Military Technical College
Kobry El-Kobbah,
Cairo, Egypt

11th International Conference
on Electrical Engineering
ICEENG 2018

A New Adaptive Chaotic Key Generator

Elsayed A. Soleit*

ABSTRACT

The chaotic generation is of great interest in Encryption/Decryption process. It is increasingly applied in Key generation that is used for encryption/decryption of plain text data before transmission to the required destination. The chaos pattern is first generated as phenomena of nonlinear unstable analog circuit. The problem is limited word length size of the key generated (small key space) which has low brittle force and it is susceptible to key estimation and as a result weak security.
In this paper a new algorithm of adaptive digital chaotic generator is proposed and keys blocks of different length are produced. The randomness of the generated key sequences is tested and evaluated for different initial conditions and different learning periods. The results are encouraged.

KEY WORDS

Adaptive Digital Chaotic Key Generator, Encryption/Decryption, Auto regressive, Adaptive algorithm, LMS adaptation algorithm and chaos pattern.

1. Introduction

Chaos is a ubiquitous nonlinear phenomenon. It is an attractive area of interest research. It is more exotic form of steady state response. A chaotic system is considered a deterministic system that exhibits random behaviors (strange behaviors). The encryption/ decryption algorithms are of great interest to secure the messages (voice, data, images and video signals) transmission/reception through the communication channels and computer networks.
The encryption/decryption algorithms are mainly based on the secret keys which are used to encrypt/decrypt the message before transmission and after reception via the communication media. The stronger the keys, the stronger of the encryption algorithms to be broken and detected by the attackers. The difficulties to decrypt the encryption algorithms depend on the Keys complexity and the time taken to estimate and predict the Keys. The encryption Keys are dependent on the type of messages to be encrypted and the encryption algorithms.

* Professor, Vice Dean for education and student affairs, Head of Electrical Eng.Dept
Higher Institute for Engineering and technology Al- Obour

A new adaptive chaotic Key generation is introduced in this paper. The New algorithm is based on the implication of the adaptive auto- recursive (AR) digital filtering techniques. The proposed algorithm passes the randomness test and it can be changed and handed in secured manners easily.

The chaos dynamical system can be defined as nonlinear system that is highly sensitive to initial conditions. These systems may be deterministic or stochastic systems. Deterministic systems mean that their future behavior is fully determined by their initial conditions, with no random elements involved. In other words, the deterministic nature of these systems does not make them predictable. This behavior is known as deterministic chaos, or simply chaos [1-15].

This paper includes six sections. Section two presents a digital chaotic generator. The adaptive chaotic generator is proposed in section three. Section four highlights the simulation performance of both the fixed coefficient digital chaotic key generator and the adaptive coefficient chaotic key one. The section five focuses on the valuable conclusions and points out to the future prospections in this field.

2. Digital Chaotic Key Generator

The digital chaotic Key generator is depicted in Fig. 1. It is represented by an n-dimensional auto-regressive (AR) filter followed by two's complement overflow. The output signal can be expressed as [5-6]:

$$y_k = z_k + \sum_{i=1}^{N} c_i y_{k-i} \qquad (1)$$

Where the input signal, z_k is considered a uniform random signal $\in (0,1)$.

$\{c_i\}$ and $\{y_{k-i}\}$ are defined respectively as the filter coefficients and the preceding outputs. The two's complement overflow nonlinearity function can be defined as:

$$\mathrm{mod}(y) = y - 2.\left\lfloor \frac{y+1}{2} \right\rfloor \qquad (2)$$

The input/output model of the digital chaotic encoder can be described by:

$$y_k = \mathrm{mod}(z_k + \sum_{i=1}^{N} c_i y_{k-i}),\, y_i \in I = (-1,1\ ) \qquad (3)$$

3. Adaptive Chaotic Key Generator

The fixed coefficients digital encoder/decoder defined by eqn. (1), can be updated adaptively using the LMS adaptation algorithm. Fig. 2. Illustrates the adaptive digital chaotic key generator. The coefficients $\{c_i\}$ are considered time varying and updated such that the mean square of the error (MSE) is minimized. The coefficients are initially set equal to zeros [6-8].

The output signal of the digital encoder in eq.(1) can be expressed in matrix notation as:

$$y_k = z_k + \alpha_k^T \beta_k \qquad (4)$$

Where the coefficients vector is defined as:

$$\alpha_k^T = [c_{1,k}, c_{2,k}, \ldots\ldots\ldots\ldots, c_{N,k}] \qquad (5)$$

and the observation vector can be expressed by:

$$\beta_k^T = [y_{k-1}, y_{k-2}, \ldots\ldots\ldots\ldots, y_{k-N}] \qquad (6)$$

The error signal is defined as:

$$\varepsilon_k = z_k - y_k \qquad (7)$$

The coefficient vector α_k is updated such that the mean square of the error signal defined in (7) is minimized. Hence the filter coefficient vector is updated as:

$$\alpha_{k+1} = \alpha_k - \mu \frac{\partial \varepsilon_k^2}{\partial C_k} \qquad (8)$$

Substituting eq. (7) in eq.(8) yields:

$$\alpha_{k+1} = \alpha_k + 2\mu \varepsilon_k \beta_k \qquad (9)$$

At the end of the learning period, the filter coefficients converge to the optimal values and the output signal, y_k is considered chaotic random signals and are used as key generations. The randomness of the Key generation is tested and compared with those are generated from the fixed coefficients AR filter.

4. Performance Results

The chaotic digital key generator depicted in Fig.1 is implemented via computer simulation using the MATLAB program. The AR filter coefficients values are considered time invariant and are fixed during the simulation. An AR digital filter is implemented with three fixed coefficients (c1=2.2,c2=3.5 and c3=2.0). The output sequences $\{y_k\}$ of the fixed coefficients chaotic Key generator are displayed versus time as shown in Fig.3. These outputs represent the chaotic Keys. Moreover, the output sequences $\{y_k\}$ are plotted versus the past output sequences $\{y_{k-1}\}$ as depicted in Fig.4. It is apparent that the output sequences seem to be in chaotic states [14].

Moreover, the adaptive chaotic key generator depicted in Fig.2 is implemented using the MATLAB program. The adaptive AR filter is implemented with three coefficients.

The coefficient values are set initially equal to zeros. The LMS adaptation algorithm defined in eqn. (9) is used to update the filter coefficients. Furthermore, the output sequences, $\{y_k\}$ are measured after a certain adaptation time, T that is called the convergence time of the adaptation algorithm (It is equal to 500 samples in this simulation). Also, the output sequences, $\{y_k\}$ are displayed versus time as shown in Fig.5. These output sequences represent the chaotic Keys. The output sequences, $\{y_k\}$ of the adaptive key generator are displayed versus the past output sequences, $\{y_{k-1}\}$ as depicted in Fig.6. It is obvious that the output sequences appear in chaotic states.

Furthermore, the randomness of the output sequences of both the fixed digital key generator and the adaptive key one are measured, tested as shown in Table 1. It is clear that the output sequences of both the key generators pass the Hypothesis Test. Also, the statistical parameters of the output sequences, for both the fixed coefficients digital Key generator and adaptive chaotic Key one are compared and listed in Table-1 [9-15].

5. Conclusion

The chaotic system is so sensitive and is dependent on the initial conditions. An adaptive chaotic key generator is proposed to obtain variable lengths keys. The keys pass the randomness Hypothesis test. The statistical parameters of the adaptive chaotic key generator is equivalent to those of the time invariant chaotic key generator. The proposed adaptive key generator is attractive and can be applied in encryption/decryption processes for its simplicity, security and ease in handling between the sender and the destination.

Figures

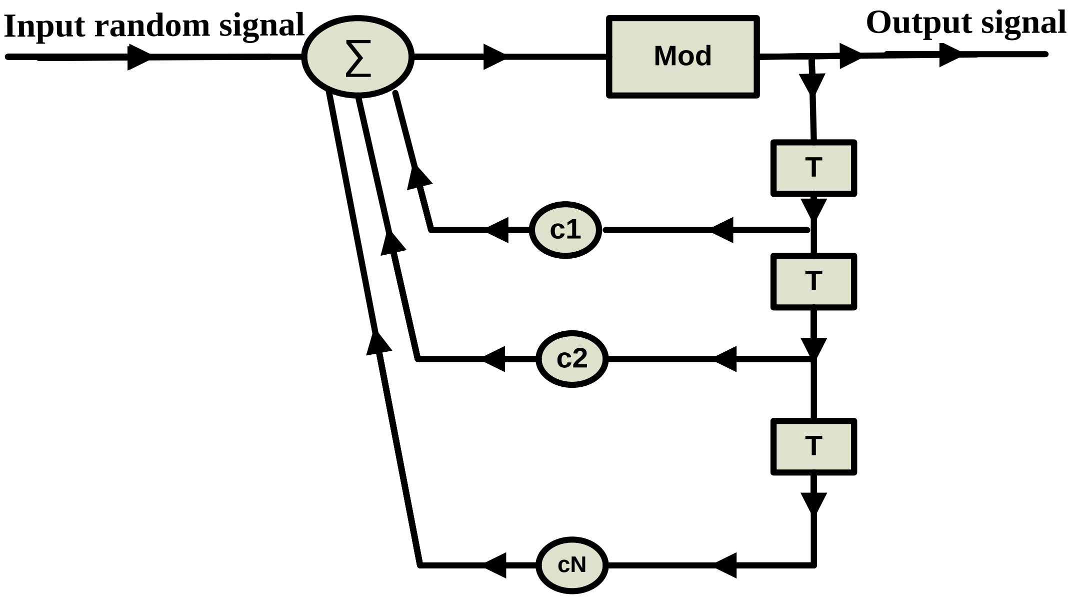

Fig.1 Digital chaotic Key generator

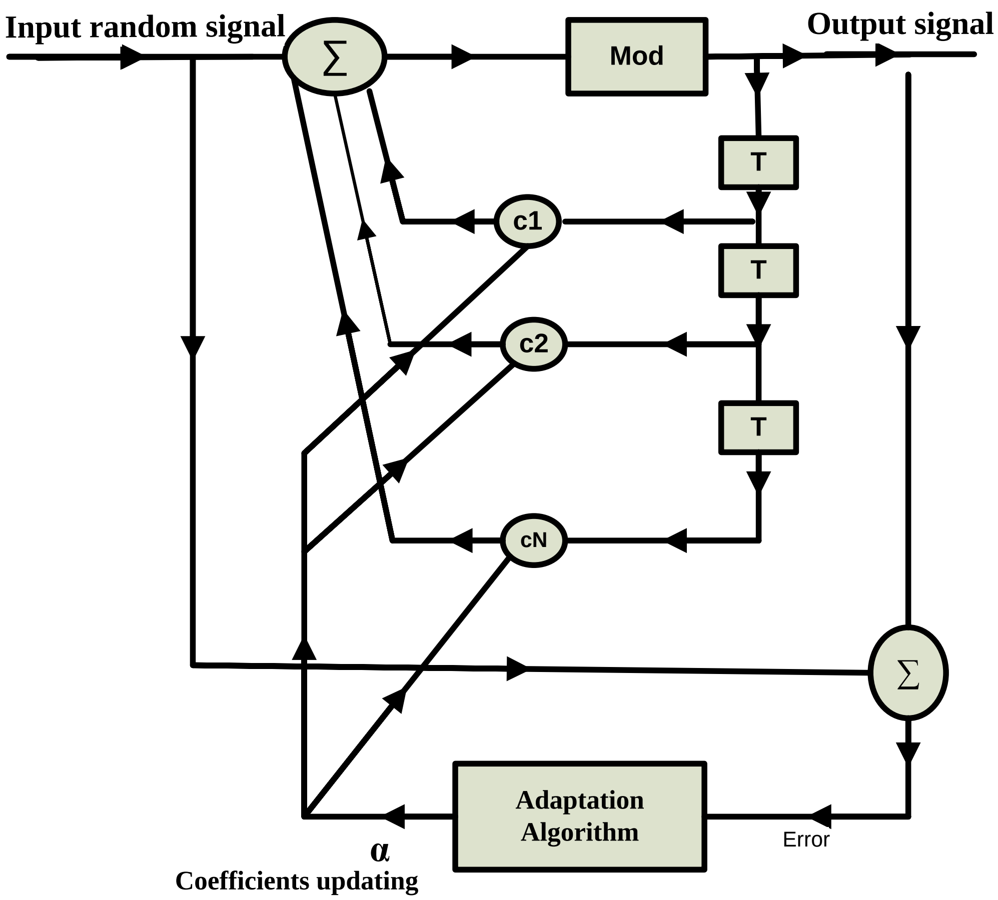

Fig.2 The adaptive digital chaotic Encoder

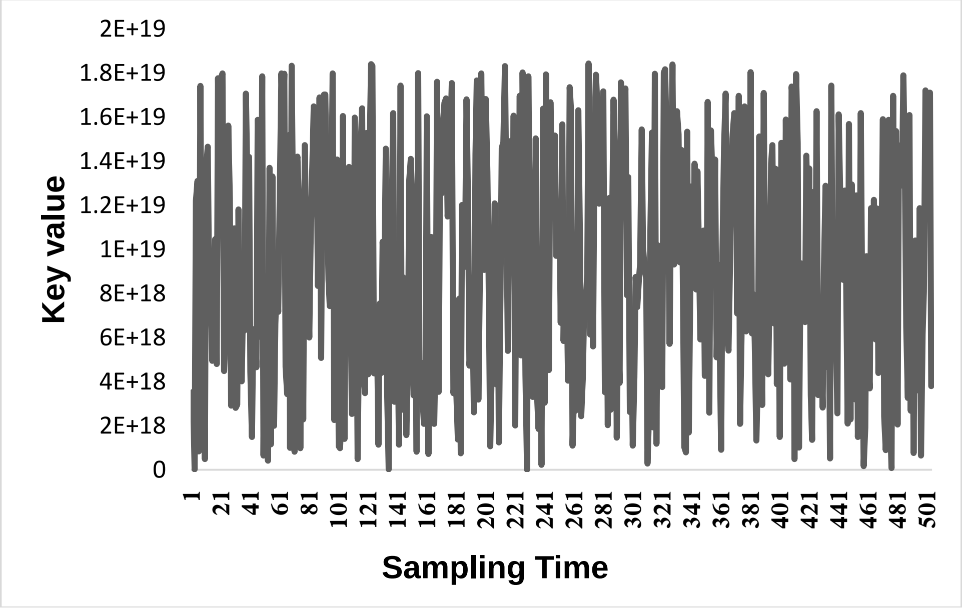

Fig.3 The output sequences of the 64 bit Key Digital Fixed coefficients Generator

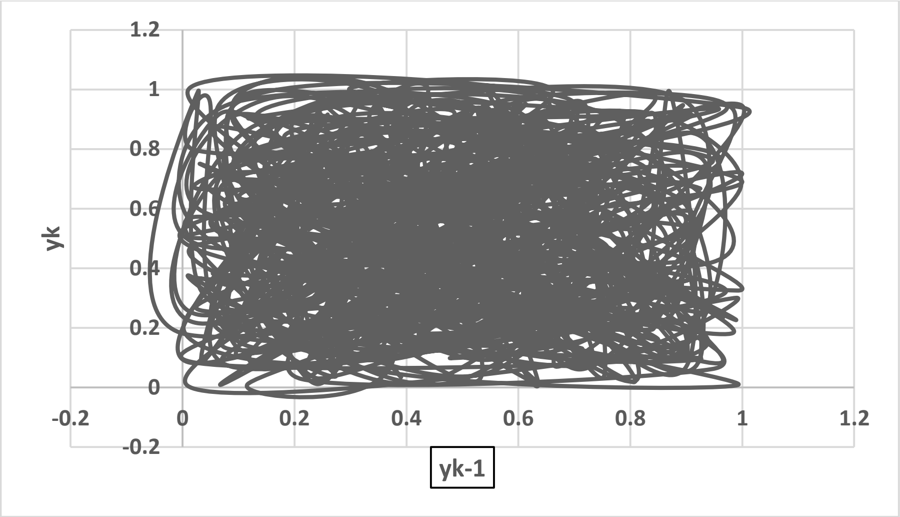

Fig.4 The Scatter output of the digital time invariant key generator

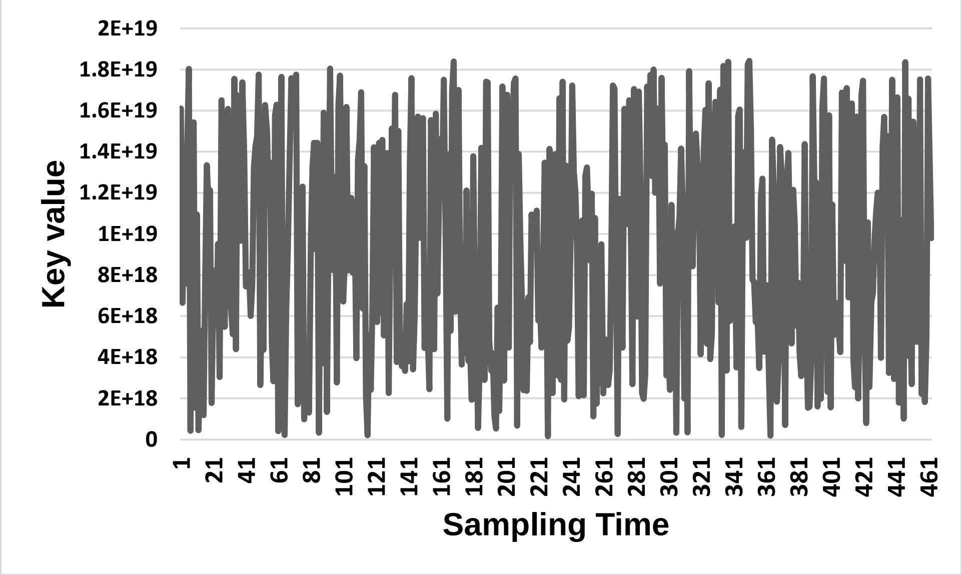

Fig. 5 The output sequences of the adaptive 64-bit Key Generator

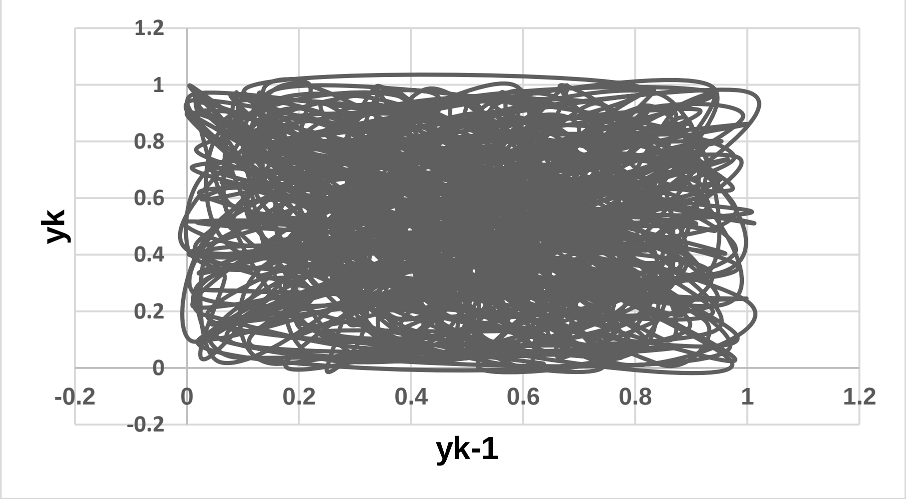

Fig.6 The Scatter output of the adaptive 64-bit Key Generator

Table-1 The statistical parameters of both the digital and adaptive Key generators

	Digital key Generator	Adaptive key Generator
Mean	0.49	0.5
Standard deviation	0.287	0.293
Correlation factor	0.000485	0.0117
Covariance	0.00005	0.001
H-Test	Pass	Pass

Reference

[1] T.S. Parker and L.O. Chua “Chaos: A Tutorial for Engineers”, Proceedings of the IEEE vol. 75, No.8, August 1987.

[2] J.C. Principe, A. Rathie and J. Kuo “Prediction of Chaotic Time series with Neural Networks and the Issue of Dynamic Modeling”, Int. Journal of Bifurcation and Chaos, vol.2, No.4 ,1992.

[3] M. N. Troparevsky” Computers and Chaos: An Example, Int. Journal of Bifurcation and Chaos, Vol.2, No.4, 1992 , 997-999.

[4] K. S. Halle and L.O Chua” Signal Amplification Via Chaos: Experimental Evidence”, Int. Journal of Bifurcation and Chaos, Vol.2, No.4, 1992 , 1011-1020

[5] K. Kelber and T. Kilias: ‘Analysis of an Encoder Decoder-System Based on Digital Filter Structures with Two's Complement Overflow Characteristic’, Proceedings of the International Symposium on Circuits and Systems, ISCAS'96, 12-15 May 1996, Atlanta GA, pp. III 166-169

[6] E. Soleit, A Fast-Adaptive Recursive Filter, IJE-96, Int. Journal of Electronics, 1997, vol. 82, No.4, pp. 327-333.

[7] L. Kocarev, ‘Chaos-Based Cryptography: A Brief Overview’, IEEE Circuits and Systems Magazine, Vol. 1, No. 3, 2001.

[8] K. K. Kelber, W. Schwartz, ‘General Design Rules for Chaos-Based Encryption Systems’ Proceedings NOLTA 2005, International Symposium on Nonlinear Theory and its Applications, Bruges, Belgium, October 18-21, 2005

[9] H. Gao, Y. Zhabg, S. Liang and D Li” A new chaotic algorithm for image encryption”, ELSEVIER Ltd., 2005, www.elsevier.com/locate/chaos.

[10] J. M. Blackledge “Multi-algorithmic Cryptography using Deterministic Chaos with Applications to Mobile Communications, ISAST Transactions on Electronics and Signal processing, Vol.1, No.2,2008.

[11] J. Zhou and O.C. Au.” Cryptoanalysis of Chaotic Convolutional Coder” 978-1-4244-5309-2/10/$26.00 ©2010 IEEE.

[12] N. Bagheli , Y. Farid and K. Ashraf" Image encryption/decryption scheme based on chaotic neural networks", Engineering Applications of Artificial Intelligence, Volume 25, Issue 4, June 2012, Pages 753-765.

[13] B. Agrawal and H. Agrawal. " Implementation of AES and RSA using Chaos System", International Journal of Scientific & engineering Research, Vol.4, Issue 5, May-2013.

[14] Yicong Zhou, Long Bao and C. L. Philip Chen, " A new 1D chaotic system for image encryption", Signal Processing April 2014, pp. 172–182. DOI 10.1109/ICSSE.2012.6257151

[15] C. Pak and L. Huang. " A new color image encryption using combination of the 1D chaotic map" ,Signal Processing, Volume 138, September 2017, Pages 129-137,https://doi.org/10.1016/j.sigpro.2017.03.011.