Ahmed S. Alshammari

University of Hail, College of Engineering, Hail, KSA

doi:10.15199/48.2020.10.09

A Stream Cipher Generator Based on a Combination of Two Non-linear Systems for Secure Signal Transmissions

Abstract. *A new cryptosystem approach based on two non-linear systems combined to satisfy a high degree of signal transmission security. These systems are Lorenz system and Rössler system. Each chaotic system has a completely different output bit stream. The system uses a stream cipher, in which the encryption key varies continuously. Therefore, a design of a secure communication system that is robust to different types of attacks such brute force attack is very important. One of the main properties of this system is the ability to retrieve the data transmitted through a noisy environment. The proposed system is a novel stream cipher which is based on combining two non-linear systems that are used in digital communication system. The key size of the system will exceed 576, which provide 2576 key space. Hence, this huge key space will provide a high security for plaintext against a brute force attack.*

Streszczenie. *Przedstawiono nowy szystem szyfrowania danych bazujący na kombinacji dwóch nieliniowych. Te dwa systemy to system Lorenza i system Rosslera. System umożliwia odzyskanie danych przy transmisji w zaszumionym środowisku.* ***Generator szyfrujący bazujący na kombinacji dwóch nieliniowych systemów Lorz\nza i Rosslera.***

Keywords: Rössler system; Lorenz System, Stream cipher; Key Space, cryptanalysis..
Słowa kluczowe: szyfrowane przesyłanie danych, system Lorenza, system Rosslera.

Introduction

Most of people interaction today tends to be electronic, such as online shopping or social engagements occurring within social media. Therefore, Sensitive personal electronic information like credit cards information, E-mails and private photos must always be protected. Hence, governments and private companies are now forced to step up to their responsibility and take actions that can protect sensitive information and prevent hacking. Cryptography and cryptanalysis are two primary techniques for facilitating secure communication. A secure communication system often contains three main parts: authentication, confidentiality and integrity. Authentication in communication systems has to be confirmed for both sender and receiver. The sender, encrypts the content of the message using a cryptography system and transmits it through the channel. The receiver is able to decrypt the data transmitted based on the private key that has already been installed. Integrity ensures that the message content has not been changed during communication between the sender and receiver. A stream cipher generates an infinite cryptographic keystream that encrypts bits individually, similar to the one-time pad. Most of the countries draw the attention to the importance of the cyber security as a strategic priority for the country. The present study aims to design and implement a high secure digital communication system based on stream cipher that uses a combination of two nonlinear systems.

Data trafficking through the various communication means such as smart phones and computers where data can be transmitted using RF links, Wi-Fi, etc. is increasing in a huge rate due to the fast growth in the medical, military and entertainment applications of digital communications. This creates a serious challenge for governments and private sector because they need to maintain high levels of security when their data are transmitted.

Shannon introduced the modern science of cryptography-based chaos, which is applied in communications systems [1-2]. The cryptography-based chaos is capable of generating an infinite amount of uncorrelated chaotic signals that are appropriate for the applications in multiuser Spread-Spectrum (SS) communication systems [3, 4, 5, 6, 7, 8]. The chaotic system is a deterministic system, which means that the generated chaotic signals are not random. However, the output signal of the chaotic system cannot be predicted due to the system's intrinsic non-linearity rather than noise [9]. The communication system based on chaotic system has several advantages such as noise immunity, fading mitigation, multiple access capability and low probability of interception [10, 11, 12, 13, 14]. A spread spectrum signal is hard to jam unless the spreading pattern is known. Hence, there is a low probability of interception. The SS system spectrum also provides resilience to fading and interference injection, and allows multiple users to use the same set of frequencies [15, 16-17]. A chaotic Direct Sequence Spread Spectrum (DSSS) system data spreading which multiply the data bits with discrete chaotic signal was proposed and investigated in [18, 19]. The performance of the chaos based DSSS system with multiple - access using bit error rate (BER) in presence of noise and fading channel is presented in [20, 21]. The study in [22] demonstrated a chaotic generator where the output sequence is truly a random number and of low complexity. The results show that the chaotic signals have a better Low Probability of Interception (LPI) than the Pseudorandom Noise (PN) signals [23]. The implementation of chaotic generator based on Filed Programmable Gate Array (FPGA) was presented in [24, 25, 26]. Binary sequences were generated using Chua's circuit in order to generate a pseudo random number sequence (PRNS) that satisfies d the cryptography requirements. The proposed method is based on using only a fraction of each signal from the three Chau's output states, then assembling the extracted parts to build one binary sequence. It has been shown that the generated binary sequences passes d the National Institute of Standard and Technology (NIST) the randomness test. In addition, The FPGA board was used to implement the chaotic generator based on Chua's circuit [27]. The study in [28-30] presented a stream cipher algorithm, which is based on a chaos system in order to increase the system degree complexity. The key stream generation depends on two logistic maps generators. One of the logistic map generator is used to generate a random numbers that are used to replace the other logistic map generator parameters. Results have shown that generator output is suitable for a stream cipher with high efficiency. In this work, two non-linear systems are combined to generate bit stream in a chaotic manner. Hence, it is very difficult for the attacker to decrypt the transmitted data through different methods of

attack. The proposed stream cipher generator is tested using Matlab and Simulink ®. The rest of this paper is organized as follows. The Rössler System is presented. The Lorenz System is presented. The scrambling scheme for Lorenz encryption generator is presented. Finally, the conclusion is given.

The Rössler System

The Rössler system is described by the following state equations, which are written in differential equation form.

$$\dot{x} = -y - z \quad \text{(a)}$$

$$\dot{y} = x + ay \quad \text{(b)}$$

$$\dot{z} = bx - cz + xz \quad \text{(c)}$$

(1)

In this system the non-linearity is represented by a multiplier which is easy to implement in digital hardware. The SIMULINK model of the Rössler is shown in Fig. 1. The x and y signals are shown in Fig. 2. It shows x y as calculated from equation 1. The x-y attractor shows in Fig. 3. It shows the phase plane of x versus y as calculated from equation 1. The attractor x y shows one is single scroll. The disadvantage of the Rössler system is that the attractor is a single loop, which results in a higher cross correlation between the state variables. However, in this work, the high correlation does not affect the degree of security because the Rössler system is used to change one of the Lorenz encryption system parameter continually.

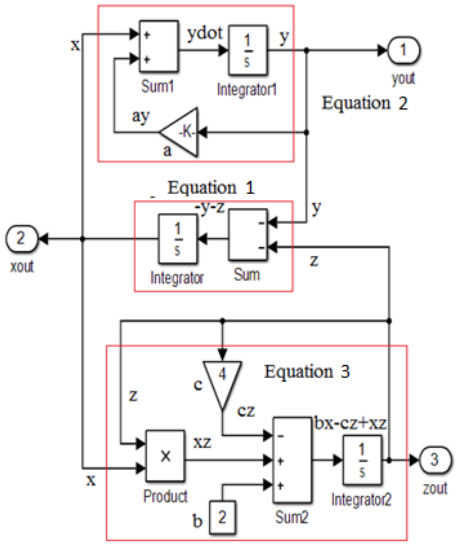

Fig. 1. SIMULINK model of The Rössler system.

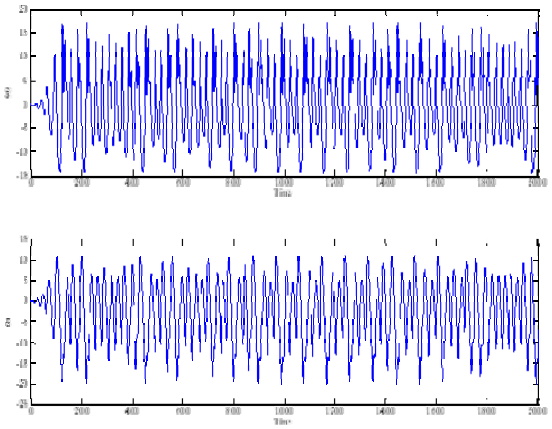

Fig. 2. The Rössler system, (a) The x signal and (b) The y signal.

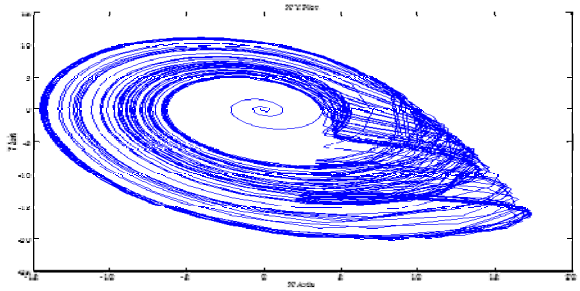

Fig. 3. The x-y attractor of the Rössler

The Lorenz System

The Lorenz system is described by the following sate equations, which are written in differential equation form.

$$\dot{x} = A(y - x)$$

$$\dot{y} = B.x - y - x.z$$

$$\dot{z} = x.y - C.z$$

(2)

Fig. 4 shows the SIMULINK Lorenz model where A, B and C are system parameters. *x*, *y* and *z* are state variables The scaling factors S_1, S_2 and S_3 are used to control the output signals frequency band and they are also part of the key in the encryption system. The *x* and *y* signals are shown in Fig.5 and the *x-y* attractor in Fig. 6.

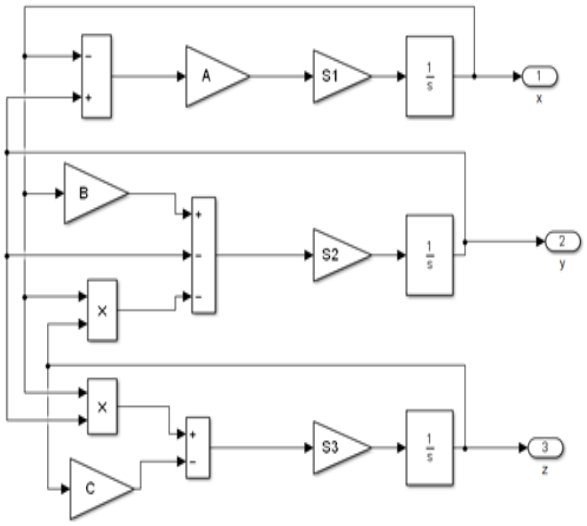

Fig. 4. SIMULINK model of The Lorenz system.

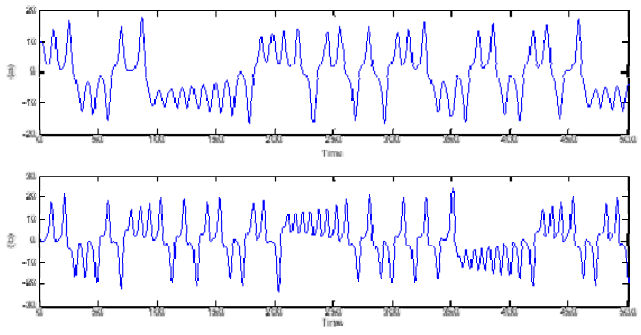

Fig. 5. The simulated signals of the Lorenz System. (a) x signal and (b) y signal.

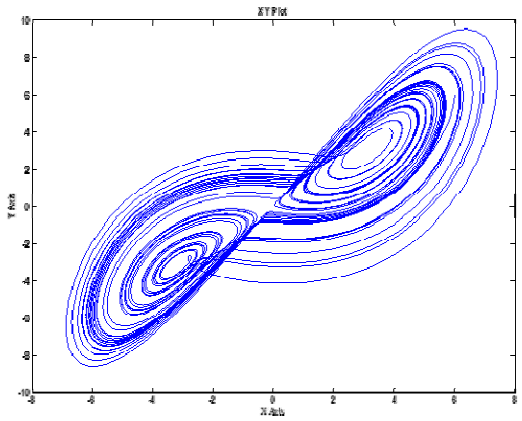

Fig. 6. The x-y attractor of the Lorenz system.

Scrambling scheme of Lorenz chaotic signal

Two non-linear bit streams (*x*-state and *y*-state) have been used to generate a truly random key. The last 12 bits in row are extracted from *x*-state and last 20 bits are extracted from *y*-state. Then, the 32 bits are assembled with a concatenate block. The 32 bits are then serialized to generate a bit stream, which is used as a key stream for data encryption. Fig. 7 shows the SIMULINK model of the scrambling method. The bit stream of the signed data type has been converted into unsigned. The constant block has been used to manipulate the 32 word length. Thus, the last 12 bits from *x*-state key stream have been extracted. The 12 bits word length has started from the least significant bit. The variable selector block has been used to extract a subject of rows from each matrix. The same operation has been used for *y*-state key stream. However, the 20 bits have been extracted from the y-state out of 32 bits word length that has started from least significant bit. After that, we concatenated the 12 bits and 20 bits using Matrix concatenation block to produce 32 word length. Then, the 32 bits has been sterilized using unbuffered block. Care is taken to ensure that the main generator always remains in the chaotic region, the output of the Auxiliary Lorenz Generator (A[n]) must remain within the range (7≤x[n]≤11). Therefore, the signal response of Lorenz Generator changes continually in a chaotic manner, based on the parameter supplied by the Rössler Generator.The bit stream after scrambling is shown in Fig. 8

Table 1 and 2 indicates that the key stream passes the National Institute of Standard and Technology (NIST) randomness test. The results are shown in Tables I and II.

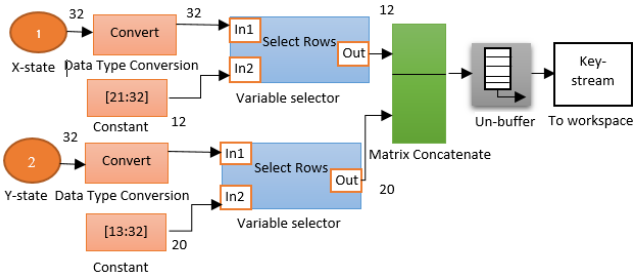

Fig. 7. Scrambling scheme of the Lorenz signals

Table 1. x and y chaotic signal

Statistical Test	Status	P-value
Frequency	pass	0.232425
Block Frequency	Pass	0.8121413
Cusum-Forward	pass	0.242325
Cusum-Reverse	pass	0.222325
Runs	pass	0.644146
Long Runs of Ones	pass	0.343309
Rank	pass	0.462485
FFT Test	pass	0.2332325
Non-overlapping	pass	0.841118
Overlapping	pass	0.211325
Approximate Entropy	pass	0.811218
Serial	pass	0.622146
Linear Complexity	pass	0.460485

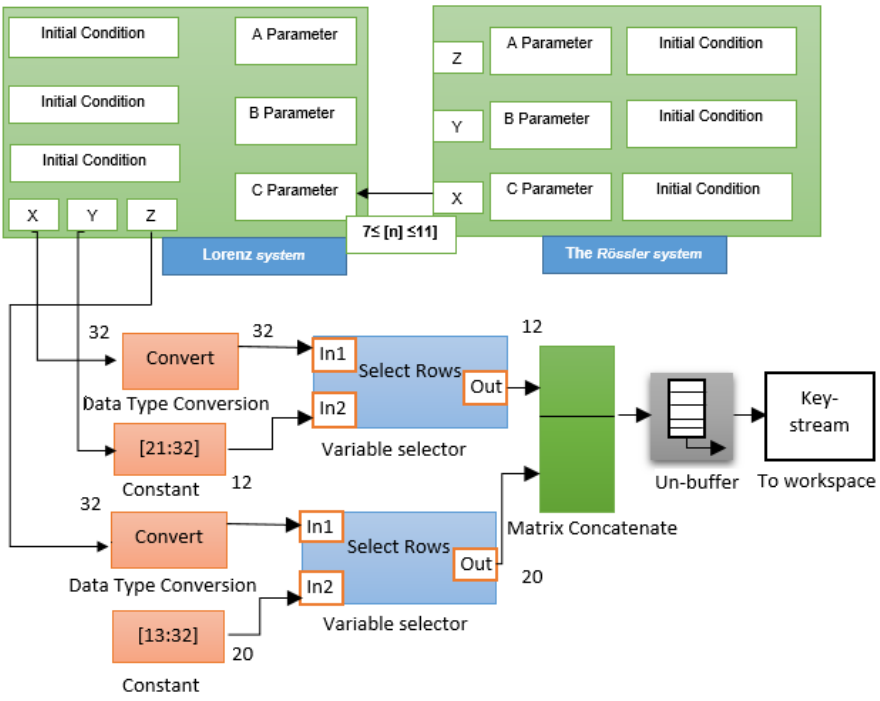

Fig. 7. The block diagram of the encryption process.

Table 2. y chaotic signal

Statistical Test	Status	P-value
Frequency	pass	0.460485
Block Frequency	Pass	0.899413
Cusum-Forward	pass	0.841118
Cusum-Reverse	pass	0.077882
Runs	pass	0.224409
Long Runs of Ones	pass	0.841118
Rank	pass	0.841118
FFT Test	pass	0.6341146
Non-overlapping	pass	0.822413
Overlapping	pass	0.841118
Approximate Entropy	pass	0.313309
Serial	pass	0.221325
Linear Complexity	pass	0.440485

Acknowledgments: This work is supported by the deanship of academic research at university of Hail (BA-2008).

***Authors**: Dr. Ahmed Saud Alshammari, Dept. of Electrical Engineering, College of Engineering, University of Hail, Hail, KSA*
E-mail: ahm.alshammari@uoh.edu.sa

REFERENCES

[1] C. Shannon, "A mathematical theory of communication, bell System technical Journal 27: 379-423 and 623–656," Mathematical Reviews (MathSciNet): MR10, 133e, 1948. H. Ettouny, L. Rizzuti, Solar desalination: A challenge for sustainable fresh water in the

[2] C. E. Shannon, "Communication theory of secrecy systems," Bell Labs Technical Journal, vol. 28, pp. 656-715, 1949.

[3] A. P. Kurian, S. Puthusserypady, and S. M. Htut, "Performance enhancement of DS/CDMA system using chaotic complex spreading sequence," IEEE Transactions on wireless communications, vol. 4, pp. 984-989, 2005.

[4] G. Kaddoum, F.-D. Richardson, and F. Gagnon, "Design and analysis of a multi-carrier differential chaos shift keying communication system," IEEE Transactions on communications, vol. 61, pp. 3281-3291, 2013.

[5] G. Kaddoum, "Wireless chaos-based communication systems: A comprehensive survey," IEEE Access, vol. 4, pp. 2621-2648, 2016.

[6] C. Tse and F. Lau, "Chaos-based digital communication systems," Operating Principles, Analysis Methods and Performance Evaluation (Springer Verlag, Berlin, 2004), 2003.

[7] R. Vali, S. Berber, and S. K. Nguang, "Accurate derivation of chaos-based acquisition performance in a fading channel," IEEE Transactions on wireless communications, vol. 11, pp. 722-731, 2012.

[8] R. Vali, S. M. Berber, and S. K. Nguang, "Analysis of chaos-based code tracking using chaotic correlation statistics," IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 59, pp. 796-805, 2012.

[9] S. Berber and S. Feng, "Chaos-based physical layer design for WSN applications," in 17th WSEAS Int. Conf. on Communications, Rhodes, Greece, pp. 157-162, 2013.

[10] J. Yu and Y.-D. Yao, "Detection performance of chaotic spreading LPI waveforms," IEEE Transactions on wireless communications, vol. 4, pp. 390396, 2005.

[11] M. Sobhy and A. Shehata, "Chaotic radar systems," in Microwave Symposium Digest. 2000 IEEE MTT-S International, pp. 1701-1704, 2000.

[12] T. Yang and L. O. Chua, "Chaotic digital code-division multiple access (CDMA) communication systems," International Journal of Bifurcation and Chaos, vol. 7, pp. 2789-2805, 1997.

[13] V. Lynnyk and S. Čelikovský, "On the anti–synchronization detection for the generalized Lorenz system and its applications to secure encryption," Kybernetika, vol. 46, pp. 1-18, 2010.

[14] Y. Xia, C. Tse, and F. C.-M. Lau, "Performance of differential chaos-shiftkeying digital communication systems over a multipath fading channel with delay spread," IEEE Transactions on Circuits and Systems II: Express Briefs, vol. 51, pp. 680-684, 2004.

[15] M. I. Sobhy and A.-E. Shehata, "Chaotic algorithms for data encryption," in Acoustics, Speech, and Signal Processing, 2001. Proceedings.(ICASSP'01). 2001 IEEE International Conference on, pp. 997-1000, 2001.

[16] L. Shujun, M. Xuanqin, and C. Yuanlong, "Pseudo-random bit generator based on couple chaotic systems and its applications in stream-cipher cryptography," Progress in Cryptology—INDOCRYPT 2001, pp. 316-329, 2001.

[17] M. A. Abu-Rgheff, Introduction to CDMA wireless communications: Academic Press, 2007.

[18] G. Heidari-Bateni and C. McGillem, "Chaotic sequences for spread spectrum: An alternative to PN-sequences," in Wireless Communications, 1992. Conference Proceedings., 1992 IEEE International Conference on Selected Topics in, pp. 437-440, 1992

[19] P. I. Martoyo, A. Susanto, E. Wijanto, H. Kanalebe, and K. Gandi, "Chaos codes vs. orthogonal codes for CDMA," in Spread Spectrum Techniques and Applications (ISITA), 2010 IEEE 11th International Symposium on, pp. 189193, 2010.

[20] R. C. Hilborn, Chaos and nonlinear dynamics: an introduction for scientists and engineers: Oxford University Press on Demand, 2000.

[21] G. Kaddoum, M. Coulon, D. Roviras, and P. Chargé, "Theoretical performance for asynchronous multi-user chaos-based communication systems on fading channels," Signal Processing, vol. 90, pp. 2923-2933, 2010.

[22] A. P. Kurian, S. Puthusserypady, and S. M. Htut, "Performance enhancement of DS/CDMA system using chaotic complex spreading sequence," IEEE Transactions on wireless communications, vol. 4, pp. 984-989, 2005.

[23] G. Mazzini, G. Setti, and R. Rovatti, "Chaotic complex spreading sequences for asynchronous DS-CDMA. I. System modeling and results," IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, vol. 44, pp. 937-947, 1997.

[24] H. Nejati, A. Beirami, and W. H. Ali, "Discrete-time chaotic-map truly random number generators: design, implementation, and variability analysis of the zigzag map," Analog Integrated Circuits and Signal Processing, vol. 73, pp. 363-374, 2012.

[25] J. Yu and Y.-D. Yao, "Detection performance of chaotic spreading LPI waveforms," IEEE Transactions on wireless communications, vol. 4, pp. 390396, 2005.

[26] L. Cong and W. Xiaofu, "Design and realization of an FPGA-based generator for chaotic frequency hopping sequences," IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, vol. 48, pp. 521-532, 2001.

[27] M. Azzaz, C. Tanougast, S. Sadoudi, and A. Dandache, "Real-time FPGA implementation of Lorenz's chaotic generator for ciphering telecommunications," in Circuits and Systems and TAISA Conference, 2009. NEWCAS-TAISA'09. Joint IEEE North-East Workshop on, 2009, pp. 1-4.

[28] D. Majumdar, R. Moritz, H. Leung, and J. M. Brent, "An enhanced data rate chaos-based multilevel transceiver design exploiting ergodicity," in MILITARY COMMUNICATIONS CONFERENCE, 2010-MILCOM 2010, pp. 1256-1261, 2010.

[29] L. Merah, A. Ali-Pacha, N. H. Said, and M. Mamat, "A pseudo random number generator based on the chaotic system of Chua's circuit, and its real time FPGA implementation," Applied Mathematical Sciences, vol. 7, pp. 2719-2734, 2013.

[30] Yunpeng ZHANG1, Lifu HUANG, Yasin Hasan KARANFIL2, , Zhenzhen WANG, A New Digital Image Hiding Encryption Algorithm Based on Dual Chaotic Systems. PRZEGLĄD ELEKTROTECHNICZNY, ISSN 0033-2097, R. 89 NR 1b/2013.