Ahmed S. Alshammari

Department of Electrical Engineering, College of Engineering, University of Hail, Hail, KSA
ORCID.

doi:10.15199/48.2022.02.03

A Novel Cryptosystem based on Chaotic Signals for Data Encryption Applications and CDMA Communication System

Abstract. *In this paper, we study the Lorenz chaotic system as a cryptosystem stream cipher. The system employs a stream cipher, in which the encryption key changes in a chaotic manner over time. For added security, one of the Lorenz generator's parameters are controlled by step function subsystem. The cryptosystem's bit stream passed the statistical randomness test. As a result, a cryptosystem's design can withstand many sorts of attacks, such as brute force. The system's key size will be greater than 256, allowing for a total of* 2^{256} *key spaces. As a result, the large key space will give strong plaintext security against a brute force attack..*

Streszczenie. *W tym artykule badamy chaotyczny system Lorenza jako szyfr strumieniowy kryptosystemu. System wykorzystuje szyfr strumieniowy, w którym klucz szyfrowania zmienia się w czasie w sposób chaotyczny. Dla zwiększenia bezpieczeństwa, jeden z parametrów generatora Lorenza jest kontrolowany przez podsystem funkcji krokowej. Strumień bitów kryptosystemu przeszedł test losowości statystycznej. W rezultacie projekt kryptosystemu może wytrzymać wiele rodzajów ataków, takich jak brutalna siła. Rozmiar klucza systemowego będzie większy niż 256, co pozwoli na łącznie 2256 miejsc na klucze. W rezultacie duża przestrzeń na klucze zapewni silne zabezpieczenie tekstu jawnego przed atakiem brute force.* (***Nowatorski kryptosystem oparty na chaotycznych sygnałach do aplikacji szyfrowania danych i systemu komunikacji CDMA***)

Keywords: Cryptosystem, Lorenz System, step function, Stream cipher; Key Space, cryptanalysis, Encryption, CDMA.
Słowa kluczowe: system kryptograficzny, szyfrowanie, sygnał chaotyczny.

1 Introduction

The majority of people's interactions today are electronic, such as online buying or social interactions on social media. As a result, sensitive personal electronic information such as credit card numbers, e-mail addresses, and private images must constantly be protected. As a result, governments and private companies take steps to protect sensitive data and avoid hacking. Cryptography is a method for assuring secure communication. Cryptanalysis, on the other hand, is used to test the system's security level. .Several governments emphasize the importance of cyber security as a strategic priority for their countries.

Traditional secure communication methods provide advantages over a digital communication system based on chaos equations for data transfer security. This system's capacity to create pseudorandom numbers based on non-linear system is one of its key advantages. As a result, we may generate an endless number of uncorrelated binary streams that can be used as a code for a huge number of users in the Code Division Multiple Access (CDMA) communication system.

Chaos is a long-term aperiodic signals in a deterministic system that is sensitive to beginning conditions [1]. The deterministic feature of a chaos system means that it has no random or noisy inputs or parameters, and system variability is caused by nonlinearity rather than the effect of noisy driving forces [1]. Aperiodicity is another chaos trait; system trajectories do not settle down to fixed points and periodic orbits [1]. The chaos system is likewise extremely sensitive to the initial state. Any little change in the initial condition causes the chaotic model's output response to alter very quickly. This means that after the initial condition is altered, the new output response is unconnected to the previous output generated. The trajectories separate exponentially quickly, and the system's Lyapunov exponent is positive [1]. The cross-correlation is a measure of similarity between two signals (an input signal and a reference signal) that is used as a signal detector in this system, whereas the autocorrelation is a measure of correlation between the signal and a time-delayed version of itself that is used as a signal detector. [1]. This means that auto-correlation functions can be used to distinguish each piece of user data delivered on a single channel, while cross-correlation functions are used to reject data from other users.

Chaotic signals can be applied to a variety of communication systems, including spread-spectrum applications [2-6]. Because of the anti-jam and low likelihood of intercept (LPI) qualities of spread-spectrum technology, it was originally developed by the military. Commercial telecommunication companies have recently employed spread-spectrum technology for wireless systems. Wideband, noise-like signals are used in spread-spectrum, which are difficult to identify and jam. Spread-spectrum transmissions are designed to have a significantly wider bandwidth than the data they transport. The transmitter employs the same transmit power level as a narrowband transmitter, for example. Because the spread-spectrum signal is wider, it has a lower power density and so transmits at a lower power density. Furthermore, the spread-spectrum technology may combine noise tolerance with a high data rate, making it ideal for wireless data communication networks in noisy areas.

There have been numerous studies of two types of chaos-based communication systems. A Coherent Detection is the first. Chaos-based direct-sequence code division multiple access, for example, uses the chaotic signal to modulate the information signal (DS-CDMA). Synchronization is required in this approach for the receiver to recover the information signal. The synchronization refers to the chaotic generator at the receiver reproducing an exact replica of the chaotic bit stream [7-11]. The goal of employing chaotic signals, particularly in chaos-based spread-spectrum systems, is to overcome the flaws in traditional Pseudo-Random Noise (PN) sequences [11]. A Non-Coherent Detection technique is used in the second type of chaos-based communication system. To recover the data, the receiver design assesses the received signal. The chaotic signal at the receiver does not require a broadcast signal to regenerate [12-15].

To accomplish data encryption, we need to generate chaotic signals in this work. There are two types of chaotic generators: autonomous and non-autonomous. Autonomous systems create their own signals and do not require external power to function. Non-autonomous systems convert a chaotic signal from an external signal,

such as a harmonic signal. Every chaotic system must contain a nonlinear element and a set of state variables, with the number of independent state variables determining the system's order. An autonomous system's minimal order is three, while a non-autonomous system's minimum order is two. In multi-user SS communication systems, cryptography-based classic pseudorandom sequence generators such as maximal length sequences (m-sequences), Walsh sequences, and GOLD sequences are employed. However, there are several drawbacks, such as the restricted amount of rounds (iterations) that encryption transformation can execute. Due to the small amount of PN sequences accessible, there is also a lack of correlation qualities. Furthermore, when there is a delay, the Walsh coding properties cross-correlate poorly, resulting in poor performance in multipath situations [15-20].

In Sect. 2, we discussed the proposed Cryptosystem. In Sect. 3, we described Lorenz system. In Sect. 4, we presented Cryptosystem scrambling scheme and finally Sect. 5 ends up with a conclusion

2 The proposed Cryptosystem Overview

The proposed cryptosystem uses Lorenz system and step function subsystem. The step function subsystem continuously changes the A parameter of the Lorenz system. The step function subsystem, which generates linearly varying values over a certain range in order to ensure the cryptosystem's chaotic nature. Thus, to encrypt the data stream, the encryption approach uses the output of the Lorenz Generator and step function subsystem. Step function and transfer function are connected using multiplex scalar blocks in the step function subsystem. The step function subsystem is visualized in Fig.1.

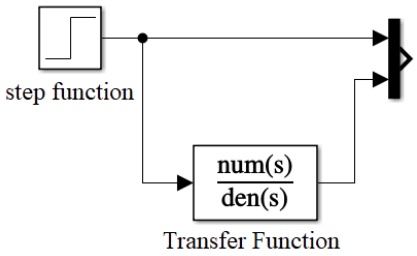

Fig. 1. SIMULINK model of The Lorenz system.

In order to improve the level of security, The Lorenz system's A parameter is continuously changed using the step function subsystem. The step function subsystem ensures the cryptosystem's chaotic character by generating linearly fluctuating values over a defined range. Fig. 2 shows the step function response.

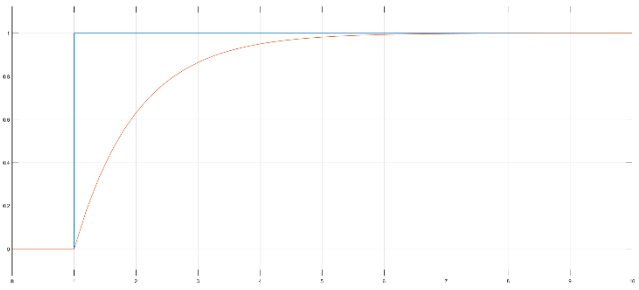

Fig. 2. The response of the step function subsystem.

3 The Lorenz System

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

$$\begin{aligned} \dot{x} &= A(y-x) \\ \dot{y} &= B.x - y - x.z \\ \dot{z} &= x.y - C.z \end{aligned} \tag{1}$$

Fig. 3 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. 4 and the *x-y* attractor in Fig. 5.

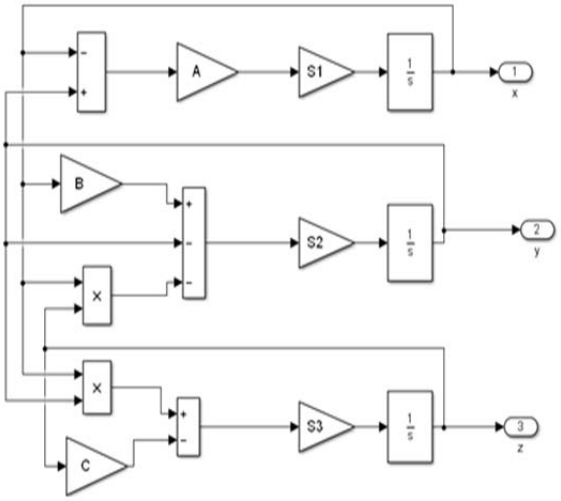

Fig. 3. SIMULINK model of The Lorenz system.

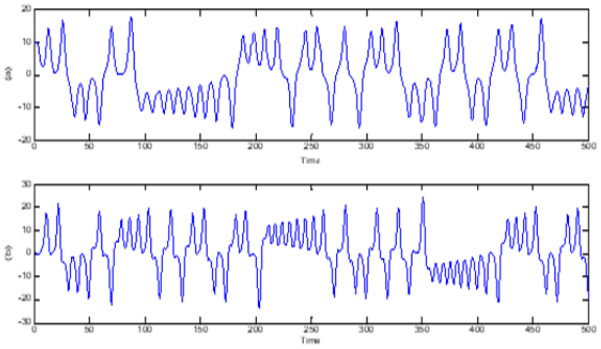

Fig. 4. The simulated signals of the Lorenz System. (a) x signal and (b) y signal.

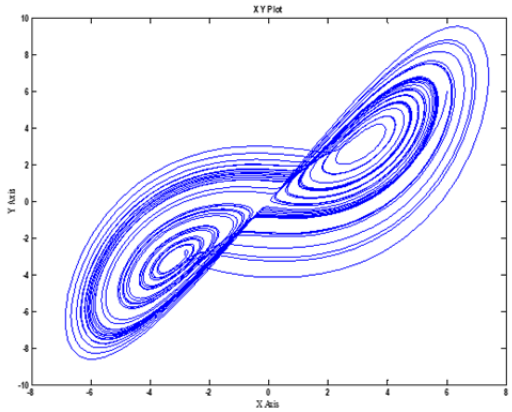

Fig. 5. The x-y attractor of the Lorenz system.

4 Cryptosystem scrambling scheme

To generate a truly random key, the cryptosystem bit streams (x-state and y-state) were used. The last 12 bits in a row are taken from the x-state, whereas the last 20 bits are taken from the y-state. The 32 bits are then put together using a concatenate block. After that, the 32 bits are serialized to create a bit stream that is utilized as a key stream for data encryption. The scrambling method's SIMULINK model is shown in Figure 7. The signed data type's bit stream has been changed to unsigned. To alter the 32-word length, the constant block was used. The last 12 bits of the x-state key stream have been retrieved as a result. The least significant bit was used to begin the 12 bit word length.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.

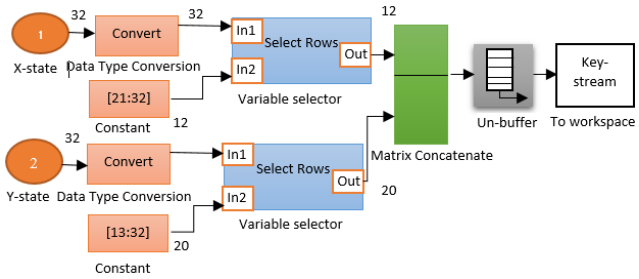

Fig. 6. Scrambling scheme of the Lorenz signals

Table 1. x and y chaotic signal

Statistical Test	Status	P-value
Frequency	pass	0.632425
Block Frequency	Pass	0.912141
Cusum-Forward	pass	0.642325
Cusum-Reverse	pass	0.522325
Runs	pass	0.544146
Long Runs of Ones	pass	0.343309
Rank	pass	0.462485
FFT Test	pass	0.433232
Non-overlapping	pass	0.842228
Overlapping	pass	0.311325
Approximate Entropy	pass	0.811218
Serial	pass	0.722146
Linear Complexity	pass	0.560485

Table 2. y chaotic signal

Statistical Test	Status	P-value
Frequency	pass	0.260485
Block Frequency	Pass	0.699413
Cusum-Forward	pass	0.641118
Cusum-Reverse	pass	0.077882
Runs	pass	0.224409
Long Runs of Ones	pass	0.852118
Rank	pass	0.852118
FFT Test	pass	0.634114
Non-overlapping	pass	0.922413
Overlapping	pass	0.941118
Approximate Entropy	pass	0.313309
Serial	pass	0.521325
Linear Complexity	pass	0.240485

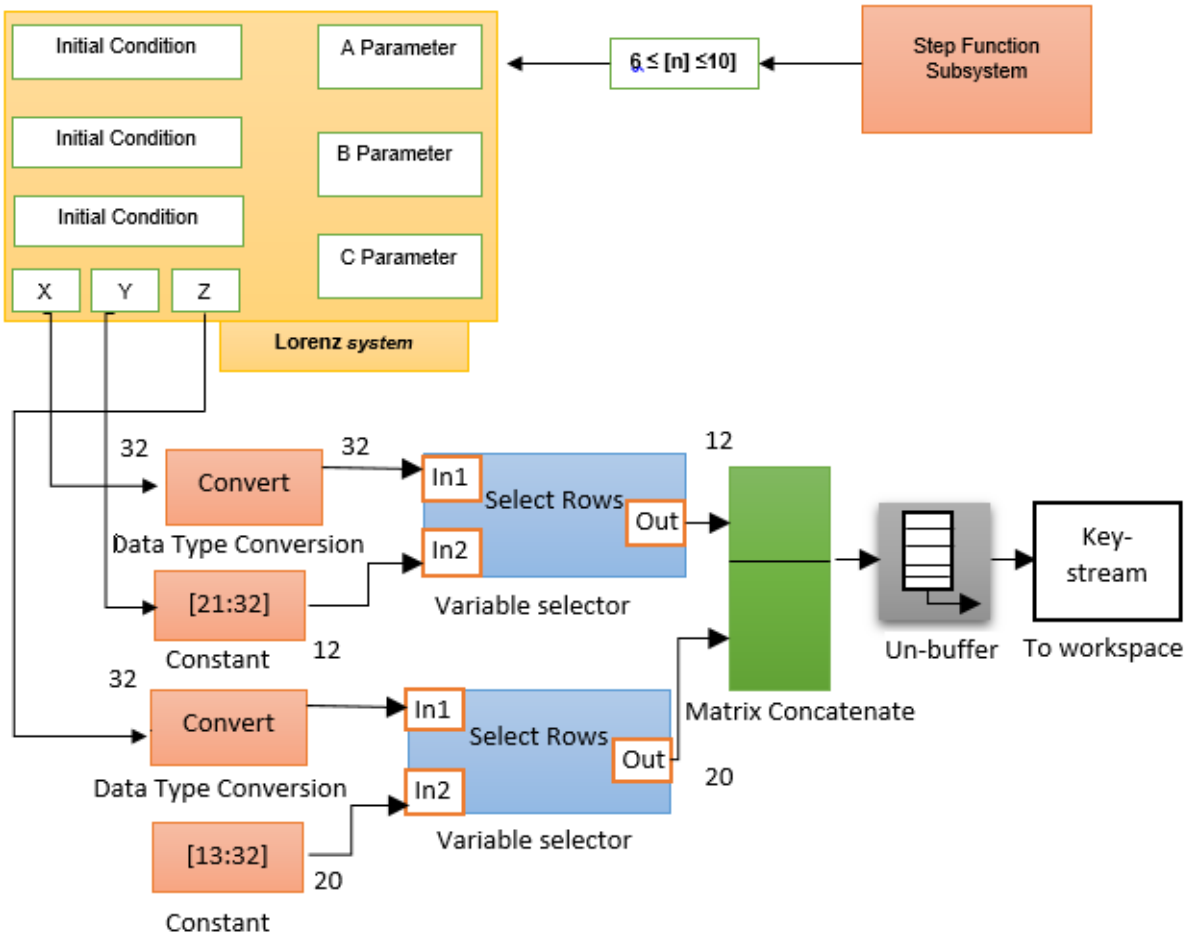

Fig. 7. The block diagram of the encryption process.

5 Conclusion

This work provides a cryptosystem system-based on chaotic stream cipher generator for safe signal transmission. The cryptosystem is made up of two subsystems: the Lorenz system and the step function subsystem. The system utilizes a stream cipher, in which the encryption key is continuously changed based on the step function subsystem. The step function subsystem has been added to improve security. In addition, the step function subsystem controls one of the Lorenz generator's parameters for further security. A symmetric cipher with a key length of 256 bits is used to encrypt the data. The number 256 is a huge space in the system. 32-bits represent the length of a word. The system's key space is (8*32). The key space of the system is $2^{(8*32)} = 2^{256}$. The scrambling scheme was created, and the binary stream generated by the cryptosystem generator passed the NIST randomness test.

***Author**: 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] Yunpeng Zhang , Lifu Huang , Yasin Karanfil , Zhenzhen Wang, 'A New Digital Image Hiding Encryption Algorithm Based on Dual Chaotic Systems', No/VOL: 01b/2013 Page no. 127
[2] Ewa Świercz ' Image encryption algorithms based on wavelet decomposition and encryption of compressed data in wavelet domain', No/VOL: 02/2018 Page no. 79
[3] Badr Alshammari, ' Cryptanalysis of a Bilateral-Diffusion image encryption algorithm based on dynamical compound chaos', 01/2021 Page no. 128
[4] S. H. Strogatz, Nonlinear dynamics and chaos: with applications to physics, biology, chemistry, and engineering: Westview press, 2014.C. E. Shannon, "Communication theory of secrecy systems," Bell Labs Technical Journal, vol. 28, pp. 656-715, 1949.
[5] J. Y. Stein, Digital signal processing: a computer science perspective: John Wiley & Sons, Inc., 2000.
[6] R. Kharel, "Design and Implementation of secure chaotic communication system," PhD thesis, March 2011.
[7] G. Kaddoum, "Wireless chaos-based communication systems: A comprehensive survey," IEEE Access, vol. 4, pp. 2621-2648, 2016.
[8] G. Kaddoum, "Wireless chaos-based communication systems: A comprehensive survey," IEEE Access, vol. 4, pp. 2621-2648, 2016.
[9] H. Dedieu, M. P. Kennedy, and M. Hasler, "Chaos shift keying: Modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuits," IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing, vol. 40, pp. 634-642, 1993.
[10] U. Parlitz, L. O. Chua, L. Kocarev, K. Halle, and A. Shang, "Transmission of digital signals by chaotic synchronization," International Journal of Bifurcation and Chaos, vol. 2, pp. 973-977, 1992.
[11] G. Kolumbán, M. P. Kennedy, and L. O. Chua, "The role of synchronization in digital communications using chaos. I. Fundamentals of digital communications," IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, vol. 44, pp. 927-936, 1997.
[12] G. Kaddoum, "Wireless chaos-based communication systems: A comprehensive survey," IEEE Access, vol. 4, pp. 2621-2648, 2016.
[13] C. Tse and F. Lau, "Chaos-based digital communication systems," Operating Principles, Analysis Methods and Performance Evaluation (Springer Verlag, Berlin, 2004), 2003.
[14] M. P. Kennedy, G. Kolumbán, G. Kis, and Z. Jákó, "Performance evaluation of FM-DCSK modulation in multipath environments," IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, vol. 47, pp. 1702-1711, 2000.
[15] A. Pande and J. Zambreno, "A chaotic encryption scheme for real-time embedded systems: design and implementation," Telecommunication Systems, pp. 1-11, 2013.
[16] 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.
[17] S. Sadoudi, M. S. Azzaz, and C. Tanougast, "Novel experimental synchronization technique for embedded chaotic communications," in Control, Decision and Information Technologies (CoDIT), 2014 International Conference on,pp. 669-672, 2014.
[18] N. X. Quyen, V. Van Yem, and T. Q. Duong, "Design and analysis of a spread-spectrum communication system with chaos-based variation of both phase-coded carrier and spreading factor," IET Communications, vol. 9, pp. 1466-1473, 2015.
[19] T. K. Ksheerasagar, S. Anuradha, G. Avadhootha, and K. S. R. Charan, "Performance analysis of DS-CDMA using different chaotic sequences," in Wireless Communications, Signal Processing and Networking (WiSPNET), International Conference on, pp. 2421-2425, 2016.
[20] Y. Wu, Y. Zhou, and L. Bao, "Discrete wheel-switching chaotic system and applications," IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 61, pp. 3469-3477, 2014.