International Journal of Computing Academic Research (IJCAR)
ISSN 2305-9184, Volume 5, Number 4 (August 2016), pp.207-214

http://www.meacse.org/ijcar

A Chaotic Random Bit Generator with Image Encryption Applications

Günyaz Ablay

Abdullah Gül University, Department of Electrical-Electronics Engineering, Kayseri, Turkey

Abstract

Random bit generators find many critical application areas in engineering and science. In this work, coupled robust chaotic maps based random bit generation algorithms are studied for cryptosystems. Some possible coupling approaches are described for the formation of high-dimensional chaotic maps to get a strong mixing nature for use in secure applications. To extract high-quality random bits from the chaotic maps, a post-processing approach is designed. The performances of the chaotic random bit generators are assessed through different statistical methods. The effectiveness of the approaches is validated with an image encryption algorithm.

Keywords: chaos, random bit, image encryption, cryptography

Introduction

Chaotic functions are a very useful building block for many distinct cryptographic structures. Examples include constructing message authentication codes and ensuring security against chosen-plaintext attacks. Their deterministic and aperiodic properties enable a clean and elegant analysis of the cryptosystems. The security of such schemes relies on the parameters and initial conditions of the chaotic systems but not related to the computational bounds or stiffness.

In recent years, chaos based random bit generations have been studied for cryptographic applications because the chaotic systems have cryptographic properties like ergodicity, deterministic dynamics, aperiodicity and sensitivity to initial conditions [1]–[7]. The chaotic random bit generators (RBGs) have a hybrid structure with the features of true and pseudo RBGs and are a good alternative to the conventional methods. A great number of chaotic systems [8]–[12] are available to serve a source for chaotic RBGs for implementation of encryption/decryption algorithms in cryptography. In such applications the discrete maps are preferred because of their convenience for digital realizations and superior performances while both continuous-time and discrete chaotic systems have been utilized [4], [13]. However, it is pointed out that the one-dimensional discrete chaotic maps can suffer from weak security and limited key space in cryptosystems [1], [4]. The security scheme of the chaos based RBGs can be improved with the robust chaotic maps as recommended in the literature [14]–[18]. The usage of high-dimensional chaotic systems, e.g. coupled chaotic maps, is also a very significant way to increase the security of the chaotic RBGs [3], [19], [20]. Another way to improve security features is to benefit from some perturbations, e.g. periodic perturbations, linear feedback shift registers and small noise injection, when constructing chaotic schemes [21]. In this work, weakly coupled and multiplied robust chaotic maps are considered for extending the key space and randomness level of the chaotic RBGs. The main feature of these maps is that they exhibit high-dimensional chaos without any periodic windows for a wide range of parameter variations.

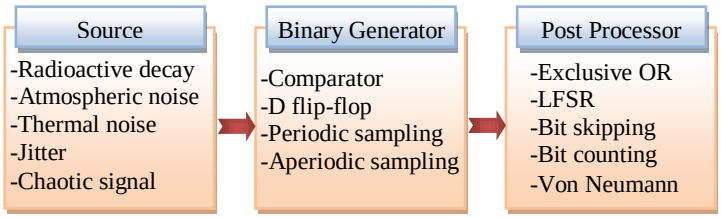


Fig. 1: Random bit generation steps and approaches.

A random bit generator often consists of three stages as demonstrated in Fig. 1 [2]. The first and main stage is the random number source. On the other hand, the binary generator and post-processor stages also have important roles for extracting statistically independent and efficient random bits. The random number sources can be true or pseudo random sources depending on the application. The true random number sources are hardware-based, nondeterministic, aperiodic and taking considerably long time to produce numbers. The pseudo-random numbers are software-based, deterministic, periodic, efficient and suitable for specifically simulation and modeling. Alternatively, in recent years it has been shown that chaotic systems can be a good source for generating random numbers for use in random bit generators. A chaotic RBG carries some features of true and pseudo RBGs since chaotic systems yield aperiodic signals, but produced from deterministic systems. Thus, the chaotic systems can be a good source for random bit generators and related applications of both cryptography and simulation. A wide range of discrete-time and continuous-time chaotic systems may be used as random number sources. As a measure of the randomness, the positive Lyapunov exponents of the chaotic systems determine the entropy of the signals. However, the positive Lyapunov exponent does not provide any indication about unbiased or uncorrelated features of random numbers. Hence, for extracting unbiased and uncorrelated random bits from chaotic sources, a post-processing is needed.

Chaotic Random Bit Generation from Coupled Maps

In general, most of the chaotic systems might be utilized as random number source, but tent map, Chua's circuit, logistic map and Lorenz's attractor have been predominantly used in the literature [2], [21]–[23]. The chaotic systems as random number sources have a very strong effect on the quality of the generated random bits. Even though many chaotic systems can be used for random bit generations, their features affect the complexity of the post-processing steps and throughput efficiency. For these reasons, robust chaotic maps, with a high mixing feature and without any periodic windows, are very good candidates for chaotic random bit generations.

A robust chaotic map can be described by the following equation

$$z_{k+1} = g(z_k, \alpha) \qquad (1)$$

where the system parameter α takes real-values and $g(.)$ is a piecewise function, $g : \mathrm{R} \to \mathrm{R}$. Positive Lyapunov exponents can be used as a measure of the randomness of the chaotic systems. Even so, the positive Lyapunov exponent does not measure bias or correlation level of the chaotic throughput. It is very important to have statistically unbiased and uncorrelated random numbers for cryptosystems. Hence, the coupled chaotic maps are considered in this work. Fig. 3 illustrates the diffusively-coupled chaotic maps based random bit generation scheme. Other types of the coupling is also possible, e.g. cross-coupled chaotic maps (Fig. 2) or two-chaotic maps. The main aim of the coupling is to extract statistically high-quality random bits. For extracting unbiased and uncorrelated random bits from these sources, a comparator is used as binary generator and a de-skewing algorithm consisting of the Von Neumann's technique and the exclusive OR (XOR) approach are used in the post-processing.

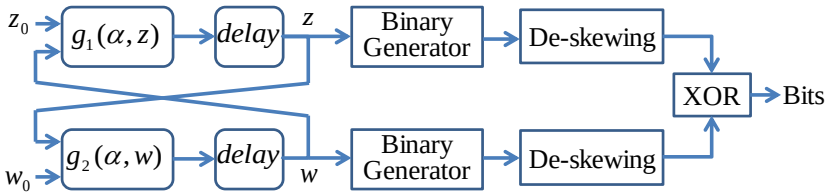


Fig. 2: Cross-coupled chaotic maps and random bit generation.

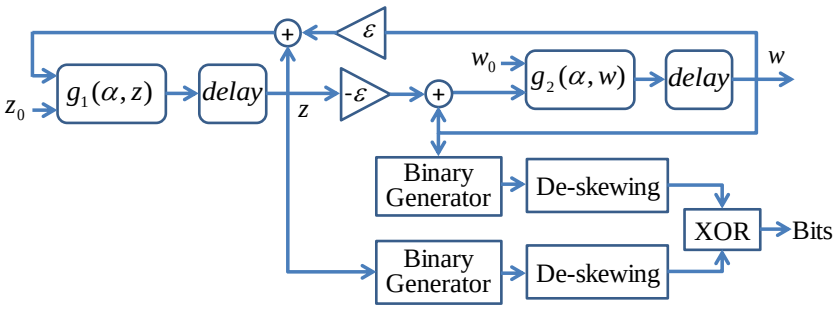


Fig. 3: Weakly-coupled chaotic maps and random bit generation.

The higher-order chaotic systems can be constructed from the different combination of the same or different chaotic systems. For comparison aim, signum map [10], tent map [24] and logistic map [25] are taken into account as sources for chaotic RBGs. First, as illustrated in Fig. 2 consider diffusively-coupled signum maps

$$\begin{cases} z_{k+1} = -\alpha x_k + \mathrm{sgn}(z_k) + \varepsilon w_k \\ w_{k+1} = -\alpha y_k + \mathrm{sgn}(w_k) - \varepsilon z_k \end{cases} \tag{2}$$

where $\varepsilon = 0.001$ and $\alpha = 1.99$. The sgn(.) function is defined by $\mathrm{sgn}(z) = 1$ if $z \geq 1$, $\mathrm{sgn}(z) = -1$ if $z \leq -1$ and $\mathrm{sgn}(z) = 0$ if $z = 0$. Second, as illustrated in Fig. 3 consider a cross-coupled tent maps with $\alpha = 1.99$, $z_0 \neq w_0$,

$$\begin{cases} z_{k+1} = \alpha - 2\alpha \left| w_k - 0.5 \right| \\ w_{k+1} = \alpha - 2\alpha \left| z_k - 0.5 \right| \end{cases} \tag{3}$$

Finally, the coupling method can also be based on the usage of two or more (the same or different) chaotic maps. While it is better to use robust chaotic maps for this algorithm, for comparison aim, two logistic maps can be written as

$$\begin{cases} z_{k+1} = \alpha z_k (1 - z_k) \\ w_{k+1} = \alpha w_k (1 - w_k) \end{cases} \tag{4}$$

where $\alpha = 3.99$, initial conditions are different, $z_0 \neq w_0$ and $z_0, w_0 \in (0,1)$. If the same chaotic maps are used in the algorithm, their initial conditions or parameter values must be different. It is also possible to use two or more dimensional chaotic maps, e.g. Baker's map, or their coupled forms in the chaotic RBGs.

The phase plots of the coupled chaotic maps are shown in Fig. 4. It is seen that the coupled discrete maps have a very nice random distribution in the two-dimensional space.

The usage of comparator or a threshold is a convenient way to generate binary values from the chaotic source signals [26], [27], e.g.,

$$s(z_k) = \begin{cases} 0\ , & if \quad z_k < \rho \\ 1\ , & else \end{cases} \tag{5}$$

The threshold, ρ, can be selected arbitrarily within the chaotic range or average values of the chaotic maps can be used for this aim. It should be noted that for symmetric chaotic systems (e.g., double scroll), multiple thresholds can also be used for each scrolls [23].

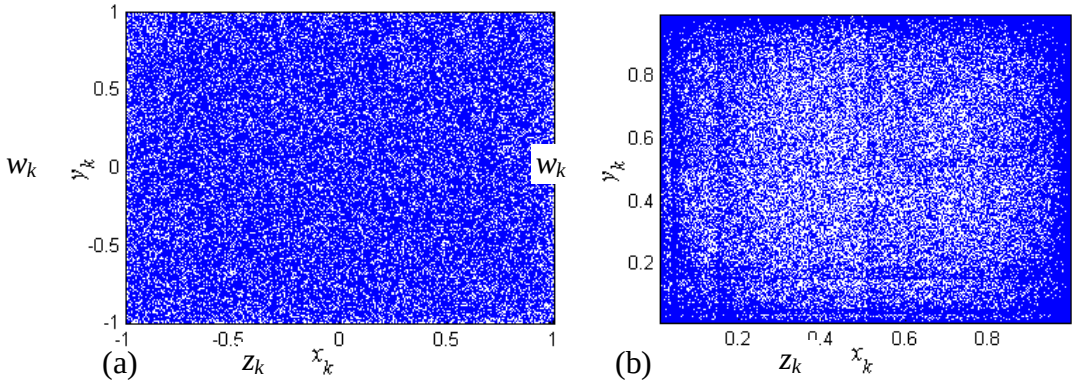


Fig. 4: Phase diagrams (z_k vs w_k) for (a) coupled signum maps and (b) two logistic maps.

It is desirable to have unbiased and uncorrelated random bits especially in cryptographic applications. Since a chaotic source might not provide unbiased and uncorrelated bits as direct output, de-skewing techniques [28] are used to eliminate possible biases and correlations in the output of the chaotic binary sequences. For this purpose, the Von Neumann technique which is one of the most known de-skewing techniques can be used. In this method, to balance the distribution of binary values, the generated binary sequences are grouped into pairs of bits and all pairs 00 and 11 are discarded, and each pair 10 is converted to 1 while each pair 01 is converted to 0. The Von Neumann's technique can easily be integrated into the hardware and it is not decreasing the bit rate too much, i.e., generating about 1 bit from 4 binary sequences. Finally, the XOR logic function is applied between coupled chaotic random outputs to produce the final bit sequence.

The effectiveness of the above chaotic RBG approaches can be analyzed with some statistical tests. The commonly used statistical testing methods including monobit, block (frequency test within a block), runs, discrete Fourier transformation (spectral), autocorrelation, serial, overlapping template matching, cumulative sums and poker tests, are taken into account. The test results for various coupling techniques based random bit generators are shown in Table 1. In terms of the random bit throughput, because of the usage of Von Neumann de-skewing technique, the coupled chaotic maps provide 1.25×10^6 random bits out of 5×10^6 observations, i.e. 25% efficiency. By taking into account the efficiencies and statistical test results given in Table I, it is obvious that the proposed chaotic RBGs provides satisfactory results and can be used in cryptosystems.

Table 1. Statistical test results for the proposed chaotic random bit generators.

Test Name	Coupled logistic maps	Coupled tent maps	Coupled signum maps	Two signum maps
Monobit	7e-7 , success	7.8e-7,success	8e-7 , success	8e-7 , success
Block	0.008, fail	0.195, success	0.226, success	0.382, success
Runs	0.835, success	0.824, success	0.010, success	0.388, success
Spectral (DFT)	0.190, success	0.142, success	0.402, success	0.019, success
Autocorrelation	2.002, success	2.253, success	0.920, success	-0.18, success
Serial	0.003, success	0.000, success	0.000, success	0.000, success
Overlapping	0.896, success	1.000, success	0.963, success	0.995, success
Cusum	1.555, success	1.425, success	1.391, success	1.077, success
Poker	2.624, success	6.851, success	10.44, success	3.911, success

Obviously, the quality of the generated random bits cannot be determined with the statistical tests alone, but we can have an idea about it. In practical applications, application specific randomness analysis tests are needed for the health of the applications.

A significant aspect of the chaotic systems is their "high sensitivity to initial conditions" features. This feature can be used in cryptosystems as well. For example, the initial condition of a chaotic map can be connected with the input devices of the application environment, e.g. mouse movement, port value, thermal noise, etc., and the security and unpredictability of the chaotic RBGs can be assured.

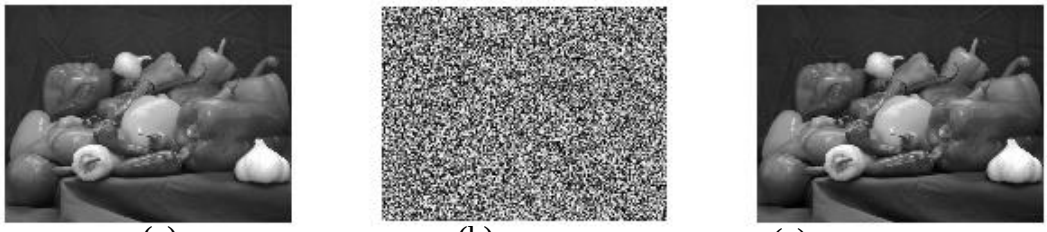
Image Encryption Using the Chaotic Random Bits

The chaotic RBGs described in the above section are applied to an image encryption and decryption scheme. The steps required to accomplish the encryption process are described in Algorithm 1. The algorithm is implemented by using MATLAB. An 8-bit gray scale image with a size of 384x512 pixels are selected. The random bits generated from the coupled maps are used in the encryption scheme and the results are illustrated in Fig. 5. The original image shown in Fig. 5a is encrypted via the chaotic key sequences. After conversion of image pixels and chaotic bits to blocks of 8-bit, the XOR operation is employed between the bit sequences for encryption (as described in [29]). The visual assessment of the cryptosystem is shown in Fig. 5b. It is obvious that the encrypted and original images are completely different and the information about the original image is completely hidden. The decrypted image after employing correct key sequence is illustrated in Fig. 5c, which shoes that the original image is correctly decrypted.

Algorithm 1: Chaotic RBG based image encryption steps

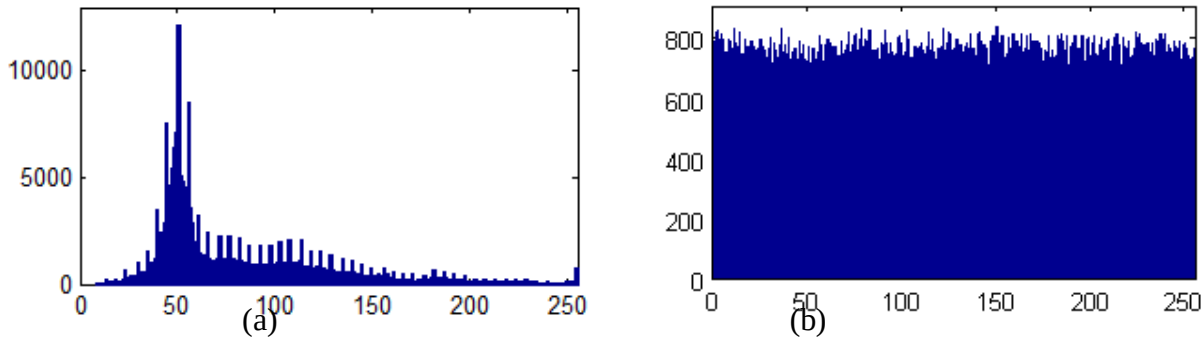
1. Convert KxL pixels of an image into one-dimensional array of pixels M_i, i=1,2,..,n, n=KxL
2. Convert each M_i pixel into m-bit blocks with 2^m shades per pixel
3. Obtain m-bit key vectors from the chaotic random bit sequence
4. Apply bit-by-bit XOR operation between random bits and image bits
5. Repeat XOR operation to encrypt all the image pixels
6. Transform all encrypted digits into KxL pixels to get encrypted image

The performance of the cryptosystem is also evaluated with histogram plots which are one of the most common cryptosystem attacks [30]. It is clear that if the encrypted image's histogram is uniformly distributed, then we can say that the cryptosystem is strong against such attacks. Figure 6 illustrates the histogram of the plain image, and its corresponding encrypted image (Fig. 6b). It is obvious that the histogram of the encrypted image exhibits a uniform distribution and completely different from the image histogram. That is to say, the encrypted image does not reveal any visual information about the original image.



(a) (b) (c)

Fig. 5: Image encryption, (a) original image with size 291x240 pixels, (b) encrypted image, (c) decrypted image.



(a) (b)

Fig. 6: Histogram plots, (a) histogram of the image, (b) histogram of the encrypted image.

Conclusion

In this paper, coupled robust chaotic maps based random bit generators are designed for use in cryptosystems. The coupled robust chaotic maps are able to provide simple, fast and efficient chaos based solutions for practical applications. They do not have any periodic windows in the chaotic regions and produce uniformly distributed random numbers. The output of the coupled maps are converted into random bits with Von Neumann de-skewing and XORing based post-processing to improve the key space and randomness level of the chaotic random bit generators. Statistical tests have been provided to show good statistical properties of the approaches. The efficiency and feasibility of the methods have been validated by an image encryption application. It is shown that the generated chaotic random bits are highly uncorrelated and unbiased, and can easily be implemented for cryptographic applications.

Acknowledgements

This work was supported by Research Fund of the Abdullah Gül University under project number FAB-2015-4.

References

[1] G. Alvarez and S. Li, “Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems,” Int J Bifurc Chaos Appl Sci Eng, vol. 16, no. 8, p. 2129, 2006.

[2] I. Cicek, A. E. Pusane, and G. Dundar, “A novel design method for discrete time chaos based true random number generators,” Integration, the VLSI Journal, vol. 47, no. 1, pp. 38–47, Jan. 2014.

[3] I. Hussain and M. A. Gondal, “An extended image encryption using chaotic coupled map and S-box transformation,” Nonlinear Dyn, vol. 76, no. 2, pp. 1355–1363, Jan. 2014.

[4] L. Kocarev and S. Lian, Chaos-based cryptography theory, algorithms and applications. Berlin: Springer, 2011.

[5] V. Lynnyk, N. Sakamoto, and S. Čelikovský, "Pseudo random number generator based on the generalized Lorenz chaotic system," IFAC-PapersOnLine, vol. 48, no. 18, pp. 257–261, 2015.

[6] A. S. Mansingka, M. Affan Zidan, M. L. Barakat, A. G. Radwan, and K. N. Salama, "Fully digital jerk-based chaotic oscillators for high throughput pseudo-random number generators up to 8.77 Gbits/s," Microelectronics Journal, vol. 44, no. 9, pp. 744–752, Sep. 2013.

[7] M. Park, J. C. Rodgers, and D. P. Lathrop, "True random number generation using CMOS Boolean chaotic oscillator," Microelectronics Journal, vol. 46, no. 12, Part A, pp. 1364–1370, Dec. 2015.

[8] G. Ablay, "Chaos in PID Controlled Nonlinear Systems," Journal of Electrical Engineering and Technology, vol. 10, no. 4, pp. 1843–1850, 2015.

[9] G. Ablay, "Novel chaotic delay systems and electronic circuit solutions," Nonlinear Dyn, vol. 81, no. 4, pp. 1795–1804, May 2015.

[10] G. Ablay, "Chaotic map construction from common nonlinearities and microcontroller implementations," International Journal of Bifurcation and Chaos, vol. to be appear, 2016.

[11] J. C. Sprott, "Simple chaotic systems and circuits," American Journal of Physics, vol. 68, no. 8, pp. 758–763, 2000.

[12] S. H. Strogatz, Nonlinear Dynamics and Chaos: With Applications to Physics, Biology, Chemistry, and Engineering, Second Edition, Second Edition edition. Boulder, CO: Westview Press, 2014.

[13] Q. V. Lawande, B. R. Ivan, and S. D. Dhodapkar, Chaos Based Cryptography: A New Approach to Secure Communications. Bombay: BARC Newsletter, 2005.

[14] S. Banerjee, J. A. Yorke, and C. Grebogi, "Robust Chaos," Physical Review Letters, vol. 80, no. 14, pp. 3049–3052, Apr. 1998.

[15] D. Fournier-Prunaret, P. Chargé, and L. Gardini, "Border collision bifurcations and chaotic sets in a two-dimensional piecewise linear map," Communications in Nonlinear Science and Numerical Simulation, vol. 16, no. 2, pp. 916–927, Feb. 2011.

[16] A. Kanso and N. Smaoui, "Irregularly decimated chaotic map(s) for binary digits generations," Int. J. Bifurcation Chaos, vol. 19, no. 04, pp. 1169–1183, Apr. 2009.

[17] H. Liu and X. Wang, "Color image encryption based on one-time keys and robust chaotic maps," Computers & Mathematics with Applications, vol. 59, no. 10, pp. 3320–3327, May 2010.

[18] D. J. W. Simpson, "On the relative coexistence of fixed points and period-two solutions near border-collision bifurcations," Applied Mathematics Letters, vol. 38, pp. 162–167, Dec. 2014.

[19] N. Romero, J. Silva, and R. Vivas, "On a coupled logistic map with large strength," Journal of Mathematical Analysis and Applications, vol. 415, no. 1, pp. 346–357, Jul. 2014.

[20] X. Wang and X. Bao, "A novel block cryptosystem based on the coupled chaotic map lattice," Nonlinear Dyn, vol. 72, no. 4, pp. 707–715, Jan. 2013.

[21] İ. Öztürk and R. Kılıç, "A novel method for producing pseudo random numbers from differential equation-based chaotic systems," Nonlinear Dyn, vol. 80, no. 3, pp. 1147–1157, Feb. 2015.

[22] K. K. S. V. Patidar, "A pseudo random generator based on chaotic logistic map and its statistical testing. Informatica," Informatica, vol. 33, no. 4, pp. 441–452, 2009.

[23] M. E. Yalcin, J. A. K. Suykens, and J. Vandewalle, "True random bit generation from a double-scroll attractor," IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 51, no. 7, pp. 1395–1404, 2004.

[24] A. S. Lima, I. C. Moreira, and A. M. Serra, "Transition between the tent map and the Bernoulli shift," Physics Letters A, vol. 190, no. 5–6, pp. 403–406, Aug. 1994.

[25] A. G. Radwan, "On some generalized discrete logistic maps," Journal of Advanced Research, vol. 4, no. 2, pp. 163–171, Mar. 2013.

[26] Z. Hong and L. Xieting, "Generating Chaotic Secure Sequences with Desired Statistical Properties and High Security," Int. J. Bifurcation Chaos, vol. 07, no. 01, pp. 205–213, Jan. 1997.

[27] T. Kohda and A. Tsuneda, "Statistics of chaotic binary sequences," IEEE Transactions on Information Theory, vol. 43, no. 1, pp. 104–112, Jan. 1997.

[28] W. Stallings, Cryptography and Network Security: Principles and Practice. Prentice Hall, 2006.

[29] S. Rohith, K. N. H. Bhat, and A. N. Sharma, "Image encryption and decryption using chaotic key sequence generated by sequence of logistic map and sequence of states of Linear Feedback Shift Register," in 2014 International Conference on Advances in Electronics, Computers and Communications (ICAECC), 2014, pp. 1–6.

[30] M. Farajallah, S. El Assad, and O. Deforges, "Fast and secure chaos-based cryptosystem for images," International Journal of Bifurcation and Chaos, vol. 26, no. 02, pp. 1650021.1–1650021.21, Feb. 2016.