RESEARCH **Open Access**

CrossMark

Adaptive coupled synchronization among three coupled chaos systems and its application to secure communications

Jiangang Zhang[1*], Li Zhang[2], Xinlei An[1], Hongwei Luo[1,3] and Kutorzi Edwin Yao[1]

Abstract

In this paper, the adaptive synchronization method of three coupled identical chaos systems is proposed. New generic criteria of global chaos synchronization and strict theoretical proofs are given. The unidirectional (bidirectional) coupled system will synchronize by adding three adaptive feedback gain equations. As an example, the three Rössler chaotic systems with unidirectional coupling are given to realize the adaptive coupled synchronization; at the same time, the three Lorenz chaotic systems donate the bidirectional coupling adaptive synchronization. This paper also extends the above adaptive synchronization method to secure chaos communications through the method of chaos masking. Based on the three coupled identical Lorenz chaotic systems, a novel method of chaos encryption is proposed, and the basic idea is that after encrypting two times in two transmitters and one receiver, information signal can be recovered exactly at the receiver end. In consideration of interfering random white noise, the results of encoding and decoding are simulated and analyzed for the multistage chaos synchronized system. By analyzing the characteristics of noise, this paper presents a de-noising method using wavelet transform. At last, a secure communications method for high amplitude information signal transmission based on chaotic masking is studied. With the MATLAB, the effects of signal de-noising could be demonstrated.

Keywords: Coupled synchronization, Secure communication, Chaos encryption, Signal de-noising, Wavelet transform

1 Introduction

In recent years, the idea of synchronization of chaotic systems has received a great deal of interest among scientists from various fields [1–8]. In their seminal paper, Pecora and Carroll addressed the synchronization of chaotic system by using a drive-response configuration. The basic idea is to use the outputs of the drive system to control the response system so that the trajectories of the response's outputs can synchronize those of drive system. So far, many synchronization schemes have been developed such as adaptive synchronization approach [9, 10], system approach [11], and system decomposition approach [12]. More recently, many useful methods have been developed. We have also investigated chaos synchronization

between two coupled identical systems, from a rigorous mathematical approach.

However, for three coupled (even more) identical systems, the stability of periodic orbit and chaos synchronization are much more complex, and there does not seem to be much result reported in the literatures about this special synchronization configuration [13–16]. In the recent work, the authors propose the simple generic criteria for realizing the chaos synchronization respectively according to the way of coupling. The generic criteria can be satisfied by choosing nine suitable coupled coefficients of three coupled chaotic systems. In the paper of Lu [17], the adaptive synchronization method for coupled system with multi-systems is proposed; this method can avoid estimating too many values of coupling coefficient by adding some adaptive feedback gain equations. In this paper, we improve the adaptive synchronization method of the paper and establish the global synchronization criteria for three coupled chaotic

* Correspondence: jiangangzhangjwcn@163.com; zhangjg114502@gmail.com
[1]School of Mathematics and Physics, Lanzhou Jiaotong University, Lanzhou 730070, China
Full list of author information is available at the end of the article

Zhang *et al. EURASIP Journal on Wireless Communications and Networking* (2016) 2016:134

Page 2 of 15

systems via unidirectional or bidirectional linear error feedback approach. In this method, the adaptive feedback gain equations are replaced with the values of coupling co-efficients. This method can avoid the difficulty of designing the adaptive feedback gain equations. At the same time, it needs estimate fewer coupling coefficients than the method in the paper [18].

Over the past decades, there has been tremendous interest in studying the behavior of chaotic system. Chaotic systems are characterized by a number of features, such as sensitive dependence on initial conditions; aperiodicity, random-like behavior, continuous broadband power spectrum, and so on. These properties coincide with the requirements for signals applied in secure communication systems. A large variety of encryption algorithms have been proposed for realizing chaotic communication since Pecora and Carroll proposed synchronization of chaotic systems. Up to now, many chaos-based secure communication systems have been proposed, which can be roughly classified into the following categories: chaotic masking (addition method) [19], chaotic switching [20], chaotic modulation (inclusion method) [21], digital communication [22], and inverse system approach [23]. One can refer to [24] for a recent survey. In chaotic communication schemes, a chaotic system is used as transmitter and the information signal is mixed at the transmitter end to generate a chaotic transmit signal, which is then transmitted to the receiver end. The receiver is also a chaotic dynamic system constructed based on the structure of transmitter and it is able to synchronize the transmitter by receiving the transmit signal. Once synchronization is achieved, the information signal is recovered by the receiver. The main idea is that chaotic signal can be used as a carrier and transmitted together with an information signal to a receiver, and at the receiver end chaos synchronization is employed to recover the information signal. There is a problem on how to improve the security of the chaos secure system. Until now, most of the literatures are all about second order of chaos synchronized secure communication system [25–32], and only a few papers investigate the multistage chaos synchronized secure communication system [33, 34].

There are many methods [35–39] to improve the security of chaotic communication. In [40], a linear output feedback synchronization approach for chaotic Genesio system with application to secure communications is described. The sufficient condition of stable asymptotic synchronization and the boundary of feedback gain are given, based on the linear stability theorem. In [41], Chua's chaotic synchronized systems and its main properties are investigated and a multistage chaotic synchronized systems for secure communication is proposed. It

is down that the message signal hidden in chaotic carrier of the systems can be perfectly reconstructed, and the bandwidth, the characteristic of distortion, and the level of security are improved. The chaos masking method based on multistage chaotic synchronization system for secure communications, to some extent, enhances the degree of security, as the message is not only just added to the chaotic carrier signal twice but is also decrypted twice. For example, in [42], a new method of global chaos synchronization among three different structures of chaotic systems is proposed under the framework of drive-response systems based on Lyapunov stabilization theorem; then, this method is applied to secure communication through chaotic masking. At last, it analyzes the characteristics of noise and then presents a de-noising method using wavelet transform. With the MATLAB, the effects of signal de-noising could be demonstrated.

This work, inspired by previous works, improves the security of the chaos secure system by adding the second order of chaos synchronized secure communication system to multistage ones, that is, it proposes a novel method of chaos encryption using three coupled identical systems. After encrypting in the first two coupled systems, encryption is done again in the later two coupled systems. This system designs simpler than the ones designed in [43, 44] and can employ more states easily. More significantly, this method can be extended to four or even more order chaos synchronized secure communication system. Due to the uniqueness of the three coupled chaos synchronization secure communication system, the possibility for an interceptor to extract the information from the transmitted signal is therefore greatly reduced.

Considering the noise in existence in the chaotic systems, we study the random white noise perturbing for the signal. In addition, eliminate the noise using wavelet transform. In order to maintain synchronization between the transmitter and receiver, the ratio of the power of the chaotic carrier to the information signal should be greater than approximately 30 dB to guarantee a fairly small distortion on the chaotic attractor. In [45, 46], Li proposes a secure communication method for high-amplitude information signal transmission based on chaotic masking. The degree of security is enhanced because the amplitude of information signal is equivalent to that of chaotic signal. At the receiving end, an adaline is adopted to maintain the chaotic synchronization of transmitting and receiving systems and simultaneously recovers the information signal. For a definite chaos system, the lower the frequency of information signal, the smaller the error of the recovered signal and original signal. Besides, Chua's circuit is considered as an illustrative example to demonstrate the effectiveness of the

Zhang et al. EURASIP Journal on Wireless Communications and Networking (2016) 2016:134

Page 3 of 15

proposed method. This paper improves the above method, designs an adaptive controller by using two attenuation factor, and adjusts the amplitude significantly. As the change of attenuation factor, the information signal can be selected within a relatively big range. Recently, Xu et al. [47–49] proposed a crowdsensing-based wireless communication data processing methods. In [50], Zheng deals with the problem of secure communication based on multi-input multi-output (MIMO) chaotic systems. Moreover, since the amplitude of messages in traditional schemes is limited because it would affect the quality of synchronization, the proposed scheme is also improved into an amplitude-independent one. This paper improves the method in [51] and transmits a high-amplitude discrete signal using two attenuation factors. At the receiving end, it restores the information signal by decrypting twice. Well effect has been acquired in the experiment.

This paper is organized as follows. In Section 2, we show the adaptive synchronization of three Rössler systems with unidirectional coupling. In Section 3, adaptive synchronization of three Lorenz systems with bidirectional coupling is discussed. In Section 4, the secure communication theory and multistage chaos synchronized system for secure communications are shown. The noise resistance effects for the transmitter of a signals and wavelet de-noise are shown in Section 5. In Section 6, we show the transmission of a high-amplitude discrete signal. Finally, conclusions are drawn.

2 Adaptive synchronization of three Rössler systems with unidirectional coupling

With respect to two coupled chaotic systems, by unidirectional coupling we mean that the behavior of response system is dependent on the behavior of another identical drive system, but the second one is not influenced by the behavior of the first. But the situation is very different to consider the synchronization of three chaotic systems with unidirectional coupling.

Consider the classical Rössler chaotic system

$$\begin{cases} \dot{x}_1 = -(x_2 + x_3) \\ \dot{x}_2 = x_1 + ax_2 \\ \dot{x}_3 = x_3(x_1-c) + b \end{cases}$$

where $x_i\,(i = 1, 2, 3)$ are the state variables and a, b, c are positive real constants, where $a = 0.2$, $b = 0.2$, and $c = 5.7$, so that the Rössler system has chaotic attractors. Here, we consider the unidirectional coupling among three identical Rössler chaotic systems

$$\begin{cases} \dot{x}_1 = -(x_2 + x_3)-d_1(x_1-y_1) \\ \dot{x}_2 = x_1 + ax_2 \\ \dot{x}_3 = x_3(x_1-c) + b \\ \dot{y}_1 = -(y_2 + y_3)-d_2(y_1-z_1) \\ \dot{y}_2 = y_1 + ay_2 \\ \dot{y}_3 = y_3(y_1-c) + b \\ \dot{z}_1 = -(z_2 + z_3)-d_3(z_1-x_1) \\ \dot{z}_2 = z_1 + az_2 \\ \dot{z}_3 = z_3(z_1-c) + b \end{cases} \quad (1)$$

Selecting the synchronization errors as follows:

$$\begin{aligned} &e_{11}(t) = x_1(t)-y_1(t), \; e_{21}(t) = y_1(t)-z_1(t), \; e_{31}(t) = z_1(t)-x_1(t) \\ &e_{12}(t) = x_2(t)-y_2(t), \; e_{22}(t) = y_2(t)-z_2(t), \; e_{32}(t) = z_2(t)-x_2(t) \\ &e_{13}(t) = x_3(t)-y_3(t), \; e_{23}(t) = y_3(t)-z_3(t), \; e_{33}(t) = z_3(t)-x_3(t) \end{aligned} \quad (2)$$

And we have $e_{31} = - e_{11} - e_{21}$, $e_{32} = - e_{12} - e_{22}$, $e_{33} = - e_{13} - e_{23}$.

Assuming that

$$\dot{d}_1 = k_1 e_{11}^2, \; \dot{d}_2 = k_2\left(e_{21}^2-e_{11}e_{21}\right), \; \dot{d}_3 = k_3\left(e_{21}^2 + e_{11}e_{21}\right).$$
$$k_1, k_2, k_3 > 0, \quad (3)$$

According to formulas (2) and (3), the dynamical error system is written as follows:

$$\begin{cases} \dot{e}_{11} = -e_{12}-e_{13}-d_1e_{11} + d_2e_{21} \\ \dot{e}_{12} = e_{11} + ae_{12} \\ \dot{e}_{13} = x_1e_{13} + y_3e_{11}-ce_{13} \\ \dot{e}_{21} = -e_{22}-e_{23}-d_2e_{21}-d_3e_{11}-d_3e_{21} \\ \dot{e}_{22} = e_{21} + ae_{22} \\ \dot{e}_{23} = y_1e_{23} + z_3e_{21}-ce_{23} \end{cases} \quad (4)$$

2.1 Theorem 1

The coupled system (1) will synchronize for any initial values $(x_1(0), x_2(0), x_3(0))$; $(y_1(0), y_2(0), y_3(0))$; $(z_1(0), z_2(0), z_3(0))$; $d_1(0)$; $d_2(0)$; $d_3(0)$. That is, $e_{ij} \to 0$ as $t \to \infty$, $(i, j = 1, 2, 3)$.

2.2 Proof

We construct a Lyapunov function

$$V = \frac{1}{2}\left[e_{11}^2 + e_{12}^2 + e_{13}^2 + e_{21}^2 + e_{22}^2 + e_{23}^2 + \frac{1}{k_1}\left(d_1-d_1^*\right)^2 \right. $$
$$\left. + \frac{1}{k_2}\left(d_2-d_2^*\right)^2 + \frac{1}{k_3}\left(d_3-d_3^*\right)^2\right]$$

where $d_1^*, d_2^*, d_3^* > 0$ are to be determined. Since the Rössler system is chaotic, we assume $|x_1|, |y_1| \le M_1$, $|y_3|, |z_3| \le M_3$, where M_1, M_3 are positive constants. The time derivative of V along the orbits of the system (1) is

Zhang et al. EURASIP Journal on Wireless Communications and Networking (2016) 2016:134

Page 4 of 15

$$
\begin{aligned}
\dot{V} &= e_{11}\dot{e}_{11} + e_{12}\dot{e}_{12} + e_{13}\dot{e}_{13} + e_{21}\dot{e}_{21} + e_{22}\dot{e}_{22} + e_{23}\dot{e}_{23} + \frac{1}{k_1}(d_1-d_1^*)\dot{d}_1 + \frac{1}{k_2}(d_2-d_2^*)\dot{d}_2 + \frac{1}{k_3}(d_3-d_3^*)\dot{d}_3 \\
&= e_{11}(-e_{12}-e_{13}-d_1e_{11}+d_2e_{21}) + e_{12}(e_{11}+ae_{12}) + e_{13}(x_1e_{13}+y_3e_{11}-ce_{13}) + e_{21}(-e_{22}-e_{23}-d_2e_{21}-d_3e_{11}-d_3e_{21}) \\
&\quad + e_{22}(e_{21}+ae_{22}) + e_{23}(y_1e_{23}+z_3e_{21}-ce_{23}) + (d_1-d_1^*)e_{11}^2 + (d_2-d_2^*)(e_{21}^2-e_{11}e_{21}) + (d_3-d_3^*)(e_{21}^2+e_{11}e_{21}) \\
&= -d_1e_{11}^2 + ae_{12}^2 + (x_1-c)e_{13}^2 - (d_2+d_3)e_{21}^2 + ae_{22}^2 + (y_1-c)e_{23}^2 - (1-y_3)e_{11}e_{13} + (d_2-d_3)e_{11}e_{21} - (1-z_3)e_{21}e_{23} \\
&\quad + (d_1-d_1^*)e_{11}^2 + (d_2-d_2^*)(e_{21}^2-e_{11}e_{21}) + (d_2-d_2^*)(e_{21}^2+e_{11}e_{21}) \le -d_1^*e_{11}^2 + ae_{12}^2 + (M_1-c)e_{13}^2 - (d_2^*+d_3^*)e_{21}^2 \\
&\quad + ae_{22}^2 + (M_1-c)e_{23}^2 + (M_3-c)e_{11}e_{13} + (d_2-d_3)e_{11}e_{21} + (M_3-1)e_{21}e_{23} \\
&= -(|e_{11}|, |e_{12}|, |e_{12}|, |e_{21}|, |e_{22}|, |e_{23}|)\mathbf{P}(|e_{11}|, |e_{12}|, |e_{12}|, |e_{21}|, |e_{22}|, |e_{23}|)^{\mathrm{T}}
\end{aligned}
$$

where

$$
\mathbf{P} = \begin{pmatrix}
d_1^* & 0 & \frac{-M_3+1}{2} & \frac{d_2^*+d_3^*}{2} & 0 & 0 \\
0 & -a & 0 & 0 & 0 & 0 \\
\frac{-M_3+1}{2} & 0 & -M_1+c & 0 & 0 & 0 \\
\frac{d_2^*+d_3^*}{2} & 0 & 0 & d_2^*+d_3^* & 0 & \frac{-M_3+1}{2} \\
0 & 0 & 0 & 0 & -a & 0 \\
0 & 0 & 0 & 0 & \frac{-M_3+1}{2} & -M_1+c
\end{pmatrix}
$$

$$(5)$$

The symmetrical matrix $\mathbf{P}$ will be positive definite if positive constants d_1^*, d_2^*, and d_3^* satisfy the following inequalities

$$
\begin{aligned}
&d_1(d_2+d_3)a^2(c-M_1)^2 - 1/4a^2(C-M_1)(d_2+d_3) \\
&\quad \times (M_3^3-2M_2+1) > 0
\end{aligned}
$$

$$(6)$$

Obviously, (6) holds if d_1^*, d_2^*, and d_3^* are large enough. That is, $\dot{V}$ is negative semi-definite for e_{11}, e_{12}, e_{13}, e_{21}, e_{22}, e_{23}, d_1, d_2, and d_3. Thus, e_{11}, e_{12}, e_{13}, e_{21}, e_{22}, e_{23}, $d_1-d_1^*$, $d_2-d_2^*$, $d_3-d_3^* \in L_\infty$.

Since $\dot{V} \le -e^{\mathrm{T}}\mathbf{P}e$ and $\mathbf{P}$ is positive definite, one has

$$
\begin{aligned}
\int_0^t \lambda_{\min}(P)(e_1^2+e_1^2+e_1^2)dt &\le \int_0^t e^{\mathrm{T}}Pedt \le -\int_0^t \dot{V}dt \le V \\
&\times (e_{11}(0), e_{12}(0), e_{13}(0), e_{21}(0), e_{22}(0), e_{23}(0))
\end{aligned}
$$

where $\lambda_{\min}(\mathbf{P})$ is the minimum eigenvalue of the symmetrical positive definite matrix $\mathbf{P}$. It follows that e_{11}, e_{12}, e_{13}, e_{21}, e_{22}, $e_{23} \in L_2$. We have $\dot{e}_{11}, \dot{e}_{12}, \dot{e}_{13}, \dot{e}_{21}, \dot{e}_{22}, \dot{e}_{23} \in L_\infty$ from error system (4). Therefore, by Barbalat's lemma, $e_{11}, e_{12}, e_{13}, e_{21}, e_{22}, e_{23} \to 0$ as $t \to \infty$.

In numerical simulations for coupled system with Rössler systems, Fig. 1 shows the synchronization errors of the coupled system with three Rössler systems for $k_1 = 0.1$, $k_2 = 0.3$, and $k_3 = 0.5$. The initial states of three coupled systems are the following: $x_1(0) = 0.1$, $x_2(0) = 0.1$, $x_3(0) = 0.1$; $y_1(0) = 0.2$, $y_2(0) = 0.2$, $y_3(0) = 0.2$; $z_1(0) = 0.3$, $z_2(0) = 0.3$, $z_3(0) = 0.3$; $d_1(0) = 0.5$, $d_2(0) = 0.4$, $d_3(0) = 0.3$.

From Fig. 1, we can see that the three coupled Rössler chaotic systems realize synchronization in a short amount of time, so the above generic criteria of global chaos synchronization are effective.

3 Adaptive synchronization of three Lorenz systems with bidirectional coupling

Next, the synchronization of three chaotic systems with bidirectional coupling is studied. In this section, we select one adaptive feedback gain equation to reach for the goal.

Consider the classical Lorenz chaotic system

$$
\begin{cases}
\dot{x}_1 = a(x_2-x_1) \\
\dot{x}_2 = cx_1-x_1x_3-x_2 \\
\dot{x}_3 = x_1x_2-bx_3
\end{cases}
$$

where $a = 10$, $b = 8/3$, and $c = 28$, so that the Lorenz system has chaotic attractors.

The three Lorenz systems using bidirectional coupling can be written as

$$
\begin{cases}
\dot{x}_1 = a(x_2-x_1)-d(2x_1-y_1-z_1) \\
\dot{x}_2 = cx_1-x_1x_3-x_2 \\
\dot{x}_3 = x_1x_2-bx_3 \\
\dot{y}_1 = a(y_2-y_1)-d(2y_1-x_1-z_1) \\
\dot{y}_2 = cy_1-y_1y_3-y_2 \\
\dot{y}_3 = y_1y_2-by_3 \\
\dot{z}_1 = a(z_2-z_1)-d(2z_1-x_1-y_1) \\
\dot{z}_2 = cz_1-z_1z_3-z_2 \\
\dot{z}_3 = z_1z_2-bz_3
\end{cases}
$$

$$(7)$$

where $a = 10$, $b = 8/3$, and $c = 28$, so that the Lorenz system has chaotic attractors.

Selecting the synchronization errors as follows:

$$
\begin{aligned}
e_1(t) &= x_1(t)-y_1(t), & e_4(t) &= y_1(t)-z_1(t), & e_7(t) &= z_1(t)-x_1(t) \\
e_2(t) &= x_2(t)-y_2(t), & e_5(t) &= y_2(t)-z_2(t), & e_8(t) &= z_2(t)-x_2(t) \\
e_3(t) &= x_3(t)-y_3(t), & e_6(t) &= y_3(t)-z_3(t), & e_9(t) &= z_3(t)-x_3(t)
\end{aligned}
$$

$$(8)$$

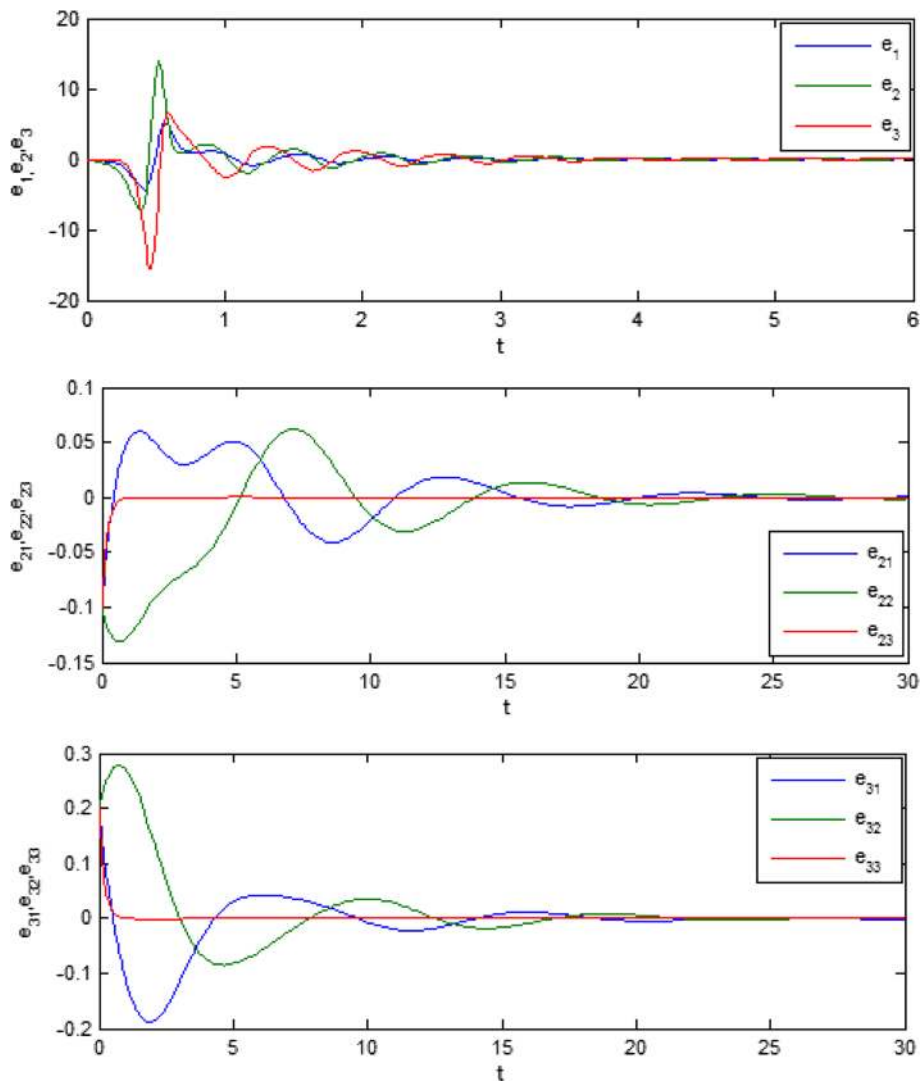and we have $e_7 = -e_1-e_4$, $e_8 = -e_2-e_5$, and $e_9 = -e_3-e_6$.

Assuming that

Zhang *et al. EURASIP Journal on Wireless Communications and Networking* (2016) 2016:134

Page 5 of 15

Fig. 1 The convergence dynamics of the error system

$$\dot{d} = k\left(3e_1^2 + 3e_4^2\right), \; k > 0. \tag{9}$$

According to formulas (8) and (9), the dynamical error system is written as follows:

$$\begin{cases} \dot{e}_1 = ae_2 - (3d+a)e_1 \\ \dot{e}_2 = ce_1 - e_2 - x_1e_3 - y_3e_1 \\ \dot{e}_3 = x_1e_2 + y_2e_1 - be_3 \\ \dot{e}_4 = ae_5 - (3d+a)e_4 \\ \dot{e}_5 = ce_4 - e_5 - y_1e_6 - z_3e_4 \\ \dot{e}_6 = y_1e_5 + z_2e_4 - be_6 \end{cases} \tag{10}$$

3.1 Theorem 2

The coupled system (7) will synchronize for any initial values $(x_1(0), x_2(0), x_3(0))$; $(y_1(0), y_2(0), y_3(0))$;

$(z_1(0), z_2(0), z_3(0))$; $d(0)$. That is, $e_i \to 0$ as $t \to \infty$, $(i = 1, 2, \cdots, 9)$.

3.2 Proof

Construct a Lyapunov function

$$V = \frac{1}{2}\left[e_1^2 + e_2^2 + e_3^2 + e_4^2 + e_5^2 + e_6^2 + \frac{1}{k}(d-d^*)^2\right]$$

where $d^* > 0$ is to be determined. Since the Lorenz system is chaotic, we assume $|y_2|, |z_2| \le M_2, |y_3|, |z_3| \le M_3$, where M_2, M_3 are positive constants. The time derivative of V along the orbits of system (7) is

$$
\begin{aligned}
\dot{V} &= e_1\dot{e}_1 + e_2\dot{e}_2 + e_3\dot{e}_3 + e_4\dot{e}_4 + e_5\dot{e}_5 + e_6\dot{e}_6 + \frac{1}{k}(d-d^*)\dot{d} \\
&= e_1[ae_2-(3d+a)e_1] + e_2(ce_1-e_2-x_3e_3-y_3e_1) + e_3(x_1e_2+y_2e_1-be_3) + e_4[ae_5-(3d+a)e_4] \\
&\quad + e_5(ce_4-e_5-y_1e_6-z_3e_4) + e_6(y_1e_5+z_2e_4-be_6) + 1/k(d-d^*)k\big(3e_1^2+3e_4^2\big) \\
&= -(3d+a)e_1^2-e_2^2-be_3^2-(3d+a)e_4^2-e_5^2-be_6^2+(a+c-y_3)e_1e_2+(a+c-z_3)e_4e_5 \ +y_2e_1e_3+z_2e_4e_6+(d-d^*) \\
&\quad \times \big(3e_1^2+3e_4^2\big) \\
&= -(a+3d^*)e_1^2-e_2^2-be_3^2-(a+3d^*)e_4^2-e_5^2-be_6^2+(a+c-y_3)e_1e_2+(a+c-z_3)e_4e_5+y_2e_1e_3+z_2e_4e_6 \\
&\leq -(a+3d^*)e_1^2-e_2^2-be_3^2-(a+3d^*)e_4^2-e_5^2-be_6^2+(a+c+M_3)|e_1||e_2|+(a+c+M_3)|e_4||e_5| \ +M_2|e_1||e_3| \\
&\quad +M_2|e_4||e_6| \\
&= -(|e_1|,|e_2|,|e_3|,|e_4|,|e_5|,|e_6|)\mathbf{P}(|e_1|,|e_2|,|e_3|,|e_4|,|e_5|,|e_6|)^{\mathrm{T}}
\end{aligned}
$$

where

$$
\mathbf{P} = \begin{pmatrix}
a+3d^* & -\dfrac{a+c+M_3}{2} & -\dfrac{M_2}{2} & 0 & 0 & 0 \\[2mm]
-\dfrac{a+c+M_3}{2} & 1 & 0 & 0 & 0 & 0 \\[2mm]
-\dfrac{M_2}{2} & 0 & b & 0 & 0 & 0 \\[2mm]
0 & 0 & 0 & a+3d^* & -\dfrac{a+c+M_3}{2} & -\dfrac{M_2}{2} \\[2mm]
0 & 0 & 0 & -\dfrac{a+c+M_3}{2} & 1 & 0 \\[2mm]
0 & 0 & 0 & -\dfrac{M_2}{2} & 0 & b
\end{pmatrix}
\tag{11}
$$

The matrix $\mathbf{P}$ will be positive definite if positive constants $d^* > \frac{M_2^2}{4b} + \frac{(a+c+M_3)^2}{4} - a$, because with this condition, all the principal minor determinants of matrix $\mathbf{P}$ are positive. Similar to the proof of Theorem 1, we obtain $e_1, e_2, e_3, e_4, e_5, e_6, \dot{e}_1, \dot{e}_2, \dot{e}_3, \dot{e}_4, \dot{e}_5, \dot{e}_6, d \in L_\infty$, $e_1, e_2, e_3, e_4, e_5, e_6 \in L_2$. By Barbalat's lemma, $e_1, e_2, e_3, e_4, e_5, e_6 \to 0$ as $t \to \infty$, then

$$
e_1, e_2, e_3, e_4, e_5, e_6, e_7, e_8, e_9 \to 0 (t\to\infty)
$$

In numerical simulations for coupled system with Lorenz systems, Fig. 2 shows the synchronization errors of the coupled system with three Lorenz systems for $k = 0.1$. The initial states of three coupled systems are $x_1(0) = 0.1, x_2(0) = 0.1, x_3(0) = 0.1; y_1(0) = 0.2, y_2(0) = 0.2, y_3(0) = 0.2; z_1(0) = 0.3, z_2(0) = 0.3, z_3(0) = 0.3; d_1(0) = 0.5$.

From Fig. 2, like in Section 2, we can see that the three coupled Rössler chaotic systems realize synchronization in a short amount of time, so the above generic criteria of global chaos synchronization is effective.

4 The secure communication theory and multistage chaos synchronized system for secure communications

In this section, the multistage chaos synchronized system scheme proposed above is applied to chaotic secure communications system. Secure communication has been an interesting field of application of chaotic synchronization since the last decade. Due to their unpredictability and broadband spectrum, chaotic signals have been used to encode information by simple masking (addition) or using modulation. These chaotic characters of sensitive dependence on initial conditions and random-like behavior make the chaos signal be fit for applying in secure communication. In chaotic communication schemes, a chaotic system is used as transmitter and the information signal is mixed at the transmitter end to generate a chaotic transmit signal, which is then transmitted to the receiver end. The receiver is also a chaotic dynamic system constructed based on the structure of transmitter and it is able to synchronize the transmitter by receiving the transmit signal. Once synchronization is achieved, the information signal is recovered by the receiver. It should be noted that the power of the information signal is required to be sufficiently lower than that of the chaotic carrier.
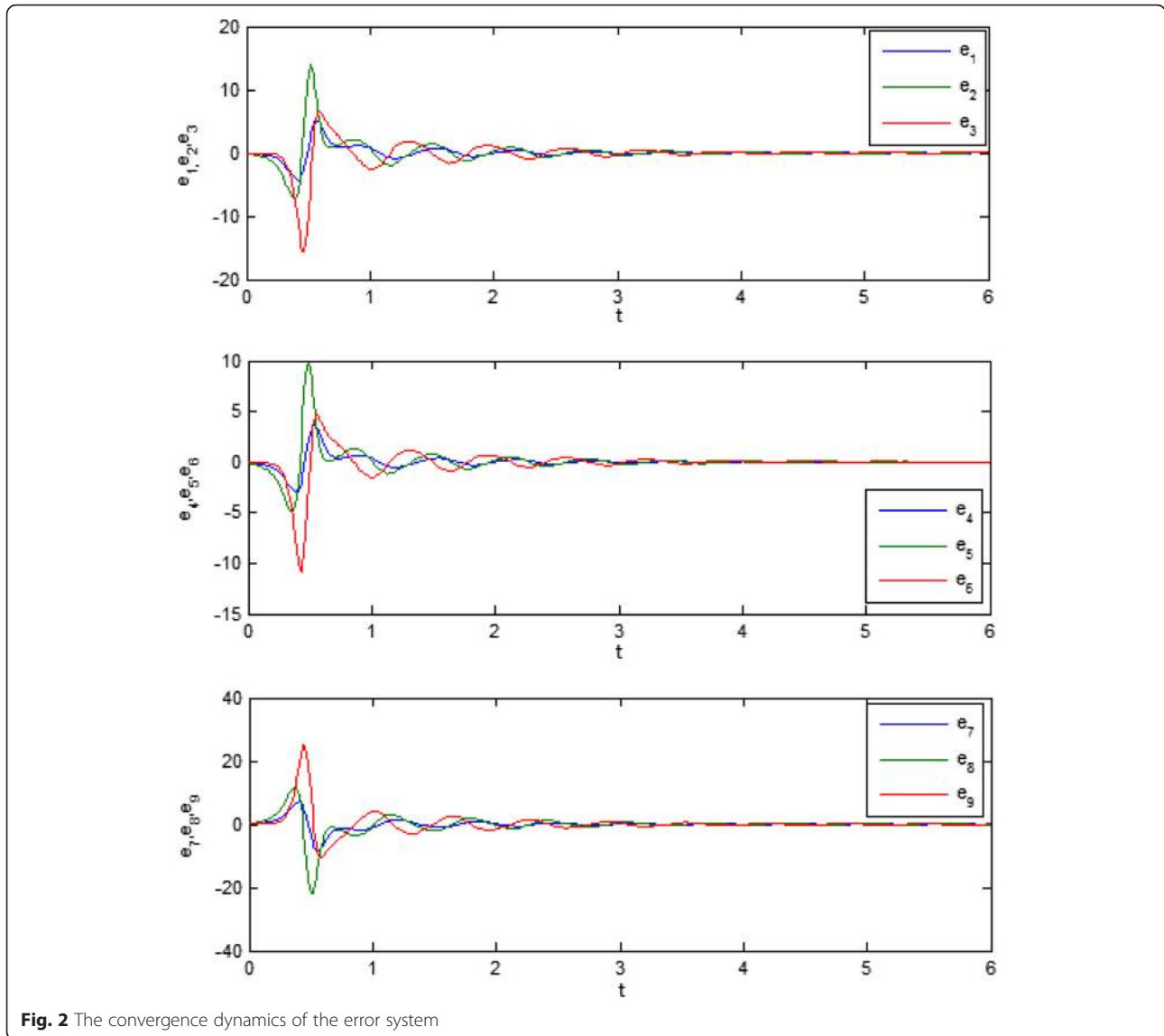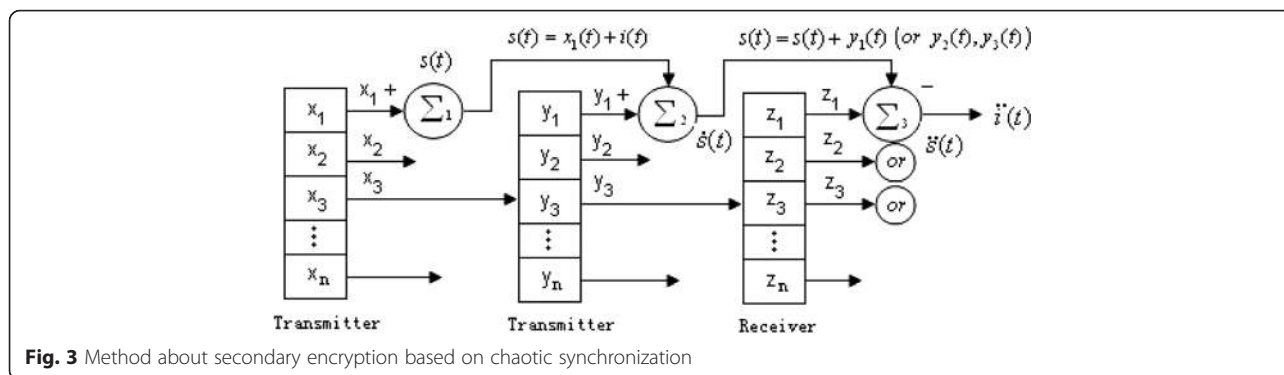
Zhang *et al. EURASIP Journal on Wireless Communications and Networking* (2016) 2016:134

Page 7 of 15

Fig. 2 The convergence dynamics of the error system

However, the recent researches show that even with chaotic dynamics completely hidden most of known models of chaotic communication are insecure. They are insecure against some very weak attacks, including nonlinear dynamics forecasting and reconstructing. Apart from this, slow encryption speed and weakness in resistance to channel noise are also the serious inherent drawbacks of chaotic cryptosystems. For the reason given above, we have to explore the algorithm with higher security.

Based on above discussion and analysis, within the drive-response configuration, this paper presents a method about twice encryption based on multistage chaos synchronized system for secure communications. Figure 3 illustrates the proposed secure communication system consisting of two transmitters (or drive systems) at the sending end and one receiver (or response systems) at the receiving end. As it is shown in Fig. 1,

x_i $(i = 1, 2, \cdots n)$ and y_i $(i = 1, 2, \cdots n)$ are the two drive chaotic systems, z_i $(i = 1, 2, \cdots n)$ is the response chaotic systems. Firstly, the transmitted signal $s(t)$ is the sum of the information signal $i(t)$ and the output variables x_1 (or x_2, x_3) of the first chaotic transmitter at the sending end. Then, the mixed signal is transmitted to the second transmitter y_i $(i = 1, 2, \cdots n)$, as is seen in Fig. 3. Add the transmitted mixed signal to the output variables y_1 (or y_2, y_3) to be the pretend of the chaos signal $.s(t)$, which will be transmitted to the receiver end. At the receiver end, when the synchronization occurrence among three identical chaos systems, the original information signal $i(t)$ can be recovered from the mixed $i(t)$. In this method, the original information signal $i(t)$ has two encryption processes, one is x_i $(i = 1, 2, \cdots n)$ and one is y_i $(i = 1, 2, \cdots n)$, so if one wants to obtain the original information signal $i(t)$, he has to decrypt the transmitted

Zhang *et al. EURASIP Journal on Wireless Communications and Networking* (2016) 2016:134

Page 8 of 15

Fig. 3 Method about secondary encryption based on chaotic synchronization

mixed signal $\dddot{s}(t)$ twice. Considering chaos signal depending on initial values, obviously, by comparison with the original chaos masking mode, this method has higher security.

5 The noise resistance effect for the transmitter of a discrete signal and wavelet de-noise

The sensitivity of noise is also an important research area for chaos communication. However, to the best of our knowledge, few profound and general results have been reported in the literature so far because of the complexity.
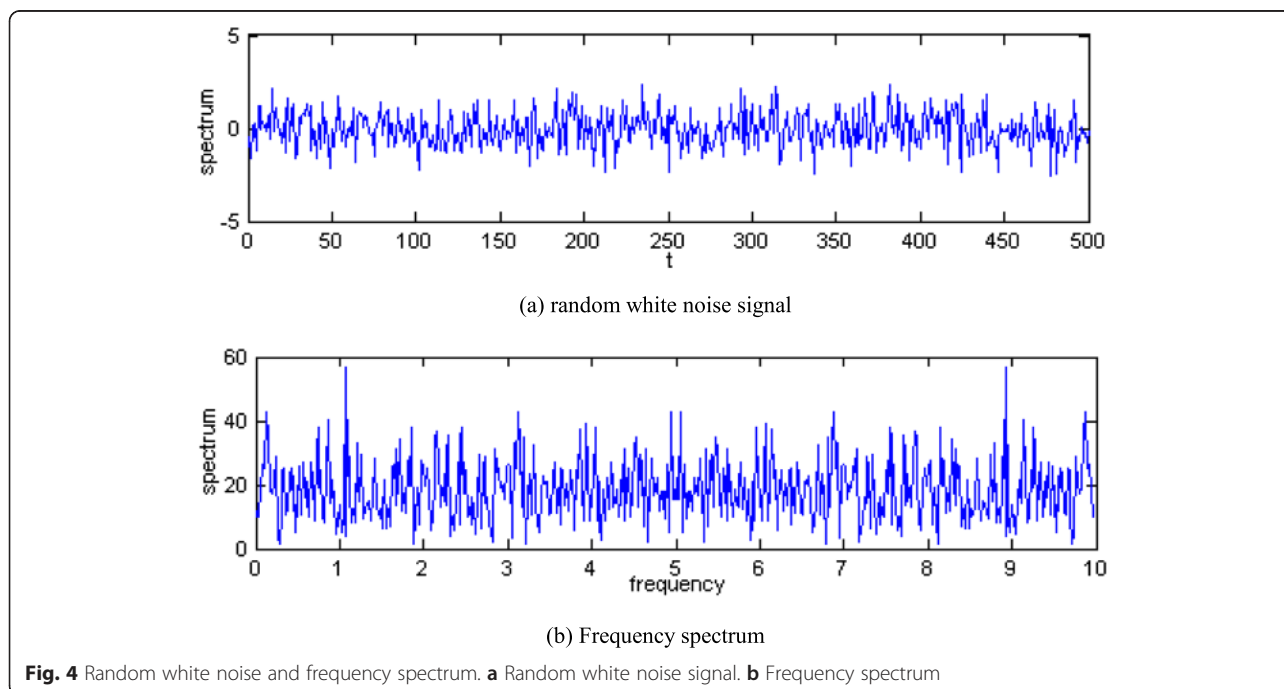
5.1 Analyzing the discrete signal with random white noise perturbation

The channel constitutes an absolutely necessary part of communication system, and noise in the channel is unavoidable. Noise and information signal existed in the same

process of radio communications. The existence of the noise is more or less inevitable. In the secure communication, the transforming information signal is easy to mask by noise. However, in certain nonlinear systems, including electronic circuits and biological sensory systems, the presence of noise can enhance the diction of weak signal.

In order to analyze the noise resistance effect for the signal, we consider the random white noise, as is shown in Fig. 4.

When the signal-noise ratio is 5 dB, we analyze its effect for the transmitter of discrete signal. Suppose $m(t)$ is the discrete signal, let the transmit signal be $s(t) = m(t) + x_1(t) + n(t)$, $n(t)$ be random white noise. From Fig. 3, we have $\dot{s}(t) = s(t) + y_1(t)$, $\ddot{s}(t) = \dot{s}(t) + z_1(t)$. Suppose $\dot{m}(t)$ is the first recovery of information signal and $\ddot{m}(t)$ is the second one. According to Fig. 3 and system (7), let the transmitters be

(a) random white noise signal

(b) Frequency spectrum

Fig. 4 Random white noise and frequency spectrum. **a** Random white noise signal. **b** Frequency spectrum

Zhang *et al. EURASIP Journal on Wireless Communications and Networking* (2016) 2016:134

Page 9 of 15

$$\begin{cases} \dot{x}_1 = a(x_2 - x_1) - d(2x_1 - y_1 - z_1) + s(t) \\ \dot{x}_2 = cx_1 - x_1x_3 - x_2 \\ \dot{x}_3 = x_1x_2 - bx_3 \end{cases}$$

and

$$\begin{cases} \dot{y}_1 = a(y_2 - y_1) - d(2y_1 - x_1 - z_1) + \dot{s}(t) \\ \dot{y}_2 = cy_1 - y_1y_3 - y_2 \\ \dot{y}_3 = y_1y_2 - by_3 \end{cases}$$

And let the receiver be

$$\begin{cases} \dot{z}_1 = a(z_2 - z_1) - d(2z_1 - x_1 - y_1) + \ddot{s}(t) \\ \dot{z}_2 = cz_1 - z_1z_3 - z_2 \\ \dot{z}_3 = z_1z_2 - bz_3 \end{cases}$$

Numerical simulation was done by the MATLAB environment. Figure 5 depicts the numerical results. From Fig. 5a, b, we can see the time series of x_1 and $x_1 + y_1$. The information signal $m(t)$ is shown in Fig. 5c; obviously, the power of the information signal $m(t)$ is lower than that of the chaotic carrier x_1 and $x_1 + y_1$. The transmitted signal $s(t)$ and the second transmitted signal $\dot{s}(t)$ with noise perturbation are shown in Fig. 5d, e; The first recovery of information noised-signal $\dot{m}(t)$ and the second recovery of information noised-signal $\ddot{m}(t)$ are shown in Fig. 5f, g. Figure 5h shows the error of the information signal $\ddot{m}(t) - m(t)$. Obviously, it is easy to find that the information signal is recovered after a short transmission. This method of secondary encryption-based chaos synchronization of three identical systems has two encryptions; compared to traditional chaos masking mode, it can additionally enhance the security of communication and is harder to decode.

From Fig. 5a–h, with the random white noise perturbing, although the information signal $m(t)$ can recover after decoding, distortion occurs at the top of the signal, and the curve is not as smooth as before. This is because the error becomes large with the random white noise perturbation. But the distorted information signal is less useful in specific areas, and we should seek to the method to mend the information signal for realizing its precision of application.

5.2 Security analysis

There are many methods to improve the security of chaotic communication; the chaos masking method based on multistage chaos synchronized secure communication system is a simple and effective technique. For the first time, chaos synchronization of three identical chaotic systems is applied to secure communication through the method of chaotic masking. In the proposed method, it can enhance the security of information

signal transmission; the reasons will be illustrated in the following. In this scheme, information signal can be transmitted in a form of any function pre-designed between a sender and a receiver and recovered exactly, since the function is arbitrary and the scaling factor in the above synchronization method is unpredictable.

For the above multistage chaos synchronized system for secure communications, the main advantage of using synchronization of three identical systems is that it is very difficult for an eavesdropper to predict the stochastic output of the chaotic transmitter. The proposed chaotic communication scheme is totally different from the traditional cryptosystems, due to employing three chaos states for synchronization and encryption. If the eavesdropper wants to receive the information signal $m(t)$, one must use the state $x_i(t)$, $(i = 1, 2, \cdots, n)$ to predict the system $(y_1, y_2, \cdots, y_n)$, but the error is existent [52]. Then, he uses the prediction information in which error exists to predict the system $(z_1, z_2, \cdots, z_n)$; obviously, this is difficult and, at the same time, the error will be magnified. So, the chaos synchronization of three identical systems method can enhance the security of signal transmission and also improve the vulnerable points of chaotic masking.

In other things, every chaotic system has a different state, and we can select a different state. For example, the information signal $m(t)$ can be added to the state $x_i(t)$ and can be also added to the state $x_j(t)$, $(i \neq j)$. In the same way, there are different state $y_i(t)$ that can be selected to carry the transmitted mixed $.s(t)$; and at the receiving end, the transmitted mixed $\ddot{s}(t)$ can be transmitted to the different state $z_i(t)$. In the mentioned cases, if the eavesdropper wants to get the information signal $m(t)$, he must detect the correct state $x_i(t)$, $y_i(t)$, and $z_i(t)$, but that is very difficult or even impossible; he can only get the inaccurate information signal. And again, we can select different chaotic systems as the transmitters (or drive systems) at the sending end and one receiver (or response systems), and they may be hyperchaotic systems, or even different order, which will be more difficult for the eavesdropper to detect. So the proposed multistage chaos synchronized secure communication system has important theoretical and experimental value.

5.3 Wavelet de-nosing

Wavelet transform makes the decomposition of the original signal into detailed signal and approximate signal, which implements by translation and expansion of wavelet mother function. Although the wavelet transforms (WTs) are being used to process fault signals of power system widely, wavelet transforms can only filter white noises and are useless to filter colored noises.
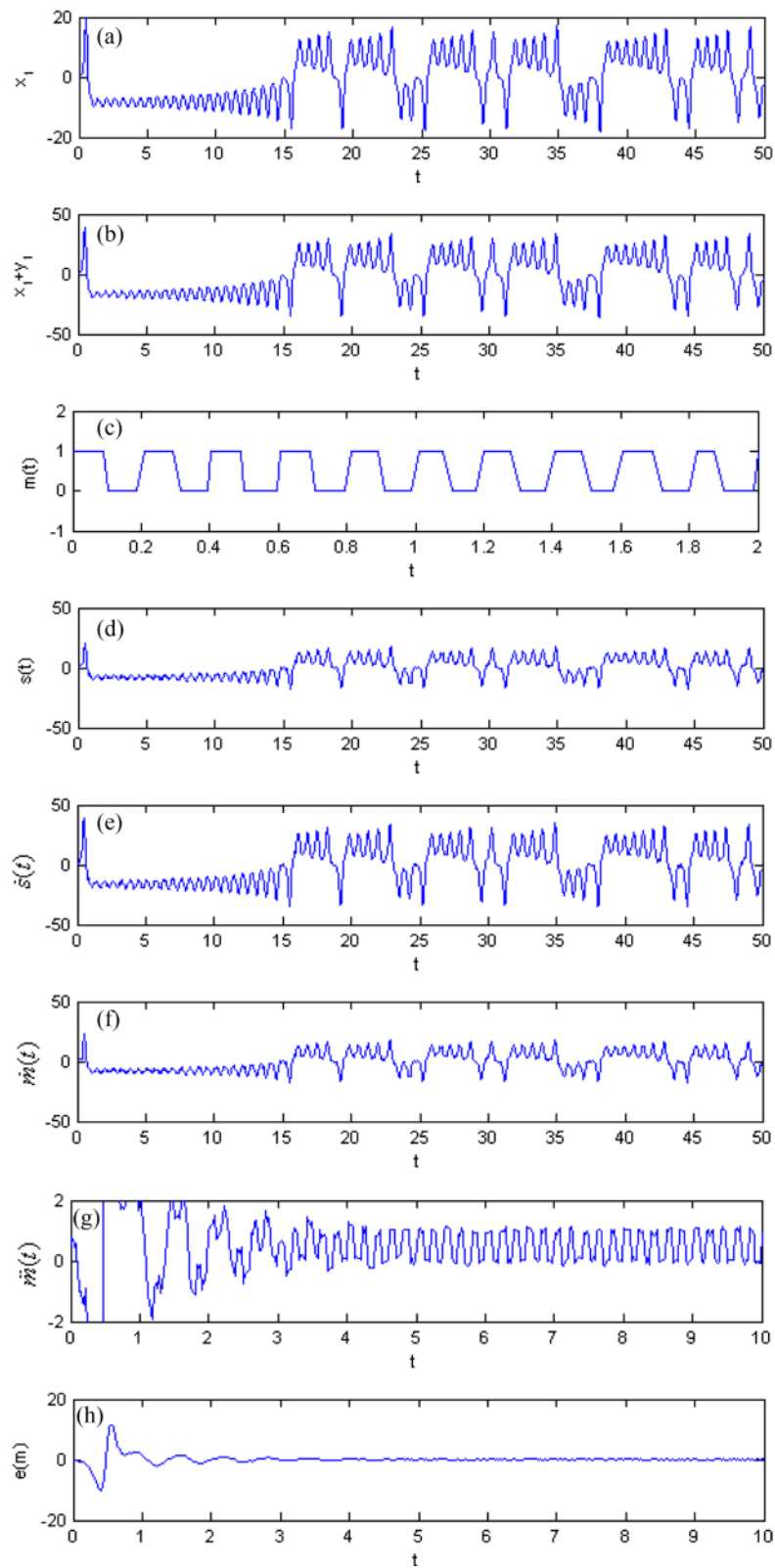
Zhang *et al. EURASIP Journal on Wireless Communications and Networking* (2016) 2016:134

Page 10 of 15

Fig. 5 Transmission of a signal through the chaotic systems. **a** The chaos signal x_1. **b** The chaos signal $x_1 + y_1$. **c** The signal $m(t)$. **d** The first transmitted noised-signal $s(t)$. **e** The second transmitted noised-signal $\dot{s}(t)$. **f** The first recovered signal $\dot{m}(t)$. **g** The second recovered signal $\ddot{m}(t)$. **h**. Error of the information signal $\ddot{m}(t) - m(t)$

Zhang *et al. EURASIP Journal on Wireless Communications and Networking* (2016) 2016:134

Page 11 of 15

The expression of wavelet function is defined as follows

$$\psi_{a,b}(t) = \frac{1}{\sqrt{|a|}} \psi\left(\frac{t-b}{a}\right) \qquad (12)$$

where a is the scale parameter and b is the time parameter. Wavelet function (12) shows an expansion.

When the parameter b varies, wavelet function activates with timeline. A cluster wavelet functions format when parameter a and b change at the same time. Signal $f(t)$ can make decomposition by the cluster wavelet functions.

Considering the arbitrary signal $f(t)$, the wavelet function can be defined as follows

$$W(a,b) = \int_{-\infty}^{\infty} f(t)\psi_{a,b}^*(t)dt$$

The steps of threshold de-noising method based on usual wavelet transform are briefly described as

(1) Obtaining wavelet coefficients W by selecting suitable wavelet and making decomposition of the original signal.
(2) Calculating wavelet threshold and selecting suitable threshold method then choosing wavelet coefficients in order to get new wavelet coefficient W_δ.
(3) Obtaining signal after de-noising by making inverse wavelet transform to wavelet coefficient W_δ.

Process the noised-signal as mentioned above. Simulated by MATLAB numerical value method, the effects of do-noising could be analyzed. After threshold de-noising, reconstruct the de-noising signal in order to highlight the trend of original signal and keep up its smooth and similarity. Figure 6 presents the recovered discrete signals after wavelet de-noising; obviously, they are much smoother than that of Fig. 5g. Simulation results show that the algorithm is effective to reduce the impacts of random noise.

6 The transmission of a high-amplitude discrete signal

One of the drawbacks of secure communication using synchronization of chaotic system is the limitation of the amplitude of the confidential messages. Usually, they have to be small enough in order to be masked by the chaotic signal (addition method) or in order to preserve the chaotic behavior (inclusion method). This constraint obviously limits the ratio of the transferred information with respect to the channel signal.

In this section, we use the three-grade chaos synchronization system for secure communication to transmit a high-amplitude discrete signal. In the transmitter, an adaptive controller is adopted to pick up the change of high-amplitude discrete signal, and to inject the controller's error into the transmitting system. At the same time, the information is directly added to the chaotic signal in transmission to drive the receiving system. In the receiver, another adaptive controller is used to maintain chaotic synchronization of the transmitting and receiving systems and to recover the information signal. Since the synchronization error is independent from the information signal and, at the same time, we adopt two attenuation factors, the power of the information signal can be equivalent to that of the chaotic signal, even
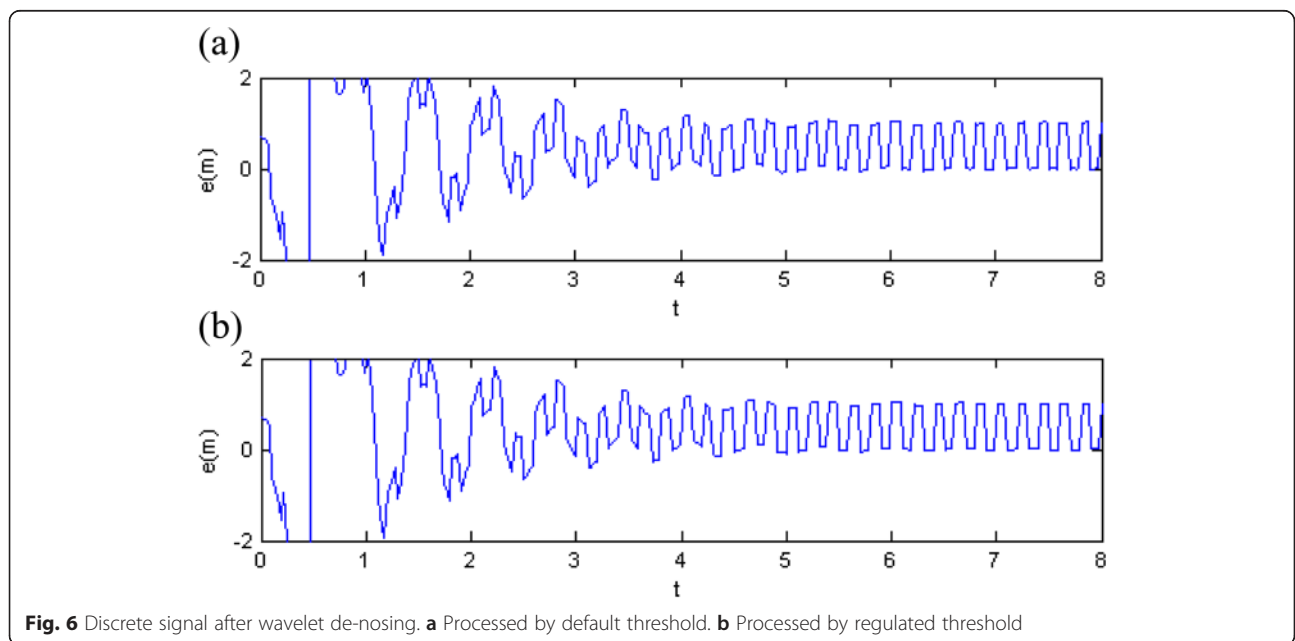

Fig. 6 Discrete signal after wavelet de-nosing. **a** Processed by default threshold. **b** Processed by regulated threshold

much lower. So the frequency of the information signal can be set within the range of the principal frequencies of the chaotic signal.

According to Fig. 3 and system (7), let Lorenz chaotic systems be the transmitters

$$\begin{cases} \dot{x}_1 = a(x_2-x_1)-d(2x_1-y_1-z_1) \\ \dot{x}_2 = cx_1-x_1x_3-x_2+mw_1 \\ \dot{x}_3 = x_1x_2-bx_3 \end{cases}$$

$$\dot{w}_1 = n(h(t)-w_1)$$

and

$$\begin{cases} \dot{y}_1 = a(y_2-y_1)-d(2y_1-x_1-z_1) \\ \dot{y}_2 = cy_1-y_1y_3-y_2+mw_2 \\ \dot{y}_3 = y_1y_2-by_3 \end{cases}$$

$$\dot{w}_2 = n(h(t)-w_2)$$

Let the receiver be

$$\begin{cases} \dot{z}_1 = a(z_2-z_1)-d(2z_1-x_1-y_1) \\ \dot{z}_2 = cz_1-z_1z_3-z_2+mw_3 \\ \dot{z}_3 = z_1z_2-bz_3 \end{cases}$$

$$\dot{w}_3 = n(h(t)-w_3)$$

where d is the control gain, and we can select it appropriately to get the synchronization of three chaotic systems with bidirectional coupling. $h(t)$ is the information signal with a high amplitude 100, as be shown in the Fig. 7. m, n are attenuation factors, which will make the information signal be transmitted successfully. Hence, the power of the information signal can be equivalent to that of the chaotic signal and the frequency of the information signal can be set within the principal frequencies of the chaotic oscillation. w_1, w_2, w_3 are adaptive controllers for trace the signal at the transmitter and receiver end.

Without the attenuation factors, transmitter systems will lose original chaos characteristic when they mask the high-amplitude signal $h(t)$. Conversely, the high amplitude has no effect on the chaotic system if it is treated by attenuation factor $m = 0.2$, $n = 0.1$, as shown in Fig. 8a, b. The experiment results show that phase

phenomena are probably caused while the amplitude of input signal increase to some extent. Obviously, the fundamental frequency of the information signal is required within the center frequency band of the chaotic signal.

This is because that the error of information signal $h(t)$ and controller w_1 is added into transmitters, rather than the information signal $h(t)$ is added into transmitters directly, therefore, the system still keep chaotic state even if the amplitude of $h(t)$ is high.

Numerical simulation was done by the MATLAB environment. The information signal $h(t)$ is transmitted at the receiving end by masking it into the chaotic signals x_2 and y_2, as been shown in Fig. 9a. Suppose $h_1(t)$ is the first recovered signal, $h_2(t)$ is the latter two recovered signal, as shown in Fig. 9b, c. From Fig. 9b, c, processed signal $h(t)$ by the two attenuation factor can recover rapidly. This method not only expands the scope of transmitted signal but it also has stronger practicability.

The results of theoretical analysis and numerical simulation show that the presented method not only enhances the degree of security of low-dimensional chaotic systems but also significantly improves the signal-to-noise ratio at the receiving end.

7 Conclusions

The paper studies an adaptive synchronization scheme of three coupled identical systems. Strict theoretical proofs are given to the method for three unidirectional coupled Rössler system and bidirectional Lorenz system. From Figs. 1 and 2, we can see that the two generic criteria of global chaos synchronization are effective; at the same time, the three coupled (even more) identical chaotic systems can be a foundation for chaos secure communication.

Meanwhile, almost all the methods of breaking ciphers are aiming mainly at second order of chaos synchronized secure communication system based on chaos masking but very few methods at multistage chaotic systems. So in the framework of multistage chaotic synchronization systems, we show that the above scheme could be applied in secure communication. We have provided an example to illustrate the implementation of the scheme for transmitting an information signal disturbed by
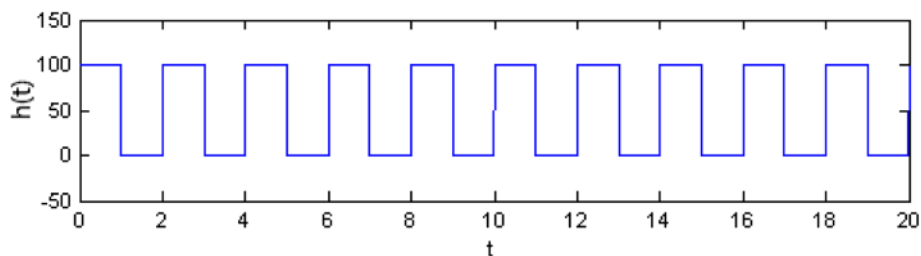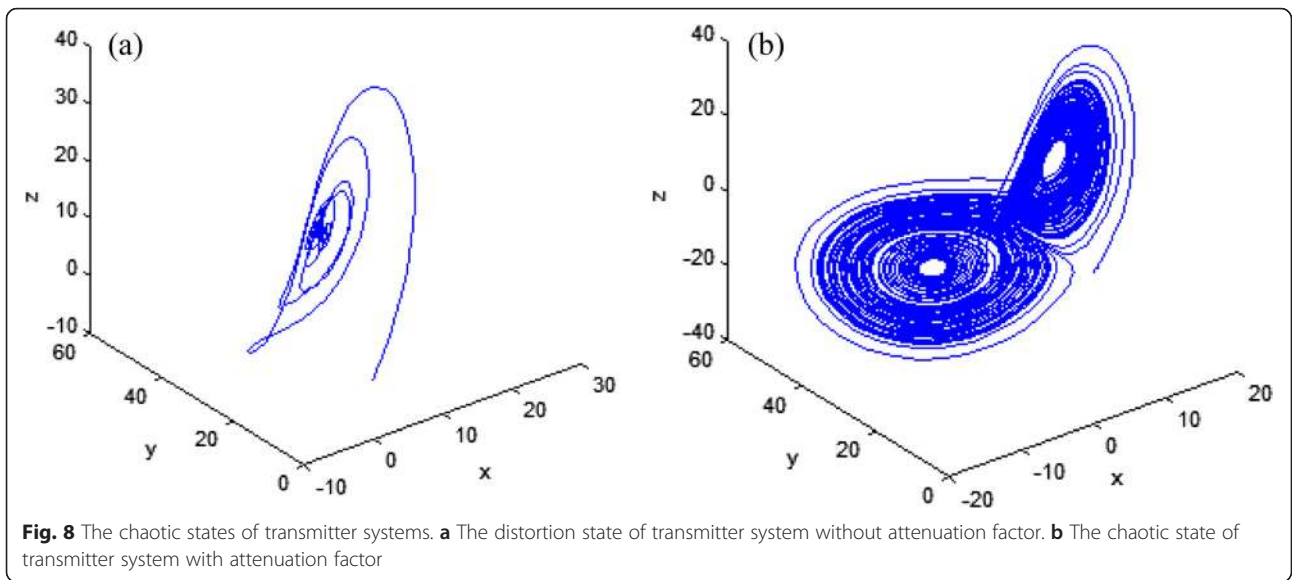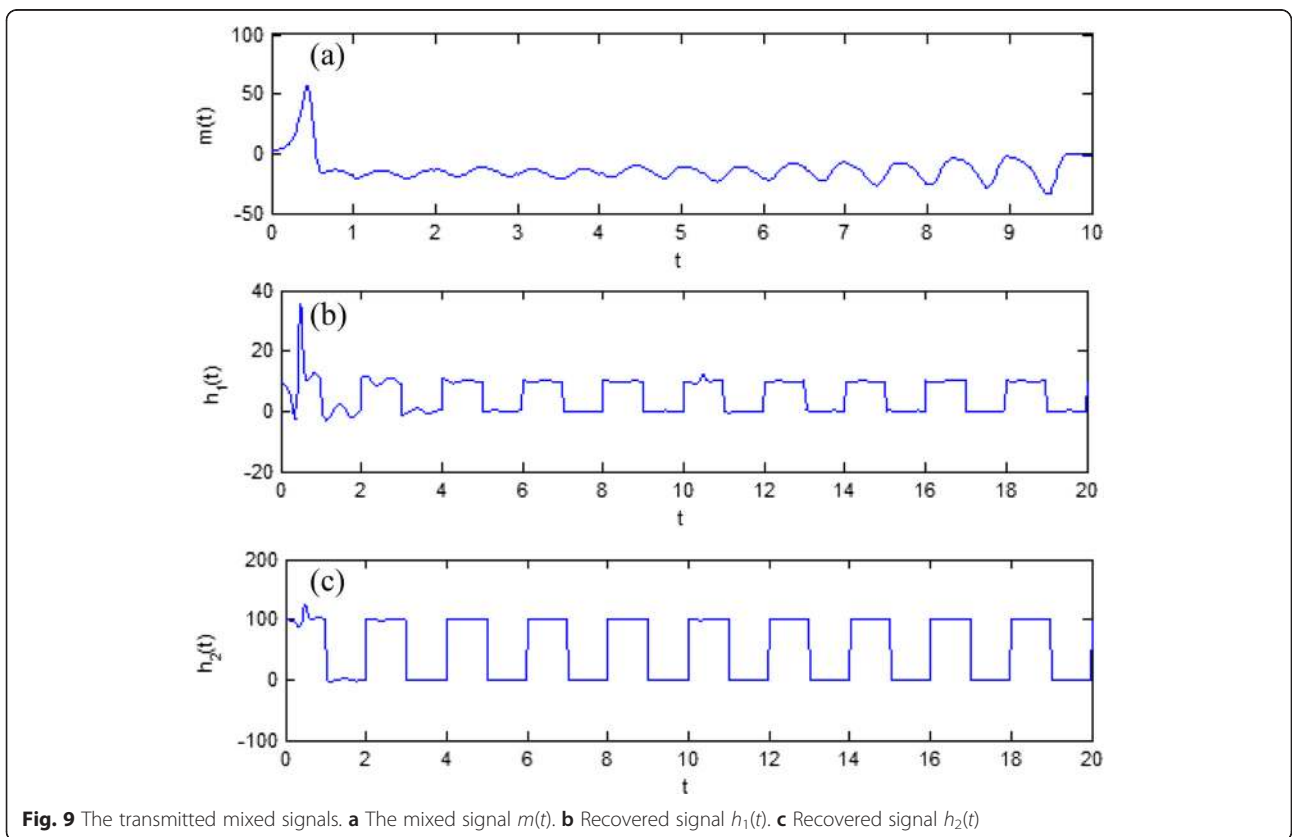
Fig. 7 The discrete information signal

Zhang *et al. EURASIP Journal on Wireless Communications and Networking* (2016) 2016:134

Page 13 of 15

Fig. 8 The chaotic states of transmitter systems. **a** The distortion state of transmitter system without attenuation factor. **b** The chaotic state of transmitter system with attenuation factor

random white noise. The information signal transmitted between two senders and one receiver can be recovered through simple operation. In addition, we reconstruct the original signal using wavelet de-nosing. Both theoretical analysis and numerical simulations demonstrate that the proposed system is of better security and high precision for recovered source signals even when channel

noise is very high. Moreover, the high-amplitude signal transmitted between two senders and one receiver can be recovered through simple operation. Numerical results show the successfulness in transmitting the information signal through chaotic carriers.

Besides, this paper mainly researches the synchronization among three same order chaotic systems and the

Fig. 9 The transmitted mixed signals. **a** The mixed signal $m(t)$. **b** Recovered signal $h_1(t)$. **c** Recovered signal $h_2(t)$

Zhang *et al. EURASIP Journal on Wireless Communications and Networking* (2016) 2016:134

Page 14 of 15

application in secure communication. Furthermore, we can seek the new methods to realize the global synchronization among three different order chaotic systems and their application in secure communication. The realization of secure communication systems based on three different order chaotic systems can enlarge the range of usable chaotic systems and increase the difficulty of information signal decryption. So, it has practical significance on the development and application of chaotic synchronization technology.

It is worth noting that the sensitivity of multistage chaotic system synchronization to initial parameter and noise is also an important research area for chaos communication. However, to the best of our knowledge, few profound and general results have been reported in the literature so far because of the complexity. Besides, in traditional schemes, the amplitude of the messages has to be smaller than that of the chaotic system's signal. In other words, the message's power spectrum should be buried into that of the chaotic signal. Therefore, in order to maintain synchronization between the transmitter and the receiver, and to ensure that the chaotic signal masks the messages, the dynamic range of the messages has to be significantly smaller than that of the chaotic scalar. In this paper, the amplitude of information signal should be smaller than that of the chaotic signal in order not to destroy the system chaotic behavior.

Competing interests

Acknowledgements

Author details

[1]School of Mathematics and Physics, Lanzhou Jiaotong University, Lanzhou 730070, China. [2]The Basic Courses Department of Lanzhou Institute of Technology, Lanzhou 730070, China. [3]Department of Information Engineering, Gansu Forestry Technological College, Tianshui, Gansu 741020, China.

References

1. LM Pecora, TL Carroll, Synchronization in chaotic systems. Phys. Rev. Lett. **64**, 821–824 (1990)
2. DY Chen, R Zhang, XY Ma, S Liu, Chaotic synchronization and anti-synchronization for a novel class of multiple chaotic systems via a sliding mode control scheme. Nonlinear. Dynam. **69**, 35–55 (2012)
3. DY Chen, C Wu, CF Liu, XY Ma, Synchronization and circuit simulation of a new double-wing chaos. Nonlinear. Dynam. **67**, 1481–1504 (2012)
4. DY Chen, R Zhang, JC Sprott, Synchronization between integer-order chaotic systems and a class of fractional-order chaotic systems via sliding mode control. Chaos **22**, 023130 (2012)
5. MF Hu, YQ Yang, ZY Xu, LX Guo, Hybrid projective synchronization in a chaotic complex nonlinear system. Math. Comput. Simulat. **79**, 449–457 (2008)
6. S Gakkhar, RK Naji, Order and chaos in a food web consisting of a predator and two independent preys. Commun. Nonlinear. Sci. Numer. Simul. **10**, 105–120 (2005)
7. XS Zhao, ZB Li, S Li, Synchronization of a chaotic finance system. Appl. Math. Comput. **217**, 6031–6039 (2011)
8. S Gakkhar, B Singh, Dynamics of modified Leslie–Gower-type prey–predator model with seasonally varying parameters. Chaos, Solitons & Fractals. **27**, 1239–1255 (2006)
9. S Teerawat, K Suwat, Adaptive synchronization of hyperchaotic systems via passivity feedback control with time-varying gains. J. Sound Vib. **329**, 2490–2496 (2010)
10. JJ Yan, ML Hung, TL Liao, Adaptive sliding mode control for synchronization of chaotic gyros with fully unknown parameters. J. Sound Vib. **298**, 298–306 (2006)
11. G Grassi, S Mascolo, Nonlinear observer design to synchronize hyperchaotic systems via a scalar signal. IEEE Trans. Circ. Syst. I. **44**, 1011–1014 (1997)
12. L Kocarev, U Parlitz, General approach for chaotic synchronization with application to communication. Phys. Rev. Lett. **74**, 5028–5031 (1995)
13. I Kyprianidis, I Stouboulos, Chaotic synchronization of three coupled oscillators with ring connection. Chaos, Solitons & Fractals. **17**, 327–336 (2003)
14. T Zhou, JH Lü, GR Chen, Synchronization stability of three chaotic systems with linear coupling. Phys Lett A. **301**, 231–240 (2002)
15. J Song, Global chaos synchronization or there coupled diffusionless Lorenz systems. Da xue shu xue. **23**, 54–58 (2007)
16. XL An, JN Yu, YD Chu, Global chaos synchronization of three coupled nonlinear autonomous systems and a novel method of chaos encryption. Chaos, Solitons & Fractals. **42**, 865–873 (2009)
17. JA Lu, XP Han, YT Li, Adaptive coupled synchronization among multi-Lorenz systems family. Chaos, Solitons & Fractals. **31**, 866–878 (2007)
18. YG Yu, SC Zhang, Global synchronization of three coupled chaotic systems with ring connection. Chaos, Solitons & Fractals. **24**, 1233–1242 (2005)
19. L Kovarev, KS Eckert, LO Chua et al., Experimental demonstration of secure communications via chaotic synchronization. Int. J. Bifurcat. Chaos. **2**, 709–713 (1992)
20. U Parlitz, LO Chua et al., Transmission of digital signals by chaotic synchronization. Int. J. Bifurcat. Chaos. **2**, 973–977 (1992)
21. CW Wu, LO Chua, A simple way to synchronize chaotic systems with applications to secure communications systems. Int. J. Bifurcat. Chaos. **3**, 1619–1627 (1993)
22. M Feki, B Robert, G Gelle et al., Secure digital communication using discrete-time chaos synchronization. Chaos, Solitons & Fractals. **18**, 881–890 (2003)
23. U Feldmann, M Hasler, W Schwarz, Communication by chaotic signals: the inverse system approach. Int J Cricuit Theory Appl. **24**, 551–576 (1996)
24. T Yang, A survey of chaotic secure communication systems. Int. J. Comp. Cognit. **2**, 81–130 (2004)
25. KM Cuomo, AV Oppenheim, Circuit implementation of synchronized chaos with applications to communications. Phys. Rev. Lett. **71**, 65–68 (1993)
26. JG Lu, YG Xi, Chaos communication based on synchronization of discrete-time chaotic systems. Chin Phys. **14**, 274–278 (2005)
27. KM Cuomo, AV Oppenheim, SH Strogatz, Robustness and signal recovery in a synchronized chaotic system. Int. J. Bifurcat. Chaos. **3**, 1629–1638 (1993)
28. J Garcia-Ojalvo, R Roy, Spatiotemporal communication with synchronized optical chaos. Phys. Rev. Lett. **86**, 5204–5207 (2001)
29. S Boccaletti, A Farini, FT Arecchi, Adaptive synchronization of chaos for secure communication. Phys Rev E. **55**, 4979–4981 (1997)
30. AA Minai, T Anand, Synchronization of chaotic maps through a noisy coupling channel with application to digital communication. Phys Rev E. **59**, 312–320 (1999)
31. M Feki, B Robert, G Gelle, Secure digital communication using discrete-time chaos synchronization. Chaos, Solitons & ractals. **18**, 881–890 (2003)
32. E Konstantinos, JC Sprott, A comparison of correlation and Lyapunov dimensions. Physica D. **200**, 156–164 (2005)
33. JB He, JP Cai, J LiN, Synchronization of hyperchaotic systems with multiple unknown parameters and its application in secure communication. Optik **127**, 2502–2508 (2016)
34. LF Zhang, XL An, JG Zhang, A new chaos synchronization scheme and its application to secure communications. Nonlinear. Dyn. **73**, 705–722 (2013)
35. XL An, L Zhang, JN Yu, Study on a new multistage chaos synchronized secure communication system. J. Sichuan University. **49**, 1087–1094 (2012)

Zhang *et al. EURASIP Journal on Wireless Communications and Networking* (2016) 2016:134

Page 15 of 15

36. C Xiao, SG Lian, LF Wang et al., A speed-adaptive media encryption scheme for real-time recording and playback system. EURASIP J. Wirel. Commun. Netw. **1–9**, 371513 (2010)
37. HL Chen, W Lou, X Sun et al., A secure localization approach against wormhole attacks using distance consistency. EURASIP J. Wirel. Commun. Netw. **1–11**, 627039 (2010)
38. HL Chen, W Lou, Z Wang, A novel secure localization approach in wireless sensor networks. EURASIP J. Wirel. Commun. Netw. **1–12**, 981280 (2010)
39. H Li, H Liu, S Vafi, Bipolar chaotic pulse position modulation communication system based on cyclic LDPC. EURASIP J. Wirel. Commun. Netw. **4**, 1–9 (2014)
40. F Liu, XL Chen, L Mu ZH et al., Feedback synchronization of chaotic system with application to secure communications. Acta Electronica Sinica. **28**, 46–48 (2000)
41. JY Kuang, LQ Pei, XJ Tang, A multistage chaotic synchronized system for secure communications. Acta Electronica Sinica. **27**, 23–268 (1999)
42. XL An, JN Yu, YZ Li, YD Chu, Design of a new multistage chaos synchronized system for secure communications and study on noise perturbation. Math Comput Model **54**, 7–18 (2011)
43. JY Kuang, LQ Pei, XJ Tang, RH Huang, A multistage chaos synchronized system for secure communications. Acta electronica. **27**, 23–26 (1999)
44. XP Guan, ZP Fan, HP Peng, LJ Li, A new multistage chaotic system and its application to secure communication. J. Yanshan University **25**, 287–289 (2001)
45. JF Li, N Li, A new chaotic masking method for secure communications based on Chua's circuit. Syst Eng Electron **24**, 41–43 (2002)
46. JF Li, N Li, A secure communication method for a high-power information signal based on chaotic masking. Chin Phys **11**(11), 1124–1127 (2002)
47. Z. Xu et al. Crowdsourcing based description of urban emergency events using social media big data. IEEE Transactions on Cloud Computing, 10.1109/TCC.2016.2517638
48. Z. Xu et al. Crowdsourcing based social media data analysis of urban emergency events. Multimedia Tools and Applications, 10.1007/s11042-015-2731-1
49. Z Xu et al., Participatory sensing based semantic and spatial analysis of urban emergency events using mobile social media. EURASIP J. Wirel. Commun. Netw. **2016**, 44 (2016)
50. G Zheng, D Boutat, T Floquet, JP Barbot, Secure communication based on multi-input multi-output chaotic system with large message amplitude. Chaos, Solitons & Fractals. **41**, 1510–1517 (2009)
51. N Li, JF Li, Generalized projective synchronization of chaotic system based on a single driving variable and its application in secure communication. Acta Physica Sinica **57**, 6093–6098(2008) (2008)
52. KM Short, Steps toward unmasking secure communications. Int J Bifurcat Chaos. **4**, 959–977 (1994)