Hindawi
Discrete Dynamics in Nature and Society
Volume 2021, Article ID 6653930, 9 pages
https://doi.org/10.1155/2021/6653930

Research Article

Generating Chaotic Series via Encryption Method in Fractional-Order Chua Systems

Bo Gong,[1] Haodong Zhang,[2] and Liguang Wan[3]

[1]*College of Foreign Studies, Hubei Normal University, Huangshi 435002, China*
[2]*Wuhan Research Institute of Posts and Telecommunications, Wuhan 430074, China*
[3]*School of Electrical Engineering and Automation, Hubei Normal University, Huangshi 435002, China*

Correspondence should be addressed to Liguang Wan; wanliguang@hbnu.edu.cn

Received 11 December 2020; Revised 31 December 2020; Accepted 28 January 2021; Published 19 February 2021

Academic Editor: Luca Pancioni

Fractional-order Chua systems have drawn wide attention in view of rich dynamic characteristics, e.g., chaos and hyperchaos. How to generate chaotic series via encryption method in fractional-order Chua systems is a difficult point all the while. In this paper, we derive several encryption methods in fractional-order Chua systems to generate chaotic series. As one of the most direct application, image encryption is also discussed by the presented methods.

1. Introduction

Chaotic system refers to the existence of seemingly random irregular motion in a deterministic system. Its behavior is characterized by uncertainty, unrepeatability, and unpredictability. Chaos is the inherent characteristic of a nonlinear dynamic system and a common phenomenon in the nonlinear system. Chaos is a deterministic and random-like process in the nonlinear dynamic system. This process is neither periodic nor convergent and is sensitive to the initial value. According to the properties of the dynamical system, chaos can be divided into four types: temporal chaos, spatial chaos, spatiotemporal chaos, and functional chaos [1–5]. The application of chaos can be divided into chaos synthesis and chaos analysis [5]. The former uses artificial chaos to obtain possible functions from chaotic dynamic system, such as associative memory of artificial neural networks; the latter analyzes chaotic signals obtained from complex artificial and natural system and looks for hidden deterministic rules, such as nonlinear deterministic prediction of time series data. Dalir and Bigdeli [1] consider robust adaptive control for uncertain fractional-order chaotic systems. Modiri and Mobayen [2] develop synchronization scheme for fractional-order master-slave-coupled chaotic systems by using adaptive terminal sliding mode control. Wang et al. [5] address the issue on image encryption via a class of delay chaotic system. Actually, chaos is a more common phenomenon than order [3]. It enables us to have a deeper understanding of the real world, opens a way for us to study the complexity of nature, and at the same time leads to some mathematical physics thinking on the epistemology of the real world.

Information encryption is to use mathematical or physical means to protect electronic information in the process of transmission and storage for preventing leakage. Essentially, encryption is the conversion of data through cipher arithmetic, which makes that no one can understand a message without the correct key [6–10]. Information security is usually achieved by information encryption technology. Traditionally, encryption technology is divided into three categories: symmetric encryption, asymmetric encryption, and Hash encryption. But there are some flaws: (1) in symmetric encryption, the secret key cannot be transmitted safely, although the speed is fast; (2) in asymmetric encryption, its speed is very slow; (3) the ciphertext in Hash encryption is limited to small, in spite of the irreversibility of ciphertext to be guaranteed. It is noted that chaotic cryptography has strong advantages in the encryption of multimedia information [10]. Whether the encryption algorithm based on chaos can be designed to make the encryption

process random and uncertain, while the ciphertext generated by encryption for a given input has unique certainty. Furthermore, the certificate generated by encryption is indecipherable. If feasible, the encryption algorithm based on chaos will provide a convenient way for information exchange, use, and dissemination [9].

Chua system as a simple circuit, which can be experimentally implemented, is a combination in theory of simple and accurate model and has become a practical system to study lots of problems of chaos theory [11–15]. Because of this, it has been the object of many studies. In particular, the emergence of fractional-order Chua system, on the one hand, greatly expands the scope of traditional Chua circuit, which can provide better circuit performance and more design freedom; on the other hand, due to the introduction of fractional-order operator, the characteristics of fractional-order Chua system are different from those of integer-order Chua circuit, thus posing some new challenges for circuit analysis and synthesis [11–13, 15]. Alkahtani [11] uses the method of numerical analysis to investigate chaotic Chua circuit model with fractional order. Atangana and Araz [12] consider a general Cauchy problem for the modified fractional Chua attractor model. Petras [13] describes chaos and other nonlinear behaviors in the fractional-order Chua system. Li et al. [15] utilize the Pecora–Carroll approach to study the chaos synchronization of active-passive-coupled Chua systems with fractional order. Rather recently, Wu and Zeng [14] innovatively use the tool of chaos in fractional-order Chua circuit to understand, manipulate, and control nonlinear systems. To make out why this is true, one must start with a working knowledge of how fractional-order Chua systems behave. Whether the related encryption algorithms can be designed to generate chaos series based on some practical fractional-order Chua systems? Meanwhile, to ensure the information security, how does one go about making the generated chaotic sequences more strictly random? In addition, whether the chaotic encryption sequences can be associated with plaintext by combining chaotic iteration and ciphertext feedback, so as to improve the ability to resist plaintext attacks? To investigate the possibility of the issues above to be resolved, we will put exploration.

2. Second-Order Chua System of Fractional Order

Consider a second-order Chua system of fractional order:

$$\begin{aligned} D^{\vartheta}x(t) &= \alpha(\beta - \varrho(y))x, \\ D^{\vartheta}y(t) &= x, \end{aligned} \tag{1}$$

where D^{ϑ} denotes Caputo derivative, fractional-order $\vartheta > 0$, α and β are parameters, $x(t)$ and $y(t)$ are system states, and

$$\varrho(y) = \begin{cases} a, & |y| < 1, \\ b, & |y| > 1, \end{cases} \tag{2}$$

in which a and b are the setting parameters.

Due to the second-order feature of (1), we adopt the encryption framework "diffusion-scrambling-diffusion": three pseudorandom matrices X, Y, and U, are generated to be used for diffusion process and scrambling process, where matrices X and Y are applied to the diffusion processes of plaintext and middle cipher, respectively, and matrix U is applied to the scrambling process of middle cipher.

(1) Using $\{x_0, y_0\}$ in secret key as the original value of (1), to iterate (1), we can get two chaotic series $\{x_i\}$ and $\{y_i\}$, $i = 1, 2, \ldots, +\infty$

(2) By the following formulas

$$\begin{aligned} X(i,j) &= \text{floor}\left[\left(x_{(i-1)\times N+j} + 500 \bmod 1\right) \times 10^{13}\right] \bmod 256, \\ Y(i,j) &= \text{floor}\left[\left(y_{(i-1)\times N+j} + 500 \bmod 1\right) \times 10^{13}\right] \bmod 256, \\ U(i,j) &= \left[\text{floor}\left(x_{(i-1)\times N+j} + y_{(i-1)\times N+j} + 500 \bmod 1\right) \times 10^{12}\right] \bmod N + 1, \end{aligned} \tag{3}$$

where N is the size of plaintext to be input

To apply the encryption method above in (1), by selecting $\vartheta = 0.5$, $\alpha = 1$, $\beta = 0.03$, $a = 0.01$, and $b = 0.05$, the chaotic time series are shown in Figure 1. Accordingly, chaotic attractor based on encryption method is displayed in Figure 2.

Through the above analysis, a second-order Chua system of fractional order with more complex dynamics is proposed by using an improved encryption framework "diffusion-scrambling-diffusion." Obviously, the algorithm not only retains the low-dimensional chaotic system to be high efficiency and simple form but also possesses large key space similar to the high-dimensional chaotic system. At the same time, the encryption process is not only related to the key but also related to the plaintext. That is, even for the same key, different plaintexts correspond to different passwords. Then, the strong plaintext sensitivity can be guaranteed, and the ability of antiplaintext attack is also enhanced.

3. Third-Order Chua System of Fractional Order

Consider a third-order Chua system of fractional order:

$$\begin{aligned} D^{\vartheta}x(t) &= \alpha(y - \varrho(z)x), \\ D^{\vartheta}y(t) &= -\xi x, \\ D^{\vartheta}z(t) &= x, \end{aligned} \tag{4}$$

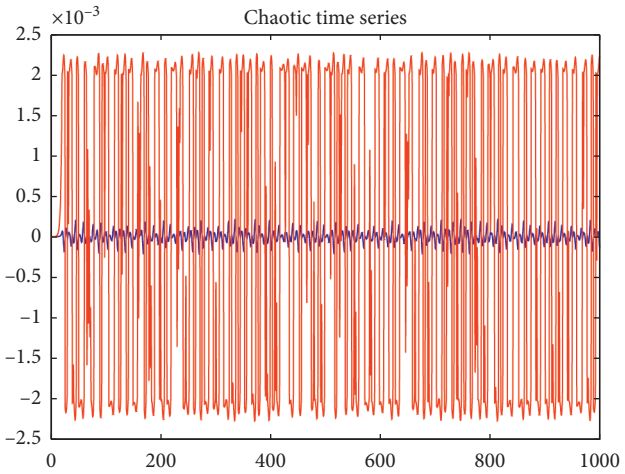


Figure 1: Chaotic time series.

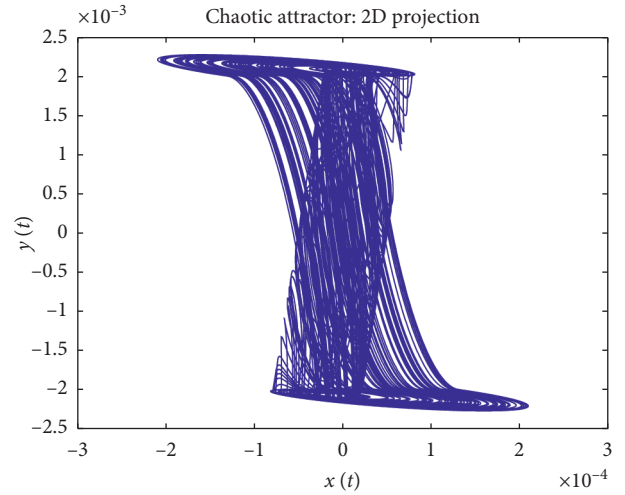


Figure 2: Chaotic attractor based on encryption method.

where D^{ϑ} denotes Caputo derivative, fractional order $\vartheta > 0$, α and ξ are parameters, $x(t)$, $y(t)$, and $z(t)$ are all system states, and

$$\varrho(z) = \begin{cases} a, & |z| < 1, \\ b, & |z| > 1, \end{cases} \tag{5}$$

in which a and b are the setting parameters.

In view of highly complex dynamic behavior in (4), we propose the new sine-sine maps:

$$\begin{aligned} x_{n+1} &= \mu \sin(\pi x_n) \times 2^{14} - \text{floor}\left(\mu \sin(\pi x_n) \times 2^{14}\right), \\ y_{n+1} &= \mu \sin(\pi y_n) \times 2^{14} - \text{floor}\left(\mu \sin(\pi y_n) \times 2^{14}\right), \\ z_{n+1} &= \mu \sin(\pi z_n) \times 2^{14} - \text{floor}\left(\mu \sin(\pi z_n) \times 2^{14}\right), \end{aligned} \tag{6}$$

where x_n, y_n, and z_n denote the outputted sequences and parameters $\mu \in (0, 10]$, x_0, y_0, and z_0 are original values of sequences.

Then, for (4), the specific process of encryption is as follows:

(1) First, using the sine-sine maps above to produce new sequences $X = \{x_n\}$, $Y = \{y_n\}$, $Z = \{z_n\}$, in ascending order, and then obtaining new permutation sequences $\widetilde{X}$, $\widetilde{Y}$, and $\widetilde{Z}$

(2) Converting plaintext into the sequences $\mathscr{K}$, $\mathscr{L}$, and $\mathscr{M}$, and then turning to the problem about displacement equations:

$$\begin{aligned} \widetilde{\mathscr{K}}(i) &= \mathscr{K}(\widetilde{X}(i)), \\ \widetilde{\mathscr{L}}(i) &= \mathscr{L}(\widetilde{Y}(i)), \\ \widetilde{\mathscr{M}}(i) &= \mathscr{M}(\widetilde{Z}(i)), \end{aligned} \tag{7}$$

where $i \in [1, 65536]$

(3) Converting the permutation sequences $\widetilde{\mathscr{K}}(i)$, $\widetilde{\mathscr{L}}(i)$, $\widetilde{\mathscr{M}}(i)$, to 256×256 matrices P_1, P_2, and P_3, respectively

(4) For P_1, P_2, and P_3, carrying out bitwise XOR operation; then, the encryption process ends, and ciphertext is generated

To apply the encryption method above in (4), by selecting $\vartheta = 0.5$, $\alpha = 1$, $\xi = 1$, $a = 0.02$, and $b = 2$, the chaotic time series are shown in Figure 3. Accordingly, the chaotic attractor in the phase diagram based on the encryption method is displayed in Figure 4, and the chaotic attractor in the three-dimensional space based on the encryption method is displayed in Figure 5.

Here, we present an encryption algorithm based on sine-sine map. In the initial stage of the encryption algorithm, the position of matrix about plaintext is replaced. After bitwise XOR operation, the key space of encryption algorithm is expanded, and the encryption algorithm is also robust.

4. Fourth-Order Chua System of Fractional Order

Consider a fourth-order Chua system of fractional order:

$$\begin{aligned} D^{\vartheta}x(t) &= \alpha(y - \varrho(l)x), \\ D^{\vartheta}y(t) &= -\xi(x + z), \\ D^{\vartheta}z(t) &= \beta y, \\ D^{\vartheta}l(t) &= x, \end{aligned} \tag{8}$$

where D^{ϑ} denotes Caputo derivative, fractional order $\vartheta > 0$, α, ξ, and β are parameters, $x(t)$, $y(t)$, $z(t)$ and $l(t)$, are all system states, and

$$\varrho(l) = \begin{cases} a, & |l| < 1, \\ b, & |l| > 1, \end{cases} \tag{9}$$

in which a and b are the setting parameters.

The high-dimensional character in (8) makes the traditional encryption method be outshone. Now, therefore, we employ the repetition quantization algorithm to encrypt (8):

(1) For (8), setting the system parameters and original values, to iterate k times, in order to eliminate the transient effect and ensure the chaotic state of system (8). Continuing to repeat, four real-valued sequences x_n, y_n, z_n, l_n are obtained.

(2) Using the formulas

$$\begin{aligned} \widetilde{x}_n &= \pi \log(x_n), \\ \widetilde{y}_n &= \pi \log(y_n), \\ \widetilde{z}_n &= \pi \log(z_n), \\ \widetilde{l}_n &= \pi \log(l_n), \end{aligned} \tag{10}$$

removing the integer parts of $\widetilde{x}_n$, $\widetilde{y}_n$, $\widetilde{z}_n$, and $\widetilde{l}_n$, and keeping decimal parts of real value:

$$\begin{aligned} \mathscr{A} &= |\widetilde{x}_n| - \operatorname{floor}(|\widetilde{x}_n|), \\ \mathscr{B} &= |\widetilde{y}_n| - \operatorname{floor}(|\widetilde{y}_n|), \\ \mathscr{C} &= |\widetilde{z}_n| - \operatorname{floor}(|\widetilde{z}_n|), \\ \mathscr{D} &= |\widetilde{l}_n| - \operatorname{floor}(|\widetilde{l}_n|). \end{aligned} \tag{11}$$

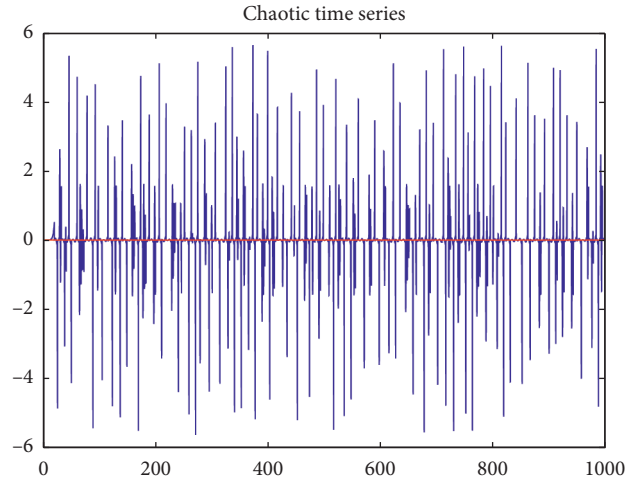


Figure 3: Chaotic time series.

(3) The decimals $\mathscr{A}$, $\mathscr{B}$, $\mathscr{C}$, and $\mathscr{D}$ are expressed in binary by the method of multiplying two and rounding.

(4) Calculating a new sequence $\mathscr{S}$, $\mathscr{S} = \mathscr{A} \oplus \mathscr{B} \oplus \mathscr{C} \oplus \mathscr{D}$.

(5) Repeating the above four steps (1)–(4) until the desired length of chaotic sequence is obtained.

To apply the encryption method above in (8), by selecting $\vartheta = 0.5$, $\alpha = 4.2$, $\xi = -1$, $\beta = -20$, $a = -2$, and $b = 9$, the chaotic time series are shown in Figure 6. Accordingly, the chaotic attractor in the phase diagram based on the encryption method is displayed in Figure 7, and the chaotic attractor in the three-dimensional space based on the encryption method is displayed in Figure 8.

Remark 1. Because of its wide frequency band, low voltage, low power consumption, high speed, simple circuit structure, and many other advantages, Chua oscillator has been concerned by the industry and has been widely used in various mode circuits. The design parameters in (1), (4), and (8) are similar to the ones in most probable Chua oscillator systems.

Remark 2. In Sections 2, 3, and 4, we analyze second-order, third-order, and fourth-order Chua systems of fractional order, respectively. With the rise of dimensions in dynamic system, the operation scale and complexity of the corresponding encryption algorithms are increasing.

Remark 3. For different dimensions about fractional-order Chua systems in Sections 2, 3, and 4, we have proposed different encryption algorithms. We should also notice that these encryption algorithms may not have overlap relationship. According to particular features of specific fractional-order Chua systems, we are aiming at a higher encryption level.

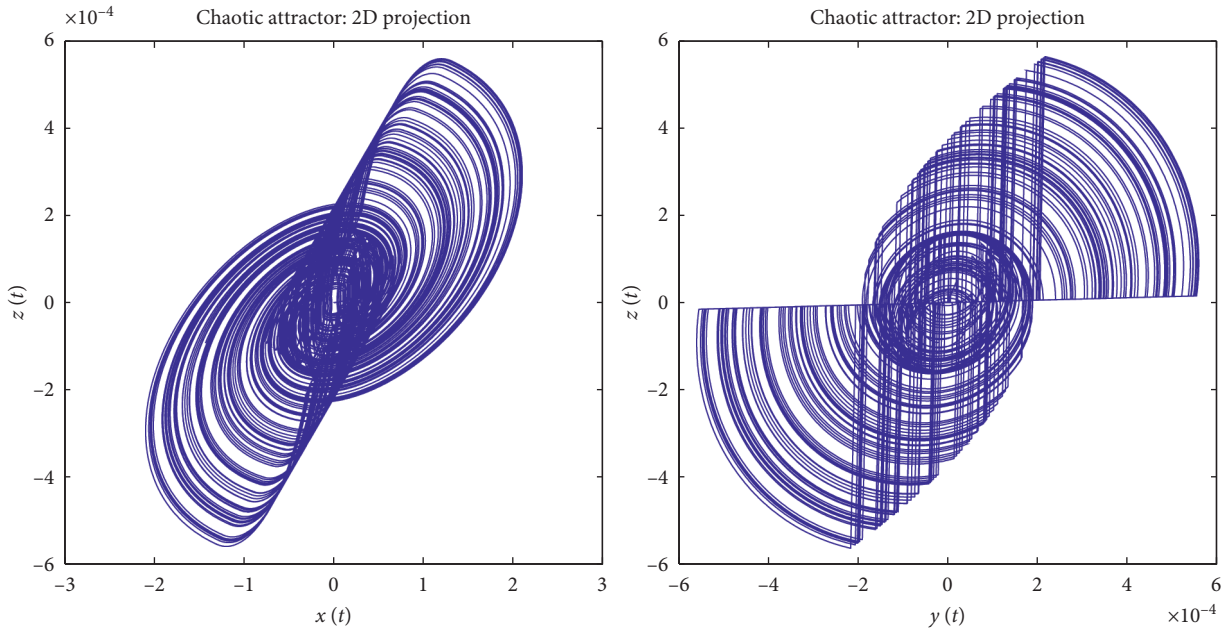


Figure 4: Chaotic attractor in the phase diagram based on the encryption method.

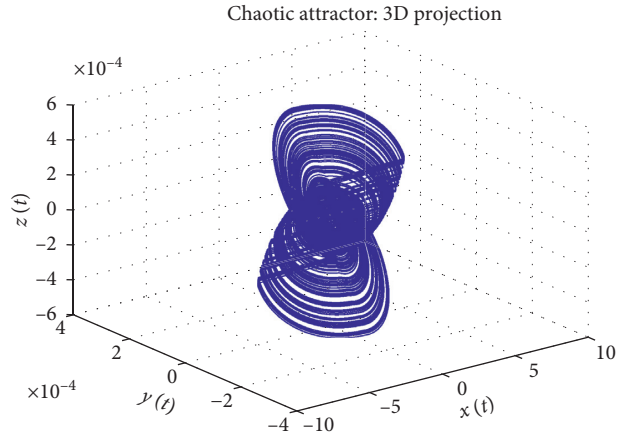


Figure 5: Chaotic attractor in the three-dimensional space based on the encryption method.

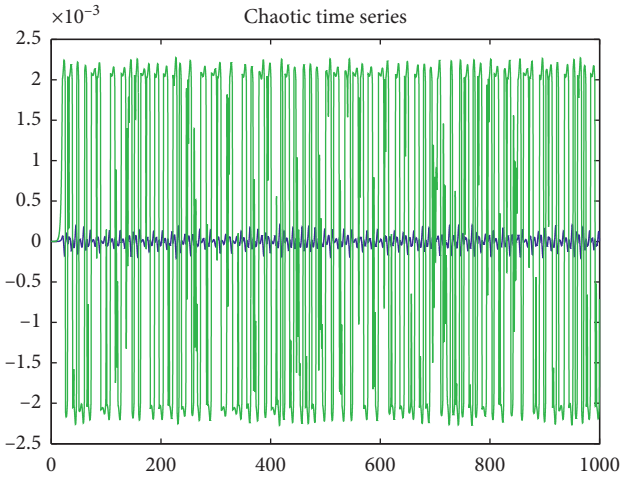


Figure 6: Chaotic time series.

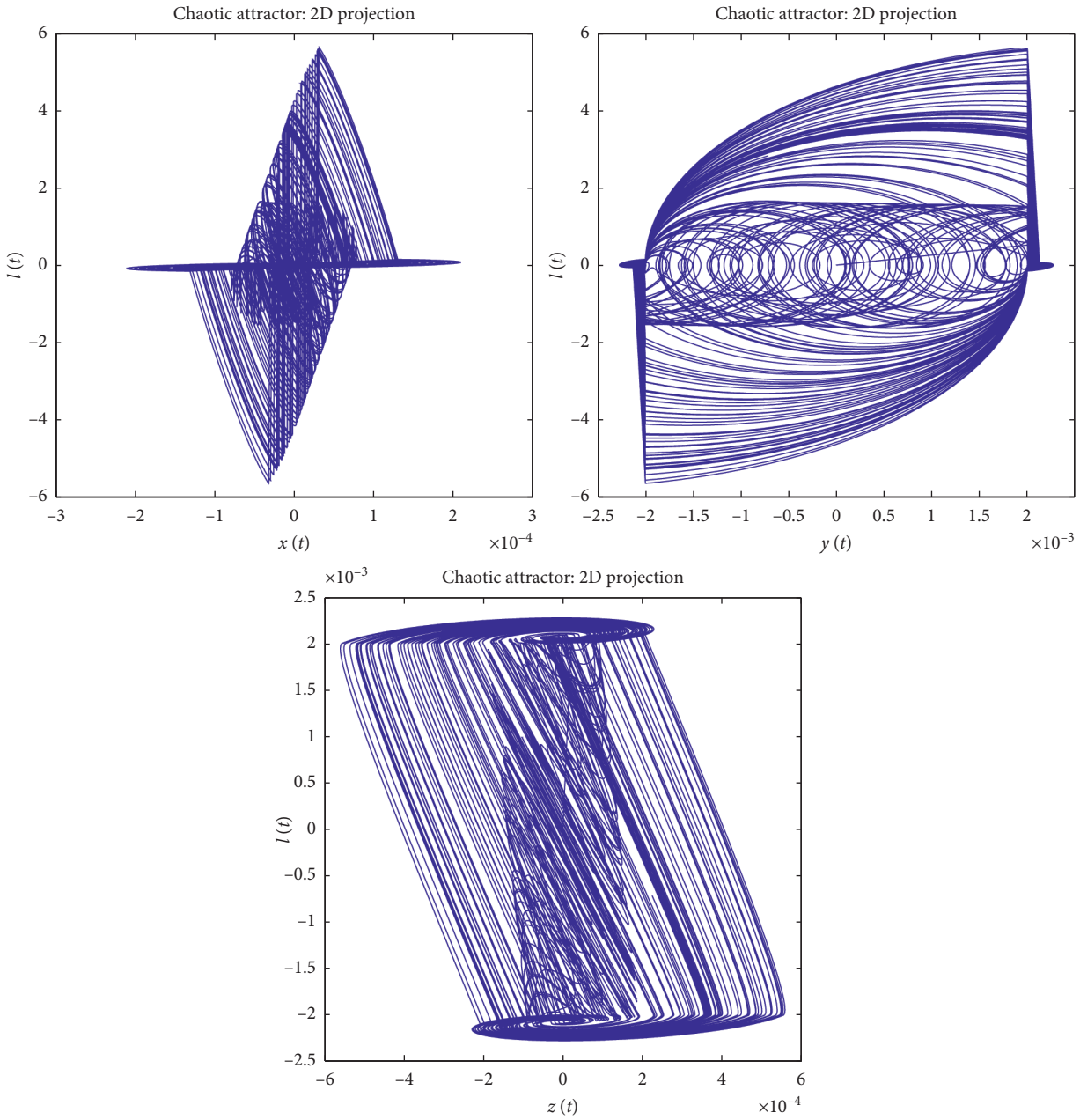


Figure 7: Chaotic attractor in the phase diagram based on the encryption method.

5. Application to Image Encryption

Correlation is an important index for testing chaotic sequences, and good correlation is an important guarantee for a system to realize reliable operation. In this section, by using the encryption methods in fractional-order Chua systems as in Sections 2–4, the generating chaotic series are used for image encryption.

The experimental test image is shown in Figure 9.

By using the encryption method in fractional-order Chua system (1) in Section 2, the encrypted image is displayed in Figure 10.

By using the encryption method in fractional-order Chua system (4) as in Section 3, the encrypted image is displayed in Figure 11.

By using the encryption method in fractional-order Chua system (8) as in Section 4, the encrypted image is displayed in Figure 12.

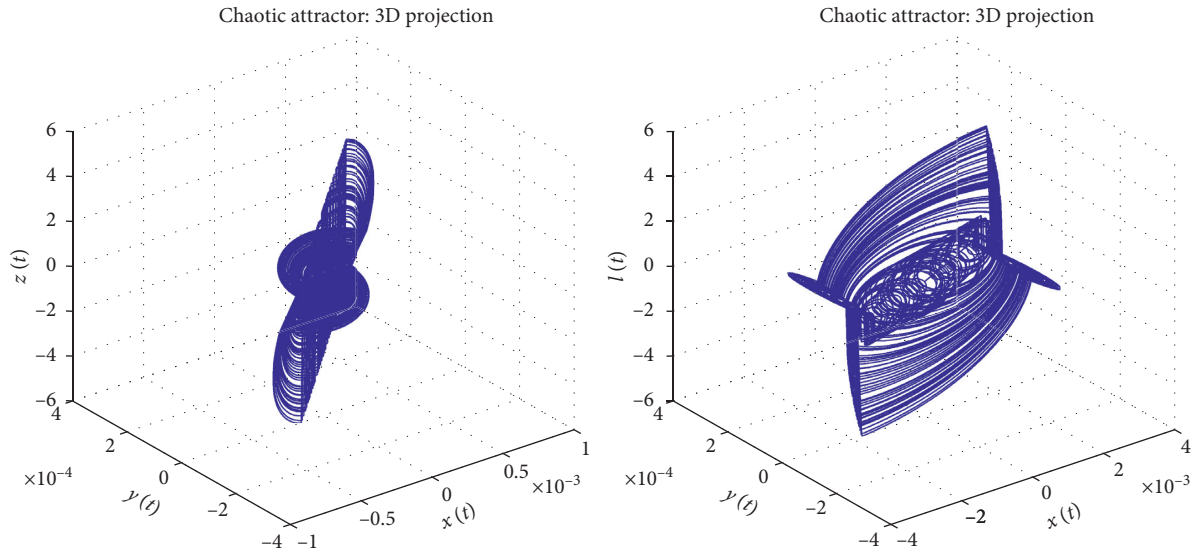


Figure 8: Chaotic attractor in the three-dimensional space based on the encryption method.

Figure 9: The experimental test image.

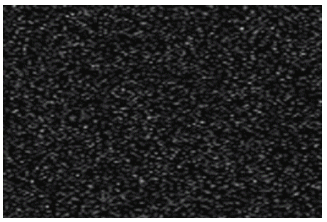


Figure 10: The encrypted image using the encryption method in fractional-order Chua system (1) as in Section 2.

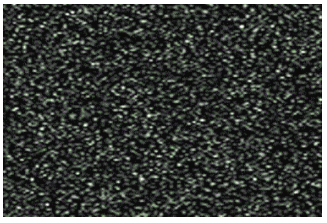


Figure 11: The encrypted image using the encryption method in fractional-order Chua system (4) as in Section 3.

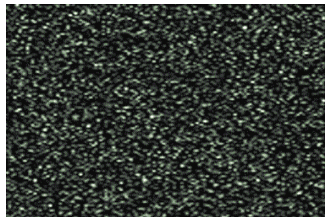
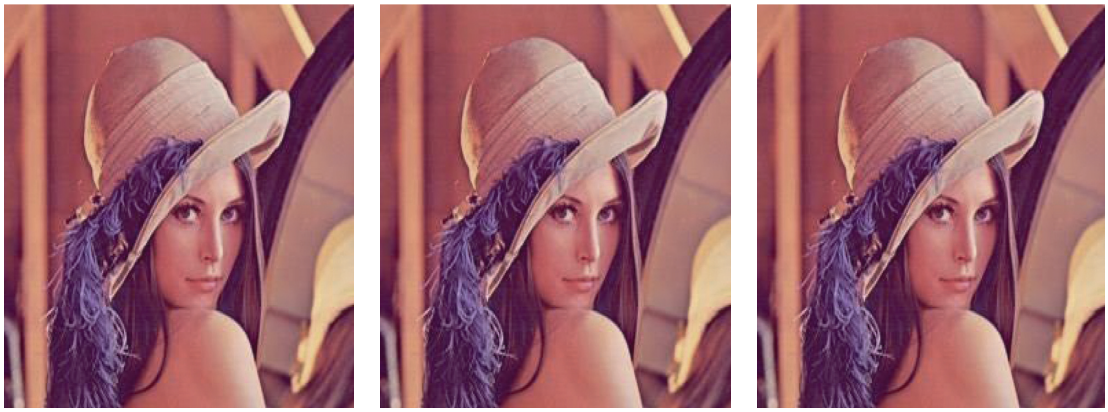


Figure 12: The encrypted image using the encryption method in fractional-order Chua system (8) as in Section 4.



(a) (b) (c)

Figure 13: The decrypted images. (a) Decrypted image (vs. the inverse process in Figure 10) (b) Decrypted image (vs. the inverse process in Figure 11) (c) Decrypted image (vs. the inverse process in Figure 12).

By adopting inverse process in encryption methods, the decrypted images are shown in Figure 13.

From the test results, in this paper, the encryption algorithms all have strong key sensitivity.

6. Conclusion

We have derived several encryption methods in fractional-order Chua systems for generating chaotic series. These encryption methods have antiattacking properties and rich nonlinear dynamics in generating chaotic series. We conclude, therefore, that the encryption methods via fractional-order Chua systems are useful for designing chaotic series in information encryption. Since zero-knowledge SNARKs can be applied to almost all scenarios on the blockchain, some relevant and interesting topics as future works include zero-knowledge cryptography and its extendibility in fractional-order Chua systems.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Authors' Contributions

Bo Gong wrote the draft of this paper. Haodong Zhang carried out the numerical simulations of this paper. Liguang Wan provided the idea of this paper. All authors read and approved the final manuscript.

Acknowledgments

This work was supported by the Scientific Research Program of Hubei Education Department under Grant B2019131 and the Youth Research Program of Hubei Normal University under Grant HS2020QN040.

References

[1] M. Dalir and N. Bigdeli, "The design of a new hybrid controller for fractional-order uncertain chaotic systems with unknown time-varying delays," *Applied Soft Computing*, vol. 87, Article ID 106000, 2020.

[2] A. Modiri and S. Mobayen, "Adaptive terminal sliding mode control scheme for synchronization of fractional-order uncertain chaotic systems," *ISA Transactions*, vol. 105, pp. 33–50, 2020.

[3] F. Ozkaynak, "On the effect of chaotic system in performance characteristics of chaos based s-box designs," *Physica A*, vol. 550, Article ID 124072, 2020.

[4] G. Savvidy, "Maximally chaotic dynamical systems," *Annals of Physics*, vol. 421, Article ID 168274, 2020.

[5] B. Wang, B. F. Zhang, and X. W. Liu, "An image encryption approach on the basis of a time delay chaotic system," *Optik*, vol. 225, Article ID 165737, 2021.

[6] M. R. Abuturab, "Multiple information encryption by user-image-based gyrator transform hologram," *Optics and Lasers in Engineering*, vol. 92, pp. 76–84, 2017.

[7] T. Etem and T. Kaya, "Self-generated encryption model of acoustics," *Applied Acoustics*, vol. 170, Article ID 107481, 2020.
[8] L. Martin, "Protecting credit card information: encryption vs tokenisation," *Network Security*, vol. 6, pp. 17–19, 2010.
[9] M. Saikia, "An efficient D2D quaternion encryption system for IoT using IEEE 754 standards," *Internet of Things*, vol. 11, Article ID 100261, 2020.
[10] A. Wu, H. Liu, and Z. Zeng, "Observer design and H∞ performance for discrete-time uncertain fuzzy-logic systems," *IEEE Transactions on Cybernetics*, p. 1, In press.
[11] B. S. T. Alkahtani, "Chua's circuit model with Atangana-Baleanu derivative with fractional order," *Chaos, Solitons & Fractals*, vol. 89, pp. 547–551, 2016.
[12] A. Atangana and S. İğret Araz, "New numerical approximation for Chua attractor with fractional and fractal-fractional operators," *Alexandria Engineering Journal*, vol. 59, no. 5, pp. 3275–3296, 2020.
[13] I. Petras, "A note on the fractional-order Chua's system, Chaos," *Solitons & Fractals*, vol. 38, no. 1, pp. 140–147, 2008.
[14] A. Wu and Z. Zeng, "Global Mittag-Leffler stabilization of fractional-order memristive neural networks," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 28, no. 1, pp. 206–217, 2017.
[15] C. P. Li, W. H. Deng, and D. Xu, "Chaos synchronization of the Chua system with a fractional order," *Physica A: Statistical Mechanics and Its Applications*, vol. 360, no. 2, pp. 171–185, 2006.