mathematics

MDPI

Article

Complex Modified Projective Difference Function Synchronization of Coupled Complex Chaotic Systems for Secure Communication in WSNs

Fangfang Zhang [1,2], Rui Gao [1,*], Zhe Huang [2], Cuimei Jiang [3] and Yawen Chen [4] and Haibo Zhang [4]

[1] School of Control Science and Engineering, Shandong University, Jinan 250061, China; zhff4u@163.com
[2] Department of Electrical Engineering and Automation, Qilu University of Technology (Shandong Academy of Sciences), Jinan 250353, China; H794607953@163.com
[3] School of Mathematics and Statistics, Qilu University of Technology (Shandong Academy of Sciences), Jinan 250353, China; jiangcuimei2004@163.com
[4] Department of Computer Science, University of Otago, Dunedin 9016, New Zealand; yawen@cs.otago.ac.nz (Y.C.); haibo@cs.otago.ac.nz (H.Z.)
* Correspondence: gaorui@sdu.edu.cn; Tel.: +86-151-6916-3982

Abstract: Complex-variable chaotic systems (CVCSs) have numerous advantages over real-variable chaotic systems in chaos communication due to their increased unpredictability, confidentiality, and the ease of implementation. Synchronization between the master and slave systems in CVCSs is key to achieving encryption and decryption. However, existing synchronization schemes for CVCSs require the amplitude of the chaotic signal to be much larger than that of the plaintext. Moreover, traditional chaotic masking of complete synchronization (CS) requires uniformity between the transmitter and receiver ends. Therefore, we propose a complex modified projective difference function synchronization (CMPDFS) of CVCSs to address these issues, where the modified projective matrix helps address the issues with the amplitude. The receiver end is reconstructed without uniformity of the transmitter. We design the CMPDFS controller and propose a new secure communication scheme for wireless sensor networks (WSNs). The basic principle is fundamentally different from traditional chaotic masking. Simulation results and security analysis demonstrate that the CMPDFS communication scheme has a large key space, high sensitivity to encryption keys, high security, and an acceptable encryption speed. Hence, the proposed scheme can improve the security of WSNs. Moreover, it also can be applied to similar communication systems.

Keywords: complex-variable chaotic systems (CVCSs); synchronization; communication; control

MSC: 94A14

Citation: Zhang, F.; Gao, R.; Huang, Z.; Jiang, C.; Chen, Y.; Zhang, H. Complex Modified Projective Difference Function Synchronization of Coupled Complex Chaotic Systems for Secure Communication in WSNs. *Mathematics* **2022**, *10*, 1202. https://doi.org/10.3390/math10071202

Academic Editor: Angel Martín-del-Rey

Received: 22 February 2022
Accepted: 2 April 2022
Published: 6 April 2022

1. Introduction

In 1963, the American meteorologist A. C. Fowler proposed the butterfly effect and Lorenz chaotic system, which attracted great attention of scholars all over the world. Nineteen years later, he and J. D. Gibbon [1] proposed the complex Lorenz system and investigated its properties given different parameters; complex-variable chaotic systems (CVCSs) had a significant influence on a number of fields [2–5], particularly in chaos secure communication [4–6]. Complex variables need more intensive computations with both real parts and imaginary parts, thus they double the transmitted contents and improve the confidentiality of the information. Moreover, they can be easily implemented in a wide range of practical applications using RLC circuits including resistors (R), inductors (L), and capacitors (C).

Chaos cryptography can be divided into two major parts: (1) chaos communication based on chaos synchronization technology [7–10] and (2) constructing new stream ciphers

and block ciphers using chaotic systems [11–13]. In traditional chaotic masking communication, chaotic signals are employed as carriers produced by the master systems to obscure the message signals. Then, the message signals are retrieved through chaos synchronization, for example, through complete synchronization (CS) between the master system at the transmitting end and the slave system at the receiving end. Hence, the type of synchronization is critical. New types of synchronization for CVCSs have attracted extensive increasing attention recently [14–31], including phase synchronization (PHS) [14], complete synchronization (CS) [15], anti-synchronization (AS) [16,17], lag synchronization (LS) [18], anti-lag synchronization [19], modified function projective synchronization (MFPS) [20], full-state hybrid synchronization [21], modified projective phase synchronization (MPPS) [22], hybrid MFPS [23], complex modified projective synchronization (CMPS) [24], time-delay chaotic system [25,26], complex function projective synchronization (MFPS) [27,28], complex anti-synchronization (CAS) [29], difference function synchronization (DFS) [30,31], etc.

Synchronization for CVCSs involves designing a controller that synchronizes the states variables of two chaotic systems synchronized, which is called a synchronization controller. More accurately, synchronization is generally for a chaotic system while control involves any system.

Over the past twenty years, the field of the synchronization and control of CVCSs has grown rapidly, and so have the communication schemes for CVCSs. In 2014, S. Liu and F. Zhang [6] developed complex function projective synchronization (CFPS) along with a new chaos communication scheme. In 2015, F. Zhang et al. applied a self-delay synchronization scheme [25] and the CS of coupled multiple time-delay CVCSs [26] to communication systems. In 2018, E. E. Mahmoud and S. M. Abo-Dahab [29] presented CAS and discussed the corresponding communication schemes.

It is worth noting that as the amplitude of the signal generated by the sender approaches zero, the denominator in CFPS also approaches zero and will, therefore, affect synchronization and message recovery. J. Liu et al. proposed fractional difference function synchronization in 2019 [30]. The type of synchronization in these two papers is modified difference function synchronization (MDFS). However, these schemes have an amplitude limitation of chaos communication, which limits its application in general chaos communication. In 2021, J. Guo et al. proposed modified fractional projective difference function synchronization (MFPDFS) for a time-delay fractional complex chaotic system [31]. Inspired by MFPDFS, we propose a complex modified projective difference function synchronization (CMPDFS) for common complex chaotic system and address issues originating from the amplitude limitation. Complete synchronization (CS), phase synchronization (PHS), projective synchronization (PS), modified projective synchronization (MPS), and modified difference function synchronization (MDFS) are all special cases of CMPDFS. CMPDFS combines the advantages from CMPS and MDFS, because CMPS can adjust the amplitude of chaotic signals according to plaintext information to be transmitted confidentially while MDFS avoids the denominator being zero.

Recently, significant improvements in hardware technology and wireless communications have enabled the use of wireless sensor networks (WSNs) in a wide range of real-world applications. The extensive application of WSNs has also attracted the attention of criminals; therefore, the security of data transmissions in WSNs is becoming increasingly crucial. A WSN is composed of at least one sink node and many sensor nodes with a number of limitations, including battery lifetime, processing power, and memory capacity. The network topology diagram of a WSN is presented in Figure 1. Because of the low cost and high security provided by the chaotic signals, the implementation of chaos communication can significantly improve the security of WSNs.

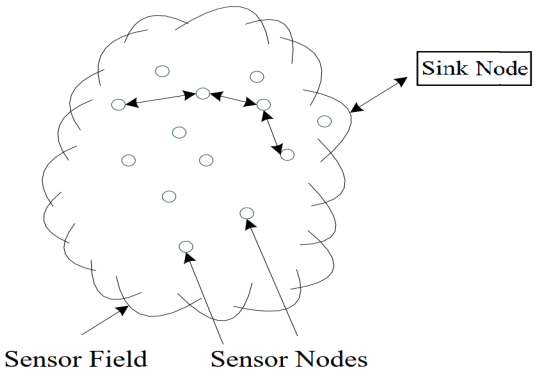

Figure 1. The topology diagram of wireless sensor networks.

Chamindra et al. investigated the chaotic modulation approach for secured wireless medical sensor network (WMSN) in e-healthcare applications [32]. Niu et al. proposed a novel asymmetric cryptographic algorithm based on matrix decomposition in wireless body area networks (WBANs) [33]. However, insufficient information is available on communication in WSNs based on CMPDFS of CVCSs in noisy conditions, and the relevant theoretical developments based on CMPDFS have seldom been studied in the literature. In order to make up for the blind spot, the relevant simulation experiments and result analysis are carried out. The main contributions of this paper are summarized as follows:

(1) We describe CMPDFS, which is a new synchronization scheme for CVCSs. The modified projective matrix is able to change the amplitude of complex chaotic signals, and effectively overcome the amplitude limitation of chaos communication. This helps diversify the available synchronization schemes and increases the security of the transmitted messages.

(2) We design control laws with guaranteed performance to construct the slave system. These laws take the bounded disturbances into consideration and ensure that the reconstructed slave system is chaotic. The controller has good robustness to the bounded noise.

(3) We propose a novel communication scheme for WSNs based on CMPDFS, which outperforms traditional chaotic masking. The communication scheme is able to theoretically achieve a bit error rate (BER) of zero. The results from simulation and security analysis demonstrate that the CMPDFS communication scheme provides a large key space, high sensitivity to encryption keys, high security, and an acceptable encryption speed.

The arrangements of our paper are as follows: we give the definition of CMPDFS in Section 2. In Section 3, we design control schemes to construct a slave system, propose the communication scheme for a WSN and discuss its special advantages. The process of WSN communication by simulation experiments are shown in Section 4. Finally, we give the conclusions of the whole paper.

The descriptions of all notations in the paper are shown in Table 1.

Table 1. The descriptions of all notations.

The Symbol	Meanings
n	The dimension of system
q	The dimension of uncoupled variables
$L1$	The drive system
$L2$	The response system
$\mathbf{y}$, $\mathbf{z}$	The complex state vector of the drive system
$\mathbf{x}$	The complex state vector of the response system
r	The real part of a complex variable
i	The imaginary part of a complex variable
$\mathbf{f}$, $\mathbf{p}$, $\mathbf{g}$	Nonlinear function of complex variables
$\mathbf{v}$	The designed controller

Table 1. *Cont.*

The Symbol	Meanings
$\mathbf{e}$	The error vector
$\mathbf{H}(t)$	The difference function vector
$\mathbf{D}$	The modified projective matrix which is the private key
$\mathbf{s}$	The transmitted signal without noise
$\mathbf{s'}$	The transmitted signal with noise
$\mathbf{A}(\varepsilon)$	The noise where A is the amplitude of the noise
$\mathbf{H_g}(t)$	The recovered signal
$\mathbf{k}$	The control strength matrix
$\mathbf{w}(\varepsilon)$	The probability density function of Gaussian distribution
E_{H^r}	The square of error in the real part of the recovered signal
E_{H^i}	The square of error in the imaginary part of the recovered signal

2. Complex Modified Projective Difference Function Synchronization (CMPDFS)

The general form of a controlled coupled complex chaotic system can be expressed by n dimensional differential equations as follows:

$$\begin{array}{l} L1: \left\{ \begin{array}{rcl} \dot{\mathbf{y}} & = & \mathbf{g}(\mathbf{y}, \mathbf{z}), \\ \dot{\mathbf{z}} & = & \mathbf{p}(\mathbf{y}, \mathbf{z}), \end{array} \right. \\ L2: \dot{\mathbf{x}} = \mathbf{f}(\mathbf{x}, \mathbf{z}) + \mathbf{v}, \end{array} \tag{1}$$

where $\mathbf{y} = (y_1, y_2, \cdots, y_q)^{\mathrm{T}}$ and $\mathbf{z} = (z_1, z_2, \cdots, z_{n-q})^{\mathrm{T}}$ are the observable complex state vectors of the drive system $L1$. The state vector $\mathbf{z}$ is treated as the coupling vector. $\mathbf{x} = (x_1, x_2, \cdots, x_q)^{\mathrm{T}}$ is the complex state vector of the response system $L2$, which is controllable and reconstructed using the controller $\mathbf{v}$. The designed controller is represented by $\mathbf{v} = \mathbf{v}^r + j\mathbf{v}^i$, where $\mathbf{v}^r = (v_1^r, v_2^r, \cdots, v_n^r)^{\mathrm{T}}$ is the real part of a complex variable, and $\mathbf{v}^i = (v_1^i, v_2^i, \cdots, v_n^i)^{\mathrm{T}}$ is the real part of a complex variable.

Definition 1. *With regard to two state vectors* $\mathbf{x}(\mathbf{t})$, $\mathbf{y}(\mathbf{t})$ *and a desired difference function vector* $\mathbf{H}(t)$, *if the square of error satisfies*

$$\begin{array}{rcl} \lim\limits_{t\to+\infty} \|\mathbf{e}(\mathbf{t})\|^2 & = & \lim\limits_{t\to+\infty} \|\mathbf{x}(\mathbf{t}) - \mathbf{H}(\mathbf{t}) - \mathbf{D}\mathbf{y}(\mathbf{t})\|^2 \\ & = & \lim\limits_{t\to+\infty} \|\mathbf{x}^r(t) - \mathbf{H}^{\mathbf{r}}(\mathbf{t}) - \mathbf{D}^r\mathbf{y}^r(t) + \mathbf{D}^i\mathbf{y}^i(t)\|^2 \\ & + & \|\mathbf{x}^i(t) - \mathbf{H}^{\mathbf{i}}(\mathbf{t}) - \mathbf{D}^r\mathbf{y}^i(t) - \mathbf{D}^i\mathbf{y}^r(t)\|^2 \\ & = & 0, \end{array} \tag{2}$$

where $\|\cdot\|$ *represents the Euclidean norm, then* $\mathbf{x}(\mathbf{t})$ *and* $\mathbf{y}(\mathbf{t})$ *will reach CMPDFS with* $\mathbf{H}(t)$ *and modified projective matrix* $\mathbf{D}$. $\mathbf{H}(t) = \{h_1(t), h_2(t), \cdots, h_q(t)\}^{\mathrm{T}}$ *is a bounded vector, and* $h_1(t), h_2(t), \cdots, h_q(t)$ *are difference function factors.* $h_l(t) : C \to C$ $(l = 1, 2, \cdots, q)$ *are bounded complex functions.* $\mathbf{D} = diag\{d_1, d_2, \cdots, d_q\}$, $d_l \in C$ *are bounded complex numbers.*

In [14], G. M. Mahmoud and E. E. Mahmoud discussed the phase synchronization (PHS) of two CVCSs, and designed a special controller to hold the error at a constant value. CS signifies that there is no difference between the two state variables while PHS indicates that the differences are constant. Therefore, the following remarks can be made.

Remark 1. *CS is a special case of CMPDFS with* $\mathbf{H}(t) = 0$ *and* $\mathbf{D}(t) = 1$.

Remark 2. *PHS (under controller in [14]) is a special case of CMPDFS with* $\mathbf{H}(t) = Constant$ *and* $\mathbf{D}(t) = 1$.

Remark 3. *MDFS is a special case of CMPDFS with* $\mathbf{D}(t) = 1$.

Remark 4. *CMPS is a special case of CMPDFS with* $\mathbf{H}(t) = 0$.

3. CMPDFS Communication Scheme for WSNs

3.1. CMPDFS Controller

According to the definition of CMPDFS, we obtain the synchronization error

$$\mathbf{e}(t) = \mathbf{x}(t) - \mathbf{H}(t) - \mathbf{D}\mathbf{y}(t), \tag{3}$$

For brevity, we denote $\mathbf{e}(t)$, $\mathbf{x}(t), \mathbf{y}(t)$, and $\mathbf{H}(t)$ as $\mathbf{e}, \mathbf{x}, \mathbf{y}$, and $\mathbf{H}$, respectively. Next, we have

$$\begin{aligned} \dot{\mathbf{e}} &= \dot{\mathbf{x}} - \dot{\mathbf{H}} - \mathbf{D}\dot{\mathbf{y}} \\ &= \mathbf{f}(\mathbf{x}, \mathbf{z}) + \mathbf{v} - \dot{\mathbf{H}} - \mathbf{D}\mathbf{g}(\mathbf{y}, \mathbf{z}) \\ &= \mathbf{f}(\mathbf{x}, \mathbf{z}) + \mathbf{v} - \mathbf{s} \end{aligned} \tag{4}$$

where $\mathbf{s} = \dot{\mathbf{H}} + \mathbf{D}\mathbf{g}(\mathbf{y}, \mathbf{z})$ is the transmitted signal without noise produced by the sender end and $\mathbf{D}$ is the private key known to the sender and the receiver.

According to active control, $\mathbf{x}$ is controllable, and $\mathbf{y}$ and $\mathbf{z}$ are observable, if we design the controller

$$\begin{aligned} \mathbf{v} &= \mathbf{s} - \mathbf{f}(\mathbf{x}, \mathbf{z}) + \mathbf{k}\mathbf{e} \\ &= \mathbf{s} - \mathbf{f}(\mathbf{x}, \mathbf{z}) + \mathbf{k}(\mathbf{x}(\mathbf{t}) - \int_0^t \mathbf{s}\, dt), \end{aligned} \tag{5}$$

where $\mathbf{k} \in R$ is the control strength matrix which is negative. Substituting Equation (5) into Equation (4), we obtain

$$\dot{\mathbf{e}} = \mathbf{k}\mathbf{e} \tag{6}$$

That is, we achieve the CMPDFS between systems L1 and L2.

3.2. The Communication Scheme for WSNs

Here, we propose a secure communication scheme based on CMPDFS for WSNs. The diagram of the proposed communication scheme is presented in Figure 2. The master system $L1$ produced by one sensor node represents the sender end. The slave system $L2$, which is constructed by the sink node, represents the receiver end. The coupled signal $\mathbf{z}$, produced by the sender, is transmitted to the receiver. H is the message signal, and D is the proportional matrix.

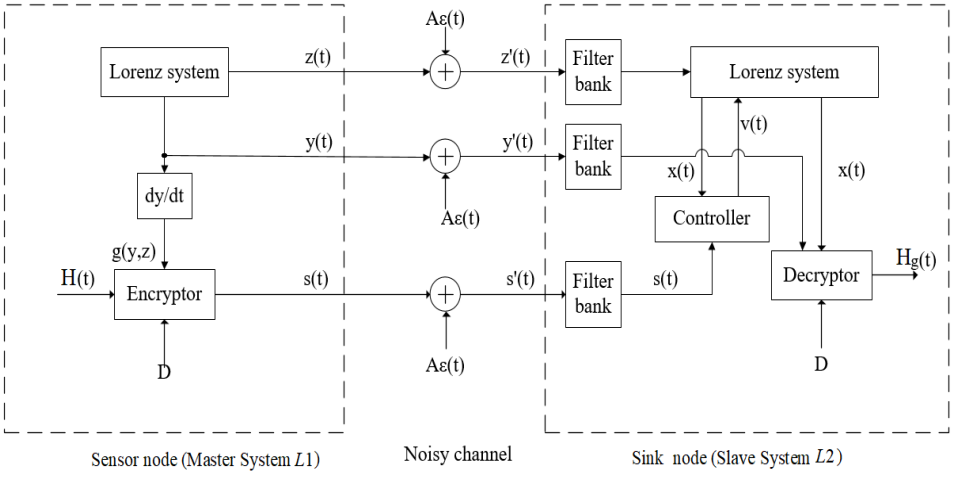

Figure 2. The diagram of communication scheme based on CMPDFS.

Considering the noise in the communication channel, we obtain the actual transmitted signal

$$\begin{aligned} \mathbf{s}'(t) &= \mathbf{s}(t) + A\varepsilon(t) \\ &= \dot{\mathbf{H}}(t) + \mathbf{D}\mathbf{g}(\mathbf{y}(t), \mathbf{z}(t)) + A\varepsilon(t) \end{aligned} \tag{7}$$

where $A\varepsilon(t)$ represents the noise in a given channel generated by all noise sources and A denotes the amplitude of the noise.

The communication process comprises two parts. First, the initial value of the coupled signal $\mathbf{z}(0)$ is broadcasted to the sink node. For communication, $\mathbf{z}(0)$ is applied to provide the sink node with a command to begin sending the information. For synchronization, $\mathbf{z}(0)$ is used to construct the decryptor at the sink node.

In the second part, after receiving the correct return signal $\mathbf{z}(0)$ from the sink node, the sensor node begins to encrypt the message signal $\mathbf{H}(t)$ (which is the plaintext in fact) and produces the encrypted message $\mathbf{s}(t)$. It is sent to the sink node with noise (we denote $\mathbf{s}'(t)$=$\mathbf{s}(t) + A\varepsilon(t)$). The encryption method of the sender end consists of both chaotic encryption and chaotic masking. At the receiving end, the controller $\mathbf{v}$ is designed using Equation (5) which includes $\mathbf{s} = \mathbf{s}' - A\varepsilon(t)$ (we filter $\mathbf{s}'$ and obtain the effective transmitted signal $\mathbf{s}$). As CMPDFS is initiated, $\mathbf{x}(t)$ synchronizes $\mathbf{H}(t) + \mathbf{D}\mathbf{y}(t)$. Therefore, the recovered signal is $\mathbf{H}_g(t) = \mathbf{H}(t) = \mathbf{x}(t) - \mathbf{D}\mathbf{y}(t)$.

The CMPDFS communication scheme is different from traditional chaotic masking in a few key ways. Firstly, the method for recovering the signal is different. The recovered signal in our communication scheme based on CMPDFS is $\mathbf{H}_g = \mathbf{x} - \mathbf{D}\mathbf{y}$, while the recovered signal in traditional chaotic masking based on CS is $\mathbf{H}_g = \mathbf{s}' - \mathbf{y}$. As $\mathbf{s}'(t)$ includes noise, the recovered signal in traditional chaotic masking is inherently inaccurate. Traditional chaotic masking also requires that the amplitude of the chaotic signals always largely outweigh the amplitude of plaintext and noise. In the proposed communication scheme, if the amplitude of chaotic signals is insufficient, we can select a large proportional matrix $\mathbf{D}$, which is large enough to outweigh the amplitude of plaintext and noise. Therefore, the accuracy of the recovered signal in the proposed method is higher than traditional chaotic masking and the BER is theoretically zero.

Secondly, the actual transmitted signal is $\mathbf{s}'(t) = \dot{\mathbf{H}} + \mathbf{D}\mathbf{g}(\mathbf{y}, \mathbf{z}) + A\varepsilon(t)$, which is the sum of all noise sources, the derivative of the plaintext (message signal), and the function of the state variables. Chaotic encryption, chaotic masking, and noise masking are developed to increase communication security. Any state variable from the sender end can be chosen. Additionally, $\mathbf{s}'(t)$ is a complex variable signal and includes the complicated calculations of complex numbers, which provide more than twice the security of real variables. Moreover, it is possible to transmit two message signals by utilizing the real part and imaginary part concurrently.

Thirdly, CMPDFS can occur between nonuniform transmitter and receiver generators (that is, $\mathbf{f}$ and $\mathbf{g}$ can be different function matrices in Equation (1)), while CS in traditional chaotic masking requires uniformity between the transmitter and receiver ends. In our method, the receiver system is constructed at the sink node where the controller $\mathbf{v}$ is crucial.

All of these advantages have been verified via numerical simulations, which are presented in the following section.

4. Numerical Simulations and Discussions

As shown in Figure 2, we apply the following coupled complex Lorenz system to the transmitter $L1$ at the sensor node and the receiver $L2$ at the sink node for secure communication.

$$\begin{aligned} L1 &: \begin{cases} \dot{y}_1 &= 35(z_1 - y_1), \\ \dot{z}_1 &= 55y_1 - z_1 - y_1 z_2, \\ \dot{z}_2 &= -8/3 z_2 + (1/2)(\bar{y}_1 z_1 + y_1 \bar{z}_1). \end{cases} \\ L2 &: \dot{x}_1 = 35(z_1 - x_1) + v_1, \end{aligned} \tag{8}$$

where y_1, z_1, z_2, and x_1 are state variables ($q = 1$). The overbar $\bar{y}_1(\bar{z}_1)$ represents the complex conjugate of $y_1(z_1)$. The designed controller is v_1. The Lyapunov exponent of the $L1$ system is $LE1 = 1.1019$, $LE2 = 0.6602$, $LE3 = -0.1350 \approx 0$, $LE4 = -0.6355$, and $LE5 = -2.0331$, which includes a positive Lyapunov index at least. It indicates that the $L1$ system is chaotic.

According to Equation (5), we construct the following controller:

$$\begin{aligned} v_1 &= \mathbf{s}' - A\varepsilon(t) - \mathbf{f}(\mathbf{x}, \mathbf{z}) + \mathbf{ke} \\ &= \dot{H} + D35(z_1 - y_1) - 35(z_1 - x_1) + k_1(x_1 - \int_0^t (s' - A\varepsilon)\, dt), \end{aligned} \tag{9}$$

where $s' - A\varepsilon$ can be processed through a filter bank.

The noise $\varepsilon(t)$ is described by the probability density function of Gaussian distribution

$$w(\varepsilon) = \frac{1}{\sqrt{2\pi}\sigma} exp(-\frac{(\varepsilon - \varepsilon_0)^2}{2\sigma^2}). \tag{10}$$

where $\sigma = 1$ and $\varepsilon_0 = 0$ are the variance and mean value [34], respectively.

The following initial conditions were selected: $\{y_1, z_1, z_2\}(0) = \{1 + 2j, 3 + 4j, 1\}$, $x_1(0) = \{-1 - 2j\}$. The fourth-order Runge–Kutta method was used with $\Delta t = 10^{-3}$ and was implemented with MATLAB software. We take the following signal as an example:

$$H(t) = 20sin^2(0.5\pi t) + jcos(\pi t) \tag{11}$$

Then, we have

$$\begin{cases} \dot{H}^r(t) = 20\pi sin(0.5\pi t)cos(0.5\pi t) \\ \dot{H}^i(t) = -\pi sin(\pi t) \end{cases} \tag{12}$$

where the derivative of $H(t)$ is continuous during the computer sampling period. Continuous range of general signal is much larger than the sampling period. If the continuous range is smaller than the computer sampling period, we can reselect a smaller sampling period.

In this section, the same control strength matrix, $k = -500$, was utilized for a better comparison.

4.1. Communication Process without Noise

Here, the case where $A = 0$ is discussed, which represents an ideal noiseless situation. When $D = 10 + 10j$, we obtain the projection spaces of L_1 and L_2 shown in Figure 3 and the state variable shown in Figure 4, where the blue line represents L_1 and the dotted line represents L_2. In fact, the receiver end L_2 is reconstructed by the controller based on CMPDFS. The CMPDFS process with $D = 10 + 10j$ is demonstrated in Figure 5. It can be observed that the error $\dot{H}^i$ is larger than that of $\dot{H}^r$, because the amplitude of H^i is much smaller than that of $(Dy_1)^i$. As $e^i(t) = x_1^i(t) - H^i(t) - (Dy_1)^i(t) \approx x_1^i(t) - (Dy_1)^i(t)$, $\mathbf{H}^i(t)$ can be ignored and cannot be recovered. In fact, the CMPDFS of imaginary part is achieved.

Next, $D = 0.1 + 0.1j$ is changed, and the CMPDFS process is shown in Figure 6. When the amplitude of the chaotic signal $(Dy_1)^r$ is smaller than that of the message H^r, the transmitted signal s^r cannot cover the message H^r. The above figures highlight the effect that D has on s'. Therefore, we can choose the appropriate D to obtain the optional CMPDFS process. This will improve the limitation imposed by the amplitude problem.

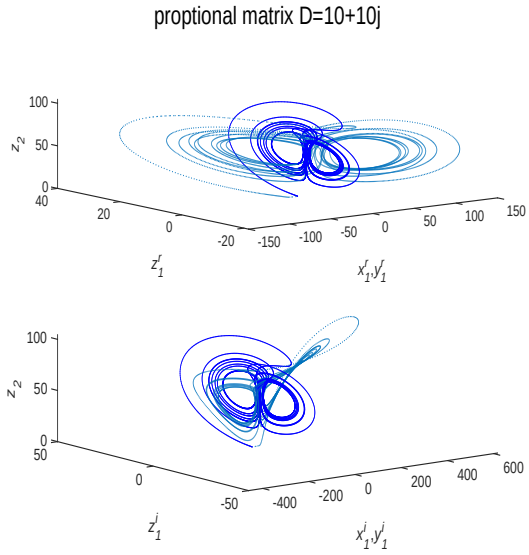

Figure 3. The projection space of chaotic systems $L1$ and $L2$ without noise.

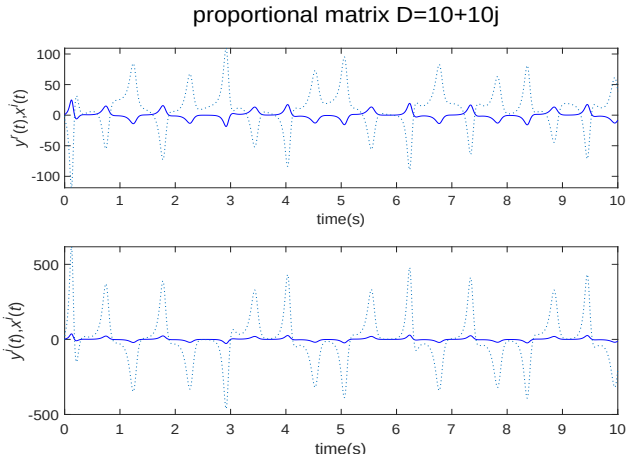

Figure 4. The diagram of state variables $\mathbf{x}_1$ and $\mathbf{y}_1$ without noise.

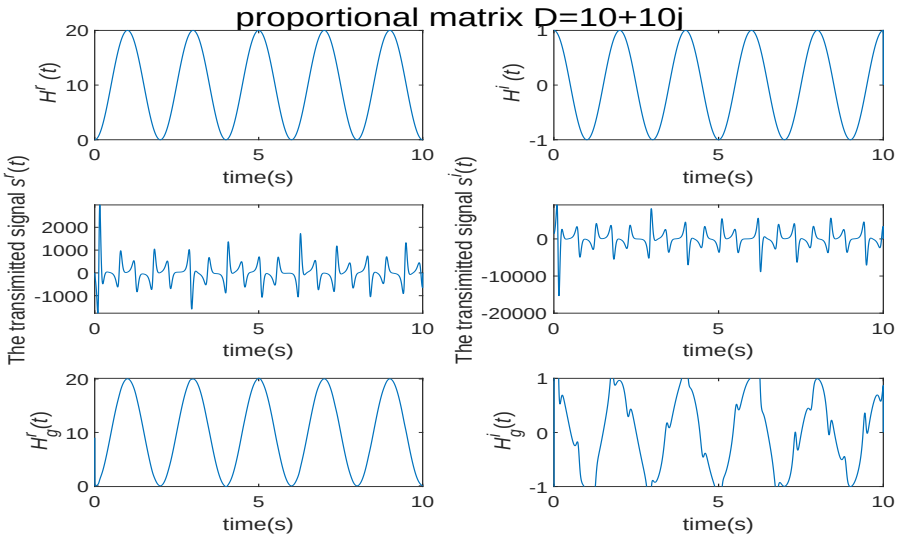

Figure 5. The CMPDFS process without noise when $D = 10 + 10j$.

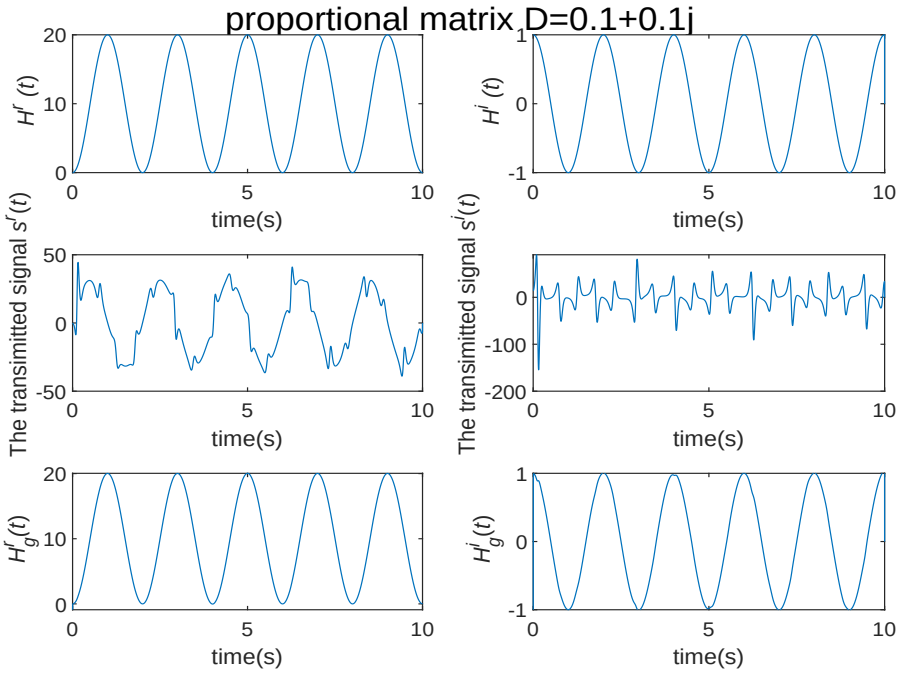

Figure 6. The CMPDFS process without noise when $D = 0.1 + 0.1j$.

Moreover, from a large number of experiments, when the amplitude of the chaotic signal Dy_1 is approximately equal to that of the message signal H, the sum of the error square is minimized. This conclusion can also be drawn from the bold fonts in Table 2, where $max(Dy_1)^r$ and $max(Dy_1)^i$ are the maximum amplitudes of the real part and imaginary part of the chaotic signal, respectively. The terms $10,000 * E_{H^r}$ and $10,000 * E_{H^i}$ represent the sum of error square of recovered signal as the simulation program runs 10,000 times. According to (11), the maximum amplitude of H^r is 10, while that of H^i is 1. When $D = 1 + j$, $max(Dy_1)^r$ is 11.9294, which is the closest to H_r, and the sum of error is the minimum 0.1927 in the fourth column; when $D = 0.01 + 0.02j$, $max(Dy_1)^i$ is 0.8632, which is the closest to H_i, and the sum of error is the minimum 0.6959 in the fifth column.

Table 2. The sum of error square with different D.

D	$max(Dy_1)^r$	$max(Dy_1)^i$	$10,000 * E_{H^r}$	$10,000 * E_{H^i}$
$10 + 10j$	119.2935	615	6.7627	92.8656
$10 + j$	211.2523	392.0710	7.6200	46.0385
$10 + 0.1j$	244.3068	369.7529	10.8091	42.2822
$1 + j$	**11.9294**	61.5253	**0.1927**	2.4379
$1 + 0.1j$	21.1252	39.2071	0.3279	1.7356
$0.5 + 0.1j$	8.7262	20.8434	0.2395	1.1375
$0.1 + 0.1j$	1.1929	6.1525	0.2062	0.7844
$0.1 + 0.02j$	1.7452	4.1687	0.2184	0.7573
$0.01 + 0.02j$	0.4866	**0.8632**	0.2128	**0.6959**

4.2. Communication Process with Noise

In this section, the noise is added with $A = 50$ and $D = 0.5 + 0.1j$. The CMPDFS process is demonstrated in Figure 7. The actual transmitted signal $s'(t)$ can entirely cover up the message signal $H(t)$, and $H_g(t)$ is recovered without distortion. The projection diagrams of $L1$ and $L2$ are presented in Figure 8 and the state variables are presented in Figure 9.

For comparison, the same noise was added using the same parameters and processed with traditional chaotic masking based on CS. The process is presented in Figure 10. Here,

the message H could not be recovered due to noise, while H can be recovered by CMPDFS in Figure 7. From Figures 7 and 10, it is clear that the CMPDFS controller in the proposed communication scheme has more significant robustness for noise.

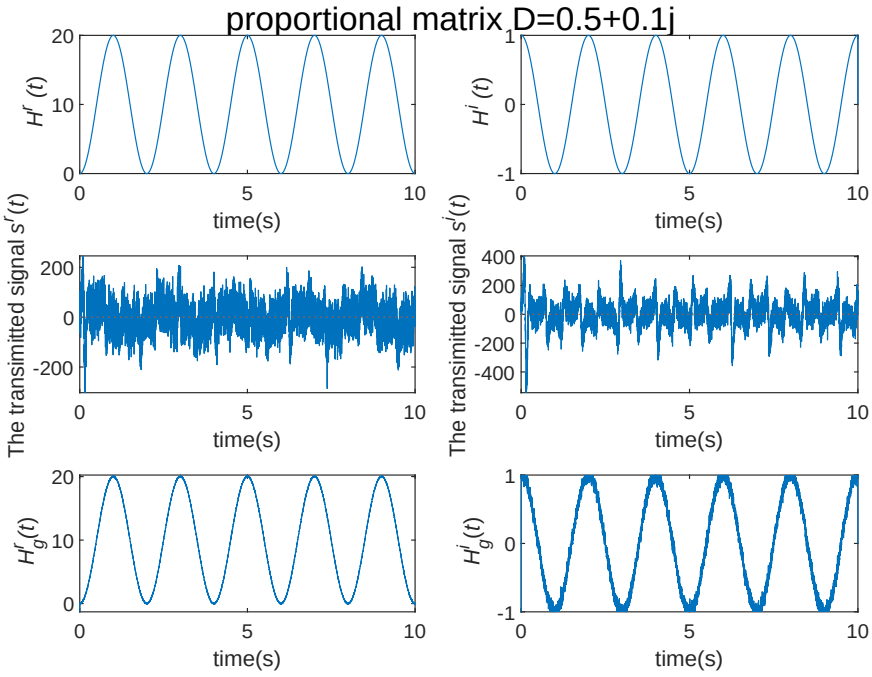

Figure 7. The CMPDFS process with noise when $D = 0.5 + 0.1j$.

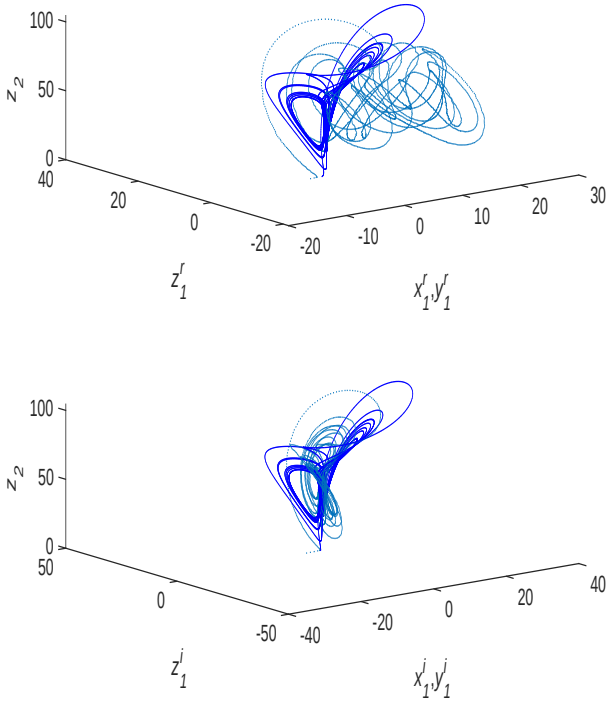

Figure 8. The projection diagram of chaotic systems $L1$ and $L2$ with noise $A = 50$.

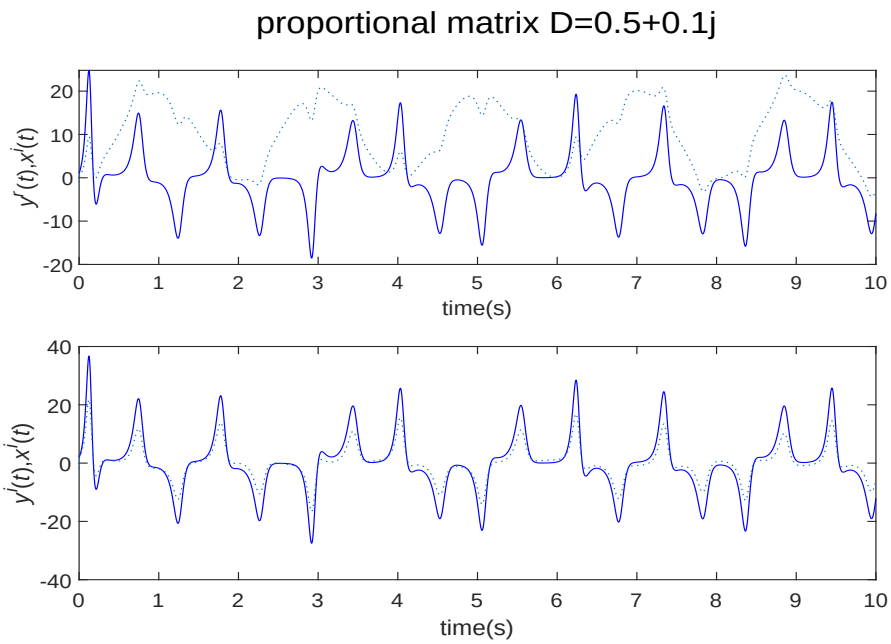

Figure 9. The diagram of state variables $\mathbf{x}_1$ and $\mathbf{y}_1$ with noise $A = 50$.

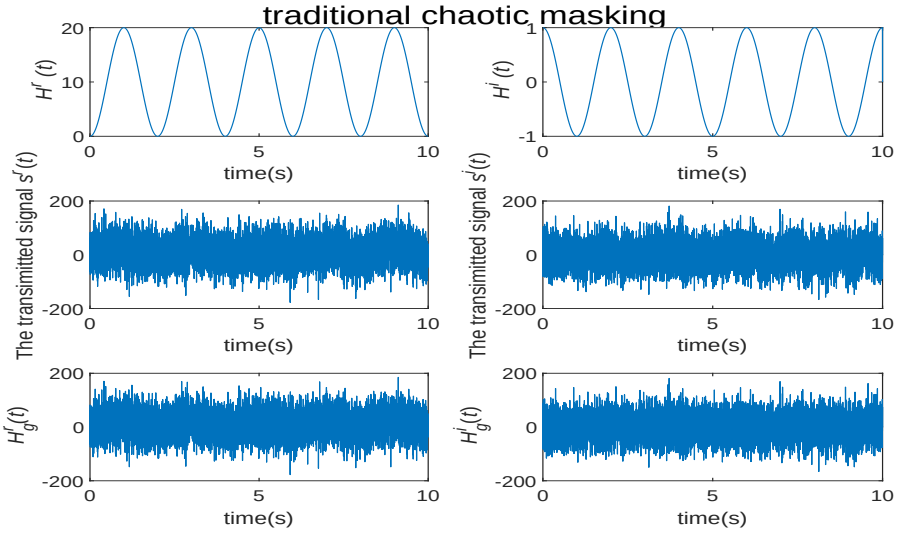

Figure 10. The traditional chaotic masking process with noise $A = 50$ and the same control strength.

5. Security Analysis

In this section, we analyze the security of the proposed CMPDFS communication scheme for WSNs.

5.1. Key Space Analysis

For the purpose of analyses, we take $q = 1$ as an example in our communication scheme. If a third party intercepts the signals of transmission channel such as $s'(t)$, $z_1(t)$ and $z_2(t)$, as $s'(t) = \dot{H} + Dg(y_1, z_1, z_2) + A\varepsilon$, the message signal H cannot be decrypted without the private keys such as D, z_1, z_2, the function g and $A\varepsilon(t)$. In particular, when the amplitude of $\dot{H}$ is much smaller than that of $Dg(y_1, z_1, z_2)$ or A, $s'(t) \approx Dg(y_1, z_1, z_2) + A\varepsilon$, it is impossible to decrypt the message signal H using only the signals of transmission channel. Therefore, for private keys D, z_1, and z_2, the key space of our algorithm is infinite.

5.2. Key Sensitivity Analysis

In the proposed scheme, the most important private key is the proportion matrix **D**. Here, the matrix is one-dimensional. To analyze the sensitivity, the message signal H was transmitted with two close initial values, $D = 0.5 + 0.1j$ in the sensor node and $D' = 0.5 + 0.11j$ at the sink node. $A = 0$ was selected to remove the effect of noise on the sensitivity. The CMPDFS process is presented in Figure 11. The error between message signal H and H_g is shown in Figure 12. The error increases with time. Compared with the original signal, the recovered signal is slightly distorted. The results demonstrate that the proposed algorithm has good sensitivity to the private key.

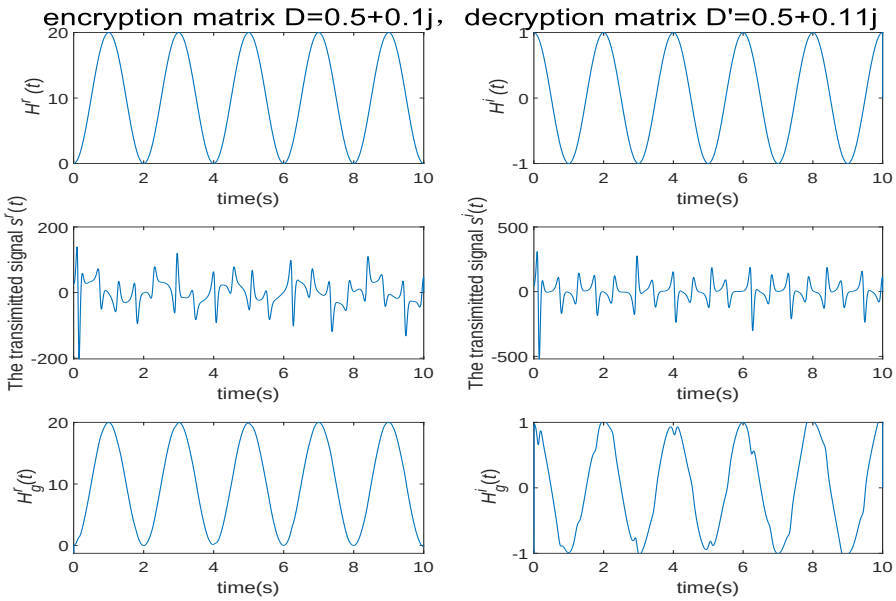

Figure 11. The CMPDFS process with $D = 0.5 + 0.1j$ and $D' = 0.5 + 0.11j$.

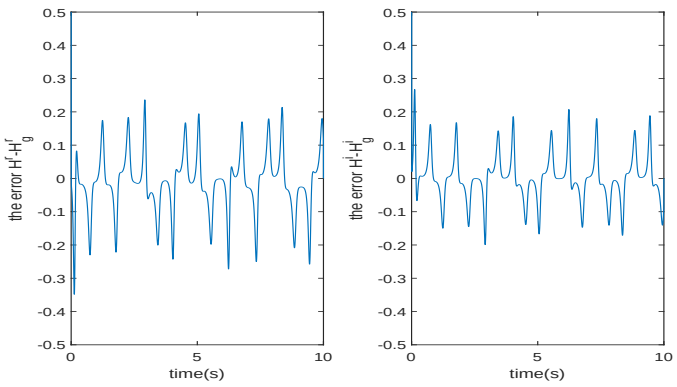

Figure 12. The error between message signal H and H_g.

5.3. Speed Analysis

The speed of the proposed scheme was tested using a computer with an Intel(R) Core(TM) i7-6700HQ 2.60 GHz CPU, 16.00 GB memory and a 500 G solid state drive. The analysis was conducted using Matlab2018a on a Windows 10 operating system. The average time required for a single simulation was 0.04 s. The comparison with digital encryption methods [35,36] are summarized in Table 3, which clearly predicts that the average encryption rate of the proposed scheme is faster than that of [35,36], thus making this communication scheme useful in WSNs.

Table 3. The comparison results with encryption methods.

Encryption Methods	Signal Size	Average Time
Adapted from [35]	768 kb	1.76 s
Adapted from [36]	768 kb	0.669 s
Our proposed algorithm	75 kb	0.02 s

6. Conclusions

We propose CMPDFS for CVCSs, which has not been previously investigated. CS, PHS, CMPS, and MDFS are all special cases of CMPDFS. We design an adaptive controller scheme for CMPDFS, and propose a novel communication scheme for WSNs, which is fundamentally different from traditional chaotic masking in methodology. The transmitted signal consists of noises, the derivative of message signal and chaotic signal. The message signal is retrieved as the desired difference function of the CMPDFS. The effectiveness of the proposed method is verified through simulation. The communication system theoretically has the ability to transmit message signals with significant robustness, zero BER, an infinite key space, and good key sensitivity at a high speed.

Therefore, the proposed scheme significantly enhances the security of WSNs. It also can be applied to similar communication systems in many fields, such as the Internet of Things and the military field.

Author Contributions: Conceptualization, F.Z. and R.G.; methodology, F.Z., Z.H. and C.J.; software, Z.H.; validation, F.Z., Z.H. and C.J.; formal analysis, F.Z. and Z.H.; investigation, F.Z. and R.G.; resources, R.G., Y.C. and H.Z.; data curation, F.Z. and Z.H.; writing—original draft preparation, F.Z., Z.H., C.J., Y.C. and H.Z.; writing—review and editing, F.Z. and Z.H.; visualization, F.Z., Y.C. and H.Z.; supervision, R.G.; project administration, R.G.; funding acquisition, R.G.; All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by National Natural Science Foundation of China (No. U1806202) and the International Collaborative Research Project of Qilu University of Technology (No. QLUT-GJHZ2018020).

Data Availability Statement: Not applicable.

Acknowledgments: This research was funded by National Natural Science Foundation of China (No.U1806202)and the International Collaborative Research Project of Qilu University of Technology (No.QLUTGJHZ2018020).

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Fowler, A.C.; Gibbon, J.D. The complex Lorenz equations. *Phys. D Nonlinear Phenom.* **1982**, *4*, 139–163. [CrossRef]
2. Gibbon, J.D.; McGuinness, M.J. The real and complex Lorenz equations in rotating fluids and laser. *Phys. D Nonlinear Phenom.* **1982**, *5*, 108–122. [CrossRef]
3. Fowler, A.C.; Gibbon, J.D.; McGuinnes, M.J. The real and complex Lorenz equations and their relevance to physical systems. *Phys. 7D* **1983**, *7*, 126–134. [CrossRef]
4. Mahmoud, G.M.; Bountis, T.; Mahmoud, E.E. Active control and global synchronization for complex Chen and L*ü* systems. *Int. J. Bifurc. Chaos* **2007**, *17*, 4295–4308. [CrossRef]
5. Mahmoud, G.M.; Mahmoud, E.E.; Arafa, A.A. On projective synchronization of hyperchaotic complex nonlinear systems based on passive theory for secure communications. *Phys. Scr.* **2013**, *87*, 055002. [CrossRef]
6. Cui, S.; Zhang, J. Chaotic Secure Communication Based on Single Feedback Phase Modulation and Channel Transmission. *IEEE Photonics J.* **2019**, *11*, 1–8. [CrossRef]
7. Zhang, F.; Li, Z.; Sun, K.; Zhang, X.; Ji, P. A new hyperchaotic complex system with parametric attractors. *Fractals* **2021**, *29*, 2150230. [CrossRef]
8. Li, Z.; Zhang, F.; Zhang, X.; Zhao, Y. A new hyperchaotic complex system and its synchronization realization. *Phys. Scr.* **2021**, *96*, 045208. [CrossRef]
9. Zhang, F.F.; Gao, R.; Liu, J. Acoustic wireless communication based on parameter modulation and complex Lorenz chaotic systems with complex parameters and parametric attractors. *Chin. Phys.* **2021**, *30*, 080503. [CrossRef]

10. Aliabadi, F.; Majidi, M.H.; Khorashadizadeh, S. Chaos synchronization using adaptive quantum neural networks and its application in secure communication and cryptography. *Neural Comput. Appl.* **2022**, *34*, 6521–6533. [CrossRef]
11. Alshammari, A.S. Synchronization of Two Chaotic Stream Ciphers in Secure CDMA Communication Systems. *Eng. Technol. Appl. Sci. Res.* **2020**, *10*, 5947–5952. [CrossRef]
12. Bai, C.; Ren, H.-P.; Kolumbán, G. Double-Sub-Stream M-ary Differential Chaos Shift Keying Wireless Communication System Using Chaotic Shape-Forming Filter. *IEEE Trans. Circuits Syst. I* **2020**, *67*, 3574–3587. [CrossRef]
13. Zheng, J.; Hu, H.P. A highly secure stream cipher based on analog-digital hybrid chaotic system. *Inf. Sci.* **2022**, *587*, 226–246. [CrossRef]
14. Mahmoud, G.M.; Mahmoud, E.E. Phase and antiphase synchronization of two identical hyperchaotic complex nonlinear systems. *Nonlinear Dyn.* **2010**, *61*, 141–152. [CrossRef]
15. Mahmoud, G.M.; Mahmoud, E.E. Complete synchronization of chaotic complex nonlinear systems with uncertain parameters. *Nonlinear Dyn.* **2010**, *62*, 875–882. [CrossRef]
16. Liu, S.T.; Liu, P. Adaptive anti-synchronization of chaotic complex nonlinear systems with unknown parameters. *Nonlinear Anal. RWA* **2011**, *12*, 3046–3055. [CrossRef]
17. Liu, P.; Liu, S.T. Anti-synchronization between different chaotic complex systems. *Phys. Scr.* **2011**, *83*, 065006. [CrossRef]
18. Mahmoud, G.M.; Mahmoud, E.E. Lag synchronization of hyperchaotic complex nonlinear systems. *Nonlinear Dyn.* **2012**, *67*, 1613–1622. [CrossRef]
19. Mahmoud, E.E. Adaptive anti-lag synchronization of two identical or non-identical hyperchaotic complex nonlinear systems with uncertain parameters. *J. Frankl. Inst.* **2012**, *349*, 1247–1266. [CrossRef]
20. Liu, P.; Liu, S.T.; Li, X. Adaptive modified function projective synchronization of general uncertain chaotic complex systems. *Phys. Scr.* **2012**, *85*, 3743–3748. [CrossRef]
21. Liu, P.; Liu, S.T. Robust adaptive full state hybrid synchronization of chaotic complex systems with unknown parameters and external disturbances. *Nonlinear Dyn.* **2012**, *70*, 585–599. [CrossRef]
22. Mahmoud, E.E. Modified projective phase synchronization of chaotic complex nonlinear systems. *Math. Comput. Simul.* **2013**, *89*, 69–85. [CrossRef]
23. Luo, C.; Wang, X.Y. Hybrid modified function projective synchronization of two different dimensional complex nonlinear systems with parameters identification. *J. Frankl. Inst.* **2013**, *350*, 2646–2663. [CrossRef]
24. Liu, J.; Liu, S.T.; Yuan, C.H. Adaptive complex modified projective synchronization of complex chaotic (hyperchaotic) systems with uncertain complex parameters. *Nonlinear Dyn.* **2015**, *79*, 1035–1047. [CrossRef]
25. Zhang, F.F.; Liu, S.T. Self time-delay synchronization of time-delay coupled complex chaotic system and its applications to communication. *Int. J. Mod. Phys. C* **2014**, *25*, 1350102. [CrossRef]
26. Zhang, F.F. Complete synchronization of coupled multiple-time-delay complex chaotic system with applications to secure communication. *Acta Phys. Pol.* **2015**, *46*, 1473–1486. [CrossRef]
27. Liu, J.; Liu, S.T.; Sprott, J.C. Adaptive complex modified hybrid function projective synchronization of different dimensional complex chaos with uncertain complex parameters. *Nonlinear Dyn.* **2016**, *83*, 1109–1121. [CrossRef]
28. Liu, J.; Liu, S.T. Complex modified function projective synchronization of complex chaotic systems with known and unknown complex parameters. *Appl. Math. Model.* **2017**, *48*, 440–450. [CrossRef]
29. Mahmoud, E.E.; Abo-Dahab, S.M. Dynamical properties and complex anti synchronization with applications to secure communications for a novel chaotic complex nonlinear model. *Chaos Soliton Fractals* **2018**, *106*, 273–284. [CrossRef]
30. Liu, J.; Wang, Z.; Shu, M.; Zhang, F.; Leng, S.; Sun, X. Secure communication of fractional complex chaotic systems based on fractional difference function synchronization. *Complexity* **2019**, *2019*, 7242791. [CrossRef]
31. Guo, J.; Ma, C.; Wang, X.; Zhang, F.; van Wyk, M.A.; Kou, L. A new synchronization method for time-delay fractional complex chaotic system and its application. *Mathematics* **2021**, *9*, 3305. [CrossRef]
32. Jayawickrama, C.; Kumar, S.; Chakrabartty, S.; Song, H. A novel chaotic modulation approach of packaged antenna for secured wireless medical sensor network in E-healthcare applications. *Microw. Opt. Technol. Lett.* **2020**, *62*, 933–942. [CrossRef]
33. Niu, Z.; Zheng, M.; Zhang, Y.; Wang, T. A new asymmetrical encryption algorithm based on semitensor compressed sensing in WBANs. *IEEE Internet Things* **2020**, *7*, 734–750. [CrossRef]
34. Olga, I.M.; Alexey, A.K.; Alexander, E.H. Generalized synchronization of chaos for secure communication: Remarkable stability to noise. *Phys. Lett. A* **2010**, *374*, 2925–2931.
35. Narendra, K.P. Design and analysis of a novel digital image encryption scheme. *Int. J. Netw.* **2012**, *4*, 95–108.
36. Jie, Z.; Nan, Z.; Hua, G. Fast color image encryption scheme based on 3D orthogonal Latin squares and matching matrix. *Opt. Laser Technol* **2020**, *131*, 106437.