An Encryption Scheme Based on Synchronization of Two-Layered Complex Dynamical Networks

Hui Liu, *Member, IEEE*, Haibo Wan, Chi K. Tse, *Fellow, IEEE*, and Jinhu Lü, *Fellow, IEEE*

***Abstract*—A novel encryption scheme based on complex chaotic networks is proposed in this paper. Compared with a single chaotic system, a network of chaotic systems possesses complex dynamic characteristics, which can be used in encryption to enhance security. We adopt the drive-response synchronization method to synchronize two identical chaotic networks at the transmitter and receiver. Analysis on encryption security shows that key space is enlarged exponentially with respect to the number of nodes in the drive network, and also shows that the encryption system is highly sensitive to parameter mismatch. The proposed scheme is competent in carrying out encryption tasks of large data. Both theoretical and numerical results demonstrate that the proposed scheme is feasible for implementation in image and data encryption.**

***Index Terms*—Chaotic systems, complex dynamical networks, encryption scheme, node-to-node synchronization, two-layered networks.**

I. Introduction

In recent years, due to the huge amount of data being stored in and transmitted through various communication networks, such as computer networks, sensor networks, and satellite networks, the importance of information security has received renewed interest and considerable attention by scientists and engineers across the computer, information and systems disciplines. Image encryption, due to the relatively large size of image data, is generally difficult to handle by using conventional encryption techniques such as Advanced Encryption Standard (AES), International Data Encryption Algorithm (IDEA), and RSA (proposed by Rivest, Shamir, and Adleman) [1]–[3]. The RSA algorithm is the most widely used asymmetric-key cryptography method for secure data transmission [3]. However, in decryption, modular exponentiation operations on long numbers are very costly, which results in the RSA being a relatively slow algorithm. Hence, the RSA performs better in encryption scenarios of small data, such as digital signatures, secret key agreements, and authentication [4]–[6].

Along another line, chaotic systems and their applications to encryption schemes have attracted a great deal of attention in the last two decades [7]–[14]. Since a large number of chaotic sequences can be generated easily and fast because of the dependence upon initial conditions and parameter variations [12], chaos provides a low-cost and high-speed means for realizing the encryption task for large-scale data, e.g., images, videos and audios [14], [15]. Chaotic signals are characterized by extreme sensitivity to variation of system parameters and initial condition perturbations, random like waveforms, and broadband frequency spectra [12], [13]. These properties make chaotic systems suitable for the application in secure communications [13]. Engineers and researchers have made concerted efforts to improve the security of chaotic encryption systems, and have made significant achievements in the past two decades [16]–[21]. The synchronization of chaotic systems has been studied and applied in encryption systems [16]. Impulsive control has been used to synchronize two identical chaotic systems, and "magnifying glass" has been introduced to increase the sensitivity of system parameters [17]. In order to overcome the negative impact of the channel noise, generalized synchronization of chaotic systems [20] and robust control based on dead-zone algorithm [6] have been applied. The hybrid of analog and digital chaotic systems can enhance the security of the system [21] by overcoming the drawbacks of the time delay signature of analog chaos and periodicity of digital chaos. Higher-dimensional digital chaotic systems are designed to deal with the problem of dynamical degradation caused by quantization [22]. However, most of the existing works adopted a single chaotic system in their secure encryption architectures.

Complex dynamical networks, composed of coupled chaotic or other nonlinear systems, have been widely studied in many fields, such as electronic engineering [23]–[25] and control engineering [26]–[28]. The complexity of the dynamical networks can be understood from the following two aspects. First, the network structures are complicated. Besides the classical regular lattices and random graphs, the structures can be small-world or scale-free networks both of which have sparse connections but short average distances [29]. Second, since the dynamics of the nodes in a network are nonlinear and possibly heterogeneous, interconnected nodes can influence each other

Manuscript received March 1, 2016; revised June 7, 2016 and July 20, 2016; accepted August 2, 2016. Date of publication September 9, 2016; date of current version October 25, 2016. This work was supported by the National Key Research and Development Program of China (No. 2016YFB0800401), the National Natural Science Foundation of China (No. 61403154, 61532020, 11072254), the Hong Kong Polytechnic University Research Project G-YBAT, and the Fundamental Research Funds for the Central Universities, China (HUST: 2014TS106). This paper was recommended by Associate Editor H. R. Karimi.

H. Liu and H. Wan are with the School of Automation and also with the Key Laboratory of Image Processing and Intelligent Control of Education Ministry of China, Huazhong University of Science and Technology, Wuhan 430074, China (e-mail:hliu@hust.edu.cn; hustwhb@hust.edu.cn).

C. K. Tse is with the Department of Electronic and Information Engineering, The Hong Kong Polytechnic University, Kowloon, Hong Kong (e-mail:encktse@polyu.edu.hk).

J. Lü is with the Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190, China (e-mail:jhlu@iss.ac.cn).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TCSI.2016.2598822

so that the whole network's dynamical evolutions become much more complicated [30], [31]. In view of these features, we use a complex dynamical network consisting of multiple heterogeneous chaotic oscillators, instead of the classical single chaotic system, to increase the complexity of chaotic signals, so that intruders can no longer obtain useful information so readily from the transmitted signals. In addition, the complex network can be equipped with different types of chaotic systems with adjustable parameters and different network structures. Therefore, the use of a complex dynamical network in our encryption system enlarges greatly its key space and offers significant improvement in its security. Besides enlarging the key space of the encryption system, the use of a complex dynamical network can speed up data encryption. Each node (i.e., a chaotic system) in the complex dynamical network is capable of data encryption. Thus, multiple encoded data streams are obtained and transmitted simultaneously, which improves the encryption speed. Therefore, the proposed scheme is especially competent in carrying out encryption tasks of large-scale data.

In the proposed secure encryption system, the synchronization of two identical chaotic networks embedded in the transmitter and receiver is crucial to correctly recovering the original message. Toward this aim, we need to explore conditions for the node-to-node synchronization in a two-layered complex network composed of two identical chaotic networks. Synchronization in multiplex networks has been a new and hot topic in recent years [32]–[34]. Generally speaking, there are two types of synchronization patterns in multiplex networks. In the first type, synchronization takes place in each layer of a multiplex network and diffuses to the whole network. For example, Gómez *et al.* [35] constructed supra-Laplacian matrices for multiplex networks and investigated diffusion processes in multiplex networks. The other type of synchronization occurs in pairwise nodes from different layers. For example, Wen *et al.* [36], [37] studied node-to-node consensus in two layered networked agent systems and applied to trajectory tracking in groups of agents. In this work, we use the drive-response synchronization method [38], [39] to synchronize pairs of nodes in the two-layered chaotic networks. Using this method, only partial states of the complex chaotic network in the transmitter need to be transmitted to the receiver, thus avoiding the chance of exposing full states to attackers during transmission. In addition, we adopt the one-time pad technique [17], in which a plaintext is paired with a pseudorandom key generated by a chaotic network, in the secure encryption scheme. Since each key is used only once and random like, the one-time pad method is considered as the most secure encryption mechanism [40].

The rest of this paper is organized as follows. In Section II, we introduce a complex chaotic network model that will be embedded in both the transmitter and the receiver, and describe our proposed encryption/decryption scheme. Then, the synchronization criteria for drive and response chaotic networks in the transmitter and receiver are derived using the Lyapunov function method in Section III. We use two numerical simulations to test the proposed encryption scheme in Section IV, and analyze its enhanced security in terms of key space, sensitivity on parameter mismatch, etc., in Section V. Finally, conclusions are given in Section VI.

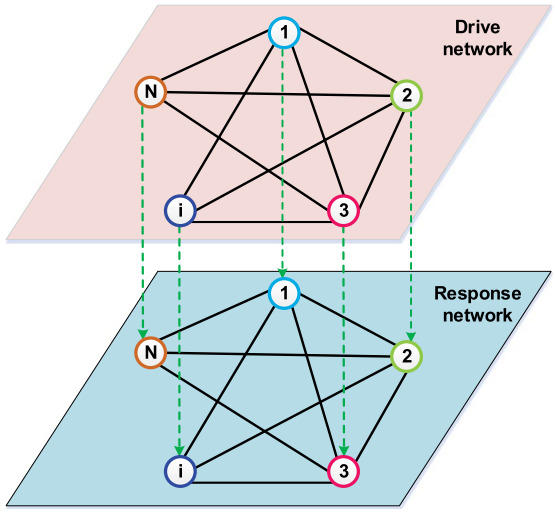


Fig. 1. Drive-response networks composed of coupled chaotic systems. The network in the top layer is the drive network; the network in the bottom layer is the response network. A solid line represents an undirected edge in a network; a dot line represents a directed edge from a node in the drive network to the one in the response network.

II. Complex Chaotic Network Model and Encryption Scheme

A. Complex Chaotic Network Model

We first present a complex chaotic network model that will be used in our encryption scheme. Two identical complex chaotic networks, namely the drive network and the response network, are located in the top and bottom layers, respectively, in Fig. 1. The drive network (i.e., the complex chaotic network in the transmitter) is composed of a set of master systems, i.e., chaos generators; the response network (i.e., the complex chaotic network in the receiver) is comprised of a set of slave systems. The nodes in the two networks are one-to-one correspondent, as shown in Fig. 1. Each network consists of N coupled nodes that are *heterogeneous* chaotic systems.

At the transmitter side, the dynamics of the drive network can be described as follows:

$$\dot{x}_i = f_i(x_i) + \sum_{j=1}^{N} w_{ij} H_i x_j, \qquad i = 1, \ldots, N \tag{1}$$

where $x_i \in \mathbb{R}^n$ is the state of the ith node, and $f_i(\cdot) : \mathbb{R}^n \to \mathbb{R}^n$ is the self-dynamics of node i. In this work, we define $\dot{x}_i = f_i(x_i)$ as the Lorenz system whose dynamics is described by

$$\begin{cases} \dot{x}_{i1} = \sigma_i(x_{i2} - x_{i1}) \\ \dot{x}_{i2} = \mu_i x_{i1} - x_{i1}x_{i3} - x_{i2} \\ \dot{x}_{i3} = x_{i1}x_{i2} - \beta_i x_{i3} \end{cases} \tag{2}$$

where $x_i = (x_{i1}, x_{i2}, x_{i3})^\top \in \mathbb{R}^3$, and σ_i, μ_i, β_i are system parameters. For different i, the parameters are different, which means heterogeneity of the nodes in the chaos generating network. The matrix $W = (w_{ij})_{N\times N}$ describes the connections between nodes in network (2). Also w_{ij} describes the weight of edge (j, i). We assume that the network graph is undirected.

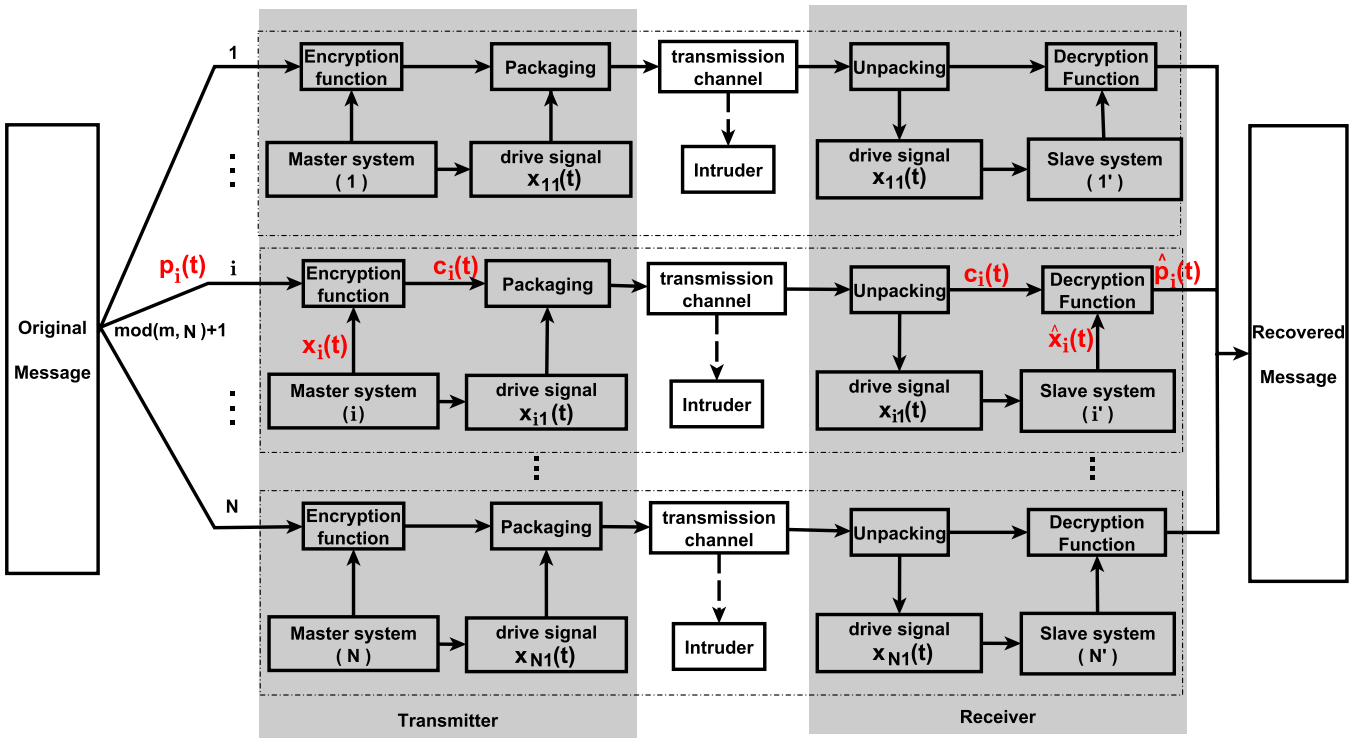


Fig. 2. Block diagram of the proposed encryption/decryption scheme. The master systems (i.e., chaos generators) on the left side of the transmission channels are connected in a specific topological structure, which is not explicitly shown in this diagram; the slave systems on the right side are connected in the same topological structure.

If there is an edge between nodes i and j, then $w_{ij} = w_{ji} > 0 (i \neq j)$; otherwise $w_{ij} = w_{ji} = 0$. We set $w_{ii} = -\sum_{j \neq i} w_{ij}$ for $i = 1, \ldots, N$. Matrix $H_i \in \mathbb{R}^{n \times n}$ is the inner-coupling matrix for node i, which defines the way in which the oscillators are coupled together. After introducing the drive network of chaos generators at the transmitter side, we construct the response network of chaos generators at the receiver side as follows:

$$\dot{\hat{x}}_i = f_i(x_i, \hat{x}_i) + \sum_{j=1}^{N} w_{ij} H_i \hat{x}_j, \qquad i = 1, \ldots, N. \tag{3}$$

We will use the drive-response method (also called the PC method) proposed by Pecora and Carrol in [38] to synchronize networks (1) and (3), i.e., $\|\hat{x}_i - x_i\| \to 0$ for $i = 1, \ldots, N$.

B. Encryption/Decryption Scheme

The block diagram of the proposed encryption/decryption system is shown in Fig. 2. The system has three major parts: the transmitter, the receiver, and the transmission channels. The transmitter is composed of N encrypters and the receiver is composed of N decrypters. As shown in Fig. 1, we use network (1) of N coupled chaotic systems to generate chaotic sequences in the encrypters. Accordingly, we use network (3) to generate chaotic sequences in the decrypters.

Let $p(t)$ denote the plaintext to be transmitted. We transform plaintext $p(t)$ to a binary sequence. Each sequence unit has a serial number m. Since there are N encrypter cells in the transmitter, we divide plaintext $p(t)$ into N components $p_1(t), \ldots, p_N(t)$ in the transmission according to the result of $\mathrm{mod}(m, N) + 1$.

1) Encrypters: Each encrypter consists of a chaos generator and an encryption function. Chaos generator i produces chaos sequence $x_i(t)$. Key sequence $s_i(t)$ is a combination of all the three components of $x_i(t)$, which is given by

$$\begin{cases} X_i(t) = K \left\lfloor \left(x_{i1}^2(t) + x_{i2}^2(t) + x_{i3}^2(t)\right)^{\frac{1}{2}} \right\rfloor \\ s_i(t) = \left(X_i(t) + \lambda\right) \bmod (M) \end{cases} \tag{4}$$

where K is a positive integer functioning as a "magnifier" that increases parameter sensitivity of the encryption system [17]. The function of K will be discussed later in Section V-B. $\lfloor a \rfloor$ is the largest integer not greater than a; M is a positive integer number determined by the quantization level of plaintext $p_i(t)$; and λ is an arbitrary integer in the range of $[0, M]$.

The encryption function executes an XOR operation on plaintext $p_i(t)$ and key sequence $s_i(t)$, and obtains ciphertext $c_i(t)$. This encryption is described by

$$c_i(t) = E\left(p_i(t), s_i(t)\right) = p_i(t) \oplus s_i(t) \tag{5}$$

where function $E(p, q)$ is a bitwise XOR operation, i.e., $p \oplus q$ [17].

We use the first component of state $x_i(t)$, i.e., $x_{i1}(t)$, as a drive signal for (3). Then, ciphertext $c_i(t)$ and drive signal $x_{i1}(t)$ constitute a package. The package is transmitted through a channel to the corresponding decrypter.

2) Decrypters: Each decrypter consists of an identical chaos generator to the one in the corresponding encrypter and a

TABLE I
XOR OPERATION RESULTS

a	b	a ⊕ b	a ⊕ b ⊕ b
0	0	1	0
0	1	0	0
1	0	0	1
1	1	1	1

decryption function. The transmitted package is immediately unpacked after it is received, i.e., the received package is decomposed into $c_i(t)$ and $x_{i1}(t)$. So we get the received ciphertext $c_i(t)$ and the drive signal $x_{i1}(t)$. Then, recovered plaintext $\hat{p}_i(t)$ is obtained from the decryption function that executes an XOR operation on ciphertext $c_i(t)$ and key sequence $\hat{s}_i(t)$. $\hat{s}_i(t)$ is a combination of all the three components of $\hat{x}_i(t)$, which is given by

$$\begin{cases} \hat{X}_i(t) = K \left\lfloor \left(\hat{x}_{i1}^2(t) + \hat{x}_{i2}^2(t) + \hat{x}_{i3}^2(t)\right)^{\frac{1}{2}} \right\rfloor \\ \hat{s}_i(t) = \left(\hat{X}_i(t)) + \lambda\right) \bmod (M) \end{cases} \tag{6}$$

where $i = 1, \ldots, N$. The decryption function is described by

$$\hat{p}_i(t) = D\left(c_i(t), \hat{s}_i(t)\right) = c_i(t) \oplus \hat{s}_i(t) \tag{7}$$

where $i = 1, \ldots, N$. As described in Table I, a binary number a taking an XOR operation with another binary number b two times is a itself. Note that $\hat{p}_i(t) = c_i(t) \oplus \hat{s}_i(t) = p_i(t) \oplus s_i(t) \oplus \hat{s}_i(t)$. Hence, one can see that $s_i(t) = \hat{s}_i(t)$ results in $\hat{p}_i(t) = p_i(t)$. Thus, it is necessary to use identical key sequences (i.e., $s_i(t) = \hat{s}_i(t)$) in each pair of encrypter and decrypter, for correctly recovering the original message from the ciphertext.

From (6), $s_i(t) = \hat{s}_i(t)$ for $i = 1, \ldots, N$ holds if and only if $x_i(t)$ and $\hat{x}_i(t)$ synchronize. So the problem left to be solved is to synchronize $\hat{x}_i(t)$ with $x_i(t)$, for $i = 1, \ldots, N$. It will be analyzed in the next section.

Remark 1: Multiple encryption/decryption cells working in a parallel mode are adopted in the transmitter/receiver, which can accelerate data encryption in real-time application.

III. SYNCHRONIZATION OF TWO-LAYERED COMPLEX DYNAMICAL NETWORKS

In this section, we adopt the drive-response synchronization method to synchronize network (1) embedded in the transmitter with network (3) embedded in the receiver, using drive signals $x_{i1}(t)$ where $i = 1, \ldots, N$. In the following, we provide a number of choices for the inner-coupling matrix H_i that yields synchronization. We prove synchronization with H_is being several diagonal and non-diagonal matrices.

A. Diagonal Inner-Coupling Matrices

Here we take the case of the inner-coupling matrix being $H_i = \text{diag}(1, 0, 0)$ as an example. Chaos generators are coupled non-identical Lorenz systems. From network (1) and system (2), the dynamics of chaos generators satisfies

$$\begin{cases} \dot{x}_{i1} = \sigma_i(x_{i2} - x_{i1}) + \sum_{j=1}^{N} w_{ij} x_{j1} \\ \dot{x}_{i2} = \mu_i x_{i1} - x_{i1} x_{i3} - x_{i2} \\ \dot{x}_{i3} = x_{i1} x_{i2} - \beta_i x_{i3} \end{cases} \tag{8}$$

where $i = 1, \ldots, N$. We take the first components of the states x_i, i.e., x_{i1} for all i as the drive signals to the response network (3). Using these drive signals, we rewrite (3) as

$$\begin{cases} \dot{\hat{x}}_{i1} = \sigma_i(\hat{x}_{i2} - \hat{x}_{i1}) + \sum_{j=1}^{N} w_{ij} \hat{x}_{j1} \\ \dot{\hat{x}}_{i2} = \mu_i x_{i1} - x_{i1} \hat{x}_{i3} - \hat{x}_{i2} \\ \dot{\hat{x}}_{i3} = x_{i1} \hat{x}_{i2} - \beta_i \hat{x}_{i3}. \end{cases} \tag{9}$$

As stated in Section II, the critical step in recovering the original message is to synchronize response network (9) [resp. (3)] with drive network (8) [resp. (1)]. This problem is addressed in the rest of this section.

Theorem 1: Suppose $\sigma_i > 0, \beta_i > 0$, for $i = 1, \ldots, N$. Then, response network (9) can synchronize with drive network (8) under the inner-coupling matrix $H_i = \text{diag}(1, 0, 0)$ for $i = 1, \ldots, N$.

Proof: Let e_i be the difference between $\hat{x}_i$ and x_i, i.e., $e_i \triangleq (e_{i1}, e_{i2}, e_{i3})^\top$ where $e_{i1} = \hat{x}_{i1} - x_{i1}$, $e_{i2} = \hat{x}_{i2} - x_{i2}$, and $e_{i3} = \hat{x}_{i3} - x_{i3}$. From (8) and (9), we obtain

$$\begin{cases} \dot{e}_{i1} = \sigma_i(e_{i2} - e_{i1}) + \sum_{j=1}^{N} w_{ij} e_{j1} \\ \dot{e}_{i2} = -x_{i1} e_{i3} - e_{i2} \\ \dot{e}_{i3} = x_{i1} e_{i2} - \beta_i e_{i3} \end{cases} \tag{10}$$

where $i = 1, \ldots, N$. In order to prove the synchronization of networks (8) and (9), we need to prove that e_i for $i = 1, \ldots, N$ converges to $\mathbf{0}$. Note that $\sigma_i > 0$. We construct the Lyapunov function [41]

$$V\left(e(t)\right) = \sum_{i=1}^{N} \left(\frac{1}{\sigma_i} e_{i1}^2 + e_{i2}^2 + e_{i3}^2 \right). \tag{11}$$

Then, we calculate the derivative of $V(e(t))$ using (10), and get

$$\begin{aligned} \frac{dV}{dt} &= \sum_{i=1}^{N} \left[\frac{2}{\sigma_i} e_{i1} \dot{e}_{i1} + 2 e_{i2} \dot{e}_{i2} + 2 e_{i3} \dot{e}_{i3} \right] \\ &= \sum_{i=1}^{N} 2 e_{i1} e_{i2} - \sum_{i=1}^{N} 2 e_{i1}^2 + \frac{2}{\sigma_i} \sum_{i=1}^{N} e_{i1} \sum_{j=1}^{N} w_{ij} e_{j1} \\ &\quad - \sum_{i=1}^{N} 2 e_{i2}^2 - \sum_{i=1}^{N} 2 \beta_i e_{i3}^2. \end{aligned}$$

Note that $2 e_{i1} e_{i2} \le e_{i1}^2 + e_{i2}^2$ and its equality sign holds if and only if $e_{i1} = e_{i2}$. With this inequality, we obtain

$$\begin{aligned} \frac{dV}{dt} \le &- \sum_{i=1}^{N} e_{i1}^2 - \sum_{i=1}^{N} e_{i2}^2 - \sum_{i=1}^{N} 2 \beta_i e_{i3}^2 \\ &+ \frac{2}{\sigma_i} \sum_{i=1}^{N} e_{i1} \sum_{j=1}^{N} w_{ij} e_{j1}. \end{aligned}$$

Let

$$D_1(e) = - \sum_{i=1}^{N} e_{i1}^2 - \sum_{i=1}^{N} e_{i2}^2 - \sum_{i=1}^{N} 2 \beta_i e_{i3}^2$$

where $\beta_i > 0$. Thus, $D_1(e) \leq 0$ and its equality sign holds if and only if $e_{i1} = e_{i2} = e_{i3} = 0$, for $i = 1, \ldots, N$. Let

$$D_2(e) = \frac{2}{\sigma_i} \sum_{i=1}^{N} e_{i1} \sum_{j=1}^{N} w_{ij} e_{j1}$$

and $E_1 = (e_{11}, e_{21}, \ldots, e_{N1})^\top$. Then, $D_2(e) = (2/\sigma_i) E_1^\top W E_1$. Note that

$$\sum_{i=1}^{N} e_{i1} \sum_{j=1}^{N} w_{ij} e_{j1} = E_1^\top W E_1 = -\sum_{j \neq i} w_{ij} (e_{i1} - e_{j1})^2 \leq 0.$$

Therefore, $D_2(e) \leq 0$ and its equality sign holds if and only if $e_{i1} = e_{j1}$, for $j \neq i$.

Combining the above analysis on $D_1(e)$ and $D_2(e)$, one has

$$\dot{V}(e) = D_1(e) + D_2(e) \leq 0$$

and $\dot{V}(e) = 0$ if and only if $D_1(e) = 0$ and $D_2(e) = 0$, i.e., $e_{i1} = e_{i2} = e_{i3} = 0$ for $i = 1, \ldots, N$ and $e_{i1} = e_{j1}$ for $j \neq i$. Therefore, $\dot{V}(e) \leq 0$ and $\dot{V}(e) = 0$ if and only if $e_{i1} = e_{i2} = e_{i3} = 0$ for $i = 1, \ldots, N$. According to the Lyapunov stability theorem [42, Ch. 4], e_i of system (10) converges to $\mathbf{0}$ as $t \to \infty$. This implies that response network (3) can synchronize with drive network (1) as $t \to \infty$. ■

One can prove the following result in the same way:

Theorem 2: Suppose $\sigma_i > 0, \beta_i > 0$, for $i = 1, \ldots, N$. Then, the response network (9) can synchronize with the drive network (8) under the inner-coupling matrix *i)* $H_i = \text{diag}(0, 1, 0)$ or *ii)* $H_i = \text{diag}(0, 0, 1)$.

B. Non-Diagonal Inner-Coupling Matrices

In this subsection, we consider the case of the inner-coupling matrix being

$$H_i = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ -1/\sigma_i & 0 & 0 \end{pmatrix} \quad \text{where } i = 1, \ldots, N \tag{12}$$

as an example. From network (1) and system (2), the dynamics of chaos generators satisfies

$$\begin{cases} \dot{x}_{i1} = \sigma_i (x_{i2} - x_{i1}) + \sum_{j=1}^{N} w_{ij} x_{j3} \\ \dot{x}_{i2} = \mu_i x_{i1} - x_{i1} x_{i3} - x_{i2} \\ \dot{x}_{i3} = x_{i1} x_{i2} - \beta_i x_{i3} - \frac{1}{\sigma_i} \sum_{j=1}^{N} w_{ij} x_{j1} \end{cases} \tag{13}$$

where $i = 1, \ldots, N$. We also apply the drive-response synchronization method to synchronize chaotic networks (1) and (3), and take x_{i1} for all i as the drive signals for response network (3). Thus, (3) can be rewritten as

$$\begin{cases} \dot{\hat{x}}_{i1} = \sigma_i (\hat{x}_{i2} - \hat{x}_{i1}) + \sum_{j=1}^{N} w_{ij} \hat{x}_{j3} \\ \dot{\hat{x}}_{i2} = \mu_i x_{i1} - x_{i1} \hat{x}_{i3} - \hat{x}_{i2} \\ \dot{\hat{x}}_{i3} = x_{i1} \hat{x}_{i2} - \beta_i \hat{x}_{i3} - \frac{1}{\sigma_i} \sum_{j=1}^{N} w_{ij} \hat{x}_{j1}. \end{cases} \tag{14}$$

The following theorem guarantees synchronization of drive network (13) [resp. (1)] and response network (14) [resp. (3)].

Theorem 3: Suppose $\sigma_i > 0, \beta_i > 0$, for $i = 1, \ldots, N$. Then, response network (14) can synchronize with drive network (13) under the inner-coupling matrix H_i given by (12).

Proof: Vector e_i is the difference between $\hat{x}_i$ and x_i. Here the dynamics of e_i can be obtained by subtracting (13) from (14), giving

$$\begin{cases} \dot{e}_{i1} = \sigma_i (e_{i2} - e_{i1}) + \sum_{j=1}^{N} w_{ij} e_{j3} \\ \dot{e}_{i2} = -x_{i1} e_{i3} - e_{i2} \\ \dot{e}_{i3} = x_{i1} e_{i2} - \beta_i e_{i3} - \frac{1}{\sigma_i} \sum_{j=1}^{N} w_{ij} e_{j1} \end{cases} \tag{15}$$

where $i = 1, \ldots, N$. To prove that (14) synchronizes with (13), we alternatively prove that $e_i \to \mathbf{0}$ for $i = 1, \ldots, N$. We also use the Lyapunov function method to prove the convergence of e_i, and choose the Lyapunov function as

$$V(e(t)) = \sum_{i=1}^{N} \left(\frac{1}{\sigma_i} e_{i1}^2 + e_{i2}^2 + e_{i3}^2 \right). \tag{16}$$

Then, calculating the derivative of $V(e(t))$ using (15), we have

$$\begin{aligned} \frac{dV}{dt} &= \sum_{i=1}^{N} \left[\frac{2}{\sigma_i} e_{i1} \dot{e}_{i1} + 2 e_{i2} \dot{e}_{i2} + 2 e_{i3} \dot{e}_{i3} \right] \\ &= \sum_{i=1}^{N} 2 e_{i1} e_{i2} - \sum_{i=1}^{N} 2 e_{i1}^2 + \frac{2}{\sigma_i} \sum_{i=1}^{N} e_{i1} \sum_{j=1}^{N} w_{ij} e_{j3} \\ &\quad - \sum_{i=1}^{N} 2 e_{i2}^2 - \sum_{i=1}^{N} 2 \beta_i e_{i3}^2 - \frac{2}{\sigma_i} \sum_{i=1}^{N} e_{i3} \sum_{j=1}^{N} w_{ij} e_{j1}. \end{aligned}$$

Note that $2 e_{i1} e_{i2} \leq e_{i1}^2 + e_{i2}^2$ and its equality sign holds if and only if $e_{i1} = e_{i2}$. With this inequality, we have

$$\begin{aligned} \frac{dV}{dt} &\leq -\sum_{i=1}^{N} e_{i1}^2 - \sum_{i=1}^{N} e_{i2}^2 - \sum_{i=1}^{N} 2 \beta_i e_{i3}^2 \\ &\quad + \frac{2}{\sigma_i} \sum_{i=1}^{N} e_{i1} \sum_{j=1}^{N} w_{ij} e_{j3} - \frac{2}{\sigma_i} \sum_{i=1}^{N} e_{i3} \sum_{j=1}^{N} w_{ij} e_{j1}. \end{aligned} \tag{17}$$

As mentioned in the previous subsection, $E_1 = (e_{11}, e_{21}, \ldots, e_{N1})^\top$. Let $E_3 = (e_{13}, e_{23}, \ldots, e_{N3})^\top$. Then we have $\sum_{i=1}^{N} e_{i1} \sum_{j=1}^{N} w_{ij} e_{j3} = E_1^\top W E_3$ and $\sum_{i=1}^{N} e_{i3} \sum_{j=1}^{N} w_{ij} e_{j1} = E_3^\top W E_1$. Note that $E_1^\top W E_3 = (E_1^\top W E_3)^\top = E_3^\top W E_1$. Thus

$$\sum_{i=1}^{N} e_{i1} \sum_{j=1}^{N} w_{ij} e_{j3} = \sum_{i=1}^{N} e_{i3} \sum_{j=1}^{N} w_{ij} e_{j1}. \tag{18}$$

Substituting (18) in inequality (17), we have

$$\frac{dV}{dt} \leq -\sum_{i=1}^{N} e_{i1}^2 - \sum_{i=1}^{N} e_{i2}^2 - \sum_{i=1}^{N} 2 \beta_i e_{i3}^2$$

where $\beta_i > 0$. Therefore, $dV/dt \leq 0$ and its equality sign holds if and only if $e_{i1} = e_{i2} = e_{i3} = 0$, for all $i = 1, \ldots, N$. According to the Lyapunov stability theorem [42, Ch. 4], $e_i \to \mathbf{0}$ as $t \to \infty$ for $i = 1, \ldots, N$. This means that response network (14) synchronizes with drive network (13). ■

In the foregoing, we have proven the synchronization of drive network (1) and response network (3) in the case of H_i given by (12). In the following, we give the synchronization criteria for other types of non-diagonal matrices H_i.

Theorem 4: Suppose $\sigma_i > 0, \beta_i > 0$, for $i = 1, \ldots, N$. Then, response network (3) can synchronize with drive network (1) under the inner-coupling matrices given below

$$i)\ H_i = \begin{pmatrix} 0 & 1 & 0 \\ -1/\sigma_i & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \text{for } i = 1, \ldots, N; \text{ or}$$

$$ii)\ H_i = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix}, \text{for } i = 1, \ldots, N.$$

Proof: This theorem can be proven in a similar way as the proof of Theorem 3, by constructing the Lyapunov function (16). We omit the detailed proof here. ■

Remark 2: Theorems 1–4 provide different coupling patterns (i.e., different H_i) for chaotic oscillators in a drive/response network. A combination of these coupling patterns can be applied in practice. Hence, we have a number of choices for coupling oscillators.

Remark 3: Theorems 1–4 hold for any undirected and weighted connection matrix W. However, we prefer to set edge weights in W to be small (no greater than 0.1), in order to maintain the chaotic dynamics of each oscillator.

Remark 4: Theorems 1–4 hold under the assumption that the nodes of the drive network are the same as those of the response network. An encryption method based on two-layered networks with different structures or sizes certainly will enhance its security. However, analysis of the synchronization becomes more complicated and is still an open and challenging issue.

According to the above described synchronization results, the original message can be recovered correctly at the receiver in the encryption/decryption scheme proposed in Section II.

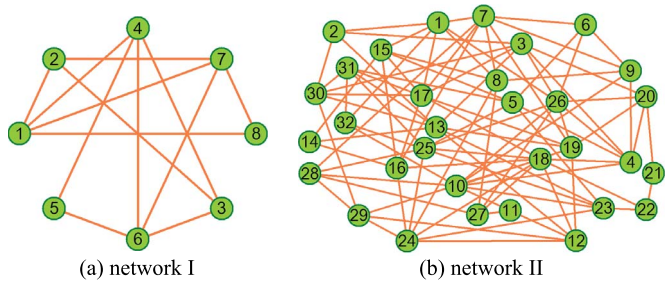
IV. Numerical Results

A. Simulation I

The chaos-generator network has $N = 8$ nodes, whose topological structure is shown in Fig. 3(a). We use Theorem 1 with the inner-coupling matrix $H_i = \text{diag}(1, 0, 0)$ for $i = 1, \ldots, 8$. In the drive and response networks (8) and (9), the system parameters are chosen randomly in the ranges

$$\sigma_i \in [8, 13],\ \mu_i \in [26, 31],\ \beta_i \in [2, 3] \tag{19}$$

for $i = 1, 2, \ldots, N$; and the weights of edges w_{ij} in the interval [0, 0.1] for $i, j = 1, \ldots, N$. The initial conditions of chaos generators are randomly chosen from the interval $[-20, 20]$. The parameters in encryption function (4) are set as $K = 100$, $\lambda = 132$. In this paper, we take the 256×256 pixels image named "Lena" shown in Fig. 6(a) as an example to illustrate the effectiveness of the proposed method. We treat the color "Lena" image as a mixture of the red, green, and blue component images. The gray-scale value of each pixel in the component image is an integer in the interval [0, 255]. Hence, $M = 256$ in (4).



(a) network I (b) network II

Fig. 3. Topological structures of chaos-generator networks. (a) *Network I*: A network of 8 nodes. (b) *Network II*: A network of 32 nodes.

In this simulation, we apply the *MATLAB ode45* function to solve the ordinary differential equations (8) and (9) and to generate chaotic sequences. We set the step size of the *ode45* to be 0.0001. Since the image to be transmitted is represented by discrete signals, we need to sample continuous chaotic sequences $s_i(t)$ and $\hat{s}_i(t)$ in (4) and (6) respectively to obtain discrete chaotic sequences $s_i(\tau_i + kT)$ and $\hat{s}_i(\tau_i + kT)$ for $k = 1, 2, \ldots$, where τ_i is the initial sampling time after (8) and (9) are synchronized, and T is the sampling time. Here, we set $T = 0.01$. We use the ith $(i = 1, \ldots, N)$ chaotic system to encrypt the gray value of the pixel at the yth row and zth column in the original image if

$$i = (z - 1) \bmod N + 1 \tag{20}$$

where $y, z \in [1, 256]$. Then we perform the encryption in (5) and obtain the encrypted sequences $c_i(k)$ for $i = 1, \ldots, N$ and $k = 1, 2, \ldots$. The sequence number k satisfies

$$k = 256(y - 1)/N + \left\lceil \frac{z}{N} \right\rceil \tag{21}$$

where $\lceil z/N \rceil$ is the smallest integer not less than z/N. The two laws (20) and (21) determine an one-to-one relation between the pixel (y, z) of the original image and the sequence order (i, k) of the encrypted message. Since discrete signals are transmitted here, each ciphertext $c_i(k)$ and its corresponding drive signal $x_{i1}(t)$ for $t \in (\tau_i + (k-1)T, \tau_i + kT]$ constitute a package, and then it is transmitted. At the receiver side, the received package is decomposed into $c_i(k)$ and $x_{i1}(t)$. Then, we execute decryptions according to (7) to recover the plaintext of the original image.

Following the above process, we run the simulation in MATLAB and obtain the results described as follows. Fig. 4(a) shows the driving signals $x_{i1}(t)$. Fig. 4(b) shows that the three-dimensional phase portraits of the dynamics $x_i(t)$. Due to space limitation, we only display these curves for nodes $i = 1, 2$ in the chaos generating network. Fig. 4(b) shows the phase portraits are chaotic and random like. The phase portraits can become more complicated resulting from interactions between chaotic oscillators. Let $\|E_1\| = [(\sum_{i=1}^{N} e_{i1}^2)/N]^{1/2}$,

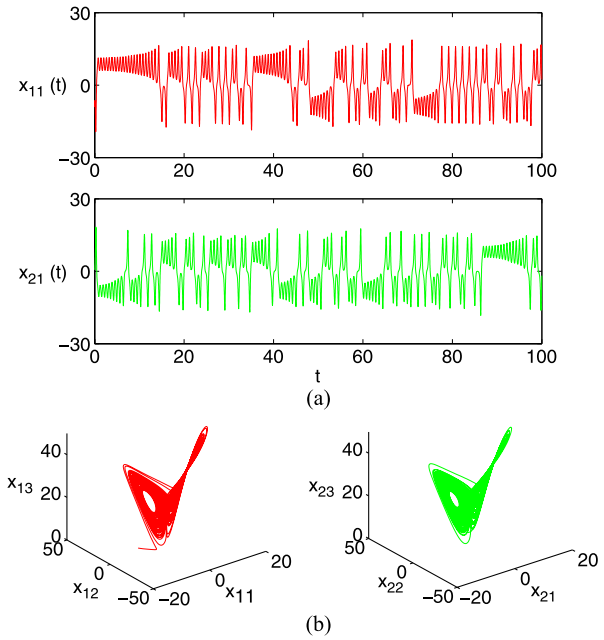


Fig. 4. (a) Drive signals $x_{i1}(t)$, where $i = 1, 2$. (b) Three-dimensional phase portraits of $x_i(t)$ for nodes $i = 1, 2$ in *network I*.

$\|E_2\| = [(\sum_{i=1}^{N} e_{i2}^2)/N]^{1/2}$, and $\|E_3\| = [(\sum_{i=1}^{N} e_{i3}^2)/N]^{1/2}$. We define

$$\|E\| = \left[\frac{(\|E_1\|^2 + \|E_2\|^2 + \|E_3\|^2)}{3}\right]^{\frac{1}{2}}. \tag{22}$$

Fig. 5(a) shows the state differences between drive network (8) and response network (9) over time. From Fig. 5(a), one can see that (8) and (9) synchronize quickly. We consider that systems (8) and (9) are synchronized when the average of the state differences $\|E\|$ is less than 10^{-6}. From Fig. 5(b), one can see that the synchronization time is 9.976. Hence, we set the start of the sampling time $\tau_i = 15$ (>9.976) for all i. With the two chaotic sequences $s_i(\tau_i + kT)$ and $\hat{s}_i(\tau_i + kT)$ for $k = 1, 2, \ldots$, we first execute the encryption algorithm given by (5) to encrypt the gray-scale image shown in Fig. 6(a). The encrypted image is obtained as shown in Fig. 6(b), in which the signals look random and do not expose any clue to the original image. Then, we implement the decryption algorithm given by (7) on the scrambled image. The recovered image after decryption is shown in Fig. 6(c), which is the same as the original one. This shows that the proposed encryption method does work.

B. Simulation II

In this simulation we apply Theorem 3 with the inner-coupling matrix H_i given by (12). We choose the chaotic generator network with $N = 32$ nodes, whose topological structure is shown in Fig. 3(b). The structure is a small-world network generated by the Newman-Watts algorithm introduced in [43]: we start with a cycle graph with N vertices, and randomly add edges with probability 0.15 between pairs of disconnected

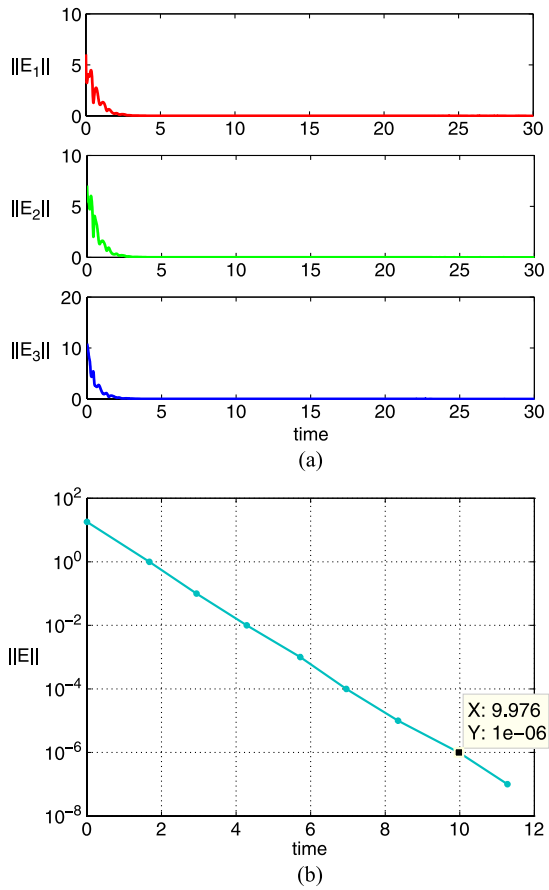


Fig. 5. (a) State differences between drive network (8) and response network (9), measured by $\|E_1\|$, $\|E_2\|$, and $\|E_3\|$ in the three different dimensions of node states. (b) Evolution of $\|E\|$.

Fig. 6. The result of Simulation I. (a) The original image. (b) Encrypted image. (c) Recovered image.

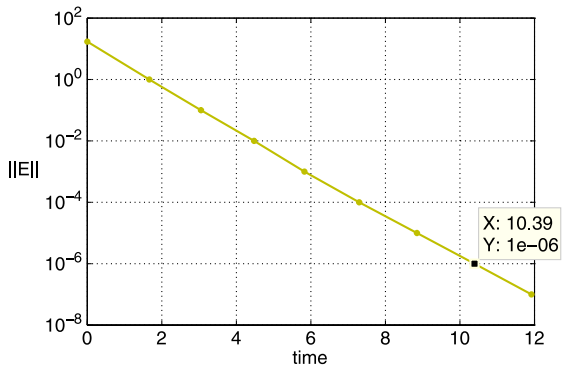


Fig. 7. Evolution of $\|E\|$, which is the average of state differences between drive network (13) and response network (14).

(a) (b)

Fig. 8. The result of Simulation II. (a) The encrypted image. (b) The decrypted one.

nodes. These randomly added edges largely shorten the average distance of the network and make the dynamics of the whole chaos-generator system more complex. We keep other parameter settings the same as those in Simulation I. Then we carry out the simulation. Fig. 7 shows the evolution of $\|E\|$ defined in (22), which measures the average of the state differences between drive network (13) and response network (14). One can see that the two networks synchronize quickly as well. This figure suggests that the synchronization time of the two networks is 10.39, which helps us determine the initial sampling time. We observe that the synchronization time does not increase significantly as the number of network nodes grows. This is a desirable property if adopting complex dynamical networks in the encryption scheme.

Finally, we implement the encryption and decryption algorithms on the image "Lena" shown in Fig. 6(a). The simulation results are shown in Fig. 8, in which subfigures (a) and (b) show the encrypted image and recovered image, respectively. The simulation results illustrate the correctness of Theorem 3 and the feasibility of the proposed encryption scheme.

V. Discussion

We discuss the quality of the proposed scheme from the following five aspects: a) key space, b) sensitivity on parameter mismatch, c) correlation of adjacent pixels, d) gray value distribution of the encrypted image, and e) synchronization time.

A. Key Space

The size of key space is the total number of different keys that can be used in an encryption [44], [45]. A good encryption algorithm is expected to resist exhaustive attack and a large key space is required. The larger the key space size, the more difficult it is for the intruder to gain the correct key[46]–[48].

In our study, the key space is decided by $[\sigma, \mu, \beta, W]$. As mentioned earlier, $8 \le \sigma_i \le 13$, $26 \le \mu_i \le 31$, $2 \le \beta_i \le 3$, and $0 \le W(i,j) \le 0.1$, where $1 \le i, j \le N$. We assume that the precision of the computer is $10^{-\gamma}$, where γ is a positive integer. Then, the key space is given by

$$\Omega = (5 \times 10^{\gamma} \times 5 \times 10^{\gamma} \times 1 \times 10^{\gamma})^{N} \times (10^{\gamma})^{\frac{N(N-1)}{2}}. \quad (23)$$

So we have

$$\begin{cases} \Omega = 1.52 \times 10^{52\gamma} & N = 8 \\ \Omega = 5.42 \times 10^{592\gamma} & N = 32. \end{cases}$$

It is observed that key space increases exponentially with the increase of N. It dramatically enhances the security of the encryption system in terms of resisting brute-force attacks.

B. Sensitivity on Parameter Mismatch

In this subsection, we analyze how K introduced in (4) affects the encryption algorithm's sensitivity on parameter mismatch. If there is a parameter mismatch between the drive and response networks, it will disturb the exact synchronization of the two networks, and thus affects the correctness of image recovery. We analyze the effect from a theoretical viewpoint. According to (4)–(7), the correctness of image recovery depends on the agreement between $X_i(t)$ and $\hat{X}_i(t)$. We estimate the difference between $X_i(t)$ and $\hat{X}_i(t)$ when considering parameter mismatch. From (4) and (6), we obtain $|X_i(t) - \hat{X}_i(t)| \approx K|(x_{i1}^2(t) + x_{i2}^2(t) + x_{i3}^2(t))^{1/2} - (\hat{x}_{i1}^2(t) + \hat{x}_{i2}^2(t) + \hat{x}_{i3}^2(t))^{1/2}| \approx \sqrt{3}K\|E(t)\|$, where $\|E(t)\|$ is the average of state differences and has been defined in (22). Although $|X_i(t) - \hat{X}_i(t)|$ is likely to be different for each i, we roughly estimate this value in an average sense. For a given parameter mismatch, $\|E\|$ at the steady state can be estimated and bounded. From $|X_i - \hat{X}_i| \approx \sqrt{3}K\|E\|$, a larger K makes the proposed encryption algorithm more sensitive to a given parameter mismatch.

First, we try to reveal the trend of $\|E\|$ at the steady state when the magnitude of parameter mismatch changes. Keeping the settings in Simulation II, we consider a mismatch of parameter μ_i for each i changing from 10^{-6} to 10^{0}. Through simulations, we plot Fig. 9(a) to show the trend. From Fig. 9(a), one can see that when the mismatch increases from 10^{-6} to 10^{0}, $\|E\|$ increases from 5.757×10^{-7} to 5.716×10^{-1}.

Second, we estimate a lower bound for K that makes the proposed encryption system sensitive to a given magnitude of the parameter mismatch. In our calculation, we find that $K\|E\| \ge 300$ (i.e., $|X_i - \hat{X}_i| \ge 300\sqrt{3}$) significantly differs the gray values of the decrypted and original pixels, and thus makes the encryption system sensitive to parameter mismatch. Combining the result of Fig. 9(a) and $K\|E\| \ge 300$, we obtain

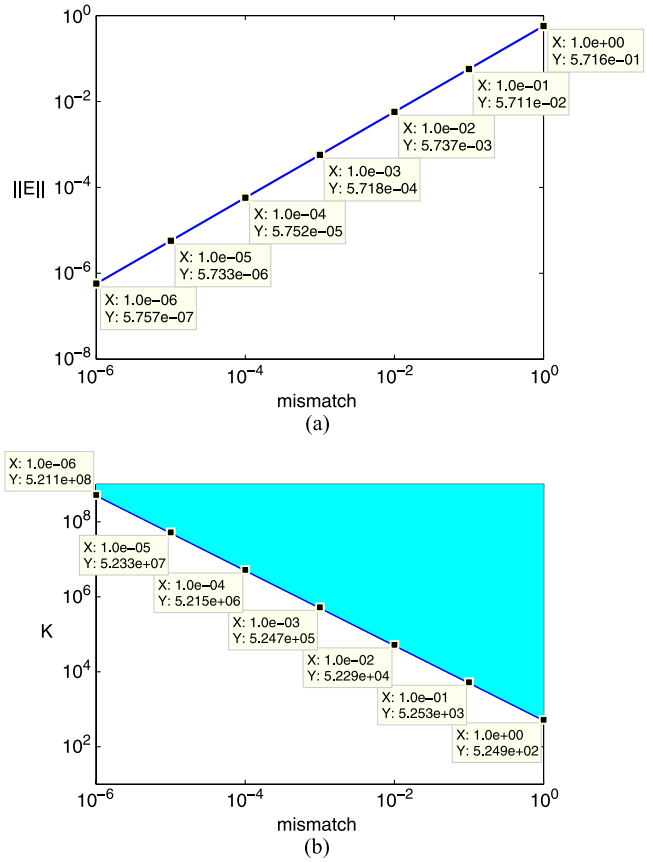


Fig. 9. (a) The trend of $\|E\|$ when the magnitude of parameter mismatch changes from 10^{-6} to 10^{0}. (b) Feasible solutions for K, shown by the upper light-blue area, to make the encryption system sensitive to given parameter mismatches.

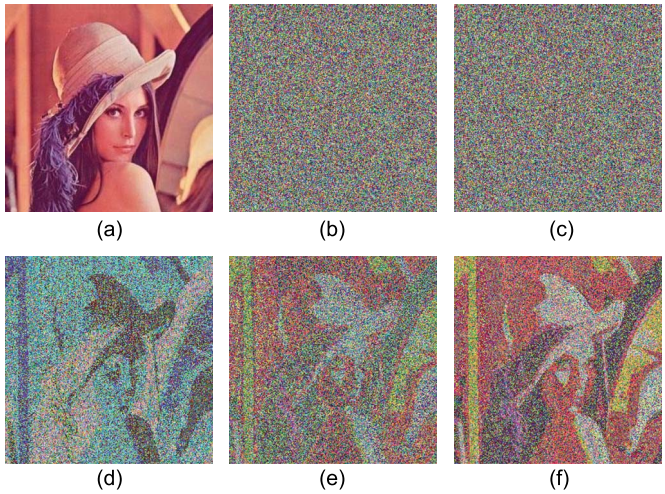


Fig. 10. Decrypted images when the encryption system using *network II*. (a) Decrypted image with right parameters, where $K = 100$. (b)–(f) Decrypted images under different Ks when μ_i has a 10^{-3} mismatch for each i: (b) $K = 2K_0$; (c) $K = K_0$, where $K_0 = 5.247 \times 10^5$; (d) $K = (1/4)K_0$; (e) $K = (1/10)K_0$; (f) $K = (1/16)K_0$.

TABLE II
CORRELATION COEFFICIENTS

		horizontal	vertical	diagonal
original image	red	0.9459	0.9724	0.9218
	green	0.9482	0.9738	0.9257
	blue	0.9005	0.9470	0.8600
encrypted image using *network I*	red	0.0061	0.0021	0.0082
	green	0.0035	0.0038	0.0051
	blue	0.0035	0.0034	0.0035
encrypted image using *network II*	red	0.0008	0.0021	0.0037
	green	0.0045	0.0036	0.0053
	blue	0.0019	0.0043	0.0014

the lower bound for K under each given parameter mismatch, which is shown in Fig. 9(b). The upper light-blue area in Fig. 9(b) shows the feasible solutions for K. Therefore, *one can choose a proper K according to* Fig. 9(b) *in real applications, to satisfy the actual requirement on sensitivity to certain magnitude of parameter mismatch*.

We also carry out a group of encryption simulations in order to check the feasibility of the obtained solution area. We fix the mismatch of μ_i at 10^{-3}. From Fig. 9(b), we know that the encryption system is sensitive to the parameter mismatch if $K \geq K_0 = 5.247 \times 10^5$. Let K vary at $2K_0$, K_0, $K_0/4$, $K_0/10$, and $K_0/16$. We execute the encryption/decryption on the "Lena" image and obtain the decrypted images shown in Fig. 10. One can see that, the decrypted images (b) and (c), in cases $K \geq K_0$, are clearly different from the original one, which means high sensitivity to the mismatch of 10^{-3}; the decrypted images (d)–(f), in cases $K < K_0$, leak information to different extents. The decrease of K reduces the sensitivity to parameter mismatch.

C. Correlation of Adjacent Pixels

Correlation of two adjacent pixels reflects the extent of image scrambling. The smaller the correlation of adjacent pixels of the encrypted image, the better scrambling effect of the encryption algorithm. In this subsection, we analyze the correction between two horizontally adjacent pixels, two vertically adjacent pixels, and two diagonally adjacent pixels in the encrypted image. We randomly choose $m = 20\,000$ pairs adjacent pixels from the image (in the horizontal, vertical, and diagonal direction). We calculate the correlation coefficient of the chosen adjacent pixels using the following formula [44], [48]–[50]:

$$R_{uv} = \frac{|\mathrm{cov}(u,v)|}{\sqrt{D(u)} \times \sqrt{D(v)}} \tag{24}$$

in which

$$\begin{cases} \mathrm{cov}(u,v) = \frac{1}{m}\sum_{i=1}^{m}\left(u_i - E(u)\right)\left(v_i - E(v)\right) \\ E(u) = \frac{1}{m}\sum_{i=1}^{m} u_i, \quad D(u) = \frac{1}{m}\sum_{i=1}^{m}\left(u_i - E(u)\right)^2 \end{cases}$$

where u_i and v_i are the gray values of the ith pair of adjacent pixels that we have chosen; $\mathrm{cov}(\cdot,\cdot)$ represents the covariance function, $E(\cdot)$ the expectation function, and $D(\cdot)$ the covariance function. Table II shows the correlations of adjacent pixels in the original and encrypted images. Each data item obtained in Table II is the average of 20 times of calculation on R_{uv} with the corresponding image and direction.

From Table II, we see that the adjacent pixels of the original image have a high correlation coefficient close to 1, but have

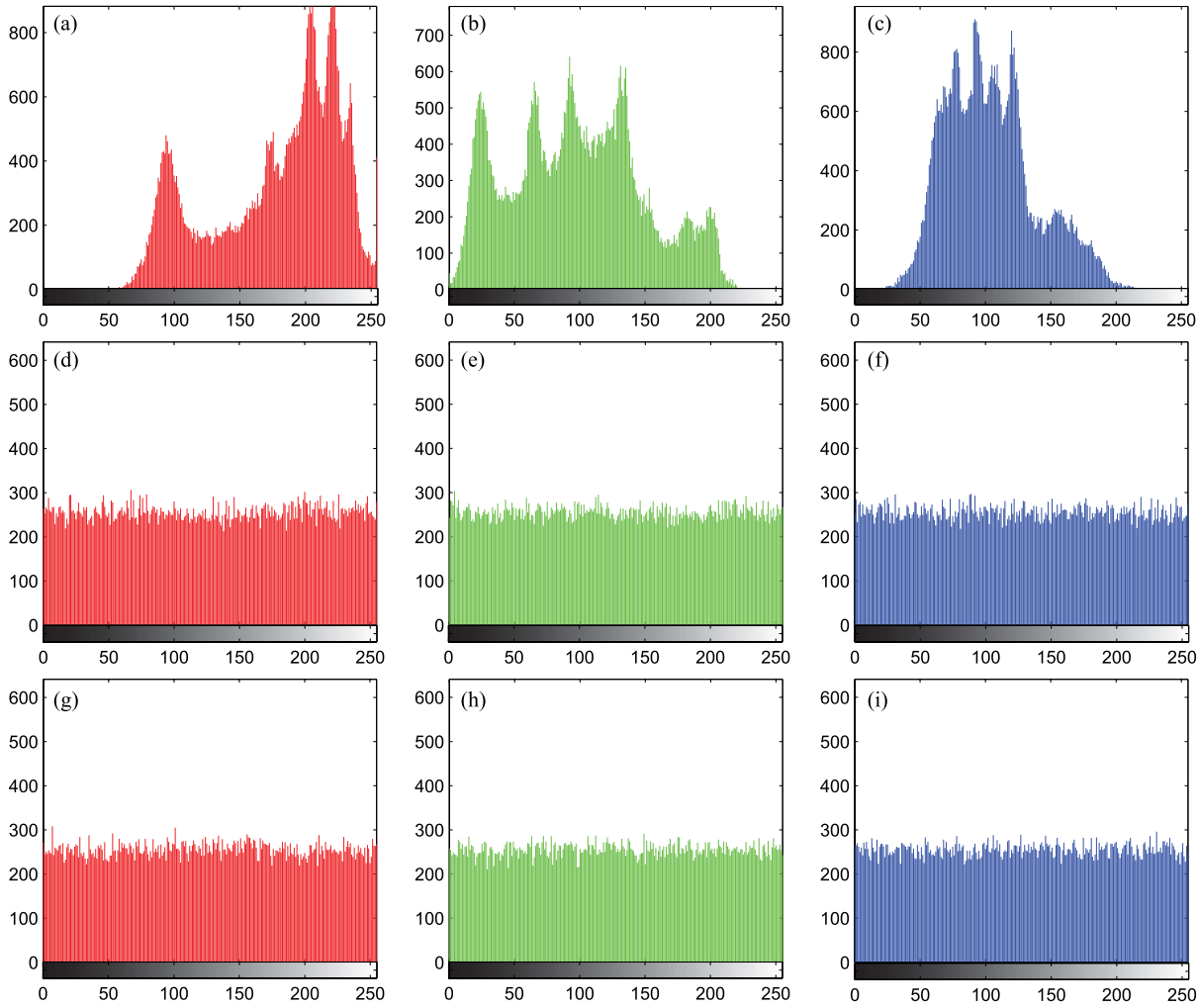


Fig. 11. Histograms of images in the red, green, and blue components. (a)–(c) Original image; (d)–(f) Encrypted image using *network I*; (g)–(i) Encrypted image using *network II*.

a very low correlation coefficient nearly 0 after the image is encrypted. So it is difficult to crack the encrypted images from statistical correlation analysis.

D. Gray Value Distribution of the Encrypted Image

A histogram of an image is the frequency statistics of the gray levels. Histogram analysis reflects the statistical characteristics of the image [48]–[50]. Intruders may attack the encrypted image by histogram analysis. A good encryption strategy should make the gray level distribution uniform. Fig. 11 shows the histograms of the original and encrypted images. In each subfigure, the x-coordinate represents the gray level of nodes in a given image; the y-coordinate represents correspondingly the number of the nodes in the image with certain gray level. From Fig. 11, we can see that the histograms of the original and encrypted images differ significantly. Both of the two encrypted histograms using *networks I* and *II* are almost uniformly distributed, and the regularity of the distribution of the original image is concealed. Therefore, it is difficult to crack the encrypted images using histogram analysis.

E. Synchronization Time of Drive and Response Networks

Synchronization is an important problem in the proposed encryption scheme, and synchronization time of drive and response networks will influence the efficiency of implementing the method. The image can only be transmitted after the drive and response networks have synchronized. In order to observe the synchronization time, we show the state differences between the drive and response networks over time in Fig. 12. We can see that synchronization times of the networks with 8 nodes, 32 nodes, 64 nodes have no significant difference, and is slightly longer than the case of 1 node. Thus, when we increase the number of nodes in the networks, the synchronization time remains unaffected. This is partially because when more nodes are added in the drive network, more drive signals are loaded to the response network correspondingly; thus, more drive signals can make the node-to-node synchronization in a two-layered dynamical network easier to achieve.

VI. Conclusion

In this paper, we have proposed a novel encryption scheme using a complex dynamical network. Compared with existing

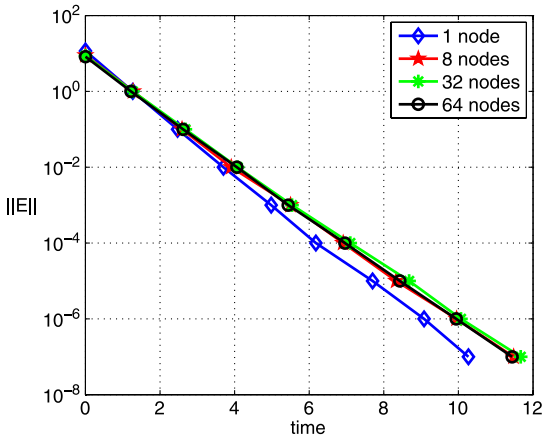


Fig. 12. State differences between drive and response networks, measured by $\|E\|$. Designations are as Fig. 7. Blue, red, green, and black lines represent the drive/response network with 1, 8, 32, 64 nodes, respectively.

similar schemes that were designed based on a single chaotic system, the proposed scheme has higher security and can achieve higher encryption speed. This makes the scheme a better candidate for real-time image encryption and transmission applications. Our encryption scheme enlarges key space exponentially with respect to the number of nodes in the network. Simulation results show that the proposed scheme achieves satisfactory performance, in terms of sensitivity, statistical characteristics, and synchronization time. Both numerical simulations and analysis have demonstrated the feasibility of the proposed scheme.

As our future work, we are interested in more applications of complex chaotic networks to secure encryption. We will also consider imperfect communications when applying encryption algorithms in practice. To date, some methods have been developed to alleviate the negative effects caused by imperfect communications. For example, the effect of data loss can be greatly reduced by scrambling image pixels before the encryption process [51], [52]. Channel noise can also be overcome by introducing generalized synchronization of chaos systems into secure communication [20], by designing robust controller [6], or by using the differential chaos shift keying (DCSK) approach [12]. These methods will be helpful to our next work. We hope that encryption schemes based on complex chaotic networks would become a competing technology for encryption systems for large-data-amount tasks in future.

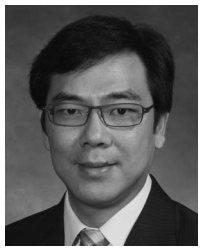
REFERENCES

[1] N. Hoffman, "A simplified IDEA algorithm," *Cryptologia*, vol. 31, no. 2, pp. 143–151, 2007.
[2] R. R. Rachh, P. A. Mohan, and B. S. Anami, "Efficient implementations for AES encryption and decryption," *Circuits, Syst., Signal Process.*, vol. 31, no. 5, pp. 1765–1785, 2012.
[3] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, 1978.
[4] F.-Y. Yang, J.-H. Lo, and C.-M. Liao, "Improving an efficient ID-based RSA multisignature," *J. Ambient Intell. Humanized Comput.*, vol. 4, no. 2, pp. 249–254, 2013.
[5] R. Kumar, H. K. Verma, and R. Dhir, "Cryptanalysis and performance evaluation of enhanced threshold proxy signature scheme based on RSA for known signers," *Math. Prob. Eng.*, vol. 2013, 2013.
[6] C.-J. Cheng, "Robust synchronization of uncertain unified chaotic systems subject to noise and its application to secure communication," *Appl. Math. Comput.*, vol. 219, no. 5, pp. 2698–2712, 2012.
[7] K. Cuomo, A. Oppenheim, and S. H. Strogatz, "Synchronization of Lorenz-based chaotic circuits with applications to communications," *IEEE Trans. Circuits Syst. II, Analog Digit. Signal Process.*, vol. 40, no. 10, pp. 626–633, 1993.
[8] T. Yang and L. O. Chua, "Impulsive stabilization for control and synchronization of chaotic systems: Theory and application to secure communication," *IEEE Trans. Circuits Syst. I, Fundam. Theory Appl.*, vol. 44, no. 10, pp. 976–988, 1997.
[9] Z. He, K. Li, L. Yang, and Y. Shi, "A robust digital secure communication scheme based on sporadic coupling chaos synchronization," *IEEE Trans. Circuits Syst. I, Fundam. Theory Appl.*, vol. 47, no. 3, pp. 397–403, 2000.
[10] K. Li, M. Zhao, and X. Fu, "Projective synchronization of driving-response systems and its application to secure communication," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 56, no. 10, pp. 2280–2291, 2009.
[11] Z. Jiang, "A note on chaotic secure communication systems," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 49, no. 1, pp. 92–96, 2002.
[12] F. C. Lau and C. K. Tse, *Chaos-Based Digital Communication Systems*, New York: Springer, 2003.
[13] B. Jovic, *Synchronization Techniques for Chaotic Communication Systems*. New York, NY, USA: Springer Science & Business Media, 2011.
[14] Z. Lin, S. Yu, J. Lü, S. Cai, and G. Chen, "Design and ARM-embedded implementation of a chaotic map-based real-time secure video communication system," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 25, no. 7, pp. 1203–1216, 2015.
[15] C. K. Volos, I. M. Kyprianidis, and I. N. Stouboulos, "Image encryption process based on chaotic synchronization phenomena," *Signal Process.*, vol. 93, no. 5, pp. 1328–1340, 2013.
[16] J.-A. Lu, X. Wu, and J. Lü, "Synchronization of a unified chaotic system and the application in secure communication," *Phys. Lett. A*, vol. 305, no. 6, pp. 365–370, 2002.
[17] Z. Li, K. Li, C. Wen, and Y. C. Soh, "A new chaotic secure communication system," *IEEE Trans. Commun.*, vol. 51, no. 8, pp. 1306–1312, 2003.
[18] G. Alvarez, L. Hernández, J. Muñoz, F. Montoya, and S. Li, "Security analysis of communication system based on the synchronization of different order chaotic systems," *Phys. Lett. A*, vol. 345, no. 4, pp. 245–250, 2005.
[19] S.-I. Huang, S. Shieh, and J. Tygar, "Secure encrypted-data aggregation for wireless sensor networks," *Wireless Netw.*, vol. 16, no. 4, pp. 915–927, 2010.
[20] O. I. Moskalenko, A. A. Koronovskii, and A. E. Hramov, "Generalized synchronization of chaos for secure communication: Remarkable stability to noise," *Phys. Lett. A*, vol. 374, no. 29, pp. 2925–2931, 2010.
[21] M. Cheng, L. Deng, X. Gao, H. Li, M. Tang, S. Fu, P. Shum, and D. Liu, "Security-enhanced OFDM-PON using hybrid chaotic system," *IEEE Photon. Technol. Lett.*, vol. 27, no. 3, pp. 326–329, 2015.
[22] Q. Wang, S. Yu, C. Li, J. Lü, X. Fang, C. Guyeux, and J. M. Bahi, "Theoretical design and FPGA-based implementation of higher-dimensional digital chaotic systems," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 63, no. 2, pp. 401–412, 2016.
[23] R. F. I. Cancho, C. Janssen, and R. V. Solé, "Topology of technology graphs: Small world patterns in electronic circuits," *Phys. Rev. E*, vol. 64, no. 4, 2001, Art. no. 046119.
[24] C. W. Wu, "Evolution and dynamics of complex networks of coupled systems," *IEEE Circuits Syst. Mag.*, vol. 10, no. 3, pp. 55–63, 2010.
[25] P. DeLellis, M. di Bernardo, and F. Garofalo, "Adaptive pinning control of networks of circuits and systems in Lur'e form," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 60, no. 11, pp. 3033–3042, 2013.
[26] H. Liu, M. Cao, and C. W. Wu, "Coupling strength allocation for synchronization in complex networks using spectral graph theory," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 61, no. 5, pp. 1520–1530, 2014.
[27] H. Liu, M. Cao, C. W. Wu, J.-A. Lu, and C. K. Tse, "Synchronization in directed complex networks using graph comparison tools," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 62, no. 4, pp. 1185–1194, 2015.
[28] Y. Zhao, G. Wen, Z. Duan, and G. Chen, "Adaptive consensus for multiple nonidentical matching nonlinear systems: An edge-based framework," *IEEE Trans. Circuits Syst. II, Express Briefs*, vol. 62, no. 1, pp. 85–89, 2015.
[29] X. Wang and G. Chen, "Complex networks: Small-world, scale-free and beyond," *IEEE Circuits Syst. Mag.*, vol. 3, no. 1, pp. 6–20, 2003.
[30] H. Liu, J.-A. Lu, J. Lü, and D. J. Hill, "Structure identification of uncertain general complex dynamical networks with time delay," *Automatica*, vol. 45, no. 8, pp. 1799–1807, 2009.
[31] W. Yang, Z.-G. Huang, X. Wang, L. Huang, L. Yang, and Y.-C. Lai, "Complex behavior of chaotic synchronization under dual coupling channels," *New J. Phys.*, vol. 17, no. 2, p. 023055, 2015.

[32] J. Aguirre, R. Sevilla-Escoboza, R. Gutiérrez, D. Papo, and J. Buldú, "Synchronization of interconnected networks: The role of connector nodes," *Phys. Rev. Lett.*, vol. 112, no. 24, p. 248701, 2014.
[33] R. Lu, W. Yu, J. Lü, and A. Xue, "Synchronization on complex networks of networks," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 25, no. 11, pp. 2110–2118, 2014.
[34] Y. Li, X. Wu, J.-A. Lu, and J. Lü, "Synchronizability of duplex networks," *IEEE Trans. Circuits Syst. II, Express Briefs*, vol. 63, no. 2, pp. 206–210, 2016.
[35] S. Gómez, A. Díaz-Guilera, J. Gómez-Gardeñes, C. J. Perez-Vicente, Y. Moreno, and A. Arenas, "Diffusion dynamics on multiplex networks," *Phys. Rev. Lett.*, vol. 110, no. 2, p. 028701, 2013.
[36] G. Wen, W. Yu, J. Wang, D. Xu, and J. Cao, "Distributed node-to-node consensus of multi-agent systems with time-varying pinning links," *Neurocomputing*, vol. 149, pp. 1387–1395, 2015.
[37] Y. Wan, G. Wen, J. Cao, and W. Yu, "Distributed node-to-node consensus of multi-agent systems with stochastic sampling," *Int. J. Robust Nonlinear Control*, vol. 26, no. 1, pp. 110–124, 2016.
[38] L. M. Pecora and T. L. Carroll, "Synchronization in chaotic systems," *Phys. Rev. Lett.*, vol. 64, no. 8, p. 821, 1990.
[39] L. M. Pecora and T. L. Carroll, "Driving systems with chaotic signals," *Phys. Rev. A*, vol. 44, no. 4, p. 2374, 1991.
[40] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, 1949.
[41] K. M. Cuomo, "Analysis and synthesis of self-synchronizing chaotic systems," Ph.D. dissertation, Research Laboratory of Electronics, Massachusetts Inst. Technol., Cambridge, MA, USA, 1994.
[42] H. K. Khalil, *Nonlinear Systems*, 3rd ed. Upper Saddle River, NJ, USA: Pearson Educ., 2002.
[43] M. E. Newman and D. J. Watts, "Renormalization group analysis of the small-world network model," *Phys. Lett. A*, vol. 263, no. 4, pp. 341–346, 1999.
[44] S. M. Seyedzadeh and S. Mirzakuchaki, "A fast color image encryption algorithm based on coupled two-dimensional piecewise chaotic map," *Signal Process.*, vol. 92, no. 5, pp. 1202–1215, 2012.
[45] Y. Zhou, L. Bao, and C. P. Chen, "Image encryption using a new parametric switching chaotic system," *Signal Process.*, vol. 93, no. 11, pp. 3039–3052, 2013.
[46] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *Int. J. Bifurcation Chaos*, vol. 16, no. 8, pp. 2129–2151, 2006.
[47] S. Li, G. Álvarez, G. Chen, and X. Mou, "Breaking a chaos-noise-based secure communication scheme," *Chaos*, vol. 15, no. 1, 2005, Art. no. 013703.
[48] N. Bigdeli, Y. Farid, and K. Afshar, "A novel image encryption/decryption scheme based on chaotic neural networks," *Eng. Appl. Artif. Intell.*, vol. 25, no. 4, pp. 753–765, 2012.
[49] Y. Mao, G. Chen, and S. Lian, "A novel fast image encryption scheme based on 3D chaotic baker maps," *Int. J. Bifurcation Chaos*, vol. 14, no. 10, pp. 3613–3624, 2004.
[50] W. Zhang, K.-W. Wong, H. Yu, and Z.-L. Zhu, "An image encryption scheme using lightweight bit-level confusion and cascade cross circular diffusion," *Opt. Commun.*, vol. 285, no. 9, pp. 2343–2354, 2012.
[51] C. Dong, "Color image encryption using one-time keys and coupled chaotic systems," *Signal Process., Image Commun.*, vol. 29, no. 5, pp. 628–640, 2014.
[52] H.-I. Hsiao and J. Lee, "Color image encryption using chaotic nonlinear adaptive filter," *Signal Process.*, vol. 117, pp. 281–309, 2015.

Hui Liu (S'11–M'14) received the B.S. and Ph.D. degrees in computational mathematics from Wuhan University, China, in 2005 and 2010, respectively, and the Ph.D. degree in systems and control from the University of Groningen, The Netherlands, in 2013. She is currently an associate professor with the School of Automation, Huazhong University of Science and Technology, Wuhan, China. She held visiting positions with the Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing, and with the Department of Electronic and Information Engineering, the Hong Kong Polytechnic University, Hong Kong. Her main research interests are in complex networks, cooperative control of networked systems, nonlinear control systems, and graph theory.

Haibo Wan received the B.Eng. degree in the School of Electrical and Information Engineering, Anhui University of Technology, Anhui, China, in 2014. He is currently working toward the M.S. degree in the School of Automation, Huazhong University of Science and Technology, Wuhan, China. His research interests are in complex networks and chaotic systems.



Chi K. Tse (M'90–SM'97–F'06) received the B.Eng. (Hons.) degree with first class honors in electrical engineering and the Ph.D. degree from the University of Melbourne, Australia, in 1987 and 1991, respectively.

He is presently Chair Professor at the Hong Kong Polytechnic University, Hong Kong, with which he served as Head of the Department of Electronic and Information Engineering from 2005 to 2012. He is author/coauthor of 10 books, 20 book chapters, and over 500 papers in research journals and conference proceedings, and holds 5 U.S. patents. He was awarded a number of research and industry awards, including Best Paper Award by IEEE TRANSACTIONS ON POWER ELECTRONICS in 2001, Best Paper Award by *International Journal of Circuit Theory and Applications* in 2003, two Gold Medals at the International Inventions Exhibition in Geneva in 2009 and 2013, and a number of recognitions by the academic and research communities, including honorary professorship by several Chinese and Australian universities, Chang Jiang Scholar Chair Professorship, IEEE Distinguished Lectureship, Distinguished Research Fellowship by the University of Calgary, Gledden Fellowship, and International Distinguished Professorship-at-Large by the University of Western Australia.

Dr. Tse serves and has served as Editor-in-Chief for the IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS—PART II (2016–2017), *IEEE Circuits and Systems Magazine* (2012–2015), Editor-in-Chief of *IEEE Circuits and Systems Society Newsletter* (since 2007), Associate Editor for three IEEE Journal/Transactions, Editor for *International Journal of Circuit Theory and Applications*, and is on the editorial boards of a few other journals. He also serves as panel member of Hong Kong Research Grants Council and NSFC, and member of several professional and government committees.

Jinhu Lü (M'03–SM'06–F'13) received the Ph.D. degree in applied mathematics from the Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing, China, in 2002. Currently, he is a Professor in the Academy of Mathematics and Systems Science, Chinese Academy of Sciences. He was a Professor in RMIT University, Australia, and a Visiting Fellow in Princeton University, Princeton, NJ, USA. He is the author of four books and more than 150 SCI journal papers published in the fields of complex networks, nonlinear circuits and systems, receiving more than 10 000 SCI citations with h-index 47. He is an ISI Highly Cited Researcher in Engineering (2014, 2015).

Prof. Lü served and is serving as a member of the Fellows Evaluating Committee of IEEE Circuits and Systems Society and IEEE Computational Intelligence Society. He served and is serving as Editors in various ranks for 14 SCI journals including 6 IEEE Transactions: IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS—PART I: REGULAR PAPERS, IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS—PART II: EXPRESS BRIEFS, IEEE TRANSACTIONS ON BIOMEDICAL CIRCUITS AND SYSTEMS, IEEE TRANSACTIONS ON NEURAL NETWORKS AND LEARNING SYSTEMS, IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS. He received the prestigious State Natural Science Award twice from the Chinese government in 2008 and 2012, respectively; the Australian Research Council Future Fellowships in 2009; and the Science and Technology Progress Award of Ho Leung Ho Lee Foundation in 2015. He is a Chief Scientist of National Key Research and Development Program of China and a Leading Scientist of Innovative Research Groups of National Natural Science Foundation of China.