y_i) mod 255$.
7. Decryption: Compute: $K_Z = \frac{V}{256}$.
   Repeat steps (1–6), and compute:
   $D_i = (E_i - Y_i) mod 255$

## 5. Results and Discussion

To analyse the encrypted image files, the generated secret key and the original image file, appropriate simulation experiments with MATLAB were used. Analysis of the results for each of the main parameters is provided in the following subsections.

### 5.1 Key Space

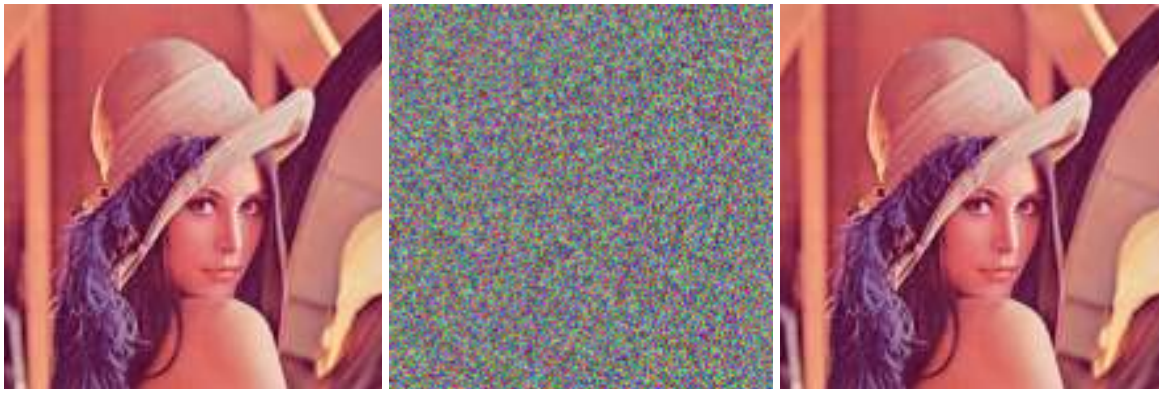
According to [9, 19, 20], an encryption system requires more than a $2^{100}$ strong secret key, which is capable of generating chaotic results to avoid brute-force attacks. In the proposed work, the key space is $[2^{128}]$, due to the used 128-bit secret-key size, in the initialization step.

### 5.2 Key Sensitivity

According to [9, 19, 20], a cryptographic system needs to be very sensitive to small variations in bits of the secret key. In the proposed work, three secret keys were used for analysis of key sensitivity; these keys differed by one bit, as shown in Table 1. Figure 1 presents the original image, the encrypted image and the corresponding decrypted image using the correct key, K3. Figure 2 presents the original image, the decrypted image using the modified key K1 and the decrypted image using the modified key K2. Table 2 presents the Pearson correlations and Hamming distances.

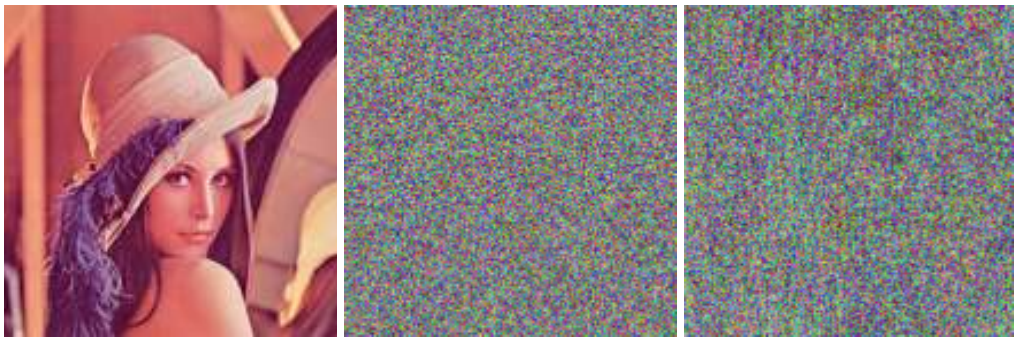
**Table 1:** Three secret keys that differ by one bit.

| Key | Secret Key |
|---|---|
| K1 | 09876543210987654321ABCDEFABCDEF |
| K2 | 0**8**76543210987654321ABCDEFABCDEF |
| K3 | 09876543210987654321ABCDEFA**A**CDEF |



a: Original Lena Image b: Encrypted Lena Image c: Decrypted Lena Image

**Figure 1.** Encryption and decryption using the correct key (K3).



a: Original Lena Image b: Decrypted Lena Image for K1 c: Decrypted Lena Image for K2

**Figure 2.** Decryption using the modified keys (K1 and K2).

**Table 2:** Pearson correlations and Hamming distances.

| Tests | S1/S2 | S1/S3 | S2/S3 |
|---|---|---|---|
| Pearson correlation | –0.00089669 | –0.00104357 | 0.00166226 |
| Hamming distance | 0.500012 | 0.500622 | 0.499150 |

### 5.3 Sensitivity

In general, for any ideal cipher system, the values of NPCR and UACI need be large enough to avoid differential attacks [9, 19, 20]. In this work, Lena plain images, which differed only by a single pixel, were encrypted. The results are shown in Table 3.

**Table 3:** NPCR and UACI values for the Lena image.

| Image name | The point | Old point value | New point value | NPCR (%) | UACI (%) |
|---|---|---|---|---|---|
| Lena Test  | (25, 130) | 45 | 46 | 0.995532 | 0.335993 |
| | (133, 211) | 215 | 216 | 0.995532 | 0.335995 |
| | (212, 150) | 188 | 189 | 0.995532 | 0.336004 |
| | (99, 191) | 10 | 11 | 0.995532 | 0.335996 |
| | (150, 181) | 136 | 137 | 0.995532 | 0.335992 |

### 5.4 Autocorrelation

It is necessary to reduce the correlation between adjacent data to avoid statistical attacks [9, 19, 20]. In the proposed work, the autocorrelations of the plain image (Lena Test image) and the cipher image, for the three channels (RGB) and in the three directions (Horizontal, Vertical and Diagonal), are shown in Table 4.

**Table 4:** Correlation analysis for Lena plain and cipher images

| Image | | Horizontal | Vertical | Diagonal |
|---|---|---|---|---|
| Plain | Red | 0.953121 | 0.929651 | 0.950553 |
| | Green | 0.960022 | 0.918631 | 0.909547 |
| | Blue | 0.982388 | 0.914872 | 0.937024 |
| Cipher | Red | 0.004077 | 0.005119 | 0.005395 |
| | Green | 0.001584 | 0.002328 | 0.003025 |
| | Blue | 0.009923 | 0.009348 | 0.009605 |

### 5.5 Histograms

A histogram is a graphical representation displaying the underlying frequency distribution of a set of continuous data. Usually, to avoid any suspicions the encrypted plain image must display a uniform distribution for its histogram, while the plain image (unencrypted) has its own histogram distribution [9, 19, 20]. In the proposed work, the histograms of the plain and cipher images are shown in Figures 3 and 4, respectively.

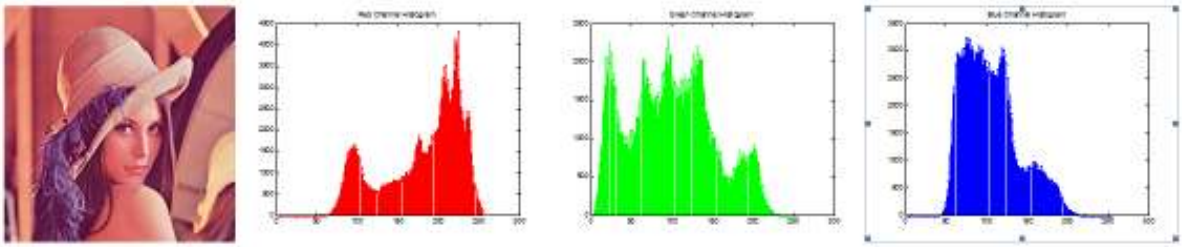


**Figure 3.** The plain Lena image and its corresponding histograms for each channel (RGB).

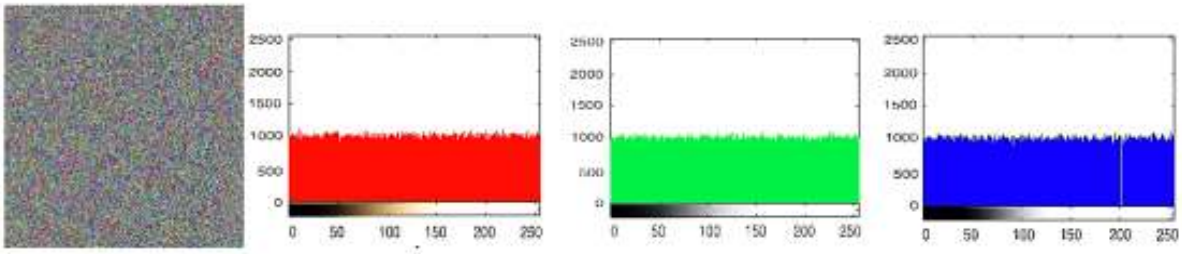


**Figure 4.** The cipher image and its corresponding histograms for each channel (RGB).

### 5.6 Information Entropy

A measure of the unpredictability of a random sequence is known as information entropy, and is given by [9, 19, 20]:

$$H(x) = \sum_{i=1}^{2^N-1} p(x_i)\log_2\left(\frac{1}{p(x_i)}\right) \quad (1)$$

In the proposed work, the plaintext (image) has 256 different symbols. The entropy for the plaintext image is 8, whereas the entropy for the ciphertext image is 7.990245.

### 5.7 Randomness

According to [9, 19, 20], they used randomness tests to determine if the encryption is a good score for randomness or not. The results of these tests used the chi-square distribution table with a significance level of $\alpha$ = 0.05 and a variable degree of freedom. The proposed work, for the Lena encrypted image, used 200 sequences of cipher, with a length of 500,000 bits and 100-bit secret key. The success of these test results is given as:

Frequency = 0.840903
Block Frequency = 0.453430
Runs = 0.890462
Longest Run = 0.631078
Rank = 0.793833
FFT = 0.814489
Non-Overlapping = 0.388411
Serial one = 0.184240
Serial two = 0.699648
Cumulative Sum = 0.061395

### 5.8 Execution Speed

Irrespective of the security concerns, other characteristics of image encryption are also important, such as the execution speed for real-time Internet applications. In this work, a laptop with Intel(R) Core™ i3 CPU with 2 GB RAM running on Windows XP Home was used to compute the execution speed for the proposed encryption/decryption. The average time for encryption/decryption of the colour Lena image, of size 256 × 256 pixels, was measured to be less than 1.7432 seconds.

## 6. Conclusion

A review of earlier work on chaotic encryption-based images revealed the following shortcomings: difficulty remembering the secret key, non-repudiation and TRNG. This work presented an application of cryptography using FPTRNG and the logistic map to overcome these problems. The FPTRNG used a secret key for two logistic maps. A sympatric

cryptographic system with the logistic map algorithm was implemented using confusion and diffusion.

The experimental results indicated that 1. The work can generate very high security levels to resist many attacks, such as statistical attacks, differential attacks and brute-force attacks. 2. According to the cryptographic speed of execution within this work, the proposed method is suitable for image-based Internet applications. 3. FPTRNG solved the problem of remembering the secret key of the logistic map, which also facilitated acquiring TRNG and non-repudiation.

## References


[1] H. M. Salman, "Proposal design: Fingerprint random number generators", the 13th International Arab Conference on Information Technology ACIT, 2012 Dec. 10–13, ISSN: 1812-0857.

[2] S. B. Sadkhan and R. S. Mohammed, "Proposed random unified chaotic map as PRBG for voice encryption in wireless communication", Procedia Computer Science, 2015, pp. 314–323.

[3] W. Liu, K. Sun, and C. Zhu, "A fast image encryption algorithm based on chaotic map", Optics and Lasers in Engineering, vol. 84, September 2016, pp. 26–36.

[4] C. Li, S. Li, M. Asim, J. Nunez, G. Alvarez, and G. Chen, "Image encryption based on the jacobian elliptic maps", Image and Vision Computing, vol. 27, 2009, pp. 1371–1381.

[5] K.-W. Wong, B. S.-H. Kwok, and W.-S. Law, "A fast image encryption scheme based on chaotic standard map", Physics Letters A, vol. 372, no. 15, 2008, pp. 2645–2652.

[6] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps", Chaos, Solitons & Fractals, vol. 21, no. 3, 2004, pp. 749–761.

[7] X. Zhang and Y. Cao, "A novel chaotic map and an improved chaos-based image encryption scheme", The Scientific World Journal, vol. 2014, Article ID 713541, 2014, 8 pages.

[8] A. Soleymani, M. Jan Nordin, and E. Sundararajan, "A chaotic cryptosystem for images based on henon- and Arnold cat map", The Scientific World Journal vol. 2014, Article ID 536930, 2014, 21 pages.

[9] F. J. Luma, H. S. Hilal, and A. Ekhlas, "New dynamical key dependent s-box based on chaotic maps", IOSR Journal of Computer Engineering, vol. 17, no. 4, 2015, pp. 91–101.

[10] E. K. Jabbar, "Video image for security system by using chaotic oscillator", Engineering & Technology Journal, vol. 27, No. 6, 2009.

[11] T. Yang, "A survey of chaotic secure communication systems", Int. J. Comp. Cognition, vol. 2, June 2004, pp. 81–130.

[12] M. S. Baptista, "Cryptography with Chaos", Physics Letters, vol. 240, no. 1–2, 1998, pp. 50–54.

[13] T. Habutsu, Y. Nishio, I. Sasase, and S. Mori, "A secret key cryptosystem by iterating a chaotic map". In: Advances in cryptology-EUROCRYPT'91. Berlin: Springer, 1991, pp. 127–140.

[14] S. Zhang, T. Gao, and G. Sheng, "A joint encryption and reversible data hiding scheme based on integer-DWT and Arnold map permutation", Journal of Applied Mathematics, vol. 2014, Article ID 861782, 2014, 12 pages.

[15] M. Hamdi, R. Rhouma, and S. Belghith, "A very efficient pseudo-random number generator based on chaotic maps and s-box tables". Int J Comput Electr Autom Control Inf Eng, vol. 9, no. 2, 2015, pp. 481–485.

[16] L. Feng and G. Xiaoxing, "A new construction of pseudorandom number generator", Journal of Networks, vol. 9, no. 8, 2014, pp. 2176–2182.

[17] A. Masmoudi, W. Puech, and M.S. Bouhlel, "An efficient PRBG based on chaotic map and Engel continued fractions", Communications and Network, vol. 2, 2010, pp. 1141.

[18] X.-Y. Wang and X. Qin, "A new pseudo-random number generator based on CML and chaotic iteration", International Journal of Nonlinear Dynamics and Chaos in Engineering Systems, vol. 70, no. 2, 2012, pp. 1589–1592.

[19] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems", Int J Bifurcat Chaos, vol. 16, no. 8, 2006, pp. 2129–2151.

[20] C. E. Shannon. Communication theory of secrecy systems, Bell Syst. Tech. J., vol. 28, Oct 1949, pp. 656–715.

**Asst. Prof. Dr. Hanaa Mohsin Ahmed**

Assistant Professor Dr. Hanaa Mohsin Ahmed Salman obtained her MSc and her PhD from the University of Technology Iraq in 2002 and 2006, respectively. Currently she is a lecturer in Computer Science and a member of the Scientific Committee and Promotion Committee in the Department of Computer Science. Dr. Hanaa has more than 23 years of experience and she has supervised graduate students. Her primary research interests include Cryptography, Computer Security, Biometrics, Image Processing and Computer Graphics.