Research Article

Analyses and Encryption Implementation of a New Chaotic System Based on Semitensor Product

Rui Wang ^{1,2} Peifeng Du,^{2,3} Wenqi Zhong,^{2,4} Han Han,^{2,5} and Hui Sun ²

¹Tianjin Key Laboratory for Civil Aircraft Airworthiness and Maintenance, Civil Aviation University of China, Tianjin 300300, China

²College of Information Engineering and Automation, Civil Aviation University of China, Tianjin 300300, China

³School of Electronics and Communication Engineering (SECE), Sun Yat-sen University, Guangzhou 510006, China

⁴School of Automation, Northwestern Polytechnical University, Xi'an 710072, China

⁵North China Research Institute of Electro-Optics, Beijing 100015, China

Correspondence should be addressed to Rui Wang; wrhappyfuture@hotmail.com and Hui Sun; shhappy1@hotmail.com

Received 4 January 2020; Revised 27 April 2020; Accepted 21 May 2020; Published 17 July 2020

Guest Editor: Viet-Thanh Pham

Copyright © 2020 Rui Wang et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Semitensor product theory can deal with matrices multiplication with different numbers of columns and rows. Therefore, a new chaotic system for different high dimensions can be created by employing a semitensor product of chaotic systems with different dimensions, so that more channels can be selected for encryption. This paper proposes a new chaotic system generated by semitensor product applied on Qi and Lorenz systems. The corresponding dynamic characteristics of the new system are discussed in this paper to verify the existences of different attractors. The detailed algorithms are illustrated in this paper. The FPGA hardware encryption implementations are also elaborated and conducted. Correspondingly, the randomness tests are realized as well, and compared to that of the individual Qi system and Lorenz system, the proposed system in this paper owns the better randomness characteristic. The statistical analyses and differential and correlation analyses are also discussed.

1. Introduction

With the coming of 5G technology, more and more information is transformed by video, and video information security becomes more and more important in practical applications especially for long-distance transmission [1, 2]. The existing traditional encryption methods, such as DES and AES, however, cannot meet the high requirements for real time [3]. Therefore, it is necessary to focus on making progresses in the encryption technology in order to meet the real-time requirements.

People never stop studying the chaotic systems since Lorenz proposed the first chaotic system. Except for the typical chaotic systems, such as Chen, Lv, and Qi systems, some new different types of chaotic systems are generated as well, such as multistable chaotic hyperjerk system [4], a class of fractional-order partial differential systems [5], multistable modified fourth-order autonomous Chua's system [6],

coexisting chaotic attractors chaotic systems [7–9], and chaotic system generation with memristors [10]. The authors in reference [11] present a MDMBCAs design method without reconstructing nonlinear function. Correspondingly, chaotic systems are employed in different areas such as modeling neurodegenerative disease [12] and image and video encryptions [13–18]. It is known that the characteristics of chaotic systems, such as pseudorandomness and sensitivity to initial values, meet the requirements of encryption discussed in the Shannon's epoch-making paper "Communication Theory of Secrecy Systems." Consequently, it is hot for researchers to focus on the image and video data encryption, where the encrypted sequences are generated by chaotic systems in order to satisfy the need for remote communications and other applications. Multiple hardware platforms are implemented on encryptions such as FPGA, ARM, or circuits implementation [19–32]. Thus, different encryption methods based on various hardware

platforms are proposed in many articles [19]. The authors in reference [20] propose chaos encryption and decryption operated on FPGA and tested by TESTU01. The study in [21, 22] implements scrambling and antisqueezing of RGB three primary color pixel position and video chaotic encryption and decryption of pixel value on arm and a digital programmable audio encryption based on chaos system on FPGA. The effectiveness of chaotic secure communication system method is proved by using adder and multiplier of FPGA [23]. A generalized improved chaotic transformation mapping is proposed in [24]. Based on this mapping, the speech encryption of position transformation network is implemented on FPGA. Meanwhile, [25] realizes FPGA circuit output of three-dimensional chaotic system without balancing points on FPGA. The study in [26] implements the multibutterfly chaotic attractor problem on FPGA. The study in [27] proposes a Kolmogorov-type three-dimensional chaotic system and implements the chaotic system on FPGA. The study in [28] implements an application of high-dimensional digital chaos system (HDDCS) in image encryption in a limited precision range on FPGA. The study in [29] proposes a fractional order three-dimensional chaotic system with four wing chaotic attractors implemented on FPGA. The study in [30] proposes a sinusoidal chaotic model (SCM) and uses FPGA to implement chaotic mapping to verify its complexity and larger chaotic range. SOPC technology is used to realize the video processing of FPGA and the data receiving and sending of ARM [15]. A method of generating pseudorandom number based on chaotic system is proposed and implemented on FPGA [31]. In addition to FPGA and arm, [32, 33] also use improved modular circuit design in hyperchaotic system. The study in [34] studies the security of the latest three-dimensional chaotic self-synchronization flow secret key and a single secret key algorithm. The study in [35] proposes a method for a high-dimension chaotic system implemented on FPGA and also provides comparison among different methods, such as Real Domain Chaotic System (RDCS), Integer Domain Chaotic System (IDCS), Chaotic Bitwise Dynamical System (CBDS), and Higher-Dimensional Digital Chaotic Systems (HDDCS) implemented on FPGA. Compared to these methods, the proposed method can solve the dynamical degradation issue. The study in [36] discusses the Orthogonal Frequency Division Multiplexing-Passive Optical Network (OFDM-PON) method which initiates a method for real-time video encryption with chaotic systems. Chen. et al. design an encryption algorithm using chaotic control methods and implement this method on FPGA and ARM hardware platforms. Furthermore, the comparisons of the encryption method based on ARM and FPGA are discussed by mixing the advantages of each platform to achieve better real-time performance [15, 23, 24].

Semitensor product is a matrix operation first proposed by Cheng et al. [37]. This method breaks the restriction of matrix product; that is, the column dimension of the front matrix must be the same with the row dimension of the back matrix. Then semitensor product realizes the multiplication for matrices with different dimensions. Therefore, this method makes the matrices product more easily and can be

applied in much wider areas. Semitensor product method is also extended in nonlinear issues and multiple areas such as Boolean network control, game theory, compressed sensing, and data fusion [38–40]. The study in [41] provides the literature review for the applications of semitensor product in engineering areas. This paper is inspired by the typical characteristics of semitensor product method mentioned previously which provides a new idea to generate chaotic systems. The new chaotic systems can be employed in real-time video encryption areas as well.

The main contribution of this paper is to employ the unique characteristic of the semitensor product to form a new chaotic system with different-order chaotic systems, Qi and Lorenz systems, in order to enhance the randomness of the sequence. Then the dynamic characteristics of the new chaotic system are analyzed, and the system is applied in video encryption. When compared to the individual chaotic system, the new one constructed by semitensor product has the overwhelmed pseudorandomness.

The rest of the paper is arranged as follows. Section 2 presents a new chaotic system formed by semitensor product theory. Furthermore, the corresponding dynamic characteristics of the system are analyzed. Section 3 provides the detailed encryption implementation based on FPGA with the new chaotic system. NIST test and the corresponding stochastic analysis are conducted as well in this section. The conclusion of the paper is drawn in Section 4.

2. A New Chaotic System Based on the Semitensor Product Theory

2.1. Preliminaries of Semitensor Product. Normally, the semitensor product operation includes left semitensor product operation and right semitensor product operation. Left semitensor product operation meets the multiple-dimension condition; that is, $n = t \times p$ ($t \in \mathbb{N}^+$). Or if $p = s \times n$ ($s \in \mathbb{N}^+$), the operation is right semitensor product operation.

Lemma 1. Assume matrix A is $m \times n$, matrix B is $p \times q$, and $n = t \times p$ ($t \in \mathbb{N}^+$) [42]. Let A be divided into a blocking matrix $[A_1, \dots, A_t]$, where A_i ($i = 1, \dots, t$) is an $m \times p$ matrix. Then the left semitensor product is defined as

$$A \ltimes B^{p \times q} = (A_1^{m \times p} B^{p \times q}, A_2^{m \times p} B^{p \times q}, A_3^{m \times p} B^{p \times q}, \dots, A_t^{m \times p} B^{p \times q})^{m \times tq}, \quad (1)$$

where “ $\ltimes$ ” is the left semitensor product.

Lemma 2. If $A \in M_{m \times tp}$ and $B \in M_{p \times q}$, then

$$A \ltimes B = A(B \otimes I_t), \quad (2)$$

where $\otimes$ is the Kronecker product of matrices [42].

2.2. A New Chaotic System Generated by Semitensor Product Theory. Qi system is a hyperchaotic system with two positive Lyapunov exponents, 3 and 13, under certain conditions [28]. And it could be used for secure communication due to its large positive Lyapunov exponents. It is known that Qi system is described as follows:

$$\begin{cases} \dot{x}_{Q1} = a(x_{Q2} - x_{Q1}) + x_{Q2}x_{Q3}, \\ \dot{x}_{Q2} = b(x_{Q1} + x_{Q2}) - x_{Q1}x_{Q3}, \\ \dot{x}_{Q3} = -cx_{Q3} - ex_{Q4} + x_{Q1}x_{Q2}, \\ \dot{x}_{Q4} = -dx_{Q4} + fx_{Q3} + x_{Q1}x_{Q2}, \end{cases} \quad (3)$$

where x_{Qi} ($i = 1, 2, 3, 4$) is the state variable and a, b, c, d , and f are the related system parameters. System (3) is a hyperchaotic system, when $49 \leq a \leq 55$, $20 \leq b \leq 24$, $c = 13$, $d = 8$, $e = 33$, and $f = 30$.

The first chaotic system under study is a Lorenz chaotic system [28]. The dynamics of the system are shown in

$$\begin{cases} \dot{x} = \sigma(y - x), \\ \dot{y} = rx - y - xz, \\ \dot{z} = xy - \beta z, \end{cases} \quad (4)$$

where x, y , and z are state variables and σ, r , and β are the related system parameters. The typical system parameters for Lorenz chaotic system are selected as $\sigma = 10$, $r = 28$, and $\beta = 8/3$.

It is relaxed for semitensor product operation only to satisfy the multiple-dimension condition. Therefore, different numbers state variables of systems can be selected and conduct semitensor operation. For example, this paper selects a two-dimension state variable $(xy)^T$ of Lorenz system and a four-dimension state variable $(x_{Q1}x_{Q2}x_{Q3}x_{Q4})$

T of Qi system to operate semitensor product. The result is shown as follows:

$$\begin{bmatrix} x \\ y \end{bmatrix} \ltimes \begin{bmatrix} x_{Q1} \\ x_{Q2} \\ x_{Q3} \\ x_{Q4} \end{bmatrix} = \begin{bmatrix} x \\ x \end{bmatrix} \begin{bmatrix} x_{Q1} \\ x_{Q2} \\ x_{Q3} \\ x_{Q4} \end{bmatrix}^T y \begin{bmatrix} x_{Q1} \\ x_{Q2} \\ x_{Q3} \\ x_{Q4} \end{bmatrix}^T. \quad (5)$$

It is observed that the result of equation (5) is eight-dimension column vector which is equivalent to the new system state variable vector $(x_1x_2x_3x_4x_5x_6x_7x_8)^T$; that is,

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \end{bmatrix} = \begin{bmatrix} xx_{Q1} \\ xx_{Q2} \\ xx_{Q3} \\ xx_{Q4} \\ yx_{Q1} \\ yx_{Q2} \\ yx_{Q3} \\ yx_{Q4} \end{bmatrix}. \quad (6)$$

Differentiate each state variable in equation (6), and substitute equations (3) and (4) into the result. Then the following equation can be derived:

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \\ \dot{x}_3 \\ \dot{x}_4 \\ \dot{x}_5 \\ \dot{x}_6 \\ \dot{x}_7 \\ \dot{x}_8 \end{bmatrix} = \begin{bmatrix} \dot{xx}_{Q1} + x\dot{x}_{Q1} \\ \dot{xx}_{Q2} + x\dot{x}_{Q2} \\ \dot{xx}_{Q3} + x\dot{x}_{Q3} \\ \dot{xx}_{Q4} + x\dot{x}_{Q4} \\ \dot{yx}_{Q1} + y\dot{x}_{Q1} \\ \dot{yx}_{Q2} + y\dot{x}_{Q2} \\ \dot{yx}_{Q3} + y\dot{x}_{Q3} \\ \dot{yx}_{Q4} + y\dot{x}_{Q4} \end{bmatrix} = \begin{bmatrix} \sigma(y-x)x_{Q1} + ax(x_{Q2} - x_{Q1}) + xx_{Q2}x_{Q3} \\ \sigma(y-x)x_{Q2} + bx(x_{Q1} + x_{Q2}) - xx_{Q1}x_{Q3} \\ \sigma(y-x)x_{Q3} - cx_{Q3} - ex_{Q4} + xx_{Q1}x_{Q2} \\ \sigma(y-x)x_{Q4} - dx_{Q4} + fx_{Q3} + xx_{Q1}x_{Q2} \\ (rx - y - xz)x_{Q1} + ay(x_{Q2} - x_{Q1}) + yx_{Q2}x_{Q3} \\ (rx - y - xz)x_{Q2} + by(x_{Q1} + x_{Q2}) - yx_{Q1}x_{Q3} \\ (rx - y - xz)x_{Q3} - cy_{Q3} - ey_{Q4} + yx_{Q1}x_{Q2} \\ (rx - y - xz)x_{Q4} - dy_{Q4} + fy_{Q3} + yx_{Q1}x_{Q2} \end{bmatrix} = \begin{bmatrix} \sigma(x_5 - x_1) + a(x_2 - x_1) + \frac{x_2x_3}{x} \\ \sigma(x_6 - x_2) + b(x_2 + x_1) - \frac{x_1x_3}{x} \\ \sigma(x_7 - x_3) - cx_3 - ex_4 + \frac{x_1x_2}{x} \\ \sigma(x_8 - x_4) - dx_4 + fx_3 + \frac{x_1x_2}{x} \\ rx_1 - x_5 - x_1z + a(x_6 - x_5) + \frac{x_6x_7}{x} \\ rx_2 - x_6 - x_2z + b(x_5 + x_6) - \frac{x_5x_7}{x} \\ rx_3 - x_7 - x_3z - cx_7 - ex_8 + \frac{x_5x_6}{x} \\ rx_4 - x_8 - x_4z - dx_8 + fx_7 + \frac{x_5x_6}{x} \end{bmatrix}. \quad (7)$$

It is obvious that the dynamics of (7) still include three state variables of Lorenz system, x, y , and z . Therefore, insert

equation (4) into equation (7) and then form a complete eleven-dimension system as illustrated in the following:

$$\begin{cases}
 \dot{x}_1 = \sigma(x_5 - x_1) + a(x_2 - x_1) + \frac{x_2 x_3}{x}, \\
 \dot{x}_2 = \sigma(x_6 - x_2) + b(x_2 + x_1) - \frac{x_1 x_3}{x}, \\
 \dot{x}_3 = \sigma(x_7 - x_3) - cx_3 - ex_4 + \frac{x_1 x_2}{x}, \\
 \dot{x}_4 = \sigma(x_8 - x_4) - dx_4 + fx_3 + \frac{x_1 x_2}{x}, \\
 \dot{x}_5 = rx_1 - x_5 - x_1 z + a(x_6 - x_5) + \frac{x_6 x_7}{y}, \\
 \dot{x}_6 = rx_2 - x_6 - x_2 z + b(x_5 + x_6) - \frac{x_5 x_7}{y}, \\
 \dot{x}_7 = rx_3 - x_7 - x_3 z - cx_7 - ex_8 + \frac{x_5 x_6}{y}, \\
 \dot{x}_8 = rx_4 - x_8 - x_4 z - dx_8 + fx_7 + \frac{x_5 x_6}{y}, \\
 \dot{x} = \sigma(y - x), \\
 \dot{y} = rx - y - xz, \\
 \dot{z} = xy - \beta z.
 \end{cases} \quad (8)$$

As seen from equation (8), if one substitutes $x \rightarrow -x$, $y \rightarrow -y$, and $z \rightarrow z$, $\dot{z} = (-x)(-y) - \beta z = xy - \beta z$, it proves that it is symmetric with respect to z variable for x and y .

2.3. Numerical Analysis of the New System. The paper analyzes some dynamics characteristics of the new system including symmetry, dissipativity, equilibrium point, equilibria, bifurcation diagram, Lyapunov diagram, and phase portraits.

2.3.1. Symmetry. As described in system (8), the system is symmetry with respect to z -axis since the system is invariant under the coordinate transformations: $(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x, y, z) \rightarrow (-x_1, -x_2, -x_3, -x_4, -x_5, -x_6, -x_7, -x_8, -x, -y, z)$.

2.3.2. Dissipativity. The divergence of system (12) is given by

$$\begin{aligned}
 \nabla \cdot f &= \frac{\partial f_1}{\partial x_1} + \frac{\partial f_2}{\partial x_2} + \dots + \frac{\partial f_8}{\partial x_8} + \frac{\partial f_9}{\partial x} + \frac{\partial f_{10}}{\partial y} + \frac{\partial f_{11}}{\partial z} \\
 &= -5\sigma - 2a + 2b - 2c - 2d - 5 - \beta,
 \end{aligned} \quad (9)$$

and when $-5\sigma - 2a + 2b - 2c - 2d - 5 - \beta < 0$, the system undergoes dissipation.

2.3.3. Equilibria. As shown in system (8), x , y , and z could not be zero when calculating equilibria. Then the equilibria of system (8) are $(0, 0, 0, 0, 0, 0, 0, 0, \pm\sqrt{\beta(r-1)}, \pm\sqrt{\beta(r-1)}, r-1)$. One has

$$J_{1,2} = \begin{bmatrix}
 -\sigma - a & a & 0 & 0 & \sigma & 0 & 0 & 0 & 0 & 0 & 0 \\
 b & b - \sigma & 0 & 0 & 0 & \sigma & 0 & 0 & 0 & 0 & 0 \\
 0 & 0 & -\sigma - c & -e & 0 & 0 & \sigma & 0 & 0 & 0 & 0 \\
 0 & 0 & f & -\sigma - d & 0 & 0 & 0 & \sigma & 0 & 0 & 0 \\
 1 & 0 & 0 & 0 & -1 - a & a & 0 & 0 & 0 & 0 & 0 \\
 0 & 1 & 0 & 0 & b & b - 1 & 0 & 0 & 0 & 0 & 0 \\
 0 & 0 & 1 & 0 & 0 & 0 & -1 - c & -e & 0 & 0 & 0 \\
 0 & 0 & 0 & 1 & 0 & 0 & f & -1 - d & 0 & 0 & 0 \\
 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -\sigma & 0 & 0 \\
 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 & 0 \\
 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \pm\sqrt{\beta(r-1)} & \pm\sqrt{\beta(r-1)} & \beta
 \end{bmatrix}_{\text{equilibria}} \quad (10)$$

The corresponding polynomial is

$$f(\lambda) = \lambda(\lambda + \beta)(\lambda - 1)f_1(\lambda) \quad (11)$$

where $f_1(\lambda)$ is an eighth-order polynomial. It is obvious that at least 0, 1, and $-\beta$ are eigenvalues of system (8) for the these equilibrium points; therefore, not each real part of the

eigenvalues is negative. Then it can be concluded that these are not stable equilibrium points.

2.3.4. Bifurcation Diagram, Lyapunov Diagram, and Phase Portraits. It is known that when $49 \leq a \leq 55$, $20 \leq b \leq 24$, $c = 13$, $d = 8$, $e = 33$, and $f = 30$, Qi system is a hyperchaotic system. When $\sigma = 10$, $r = 28$, and $\beta = 8/3$, Lorenz system is a chaotic system. Therefore, the paper selects the parameters $a = 50$, $c = 13$, $d = 8$, $e = 33$, $f = 30$, $\sigma = 10$, $r = 28$, and $\beta = 8/3$ and varies b to analyze the bifurcation of system (12) as shown in Figure 1(a). As the bifurcation diagram shows, the system demonstrates the chaotic characteristics when $b \in [-5, 26]$. The corresponding Lyapunov diagram is illustrated in Figure 1(b). Furthermore, partial phase portraits of system (7) for different initials when $b = 24$ are shown in Figures 1(c). One has

$$\left\{ \begin{array}{l} \dot{x}_1 = 10(x_5 - x_1) + 50(x_2 - x_1) + \frac{x_2 x_3}{x}, \\ \dot{x}_2 = 10(x_6 - x_2) + b(x_2 + x_1) - \frac{x_1 x_3}{x}, \\ \dot{x}_3 = 10(x_7 - x_3) - 13x_3 - 33x_4 + \frac{x_1 x_2}{x}, \\ \dot{x}_4 = 10(x_8 - x_4) - 8x_4 + 30x_3 + \frac{x_1 x_2}{x}, \\ \dot{x}_5 = 28x_1 - x_5 - x_1 z + 50(x_6 - x_5) + \frac{x_6 x_7}{y}, \\ \dot{x}_6 = 28x_2 - x_6 - x_2 z + b(x_5 + x_6) - \frac{x_5 x_7}{y}, \\ \dot{x}_7 = 28x_3 - x_7 - x_3 z - 13x_7 - 33x_8 + \frac{x_5 x_6}{y}, \\ \dot{x}_8 = 28x_4 - x_8 - x_4 z - 8x_8 + 30x_7 + \frac{x_5 x_6}{y}, \\ \dot{x} = 10(y - x), \\ \dot{y} = 28x - y - xz, \\ \dot{z} = xy - \frac{8}{3z}. \end{array} \right. \quad (12)$$

Figures 1(c)–1(f) illustrate different phase portraits including x_1 versus x_2 , x_2 versus x_4 , x_3 versus x , and x versus z when $b = 24$ for two initial value sets, the initial values for the blue line phase portraits are 0.01418, 0.04217, 0.09157, 0.07922, 0.09594, 0.06557, 0.00357, 0.08491, 0.09339, 0.06787, and 0.07577, and those for the red line phase

portraits are 0.01417, 0.04218, 0.09156, 0.07921, 0.09593, 0.06558, 0.00356, 0.08492, 0.09338, 0.06788, and 0.07576. These portraits demonstrate that system (12) has obvious chaotic attractors and approaches periodic characteristics as initial values changes.

3. Encryption Implementation with the New Chaotic System Based on FPGA

This paper employs the random sequence of system (12) as the random sequence to encrypt video data and realize the hardware implement on FPGA. Figure 2 is the FPGA hardware diagram used for the encryption. The main components are HDMI, ZYNQ, JTAG, and source interface. The video is collected from JTAG, then the encryption algorithm is performed in ZYNQ powered by 5 V DC, and the outputs will be shown in the monitor through HDMI.

The encryption algorithm is described in the following, and the corresponding block diagram is demonstrated in Figure 3:

Step 1: to generate the random sequences for each state variable for both discretized Qi system and Lorenz system, respectively.

Step 2: to generate the random sequence for the new system (12) constructed by semitensor product operation on $(x_{Q1} \ x_{Q2} \ x_{Q3} \ x_{Q4})^T$ and $(x \ y)^T$.

Step 3: to generate the sequence $x_i = (x_{i1}, x_{i2}, x_{i3}, \dots, x_{i32})$ by the new system ($i = 1, 2, \dots, 8, j = 1, 2, \dots, 32$), where x_{ij} is a binary number, i represents the number of state variables, and j is the bit number for each state variable. Choose a sequence x_i with fixed bits from t to q ; that is,

$$c_i(n) = ((x_i \bmod 2^q) \bmod 2^{t-q}), \quad (i = 1, 2, \dots, 8, 1 \leq t < q \leq 32). \quad (13)$$

Make an XOR operation on $c_i(n)$ and divide video data based on pixels; that is,

$$m(n) = ((x_i \bmod 2^{t-1}) \bmod 2^{t-q}) \oplus (m), \quad (14)$$

where $\oplus$ is the XOR operation.

3.1. Discretization for the New System and Its Implementation Based on FPGA. In the hardware experiment, it is impossible to implement the continuous Lorenz and Qi chaotic systems because of limitation of the bit width in FPGA. Therefore, it is necessary to discretize continuous system first. Multiple methods can be used to discretize a differential equation such as Euler method, improved Euler method, and Runge-Kutta method. To meet the requirement of real-time performance and the limitation of hardware implementation, Euler method is used to discretize the differential equations due to its low computation complexity. First, Euler method is used to discretize Qi and Lorenz systems, respectively. The corresponding process of Qi system is proposed as follows:

FIGURE 1: Continued.

FIGURE 1: Bifurcation diagram along with b variation and partial phase portraits for different initial values (blue line for the first initial value set and red line for the second initial value set).

FIGURE 2: FPGA hardware diagram.

FIGURE 3: Block diagram of encryption algorithm.

$$\begin{cases} \frac{(x_{Q1}(n+1) - x_{Q1}(n))}{\tau} = a(x_{Q2}(n) - x_{Q1}(n)) + x_{Q2}(n)x_{Q3}(n), \\ \frac{(x_{Q2}(n+1) - x_{Q2}(n))}{\tau} = b(x_{Q1}(n) + x_{Q2}(n)) - x_{Q1}(n)x_{Q3}(n), \\ \frac{(x_{Q3}(n+1) - x_{Q3}(n))}{\tau} = -cx_{Q3}(n) - ex_{Q4}(n) + x_{Q1}(n)x_{Q2}(n), \\ \frac{(x_{Q4}(n+1) - x_{Q4}(n))}{\tau} = -dx_{Q4}(n) + fx_{Q3}(n) + x_{Q1}(n)x_{Q2}(n). \end{cases} \quad (15)$$

Then, the iteration equations of Qi system are shown in

$$\begin{cases} x_{Q1}(n+1) = a\tau x_{Q2}(n) + (1 - a\tau)x_{Q1}(n) + \tau x_{Q2}(n)x_{Q3}(n), \\ x_{Q2}(n+1) = b\tau x_{Q1}(n) + (1 + b\tau)x_{Q2}(n) - \tau x_{Q1}(n)x_{Q3}(n), \\ x_{Q3}(n+1) = (1 - c\tau)x_{Q3}(n) - e\tau x_{Q4}(n) + \tau x_{Q1}(n)x_{Q2}(n), \\ x_{Q4}(n+1) = (1 - d\tau)x_{Q4}(n) + f\tau x_{Q3}(n) + \tau x_{Q1}(n)x_{Q2}(n). \end{cases} \quad (16)$$

Similarly, the discrete Lorenz system is

$$\begin{cases} \frac{x(n+1) - x(n)}{\tau} = \sigma(y(n) - x(n)), \\ \frac{y(n+1) - y(n)}{\tau} = rx(n) - y(n) - x(n)z(n), \\ \frac{z(n+1) - z(n)}{\tau} = x(n)y(n) - \beta z(n). \end{cases} \quad (17)$$

Correspondingly, the iteration equations of Lorenz system are

$$\begin{cases} x(n+1) = \sigma\tau y(n) + (1 - \sigma\tau)x(n), \\ y(n+1) = r\tau x(n) + (1 - \tau)y(n) - \tau x(n)z(n), \\ z(n+1) = \tau x(n)y(n) + (1 - \beta\tau)z(n). \end{cases} \quad (18)$$

In general, FPGA can store float data and fixed-point data. Since fixed-point data require less computing resources than that of float data, this paper uses 64-bit fixed-point

number to represent the data. The detailed data format of 64-bit fixed-point numbers is shown in Figure 4.

In Figure 4, I represents the integer part of 64-bit fixed-point numbers, and f is the fractional part.

As mentioned before, because of the limitation of bit width in FPGA, all data are truncated numbers in hardware implementation. Therefore, the Qi and Lorenz system becomes

$$\begin{cases} \lfloor x_{Q1}(n+1) \rfloor = a\tau \lfloor x_{Q2}(n) \rfloor + (1 - a\tau) \lfloor x_{Q1}(n) \rfloor + \tau \lfloor x_{Q2}(n) \rfloor \lfloor x_{Q3}(n) \rfloor, \\ \lfloor x_{Q2}(n+1) \rfloor = b\tau \lfloor x_{Q1}(n) \rfloor + (1 + b\tau) \lfloor x_{Q2}(n) \rfloor - \tau \lfloor x_{Q1}(n) \rfloor \lfloor x_{Q3}(n) \rfloor, \\ \lfloor x_{Q3}(n+1) \rfloor = (1 - c\tau) \lfloor x_{Q3}(n) \rfloor - e\tau \lfloor x_{Q4}(n) \rfloor + \tau \lfloor x_{Q2}(n) \rfloor \lfloor x_{Q1}(n) \rfloor, \\ \lfloor x_{Q4}(n+1) \rfloor = (1 - d\tau) \lfloor x_{Q4}(n) \rfloor + f\tau \lfloor x_{Q3}(n) \rfloor + \tau \lfloor x_{Q1}(n) \rfloor \lfloor x_{Q2}(n) \rfloor, \end{cases} \quad (19)$$

$$\begin{cases} \lfloor x(n+1) \rfloor = \sigma\tau \lfloor y(n) \rfloor + (1 - \sigma\tau) \lfloor x(n) \rfloor, \\ \lfloor y(n+1) \rfloor = r\tau \lfloor x(n) \rfloor + (1 - \tau) \lfloor y(n) \rfloor - \tau \lfloor x(n) \rfloor \lfloor z(n) \rfloor, \\ \lfloor z(n+1) \rfloor = \tau \lfloor x(n) \rfloor \lfloor y(n) \rfloor + (1 - \beta\tau) \lfloor z(n) \rfloor. \end{cases} \quad (20)$$

Let the iteration step be $\tau=0.00001$ and use the same parameters in system (12). Then substitute them into (19)

and (20), respectively. Therefore, Qi system and Lorenz system are changed as follows:

$$\begin{cases} \lfloor x_{Q1}(n+1) \rfloor = 0.9995 \lfloor x_{Q2}(n) \rfloor + 0.0005 \lfloor x_{Q1}(n) \rfloor + 0.00001 \lfloor x_{Q2}(n) \rfloor \lfloor x_{Q3}(n) \rfloor, \\ \lfloor x_{Q2}(n+1) \rfloor = 0.0002 \lfloor x_{Q1}(n) \rfloor + 1.0002 \lfloor x_{Q2}(n) \rfloor - 0.00001 \lfloor x_{Q1}(n) \rfloor \lfloor x_{Q3}(n) \rfloor, \\ \lfloor x_{Q3}(n+1) \rfloor = 0.99987 \lfloor x_{Q3}(n) \rfloor - 0.00033 \lfloor x_{Q4}(n) \rfloor + 0.00001 \lfloor x_{Q2}(n) \rfloor \lfloor x_{Q1}(n) \rfloor, \\ \lfloor x_{Q4}(n+1) \rfloor = 0.00008 \lfloor x_{Q4}(n) \rfloor + 0.9997 \lfloor x_{Q3}(n) \rfloor + 0.00001 \lfloor x_{Q1}(n) \rfloor \lfloor x_{Q2}(n) \rfloor, \end{cases} \quad (21)$$

$$\begin{cases} \lfloor x(n+1) \rfloor = 0.0001 \lfloor y(n) \rfloor + 0.9999 \lfloor x(n) \rfloor, \\ \lfloor y(n+1) \rfloor = 0.00028 \lfloor x(n) \rfloor + 0.99999 \lfloor y(n) \rfloor - 0.00001 \lfloor x(n) \rfloor \lfloor z(n) \rfloor, \\ \lfloor z(n+1) \rfloor = 0.00001 \lfloor x(n) \rfloor \lfloor y(n) \rfloor + 0.9999733 \lfloor z(n) \rfloor. \end{cases} \quad (22)$$

To iterate Qi system and Lorenz system and make semitensor product operation on these two systems after each iteration, respectively, the discretized first 8 state variables of the new system are obtained:

$$\begin{cases} x_1(n+1) = \lfloor x(n+1) \rfloor \times \lfloor x_{Q1}(n+1) \rfloor, \\ x_2(n+1) = \lfloor x(n+1) \rfloor \times \lfloor x_{Q2}(n+1) \rfloor, \\ x_3(n+1) = \lfloor x(n+1) \rfloor \times \lfloor x_{Q3}(n+1) \rfloor, \\ x_4(n+1) = \lfloor x(n+1) \rfloor \times \lfloor x_{Q4}(n+1) \rfloor, \\ x_5(n+1) = \lfloor y(n+1) \rfloor \times \lfloor x_{Q1}(n+1) \rfloor, \\ x_6(n+1) = \lfloor y(n+1) \rfloor \times \lfloor x_{Q2}(n+1) \rfloor, \\ x_7(n+1) = \lfloor y(n+1) \rfloor \times \lfloor x_{Q3}(n+1) \rfloor, \\ x_8(n+1) = \lfloor y(n+1) \rfloor \times \lfloor x_{Q4}(n+1) \rfloor, \end{cases} \quad (23)$$

where $x_i(n+1)$ and $x_i(n)$ are system state variables. $\lfloor y(n+1) \rfloor$ is the approximate value of $y(n+1)$ using fixed-point number.

3.2. Implementation and Analysis of Encryption Algorithm of the New Chaotic System. In order to ensure the randomness of the random sequence, therefore, select the low bits from t to q as shown in Figure 5. The positions of these bits are not close to those of sign and exponent bits. Then the chosen random encryption sequence, $c_i(n)$, is shown in equation (17). This paper selects $t=1$ and $q=6$:

$$c_i(n) = \text{mod} \left(\left(\frac{\lfloor x_i(n) \rfloor}{2^{t-1}} \right), 2^{q-t+1} \right), \quad i = 1, 2, \dots, 8. \quad (24)$$

Random sequences which are selected from eight states based on the method mentioned previously are combined to generate the random sequence, $c(n)$:

$$c(n) = (c_1(n), c_2(n), \dots, c_8(n)). \quad (25)$$

In order to resist the differential attack and decrease the correlation between adjacent random sequences, the paper selects the very first iteration sequence among every N iterations and stacks these selected sequences to construct a

FIGURE 4: Data format for 64-bit fixed-point numbers.

FIGURE 5: The schematics of numbered data bits.

random sequence, $c(n)$, as shown in equation (18). This can improve the randomness of the random sequence.

Next, the random sequence, $c(n)$, conducts XOR operation with the divided video data. Since a frame video data includes tricolor integer sequences, $R(n)$, $G(n)$, and $B(n)$, these three sequences will be encrypted simultaneously after changing the random sequence, $c(n)$, into three columns evenly, $c^1(n)$, $c^2(n)$, and $c^3(n)$:

$$\begin{aligned} p_1(n) &= c^1(n) \oplus R(n), \\ p_2(n) &= c^2(n) \oplus G(n), \\ p_3(n) &= c^3(n) \oplus B(n), \end{aligned} \quad (26)$$

where $p_1(n)$, $p_2(n)$, and $p_3(n)$ are encrypted sequences and $\oplus$ is an XOR operation. One has

$$\begin{aligned} \hat{R}(n) &= \text{mod} \left(\frac{\lfloor \hat{x}_1(n) \rfloor}{2^t}, 2^{q-t+1} \right) \oplus p_1(n) \\ &= \text{mod} \left(\frac{\lfloor \hat{x}_1(n) \rfloor}{2^t}, 2^{q-t+1} \right) \oplus c^1(n) \oplus R(n), \\ \hat{G}(n) &= \text{mod} \left(\frac{\lfloor \hat{x}_2(n) \rfloor}{2^t}, 2^{q-t+1} \right) \oplus p_2(n) \\ &= \text{mod} \left(\frac{\lfloor \hat{x}_2(n) \rfloor}{2^t}, 2^{q-t+1} \right) \oplus c^2(n) \oplus G(n), \\ \hat{B}(n) &= \text{mod} \left(\frac{\lfloor \hat{x}_3(n) \rfloor}{2^t}, 2^{q-t+1} \right) \oplus p_3(n) \\ &= \text{mod}(\text{mod}(\lfloor \hat{x}_3(n) \rfloor, 2^t), 2^{t-q}) \oplus c^3(n) \oplus B(n), \end{aligned} \quad (27)$$

where $\lfloor \hat{x}_{p'}(n) \rfloor$, $p' = 1, 2, 3$ are receiver terminal sequences.

3.3. Analysis for NIST Test. NIST test is provided by National Institute of Standards and Technology, and it is a standard to test the randomness of a random sequence. According to the encryption algorithm in this paper, $c(n)$ in equation (25) should be tested by NIST standard. The comparisons of the random sequence among the new system, Qi system, and Lorenz system, $c(n)$, $c_L(n)$, and $c_Q(n)$, are conducted which are obtained from serial interfaces. The results of the tests are shown in Table 1.

As shown in Table 1, all the test results for the random sequences of the new system meet the NIST test index

standards. Partial test results are larger than 0.8, which means these random indexes are quite close to those of the real random sequences. The randomness indexes and some other test results are better than those generated from Lorenz system and Qi system, such as frequency, block frequency, cumulative sums, nonoverlapping template, approximate entropy, random excursions, random excursions variant, and linear complexity.

3.4. Statistical Analyses. Vivado IDE is used to conduct the hardware simulation. The paper also performs the statistics analysis for the encrypted video data generated by hardware. Figure 6(a) is one picture of a video before encryption. Figure 6(b) is the encrypted picture of a video.

Figure 7 demonstrates the comparisons of statistics histogram between the original and encrypted pictures.

Figure 7 demonstrates the comparisons of statistics histograms between the original and encrypted pictures. As illustrated in Figure 7(a), the difference of the pixels distribution is obvious. However, distribution of different pixels for the encrypted picture shown in Figure 7(b) is the approximately uniform distribution. It can be concluded that the proposed encryption algorithm for the new system can better resist statistic attack effectively.

3.5. Differential Analysis. Differential attack is used to measure the sensitivity of plaintext change for the encryption algorithm and commonly uses NPCR (Number of Pixels Change Rate) and UACI (Unified Average Changing Intensity) as indexes defined as follows:

$$\begin{cases} \text{NPCR} = \frac{\sum_{e,f} D(e,f)}{W \times H} \times 100\%, \\ \text{UACI} = \frac{1}{W \times H} \times \sum_{e,f} \frac{|C(e,f) - C'(e,f)|}{255} \times 100\%, \end{cases} \quad (28)$$

$$\begin{cases} \overline{\text{NPCR}} = \sum_m \text{NPCR}(m), \\ \overline{\text{UACI}} = \sum_m \text{UACI}(m), \end{cases} \quad (29)$$

where $C(e, f)$ is the pixel value before encryption and $C'(e, f)$ is the pixel value after encryption. If $C(e, f) = C'(e, f)$, $D(e, f) = 0$, else 1. $\overline{\text{NPCR}}$ and $\overline{\text{UACI}}$ calculated by (29) and the proposed system and encryption algorithm are 99.60% and 12.28% for the first-time encryption, respectively. Therefore, the ability to resist differential attack improves to some extent. In video encryption application, the requirement for encryption speed is more concerned.

3.6. Correlation Analysis. Correlation analysis is used to check whether the neighbor pixels are close or not. This paper analyzes the correlation for Figure 6. The paper selects 5000 random pixels from the original and the encrypted images and analyzes the correlation among these random-pixel pairs as shown in Figure 8. As Figure 8 illustrates, the

TABLE 1: NIST test results for the random sequences of the new system, Lorenz system, and Qi system (the number of sequences is 100, and their lengths are 1000000).

Statistical test	P value of $c_L(n)$	P value of $c_Q(n)$	P value of $c(n)$	Test results of $c(n)$	Proportion
Frequency	0.000000	0.236810	0.474986	✓	100/100
Block frequency ($m = 128$)	0.289667	0.699313	0.946308	✓	99/100
Cumulative sums	0.000000	0.108791	0.779188	✓	100/100
Runs	0.000000	0.554420	0.075719	✓	100/100
Longest run	0.419021	0.383827	0.289667	✓	100/100
Rank	0.851383	0.996335	0.289667	✓	100/100
FFT	0.911413	0.911413	0.213309	✓	99/100
Nonoverlapping template ($m = 9$)	0.000003	0.181557	0.983453	✓	100/100
Overlapping template ($m = 9$)	0.181557	0.935716	0.924076	✓	100/100
Universal	0.616305	0.289667	0.014550	✓	97/100
Approximate entropy ($m = 10$)	0.000000	0.798139	0.816537	✓	99/100
Random excursions	0.008879	0.319084	0.739918	✓	64/64
Random excursions variant	0.213309	0.289667	0.949602	✓	64/64
Linear complexity ($M = 500$)	0.010988	0.013569	0.108791	✓	99/100
Serial ($m = 16$)	0.616305	0.028817	0.262249	✓	100/100

(a)

(b)

(c)

FIGURE 6: The original and encrypted pictures of a video and the corresponding encrypted video data through FPGA. (a) The original picture of a video. (b) The encrypted picture of a video. (c) Encrypted video data shown on a monitor.

(a)

(b)

FIGURE 7: Histogram between the original and encrypted pictures. (a) Histogram of the original picture. (b) Histogram of the encrypted picture.

FIGURE 8: Correlation analyses for the original and encrypted figures in Figure 6. (a) Correlation analysis for the original figure as shown in Figure 6(a). (b) Correlation analysis for the encrypted figure as shown in Figure 6(b).

correlation dramatically decreases when comparing two figures before and after encryption as shown in Figure 6.

4. Conclusions

This paper proposed a new chaotic system generated by using semitensor product on two chaotic systems, and the related dynamic characteristics are analyzed. The new system is employed in video encryption as well, and the proposed method can generate 8 or even 12 state variables when compared to Qi system and Lorenz system which only generate 7 state variables at most in one iteration period. The proposed method can improve the speed of random sequence generation. The NIST test results demonstrate that the pseudorandomness of new system is better than that of single Qi system and single Lorenz system.

The proposed encryption algorithm based on semitensor product can be used in other chaotic systems. The synchronization of the new system can be implemented by synchronizing two original chaotic systems separately. In this paper, FPGA is used to implement the generation of the new chaotic system and to encrypt video data. The corresponding statistics and differential and correlation analyses were also conducted which demonstrates that the new system has obvious advantages, such as better random features, better resistance to differential attacks, and lower pixel correlation for encrypted images. The future work will focus on the decryption of video information by the proposed chaotic system generated by the semitensor product method in hardware.

Data Availability

The figures' .zip data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

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

Acknowledgments

This work was supported by the Fundamental Research Funds for the Central Universities-Civil Aviation University of China (3122019044).

References

- [1] J. Li, J. Li, X. Chen, C. Jia, and W. Lou, "Identity-based encryption with outsourced revocation in cloud computing," *IEEE Transactions on Computers*, vol. 64, no. 2, pp. 425–437, 2015.
- [2] J. Li, Y. K. Li, X. Chen, P. P. C. Lee, and W. Lou, "A hybrid cloud approach for secure authorized deduplication," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 5, pp. 1206–1216, 2015.
- [3] M. Feki, B. Robert, G. Gelle, and M. Colas, "Secure digital communication using discrete-time chaos synchronization," *Chaos, Solitons & Fractals*, vol. 18, no. 4, pp. 881–890, 2003.
- [4] V. T. Pham, S. Vaidyanathan, C. Volos, S. Jafari, and T. Kapitaniak, "A new multi-stable chaotic hyperjerk system, its special features, circuit realization, control and synchronization," *Archives of Control Sciences*, vol. 30, no. 1, pp. 23–45, 2020.
- [5] A. Ouannas, X. Wang, V. T. Pham, G. Grassi, and V. V. Huynh, "Synchronization results for a class of fractional-order spatiotemporal partial differential systems based on fractional lyapunov approach," *Boundary Value Problems*, vol. 2019, no. 1 2019.
- [6] F. Yu, H. Shen, L. Liu et al., "CCII and FPGA realization: a multistable modified fourth-order autonomous Chua's

- chaotic system with coexisting multiple attractors,” *Complexity*, vol. 2020, Article ID 5212601, 17 pages, 2020.
- [7] Q. Lai, P. D. K. Kuate, F. Liu, and H. H. Lu, “An extremely simple chaotic system with infinitely many coexisting attractors,” *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 67, no. 6, 2019.
 - [8] Q. Lai, A. Akgul, C. B. Li, G. H. Xu, and U. Cavusoglu, “A new chaotic system with multiple attractors: dynamic analysis, circuit realization and s-box design,” *Entropy*, vol. 20, no. 1, 2018.
 - [9] Q. Lai, B. Norouzi, and F. Liu, “Dynamic analysis, circuit realization, control design and image encryption application of an extended lü system with coexisting attractors,” *Chaos, Solitons & Fractals*, vol. 114, pp. 230–245, 2018.
 - [10] R. Wang, M. Li, Z. Gao, and H. Sun, “A new memristor-based 5D chaotic system and circuit implementation,” *Complexity*, vol. 2018, Article ID 6069401, 12 pages, 2018.
 - [11] Q. Hong, Y. Li, X. Wang, and Z. Zeng, “A versatile pulse control method to generate arbitrary multidirection multi-butterfly chaotic attractors,” *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 38, no. 8, pp. 1480–1492, 2019.
 - [12] P. S. Shabestari, Z. Rostami, V. T. Pham, F. E. Alsaadi, and T. Hayat, “Modeling of neurodegenerative diseases using discrete chaotic systems,” *Communications in Theoretical Physics*, vol. 71, no. 10, pp. 1241–1245, 2019.
 - [13] Q. Jiang, J. Jiang, and J. Li, “An image encryption algorithm based on high-dimensional chaotic systems,” in *Proceedings of the IEEE International Conference on Signal Processing, Communications and Computing*, pp. 1–4, Hong Kong, China, August 2016.
 - [14] S. Singh, M. Ahmad, and D. Malik, “Breaking an image encryption scheme based on chaotic synchronization phenomenon,” in *Proceedings of the 2016 Ninth International Conference on Contemporary Computing (IC3)*, Noida, India, August 2016.
 - [15] P. Chen, S. Yu, B. Chen, L. Xiao, and J. Lu, “Design and SOPC-based realization of a video chaotic secure communication scheme,” *International Journal of Bifurcation and Chaos*, vol. 28, no. 13, Article ID 1850160, 24 pages, 2018.
 - [16] P. R. Sankpal and P. A. Vijaya, “Image encryption Using chaotic maps: a survey,” in *Proceedings of the 2014 Fifth International Conference on Signal and Image Processing*, pp. 102–107, IEEE, Bangalore, India, January 2014.
 - [17] A. Rani and B. Raman, “An image copyright protection system using chaotic maps,” *Multimedia Tools and Applications*, vol. 76, no. 2, pp. 3121–3138, 2016.
 - [18] N. Shyamala and K. Anusudha, “Reversible chaotic encryption techniques for images,” in *Proceedings of the 2017 Fourth International Conference on Signal Processing, Communication and Networking (ICSCN)*, Chennai, India, March 2017.
 - [19] S. Chen, S. Yu, J. Lu, G. Chen, and J. He, “Design and FPGA-based realization of a chaotic secure video communication system,” *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 28, no. 9, pp. 2359–2371, 2018.
 - [20] Z. Lin, S. Yu, J. Lu, S. Cai, and G. Chen, “Design and ARM-embedded implementation of a chaotic map-based real-time secure video communication system,” *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 25, no. 7, pp. 1203–1216, 2015.
 - [21] D. Chang, Z. Li, M. Wang, and Y. Zeng, “A novel digital programmable multi-scroll chaotic system and its application in FPGA-based audio secure communication,” *AEU—International Journal of Electronics and Communications*, vol. 88, pp. 20–29, 2018.
 - [22] F. J. Farsana and K. Gopakumar, “Private key encryption of speech signal based on three dimensional chaotic map,” in *Proceedings of the International Conference on Communication & Signal Processing*, pp. 2197–2201, Chennai, India, April 2017.
 - [23] H. Jia, Z. Guo, S. Wang, and Z. Chen, “Mechanics analysis and hardware implementation of a new 3D chaotic system,” *International Journal of Bifurcation and Chaos*, vol. 28, no. 13, Article ID. 1850161, 14 pages, 2018.
 - [24] E. Tlelo-Cuautle, L. G. De La Fraga, V.-T. Pham, C. Volos, S. Jafari, and A. D. J. Quintas-Valles, “Dynamics, FPGA realization and application of a chaotic system with an infinite number of equilibrium points,” *Nonlinear Dynamics*, vol. 89, no. 2, pp. 1129–1139, 2017.
 - [25] A. Akgul, H. Calgan, I. Koyuncu, I. Pehlivan, and A. Istanbulu, “Chaos-based engineering applications with a 3D chaotic system without equilibrium points,” *Nonlinear Dynamics*, vol. 84, no. 2, pp. 481–495, 2016.
 - [26] Q. Lai, X. Zhao, K. Rajagopal, G. Xu, A. Akgul, and E. Guleryuz, “Dynamic analyses, FPGA implementation and engineering applications of multi-butterfly chaotic attractors generated from generalised spott c system,” *Pramana*, vol. 90, no. 1, p. 12, 2018.
 - [27] W. S. Sayed, M. F. Tolba, A. G. Radwan, and S. K. Abd-El-Hafiz, “FPGA realization of a speech encryption system based on a generalized modified chaotic transition map and bit permutation,” *Multimedia Tools and Applications*, vol. 78, no. 12, pp. 16097–16127, 2019.
 - [28] Q. Wang, S. Yu, C. Li et al., “Theoretical design and FPGA-based implementation of higher-dimensional digital chaotic systems,” *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 63, no. 3, pp. 401–412, 2016.
 - [29] E. Dong, Z. Wang, Z. Chen, and Z. Wang, “Topological horseshoe analysis and field-programmable gate array implementation of a fractional-order four-wing chaotic attractor,” *Chinese Physics B*, vol. 27, no. 1, pp. 300–306, 2018.
 - [30] Z. Hua, B. Zhou, and Y. Zhou, “Sine chaotification model for enhancing chaos and its hardware implementation,” *IEEE Transactions on Industrial Electronics*, vol. 66, no. 2, pp. 1273–1284, 2019.
 - [31] İ. Öztürk and R. Kılıç, “A novel method for producing pseudo random numbers from differential equation-based chaotic systems,” *Nonlinear Dynamics*, vol. 80, no. 3, pp. 1147–1157, 2015.
 - [32] R. Wang, Q. Xie, Y. Huang, H. Sun, and Y. Sun, “Design of a switched hyperchaotic system and its application,” *International Journal of Computer Applications in Technology*, vol. 57, no. 3, pp. 207–218, 2018.
 - [33] R. Wang, H. Sun, J. Wang, L. Wang, and Y. Wang, “Applications of modularized circuit designs in a new hyper-chaotic system circuit implementation,” *Chinese Physics B*, vol. 24, no. 4, Article ID 020501, 2015.
 - [34] Z. Lin, S. Yu, and J. Li, “Chosen ciphertext attack on a chaotic stream cipher,” in *Proceedings of the 30th Chinese Control and Decision Conference*, pp. 1238–1242, Shenyang, China, June 2018.
 - [35] G. Qi, G. Chen, M. A. Van Wyk, and B. J. Van Wyk, “On a new hyperchaotic system,” *Physics Letters A*, vol. 372, no. 2, pp. 124–136, 2008.
 - [36] Z. Hu and C.-K. Chan, “A real-valued chaotic orthogonal matrix transform-based encryption for OFDM-PON,” *IEEE*

- Photonics Technology Letters*, vol. 30, no. 16, pp. 1455–1458, 2018.
- [37] D. Cheng, H. Qi, and Y. Zhao, *An Introduction to Semi-Tensor Product of Matrices and Its Applications*, World Scientific, Singapore, 2012.
 - [38] T. Akutsu, M. Hayashida, W.-K. Ching, and M. K. Ng, “Control of boolean networks: hardness results and algorithms for tree structured networks,” *Journal of Theoretical Biology*, vol. 244, no. 4, pp. 670–679, 2007.
 - [39] D. Cheng, “On finite potential games,” *Automatica*, vol. 50, no. 7, pp. 1793–1801, 2014.
 - [40] X. Liu and J. Zhu, “On potential equations of finite games,” *Automatica*, vol. 68, pp. 245–253, 2016.
 - [41] H. Li, G. Zhao, M. Meng, and J. Feng, “A survey on applications of semi-tensor product method in engineering,” *Science China Information Sciences*, vol. 61, no. 1, pp. 24–40, 2018.
 - [42] D. Cheng and H. Qi, *Semi-Tensor Product of Matrices-Theory and Applications*, Science Publication, Washington, DC, USA, 2nd edition, 2011.