

RESEARCH

Open Access



# Application adaptive exponential synchronization of chaotic dynamical systems in secure communications

Mahmoud Maheri<sup>1\*</sup> and Norihan Md Arifin<sup>2</sup>

\*Correspondence:  
mahmoud.maheri@gmail.com  
<sup>1</sup>Institute for Mathematical  
Research, University Putra Malaysia  
(UPM), Serdang, Selangor 43400,  
Malaysia  
Full list of author information is  
available at the end of the article

## Abstract

Synchronization of chaotic systems which is defined based on the exponential stability for encrypts of signals is presented in this paper. An adaptive control scheme is proposed, and the convergence of the synchronized error is guaranteed. Masking and modulation methods are applied for encryption. To verify the effectiveness of the proposed schemes, numerical simulation was applied on a well-known system without linear term chaotic using MatLab software. The comparison of the proposed chaotic synchronization in the case of the synchronization rate and in the decryption precision of sent signal and image are shown.

**Keywords:** synchronization; chaos; exponential; stability; encryption

## 1 Introduction

Chaotic systems are nonlinearly deterministic and sensitive to initial conditions, they have been studied since the two most recent decades [1–4]. Chaotic systems have a lot of applications in different sciences such as laser, secure communication, biology sciences, nonlinear circuits, neural and computer networks [5–10].

The control of chaos is one of the main issues in the study of chaotic systems. The synchronization is one of the main control methods of these systems, which were introduced in a paper by Pecorra and Carrol in 1990 [3]. In recent years, synchronization of chaotic systems has become very attractive and has been applied in vast area of engineering, physic, computer networks, and so on which aroused increasing interest as regards use in new areas such as cryptography [11–15].

Up to now, many synchronization methods such as adaptive control, nonlinear feedback control and sliding mode control were proposed and applied successfully on chaotic systems [16–21]. But almost all of them used Lyapunov stability theorems to guarantee asymptotically synchronization and convergence is slow to the origin.

The exponential synchronization is another proposed method in this field, which has certain precision and stability in error systems. This method is robust and faster than the Lyapunov stability one. Tong *et al.* [22] applied exponential synchronization for stochastic neural networks with multi-delayed and Markovian switching via adaptive feedback control, Yan and Yu [23], Lio and Yu [18] studied exponential synchronization for some

well-known classical dynamical systems. Yang used exponential stability in synchronization of a higher order chaotic system [17] *etc.*

So far, to the best of the authors' knowledge, the problem of adaptive exponential synchronization and its applications for chaotic dynamical systems have received very little research attention.

In the recent work, the authors have proposed the adaptive based on exponential stability methods to secure chaos communication through the method of chaos masking and modulation. The general idea in the utilization of chaotic systems in using a transition of the desired signal is integration of it with a chaotic system and production of a chaotic signal. This signal is recoverable after synchronization. There are two major issues in this case; one includes how to produce the chaotic signal; this is usually conducted by both masking and modulation methods [24, 25].

The other most important issue is the time of transmittance and reception of the signal. The signal is produced and transmitted after synchronization of both slave and master systems. Thus, as the synchronization rate is high, the signal, with regard to its dependency on synchronization error, could be transmitted faster with better approximation.

This paper was conducted by introducing theorems related to the exponential stability and comparison of results in the encryption of signals based on Lyapunov stability and exponential stability.

The main contributions of this paper can be highlighted as follows. (1) A new adaptive synchronization method is studied for a fully nonlinear chaotic dynamical system based on the exponential stability theorem. (2) Application of the adaptive exponential synchronization obtained in encryption using modulation and masking methods.

The paper was organized as follows. Section 2, the definitions and theorems related to exponential and Lyapunov stability were provided. In Section 3, synchronization of a system without linear term is provided. Transmission and reception of the signal text by the modulation method was given for a well-known system using exponential and Lyapunov stability in Section 4. Then the masking method and adaptive exponential stability were utilized to transmit a pictorial signal. Concluding remarks were provided in Section 5.

## 2 Preliminaries

### 2.1 Stability of autonomous systems

Consider the autonomous system

$$\dot{x} = f(x), \tag{1}$$

where  $f : D \rightarrow R^n$  is the local Lipschitz map of domain  $D \subset R^n$  to  $R^n$ .

**Definition 2.1** Suppose  $x_0 = 0$  is one of the fixed points of equation (1), in this case [26].

- It is stable if, for any  $\epsilon$ , there exists the value of  $\delta = \delta(\epsilon)$  so that

$$\|x(0)\| < \delta \implies \|x(t)\| < \epsilon, \quad \forall t > 0.$$

- It is unstable if it is not stable.
- It is asymptotically stable, if it is stable and there exist  $\delta$  so that

$$\|x(0)\| < \delta \implies \lim_{t \rightarrow \infty} x(t) = 0.$$

For studying stability, a practical way is finding a Lyapunov function in linear and non-linear systems without obtaining the response of them.

**Theorem 2.1** (Lyapunov stability theorem) *Suppose  $\dot{x} = f(x)$ ,  $x \in D \subseteq R^n$  to have a fixed point in the origin. If there exists a real function  $V$  in a neighborhood of  $N$  at the origin [27] where:*

- $\frac{\partial V}{\partial x_i}$ ,  $i = 1, 2, \dots, n$ , exists and is continuous;
- $V$  is positive definite,

then:

- If  $\dot{V}$  is semi negative definite, then the origin is a stable fixed point of the system.
- If  $\dot{V}$  is negative definite, then the origin is a fixed point and asymptotically stable.
- If  $\dot{V}$  is positive definite, then the origin is an unstable fixed point.

### 2.2 Stability of non-autonomous systems

Consider the following non-autonomous system:

$$\dot{x} = f(t, x), \tag{2}$$

where the function  $f : [0, \infty) \times D \rightarrow R^n$  is piecewise continuous with respect to  $t$  and is local Lipschitz with respect to  $x$  on  $[0, \infty) \times D$ , which includes the origin. In this case  $x = 0$  is the fixed point of equation (2) on  $t = 0$  if

$$f(t, 0) = 0, \quad \forall t \geq 0.$$

It could be interpreted as follows: the fixed point is located on the origin as a non-zero fixed point or in a more general case, as the non-zero response of system.

The concepts of stability and asymptotically stability of a fixed point in non-autonomous systems correspond to Definition 2.1 in autonomous systems unless there is a new case, in that the response of autonomous system only depends on  $(t - t_0)$ , and the response of the non-autonomous system also depends on both  $t$  and  $t_0$ . Thus, in the general state, the stability of fixed point depends on  $t_0$ .

**Definition 2.2** Fixed point  $x = 0$  related to equation (2):

- It is stable if, for any  $\epsilon > 0$ , the value of  $\delta = \delta(\epsilon, t_0)$  is such that

$$\|x(t_0)\| < \delta \quad \Rightarrow \quad \|x(t)\| < \epsilon, \quad \forall t \geq t_0 \geq 0. \tag{3}$$

- It is uniformly stable if, for any  $\epsilon > 0$ , the value of  $\delta = \delta(\epsilon)$  (independent of  $t_0$ ) is such that equation (3) holds.
- It is unstable, if is not stable.
- It is asymptotically stable if is stable and there is a value such as  $c = c(t_0) > 0$  so that, for all values of  $\|x(t_0)\| < c$ , we have  $\lim_{t \rightarrow \infty} x(t) = 0$ .
- It is uniform asymptotically stable if it is uniformly stable and there is a value such as  $c > 0$  (independent of  $t_0$ ) so that, for all values of  $\|x(t_0)\| < c$ , as  $t_0$  tends to infinity,  $x(t)$  monotonically tends to zero with respect to  $t_0$ , in other words, for any  $\epsilon > 0$ , there exists a value such as  $t = T(\epsilon)$  so that

$$\|x(t)\| < \epsilon, \quad \forall t \geq t_0 + T(\epsilon), \forall \|x(t_0)\| < c.$$

- It is globally uniform asymptotically stable, if it is uniformly stable and, for any pair of positive numbers  $\epsilon$  and  $c$ , there is a value  $t = T(\epsilon, c) > 0$  so that

$$\|x(t)\| < \epsilon, \quad \forall t \geq t_0 + T(\epsilon, c), \forall \|x(t_0)\| < c.$$

The uniform stability and uniform asymptotical stability could also be indicated based on specific numerical functions, *i.e.* class  $\kappa$  and class  $\kappa\iota$  functions [28].

**Definition 2.3** The continuous function  $\alpha : [0, a) \rightarrow [0, \infty)$  belongs to class  $\kappa$  if it strictly is increasing and  $\alpha(0) = 0$ . This function belongs to  $\kappa_\infty$  if  $a = \infty$  and with  $r$  increasing to infinity,  $\alpha(r)$  also tends to infinity.

**Definition 2.4** The continuous function  $\beta : [0, a) \times [0, \infty) \rightarrow [0, \infty)$  belongs to class  $\kappa\iota$  if for any specific value  $s$ , the mapping  $\beta(r, s)$  with respect to  $r$  belongs to class  $\kappa$  and also for any specific value  $r$ , the mapping  $\beta(r, s)$  is decreasing with respect to  $s$ , and by increasing  $s$  to infinity,  $\beta(r, s)$  tends to zero.

**Example 2.1** The function  $\alpha(r) = \arctan r$  is increasing strictly because  $\dot{\alpha}(r) = 1/(1+r^2) > 0$ . This function belongs to class  $\kappa$ , but it does not belong to class  $\kappa_\infty$ , because  $\lim_{r \rightarrow \infty} \alpha(r) = \pi/2 < \infty$ .

The following lemma indicates some of explicit features of functions, class  $\kappa$  and  $\kappa\iota$ .

**Lemma 2.2** Suppose  $\alpha_1(\cdot)$  and  $\alpha_2(\cdot)$  in the interval  $[0, a)$  are class  $\kappa$  functions and  $\alpha_3(\cdot)$  and  $\alpha_4(\cdot)$  to be class  $\kappa_\infty$  ones. If we show the converse of  $\alpha_i(\cdot)$  with  $\alpha_i^{-1}(\cdot)$ , then we have [29]

- $\alpha_1^{-1}(\cdot)$  is defined in the interval  $[0, \alpha_1(a)]$  belongs to class  $\kappa$ .
- $\alpha_3^{-1}(\cdot)$  is defined in the interval  $[0, \infty)$  and belongs to class  $\kappa_\infty$ .
- $\alpha_1\alpha_2$  belongs to class  $\kappa_\infty$ .
- $\alpha_3\alpha_4$  belongs to class  $\kappa_\infty$ .
- $\sigma(r, s) = \alpha_1(\beta(\alpha_2(r), s))$  belongs to class  $\kappa_\infty$ .

The following lemma explains the equivalence definitions for uniform stability and uniformly asymptotically stability based on class  $\kappa$  and  $\kappa\iota$  functions.

**Lemma 2.3** ([30]) For the fixed point  $x = 0$  related to equation (2):

- It is uniformly stable, if and only if function  $\alpha(\cdot)$  belongs to class  $\kappa$  and there is a positive constant  $c$  (independent of  $t_0$ ) so that

$$\|x(t)\| \leq \alpha(\|x(t_0)\|), \quad \forall t \geq t_0 \geq 0, \forall \|x(t_0)\| < c. \tag{4}$$

- It is uniformly asymptotically stable, if and only if function  $\beta(\cdot, \cdot)$  belongs to class  $\kappa\iota$  and there is a positive constant  $c$  (independent of  $t_0$ ) so that

$$\|x(t)\| \leq \beta(\|x(t_0)\|), \quad \forall t \geq t_0 \geq 0, \forall \|x(t_0)\| < c. \tag{5}$$

- It is globally uniform asymptotically stable if and only if inequality (5) holds for any initial state of  $x(t_0)$ .

### 2.3 Exponential stability

As one of Lemma 2.3 results, it could be considered that in the case of non-autonomous systems, the stability and asymptotical stability based on definition (1) mean that there are functions of class  $\kappa$  and  $\kappa_l$  so that inequality (4) and (5) hold. Because in the non-autonomous systems, the stability and asymptotically stability of origin are uniform with respect to the initial time  $t_0$ .

One particular case of uniform asymptotically stability occurs when, in equation (5), the function  $\beta$  belongs to class  $\kappa_l$  as  $\beta(r, s) = kre^{-\gamma s}$ . This case is very important and could be considered one of distinctive features of fixed point stability.

**Definition 2.5** The fixed point  $x = 0$  related to equation (2) is exponentially stable, if inequality (5) holds for any of the following values:

$$\beta(r, s) = kre^{-\gamma s}, \quad k > 0, \gamma > 0.$$

In addition, it is globally exponentially stable if the above condition holds for all initial values.

Now, we explain the main theorem.

**Theorem 2.4** Suppose  $x = 0$  to be one of the fixed points of equation (2) and  $D \subset R^n$  to be a domain including the origin. In addition, suppose  $V(x) : [0, \infty) \times D \rightarrow R$  to be a continuous and derivable function where for all values of  $t \geq 0$  and  $x \in D$  the following relations are satisfied:

$$\omega_1(x) \leq V(t, x) \leq \omega_2(x), \tag{6}$$

$$\frac{\partial V}{\partial t} + \frac{\partial V}{\partial x} f(t, x) \leq -\omega_3(x), \tag{7}$$

where  $\omega_1(x)$ ,  $\omega_2(x)$  and  $\omega_3(x)$  are positive definite and continuous functions on  $D$ . Then the point  $x = 0$  is uniformly asymptotically stable [31].

If the class  $\kappa$  functions are of the particular form  $\alpha_i(r) = k_i r^c$ , its application is easy in the proof of Theorem 2.4. In this case, it could be shown that the origin is exponentially stable.

**Theorem 2.5** Suppose all hypotheses of Theorem 2.4 are satisfied along with the following conditions:

$$\omega_1(x) \geq k_1 \|x\|^c, \quad \omega_2(x) \leq k_2 \|x\|^c, \quad \omega_3(x) \geq k_3 \|x\|^c,$$

when  $k_1, k_2, k_3$  and  $c$  are positive constants, then  $x = 0$  is exponentially stable. Also, if all globally hypotheses hold,  $x = 0$  is globally exponentially stable [29].

*Proof* The functions  $V$  and  $\dot{V}$  satisfy the following inequalities:

$$\begin{aligned} k_1 \|x\|^c &\leq V(t, x) \leq k_2 \|x\|^c, \\ \dot{V} &\leq -k_3 \|x\|^c \leq -\frac{k_3}{k_2} V(t, x). \end{aligned} \tag{8}$$

By using the deduction lemma, we could write

$$V(t, x(t)) \leq V(t, x(t_0))e^{-(k_3/k_2)(t-t_0)}.$$

Therefore,

$$\|x(t)\| \leq \left[ \frac{V(t, x(t))}{k_1} \right]^{1/c} \tag{9}$$

$$\leq \left[ \frac{V(t_0, x(t_0))e^{-(k_3/k_2)(t-t_0)}}{k_1} \right]^{1/c}$$

$$\leq \left[ \frac{k_2 \|x(t_0)\|^c e^{-(k_3/k_2)(t-t_0)}}{k_1} \right]^{1/c}$$

$$= \left( \frac{k_2}{k_1} \right)^{1/c} \|x(t_0)\| e^{-(k_3/k_2c)(t-t_0)}. \tag{10}$$

As a result, the origin is exponentially stable, so that all hypotheses are satisfied globally, the above inequality would hold for all values of  $x(t_0) \in R^n$ . □

### 3 Synchronization based on the exponential stability

In this section, the synchronization system without linear term is introduced based on exponential and Lyapunov stability using nonlinear control functions.

Consider the nonlinear chaotic system [32]

$$\begin{aligned} \dot{x}_1 &= \ln(a + e^{y_1-x_1}), \\ \dot{y}_1 &= x_1 z_1, \\ \dot{z}_1 &= b - x_1 y_1, \end{aligned} \tag{11}$$

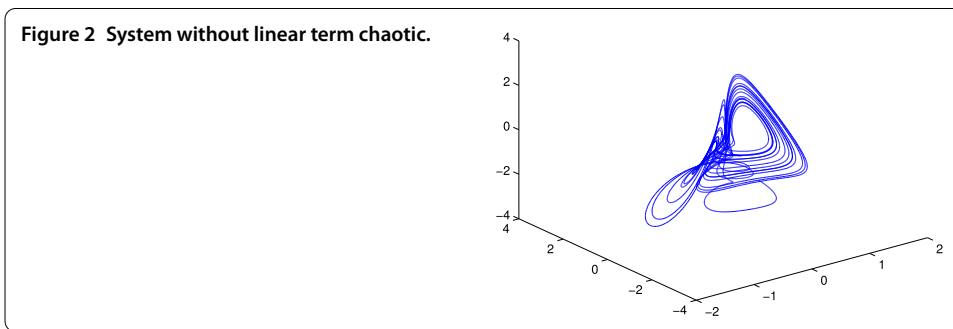
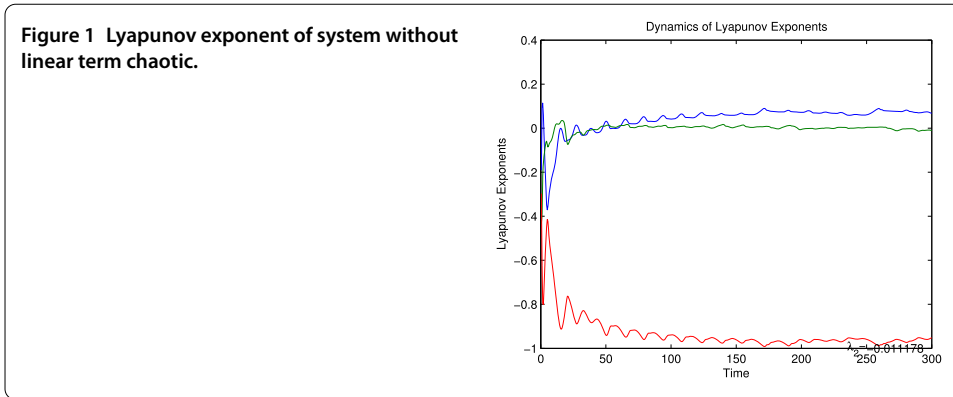
where  $x_1, y_1$  and  $z_1$  are the state variables and  $a, b$  are real parameters. Figures 1 and 2 show the Lyapunov exponent and the chaotic behavior of the system (11) for  $a = 0.1$  and  $b = 0.25$ .

For synchronization, let system (11) be the drive system and the corresponding response system be written as follows:

$$\begin{aligned} \dot{x}_2 &= \ln(a + e^{y_2-x_2}) + u_1, \\ \dot{y}_2 &= x_2 z_2 + u_2, \\ \dot{z}_2 &= b - x_2 y_2 + u_3, \end{aligned} \tag{12}$$

where  $u_1, u_2$  and  $u_3$  are the input nonlinear control functions. By defining the synchronization error as  $e_1 = x_2 - x_1, e_2 = y_2 - y_1, e_3 = z_2 - z_1$ , and using equation (12), the synchronization error dynamics can be written as

$$\begin{aligned} \dot{e}_1 &= \ln\left( \frac{a + e^{e_2-e_1} e^{y_1-x_1}}{a + e^{y_1-x_1}} \right) + u_1, \\ \dot{e}_2 &= e_1 e_3 + e_1 z_1 + e_3 x_1 + u_2, \\ \dot{e}_3 &= -(e_2 e_1 + y_1 e_1 + x_1 e_2) + u_3. \end{aligned} \tag{13}$$



**Definition 3.1** The response system (12) will synchronize exponentially with the drive system (11) for any initial values if the error system satisfies the following estimation:

$$E(t)^T E(t) \leq \alpha e^{-\sigma(t-t_0)}, \tag{14}$$

where  $E^T = [e_1(t), e_2(t), e_3(t)]$  and  $\alpha, \sigma$  are positive constants, respectively, dependent and independent from  $E(t_0)$ , which is called the convergence rate. In this case the zero solution of error system (13) is stable and the two systems (11) and (12) are called synchronized [17].

**Lemma 3.1** The system (13) can be exponentially stabilized at the origin if there exists a positive definite function  $V(t)$  such that

$$k_1 E^T(t)E(t) \leq V(t) \leq k_2 E^T(t)E(t), \tag{15}$$

$$\dot{V}(t) \leq -k_3 E^T(t)E(t), \tag{16}$$

where  $k_1, k_2$  and  $k_3$  are positive constants,  $V(t) \equiv V(E(t))$  and  $k_1 \leq k_2$ . Therefore, the drive system (11) and the response system (12) are exponentially synchronized [17].

*Proof* Let  $V(t) = E(t)PE^T(t)$  where  $P$  is a symmetric positive definite matrix. Choose  $k_1 = \lambda_{\min}(P) > 0$  and  $k_2 = \lambda_{\max}(P) > 0$  where  $k_1$  and  $k_2$  are minimum and maximum eigenvalues of the matrix  $P$ . Then the time derivative of  $V(t)$  satisfies the inequality

$$\dot{V}(t) \leq -\frac{k_3}{k_2} V(t) = -\sigma V(t), \quad \sigma = \frac{k_3}{k_2} > 0. \tag{17}$$

It can be concluded that

$$V(t) \leq V(t_0)e^{\sigma(t-t_0)}. \tag{18}$$

Hence

$$E^T(t)E(t) \leq \frac{V(t)}{k_1} \leq \frac{V(t_0)}{k_1}e^{-\sigma(t-t_0)} \leq \frac{k_2}{k_1}E^T(t_0)E(t_0)e^{-\sigma(t-t_0)}. \tag{19}$$

From Definition 3.1,  $\alpha = \frac{k_2}{k_1}E^T(t_0)E(t_0)$ . Therefore, in this case, system (13) is exponentially stable and the synchronization of the drive system (12) and the response system (11) sufficiently achieved.  $\square$

**Lemma 3.2** For any  $k \in R^+$  and  $x, y \in R$  the following inequality holds:

$$2|x||y| \leq kx^2 + k^{-1}y^2. \tag{20}$$

**Theorem 3.3** The drive system (11) and response system (12) are exponentially synchronized if the nonlinear feedback controls are chosen as

$$\begin{aligned} u_1 &= -C - \omega_1 e_1, \\ u_2 &= -\omega_1 e_2, \\ u_3 &= -\omega_3 e_3, \end{aligned} \tag{21}$$

and

$$\begin{aligned} C &> \ln\left(\frac{a + \text{Exp}(e_2 - e_1)\text{Exp}(y_1 - x_1)}{a + \text{Exp}(y_1 - x_1)}\right), \\ \omega_1 &> \frac{1}{2}\left(\frac{k_3}{\rho_1} + \frac{k_2}{\rho_2}\right), \\ \omega_2 &> \frac{1}{2}(k_3\rho_1), \\ \omega_3 &> \frac{1}{2}(k_2\rho_2), \end{aligned} \tag{22}$$

where  $\omega_1, \omega_2, \omega_3 > 0$ ,  $|x_1| < k_1$ ,  $|y_1| < k_2$  and  $|z_1| < k_3$  and  $\rho_1$  and  $\rho_2$  are positive constants.

*Proof* Let

$$V(t) = E^T P E = \frac{1}{2}e_1^2 + e_2^2 + e_3^2, \tag{23}$$

where  $P = \text{diag}(1/4, 1/2, 1/2)$  is diagonal positive definite matrix. The time derivative of the function (23) for the error system (13) and control laws (21) are

$$\begin{aligned} \dot{V}(t) &= \dot{e}_1 e_1 + \dot{e}_2 e_2 + \dot{e}_3 e_3 \\ &= e_1 \left( \ln\left(\frac{a + \text{Exp}(e_2 - e_1)\text{Exp}(y_1 - x_1)}{a + \text{Exp}(y_1 - x_1)} + u_1\right) \right) + e_2(e_1 e_3 + e_1 z_1 + e_3 x_1 + u_2) \\ &\quad + e_3(-e_1 e_2 + e_1 y_1 + e_2 x_1 + u_3). \end{aligned} \tag{24}$$



Substituting (22) in (24) yields

$$\begin{aligned} \dot{V}(t) &< -(\omega_1 e_1^2 + \omega_2 e_2^2 + \omega_3 e_3^2) + e_2 e_1 z_1 - y_1 e_3 e_1 \\ &< -(\omega_1 e_1^2 + \omega_2 e_2^2 + \omega_3 e_3^2) + k_3 |e_2| |e_1| + k_2 |e_3| |e_1|. \end{aligned} \tag{25}$$

From Lemma 3.2, for any  $\rho_1$  and  $\rho_2$ , we obtain

$$\begin{aligned} \dot{V}(t) &< -(\omega_1 e_1^2 + \omega_2 e_2^2 + \omega_3 e_3^2) + \frac{k_3}{2} (\rho_1 e_2^2 + \rho_1^{-1} e_1^2) + \frac{k_2}{2} (\rho_2 e_3^2 + \rho_2^{-1} e_1^2) \\ &= -e_1^2 \left( \omega_1 - \frac{k_3}{2\rho_1} - \frac{k_2}{2\rho_2} \right) - e_2^2 \left( \omega_2 - \frac{k_3\rho_1}{2} \right) - e_3^2 \left( \omega_3 - \frac{k_2\rho_2}{2} \right). \end{aligned} \tag{26}$$

For  $\omega_1, \omega_2, \omega_3 > 0$ , then

$$\begin{aligned} \omega_1 &> \frac{k_3}{2\rho_1} + \frac{k_2}{2\rho_2}, \\ \omega_2 &> \frac{k_3\rho_1}{2}, \\ \omega_3 &> \frac{k_2\rho_2}{2}. \end{aligned} \tag{27}$$

Therefore,

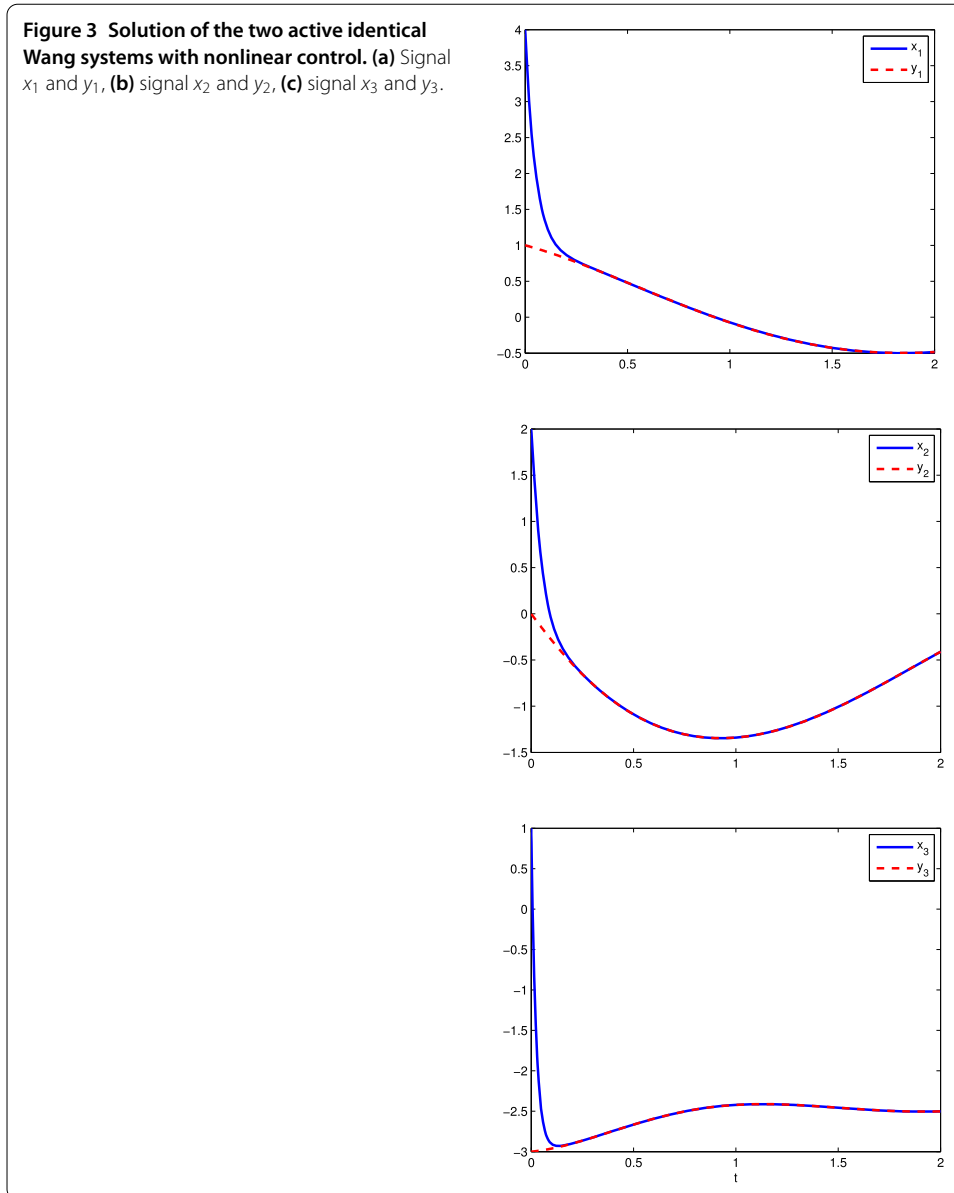
$$\dot{V}(t) < -\alpha E^T E, \tag{28}$$

where  $\alpha = \min\{\omega_1 - \frac{k_3}{2\rho_1} - \frac{k_2}{2\rho_2}, \omega_2 - \frac{k_3\rho_1}{2}, \omega_3 - \frac{k_2\rho_2}{2}\}$ . According to Lemma 3.1 and inequality (28), the systems (11) and (12) are exponentially synchronized.  $\square$

Simulation results: to show the validity of the proposed method, MatLab software is applied for synchronization of the drive system (11) and the response system (12) using control laws (21). The initial conditions for drive and response systems, respectively, are chosen as  $(x_1(0), y_1(0), z_1(0)) = (1, -1, 2)$  and  $(x_2(0), y_2(0), z_2(0)) = (3, 1, -1)$ . Figures 3 and 4 show the simulation results for the drive-response and error system, which confirms that the error system converges to zero and the two systems are exponentially synchronized.

To show the advantage of our applied exponential synchronization method using a non-linear control function, the results are compared with synchronization based on the Lyapunov stability theorem. For the same system and initial conditions as shown in Figure 5, it is obvious that our methods have the advantage by compression synchronization times in Figure 3 of almost 0.1 second over approximately 4 second in Figure 5.

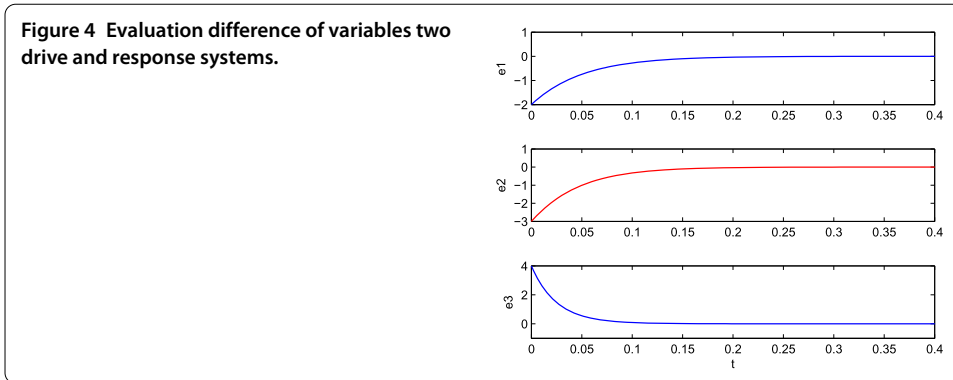
The main benefit of the exponential synchronization method is the fast convergence. But there is a disadvantage in that, in practice, for some systems it is impossible or very difficult to obtain the exponential synchronization conditions. In this case, the exponential synchronization will change to synchronization based on the Lyapunov stability theorem. In simple terms, we can say exponential stability is Lyapunov stability, but the reverse is not true.



#### 4 Application of chaos to secure communication

Encryption of information is carried out when two persons want to communicate with each other by an insecure communicative channel that can be a telephone or network but the third person could not identify the exchanged information by listening to them. What the first person wants to send to the second person is called the context text; it can be an image or a text by any language that is completely optional. Before sending the message, the transmitter of information should encrypt the information by a specific key. In this case, the context text is converted into the encrypted text. The encrypted text passes through a communicative channel of two individuals and the second person could decrypt the text by using the key and the text is converted into a context text.

Our goal is to use chaotic systems for encryption. Since aperiodic waves of the chaotic systems cannot be predicted, these systems are important in secure communication. Also chaotic systems are sensitive to initial conditions, which is another advantage for using



these systems in different applications of secure communication. Here encryption using modulation and the masking method is studied.

#### 4.1 Text modulation via adaptive exponential stability

In chaos modulation the information signal is injected into the transmitter. First we introduce some definitions, then we propose a fast mechanism for synchronization the chaotic systems without linear term (11) based on the drive-response approach. Using exponential synchronization, the secure communication scheme is studied.

**Definition 4.1** ([33]) Consider the smooth system that is described by a variables vector  $X = \{x_i\}_1^n \in R^1$  where the output vector is presented by  $Y = \{y_i\}_1^m \in R^1$ :

$$\dot{x} = f(X, C), \quad Y = h(X), \tag{29}$$

where the function  $h(\cdot)$  is a smooth vector and the vector  $C \in R^1$  is for constant parameters. Let  $Y^i$ , denote the  $j$ th time derivative of the vector  $Y$ . It is said that the vector state  $X$  is observable algebraically, if it is expressed uniquely by

$$X = \phi(Y, Y^{(1)}, \dots, Y^{(i)}), \tag{30}$$

for integer  $j$  and for smooth function  $\phi$ .

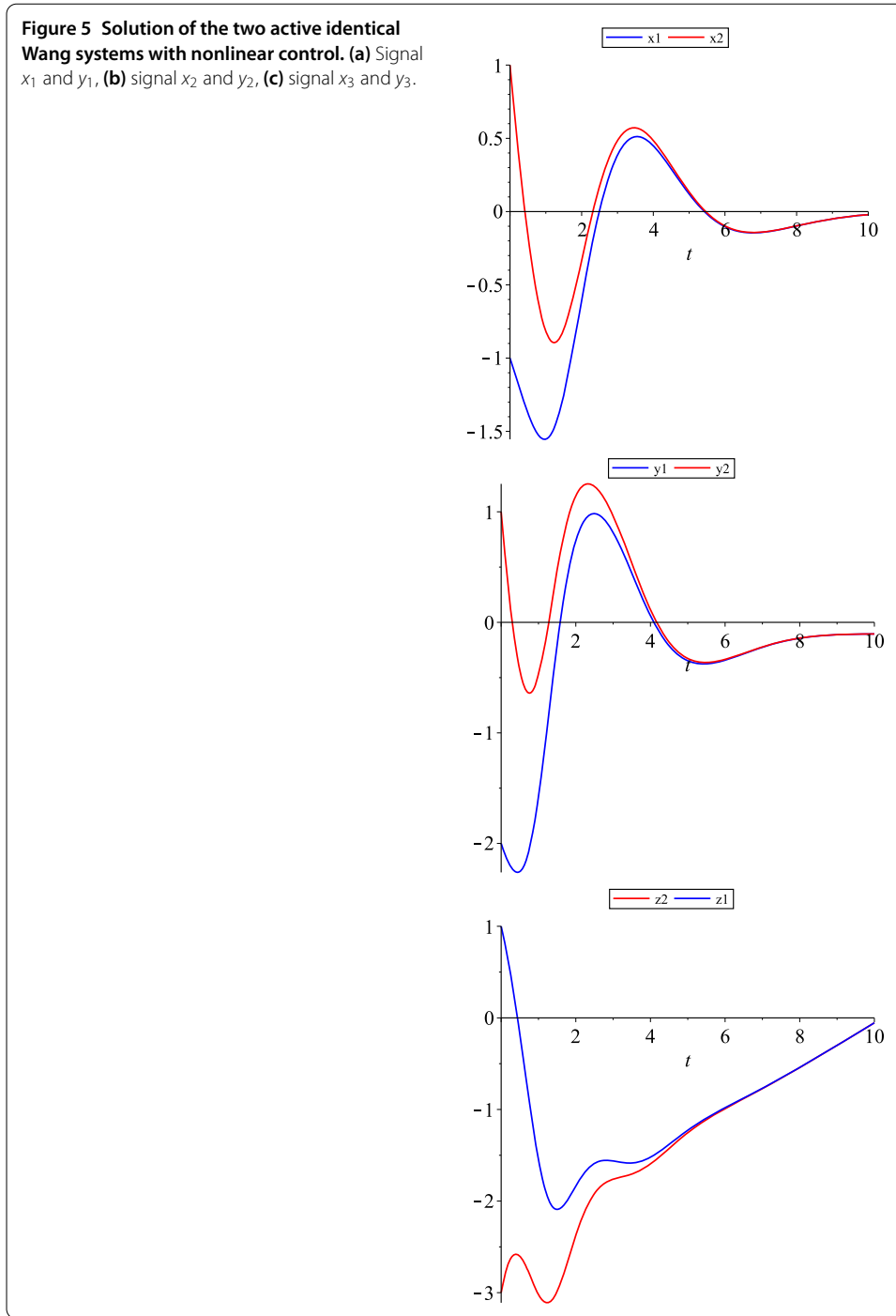
**Definition 4.2** ([33]) With the same conditions of Definition 4.2, if the vector of parameters,  $C$ , satisfies the following equation:

$$\psi_1(Y, Y^{(1)}, \dots, Y^{(i)}) = \psi_2(G, G^{(1)}, \dots, G^{(i)})C, \tag{31}$$

where  $\psi_1(\cdot)$  and  $\psi_2(\cdot)$  are, respectively,  $n \times 1$  and  $n \times n$  smooth parameters matrices, then  $C$  is said to be identifiable algebraically with respect to the output vector  $Y$ .

Now, assume the second differential equation of system (11) to be

$$x_1 = \frac{\dot{y}_1}{z_1}, \tag{32}$$



then substituting equation (32) into the third differential variables of system (11) leads to

$$\dot{z}_1 z_1 + \dot{y}_1 y_1 = b z_1. \tag{33}$$

According to Definitions 4.1 and 4.2 the system (11) is observable algebraically with respect to the two outputs  $y_1$  and  $z_1$ . The parameter  $b$  in equations (33) and (11) is identifiable algebraically with respect to the two other available outputs. Therefore, the non-available

state variable  $x_1$  and the parameter  $b$  can be recovered simultaneously from the two other available outputs.

In the transmitter system, the parameter  $b$  is considered to transmit the message signal and the following drive system is defined:

$$\begin{aligned} \dot{x}_1 &= \ln(a + e^{y_1 - x_1}), \\ \dot{y}_1 &= x_1 z_1, \\ \dot{z}_1 &= b(t) - x_1 y_1, \end{aligned} \tag{34}$$

where  $x_1, y_1, z_1$  are the state variables of chaotic system (11) with the modulation law

$$b(t) = o(t) + b, \tag{35}$$

where  $o(t)$  is the input message signal, which needs to be transmitted. In the receiver system, the response system is assumed to be the partly uncertain system (11) where the available outputs variables are  $y_1$  and  $z_1$ . Hence, the response system is defined with controllers as follows:

$$\begin{aligned} \dot{x}_2 &= \ln(a + e^{y_1 - x_2}) + u_1, \\ \dot{y}_2 &= x_2 z_1 + u_2, \\ \dot{z}_2 &= \hat{b}(t) - x_2 y_1 + u_3, \end{aligned} \tag{36}$$

where  $x_2, y_2$  and  $z_2$  are the state variables of system (11) with the modulation laws

$$\hat{b}(t) = \hat{o}(t) + \hat{b}, \tag{37}$$

where  $\hat{o}(t)$  is the recovered signal and  $\hat{b}$  is the approximation of the unknown parameter  $b$ .  $U = [u_1, u_2, u_3]^T$  is the input nonlinear control to achieve synchronization of the systems (34) and (36).

Subtracting the drive system (34) from the response system (36), the error system is obtained:

$$\begin{aligned} \dot{e}_1 &= \ln\left(\frac{a + e^{-e_1} e^{y_1 - x_1}}{a + e^{y_1 - x_1}}\right) + u_1, \\ \dot{e}_2 &= e_1 z_1 + u_2, \\ \dot{e}_3 &= \tilde{o}(t) + \tilde{b}(t) - e_1 y_1 + u_3, \end{aligned} \tag{38}$$

where

$$\tilde{o} = \hat{o} - o, \quad \tilde{b} = \hat{b} - b. \tag{39}$$

Therefore, for chaos synchronization, we need to define the controller  $U$  and a parameter approximation law to set the error system to converge to zero exponentially.

**Theorem 4.1** *If the controller in the receiver system (36) is defined as follows:*

$$\begin{aligned} \dot{u}_1 &= -c - 2\omega_1 e_1, \\ \dot{u}_2 &= -\omega_2 e_2, \\ \dot{u}_3 &= -\omega_3 e_3, \end{aligned} \tag{40}$$

*with the law parameter and message signal, respectively, chosen as*

$$\begin{aligned} \dot{\tilde{o}} &= -e_3 - \omega_5 \tilde{o}, \\ \dot{\tilde{b}} &= -e_3 - \omega_4 \tilde{b}, \end{aligned} \tag{41}$$

and

$$\begin{aligned} c &> \ln\left(\frac{a + \text{Exp}(-e_1) \text{Exp}(\gamma_1 - x_1)}{a + \text{Exp}(\gamma_1 - x_1)}\right), \\ \omega_1 &> \frac{1}{2} \left( \frac{k_3}{\rho_1} + \frac{k_2}{\rho_2} \right), \\ \omega_2 &> \frac{k_3}{2\rho_1}, \\ \omega_3 &> \frac{k_2}{2\rho_2}, \\ \omega_4 &> 0, \\ \omega_5 &> 0, \end{aligned} \tag{42}$$

where  $\omega_1, \omega_2, \omega_3, \omega_4, \rho_1, \rho_2$  are positive and  $|x_i| < k_i, i = 1, 2, 3$ , then the response system (36) will synchronize the drive system (34) exponentially. Moreover, the message signal  $s(t)$  will recover by the receiver system (36), which is combined into the chaotic transmitter (34) via the modulation laws (40) and (42).

*Proof* Assume  $E = [e_1, e_2, e_3, \tilde{b}, \tilde{o}]$ , by defining the quadratic Lyapunov function as

$$V(t) = EPE^T = \frac{1}{4}e_1^2 + \frac{1}{2}e_2^2 + \frac{1}{2}e_3^2 + \frac{1}{2}\tilde{b}^2 + \frac{1}{2}\tilde{o}^2, \tag{43}$$

by the same proof as Theorem 3.3 exponential stability can be achieved. □

To demonstrate and verify the validity of the modulation schemes, we confirmed our analytical studies by numerical simulations via MatLab software. We solve the dynamical systems using the fourth order Runge-Kutta numerical method. At the transmitter system side, the system parameters are chosen as  $a = 0.1, b = 0.25$ , while the arbitrary initial conditions are set as  $x_1(0) = 1, x_2(0) = 1, x_3(0) = -3$ . At the receiver system side, we fix the arbitrary initial conditions as  $\gamma_1(0) = -1, \gamma_2(0) = -2, \gamma_3(0) = 1, a = 0.1, \hat{b}(0) = 1$  and  $\hat{o}(0) = 0.8$ . Suppose the message signal  $o(t)$  is a trigonometric signal such as

$$o(t) = 0.05 \sin(60\pi t).$$

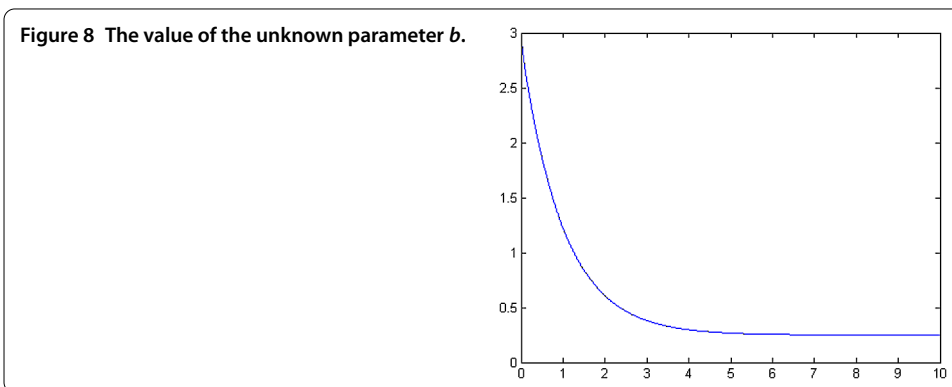
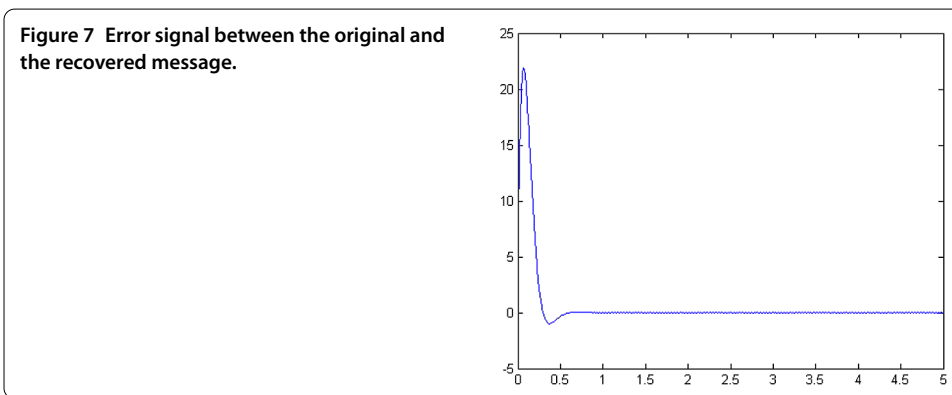
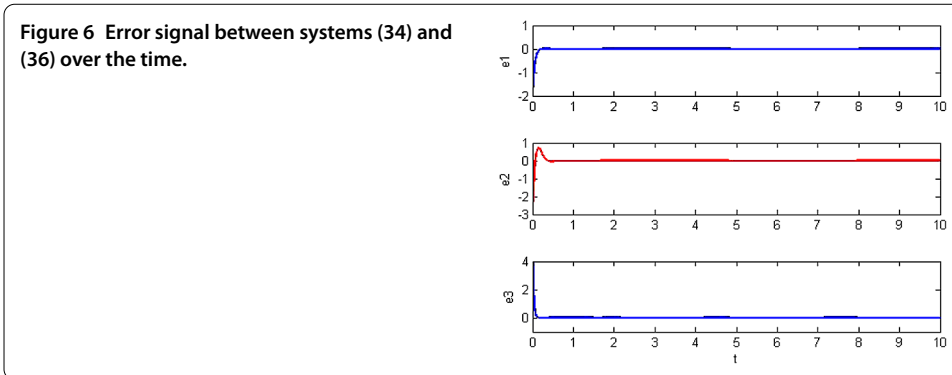


Figure 6 displays the synchronization difference (error) between systems (34) and (36). It confirms that synchronized errors between system (34) and (36) converge exponentially to zero. Figure 7 shows the error signal between the original message and the recovered one that confirms the message signal  $o(t)$  is recovered accurately. Figure 8 shows the value of the unknown parameters  $b$  which converge exponentially to the exact value.

#### 4.2 Modulation-based adaptive Lyapunov stability

Consider two drive and response systems, respectively, as drive system

$$\begin{aligned}
 \dot{x}_1 &= \ln(a + e^{y_1 - x_1}), \\
 \dot{y}_1 &= x_1 z_1, \\
 \dot{z}_1 &= b - x_1 y_1,
 \end{aligned}
 \tag{44}$$

and

$$\begin{aligned} \dot{x}_2 &= \ln(a + e^{y_2 - x_2}) + u_1, \\ \dot{y}_2 &= x_2 z_2 + u_2, \\ \dot{z}_2 &= b - x_2 y_2 + u_3. \end{aligned} \tag{45}$$

We have introduced the three control functions  $u_1, u_2$  and  $u_3$  and define the error variables as

$$e_1 = y_1 - x_1, \quad e_2 = y_2 - x_2, \quad e_3 = y_3 - x_3. \tag{46}$$

Subtracting (44) from (45) and using the notation (46), we obtain the error system as

$$\begin{aligned} \dot{e}_1 &= \ln(a + e^{y_2 - x_2}) - \ln(a + e^{y_1 - x_1}) + u_1, \\ \dot{e}_2 &= x_2 z_2 - x_1 z_1 + u_2, \\ \dot{e}_3 &= -y_2 x_2 + y_1 x_1 + u_3. \end{aligned} \tag{47}$$

**Theorem 4.2** *For any initial conditions, if the controller functions  $u_1, u_2$  and  $u_3$  are designed with*

$$\begin{aligned} u_1 &= \ln\left(\frac{a + e^{y_1 - x_1}}{a + e^{y_2 - x_2}}\right) - e_1, \\ u_2 &= e_3 e_1 + e_1 z_1 + x_1 e_3 - e_2, \\ u_3 &= -e_1 e_2 - e_2 x_1 - e_1 y_1 - e_3, \end{aligned} \tag{48}$$

and the updating laws of the unknown parameters are chosen by

$$\dot{\hat{a}}(t) = \tilde{a}_1, \quad \dot{\hat{b}}(t) = \tilde{b}_1, \tag{49}$$

where  $\hat{a} = a - \tilde{a}$  and  $\hat{b} = b - \tilde{b}$  are the estimates of the unknown parameters,  $a$  and  $b$ , then the trajectory of the error system converge to zero exponentially.

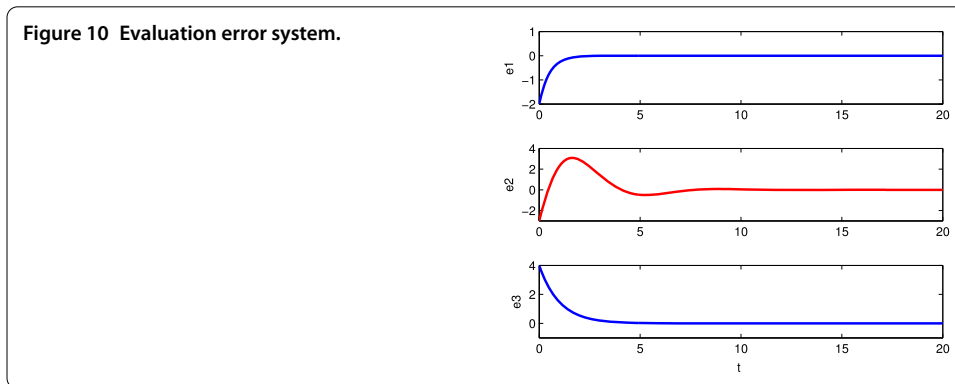
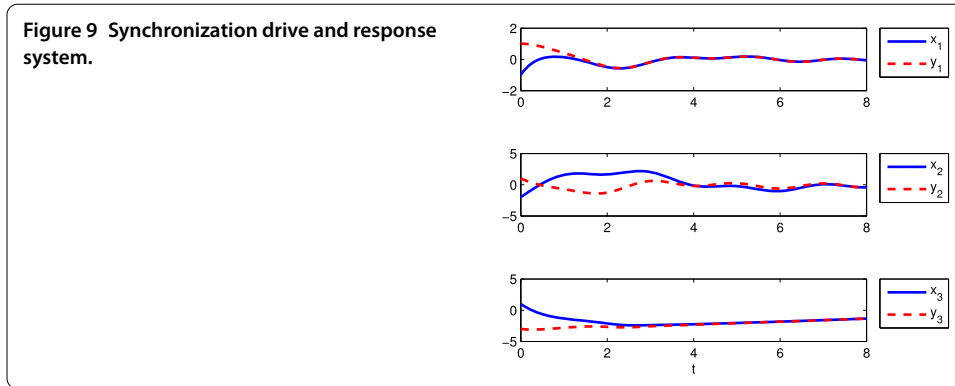
*Proof* If the positive Lyapunov function is chosen as

$$V = \frac{1}{2}(e_1^2 + e_2^2 + \tilde{a}^2 + \tilde{b}^2),$$

with the choice of the controller (48) and updating laws (49), then the time derivative of  $V$  along the trajectory of the system (44) and (45) is negative definite. So, according to the Lyapunov theorem, the synchronization of systems (44) and (45) is achieved under the chosen controller  $u$  and parameters updating laws.  $\square$

To demonstrate and verify the validity of the modulation schemes, we confirmed our analytical studies be numerical simulations via MatLab software. We solve the dynamical systems using the fourth order Runge-Kutta numerical method. At the transmitter system





side, the system parameters are chosen as  $a = 0.1$ ,  $b = 0.25$  while the arbitrary initial conditions are set as  $x_1(0) = 1$ ,  $y_1(0) = 1$ ,  $z_1(0) = -3$ . At the receiver system side, we fix the arbitrary initial conditions as  $x_2(0) = -1$ ,  $y_2(0) = -2$ ,  $z_2(0) = 1$ ,  $a = 0.1$ ,  $\hat{b}(0) = 1$  and  $\hat{\delta}(0) = 0.8$ . Suppose the message signal  $o(t)$  is trigonometric signal such as  $o(t) = 0.05 \sin(60\pi t)$ , which is added on the second state variable of the drive system.

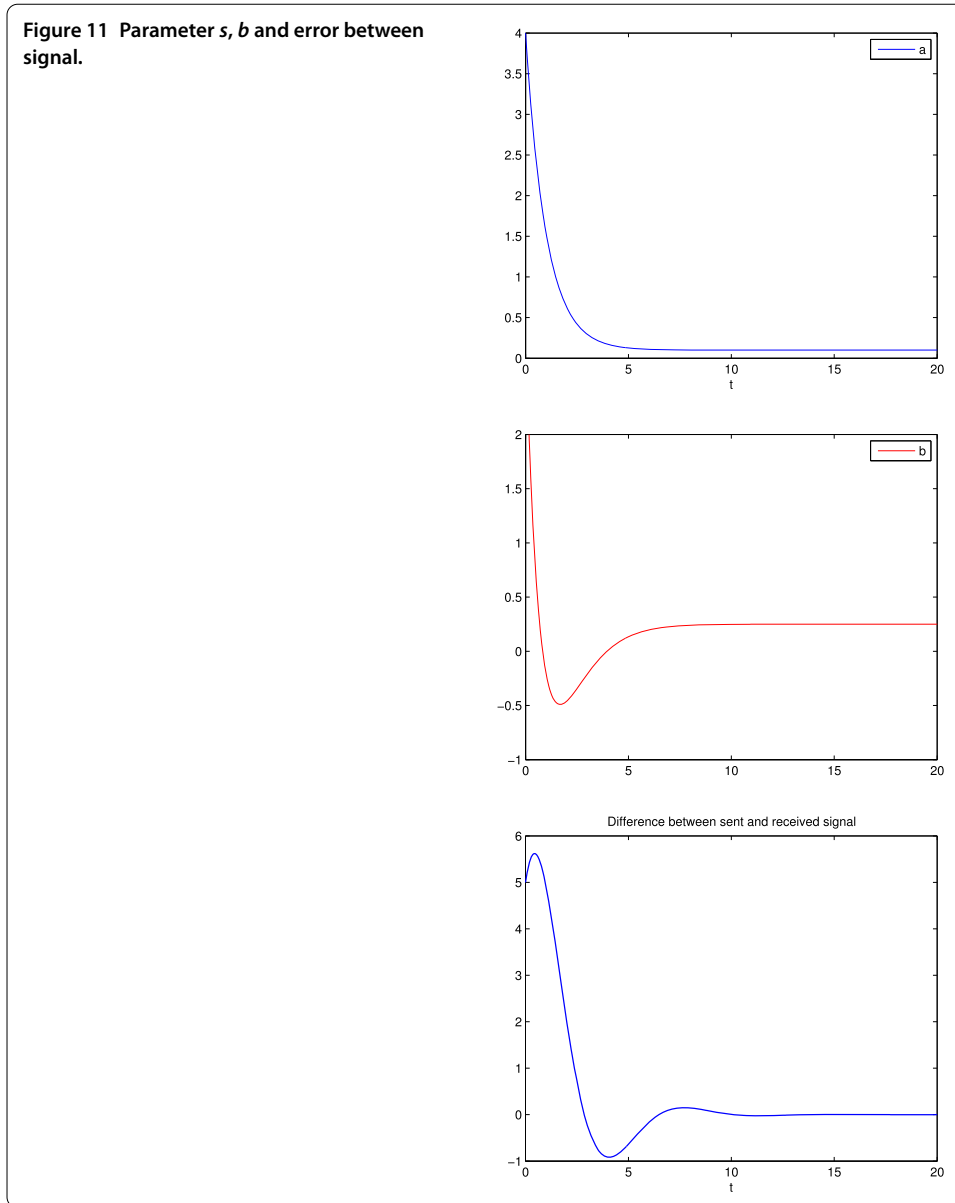
Figure 9 displays the synchronization difference (error) between systems (44) and (45). Figure 10 shows the error signal between the original message and the recovered one that confirms that the message signal  $o(t)$  is recovered accurately. Figure 11 shows the value of the unknown parameters  $a$ ,  $b$  and the error between sent and received signal.

By compression of results, it is obvious that in exponential synchronization the error system very fast tends to zero, which results in sending and receiving the signal faster with a better accuracy.

### 4.3 Image encryption using exponential stability

Almost in all cases the image encryption is often conducted along with data compression before be saved or transmitted. This is because of high volume of pictorial data and their adjuncts. Thus, it is so important to combine security demands with compression systems. In view of security, the pictorial data is not sensitive the same as the context data. In block method of encryption, firstly, one encryption key with equal dimensions with designed images one is produced by using of chaotic system and then the primary image encoded by block cipher.

Here, we have only one block. The given method could be exercised by producing keys with small sizes in a higher block number.

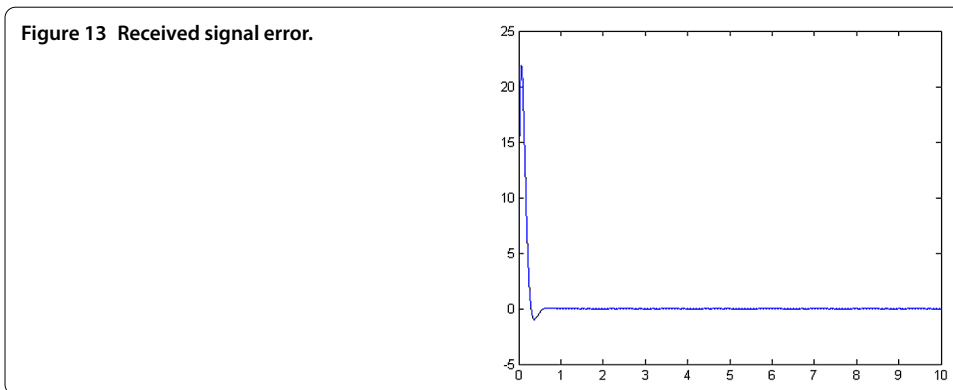
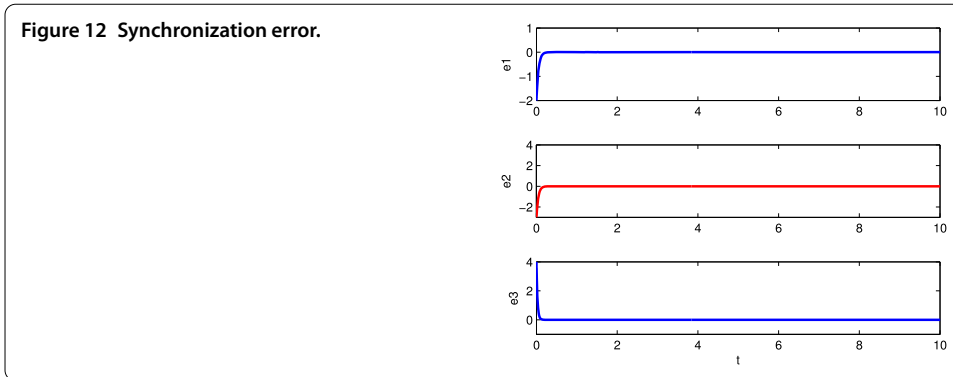


In order to decode, the encrypted image is produced by applying the same chaotic system and utilization of an equal initial value and by considering inversion methods in the decoding key.

In the masking method for image encryption, the information signal is combined linearly and added to the drive system. Suppose  $o(t)$  is the original image, the transmitted message  $s(t)$  is assumed as

$$s(t) = o(t) + k_1x_1(t) + k_2y_1(t) + k_3z_1(t), \tag{50}$$

where  $k_i > 0$ ,  $i = 1, 2, 3$  and  $x_1, y_1, z_1$  are the state variables. The encrypted signal is masked using an arbitrary function of master chaotic system variables to send and receive via a public channel. The assumed  $T_s$  is the synchronization time and the image is added after



that time. The recovered image  $r(t)$  is obtained using the following relation:

$$r(t) = s(t) - k_1x_2(t) - k_2y_2(t) - k_3z_2(t). \tag{51}$$

Because

$$\begin{aligned} r(t) &= s(t) - k_1x_2 - k_2y_2 - k_3z_2 \\ &= o(t) + k_1x_1 + k_2y_1 + k_3z_1 - k_1x_2 - k_2y_2 - k_3z_2 \\ &= o(t) + k_1e_1 + k_2e_2 + k_3e_3 \\ &\cong o(t). \end{aligned} \tag{52}$$

That obviously depends on the synchronization time.

To show the validity of the proposed method, simulation results using Matlab software and the Runge-Kutta method are applied for the initial condition  $(x_1(0), y_1(0), z_1(0)) = (1, -1, 2)$  and  $(x_2(0), y_2(0), z_2(0)) = (3, 1, -1)$  on the system (11) without linear term and a digital image as a signal in Figure 12, Figure 13 and Figure 14.

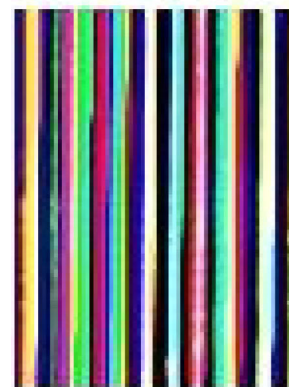
### 5 Conclusion

In this paper, we showed that exponential stability method for the synchronization of chaotic dynamical systems is faster than of the Lyapunov stability theorem which it confirmed by the results obtained for a system without linear term. By using presented syn-

**Figure 14** Image encryption using synchronization.



(a) Original picture



(b) Encrypted picture



(c) Received picture

chronization, cryptography of text and image were given through both modulation and masking methods in both active and adaptive cases. The results confirm the rate and precision of reception and transmittance of the desired signal.

Further research topics include the applying optimal control in the exponential synchronization of classical and fractional order chaotic systems and study of the other encryption methods such as the Rivest-Shamir-Adlemen (RSA) and Data Encryption Standard (DES) to compare them with the chaos-based encryption.

**Competing interests**

The authors declare that they have no competing interests.

**Authors' contributions**

All authors jointly worked on deriving the results and approved the final manuscript.

**Author details**

<sup>1</sup>Institute for Mathematical Research, University Putra Malaysia (UPM), Serdang, Selangor 43400, Malaysia. <sup>2</sup>Department of Mathematics, University Putra Malaysia (UPM), Serdang, Selangor 43400, Malaysia.

**Publisher's Note**

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Received: 21 October 2016 Accepted: 21 March 2017 Published online: 29 March 2017

**References**

- Lorenz, EN: Deterministic nonperiodic flow. *J. Atmos. Sci.* **20**(2), 130-141 (1963)
- Ott, E, Grebogi, C, Yorke, JA: Controlling chaos. *Phys. Rev. Lett.* **64**(11), 1196 (1990)
- Pecora, LM, Carroll, TL: Synchronization in chaotic systems. *Phys. Rev. Lett.* **64**(8), 821 (1990)
- Yu, S, Lu, J, Leung, H, Chen, G: Design and implementation of n-scroll chaotic attractors from a general jerk circuit. *IEEE Trans. Circuits Syst. I, Regul. Pap.* **52**(7), 1459-1476 (2005)
- Yu, F, Wang, C: Secure communication based on a four-wing chaotic system subject to disturbance inputs. *Optik* **125**(20), 5920-5925 (2014)
- Grassi, G, Mascolo, S: Synchronizing high dimensional chaotic systems via eigenvalue placement with application to cellular neural networks. *Int. J. Bifurc. Chaos* **9**(4), 705-711 (1999)
- Hsieh, J-Y, Hwang, C-C, Wang, A-P, Li, W-J: Controlling hyperchaos of the Rossler system. *Int. J. Control* **72**(10), 882-886 (1999)
- Kapitaniak, T, Chua, LO, Zhong, G-Q: Experimental hyperchaos in coupled Chua's circuits. *IEEE Trans. Circuits Syst. I, Fundam. Theory Appl.* **41**(7), 499-503 (1994)
- Peng, JH, Ding, EJ, Ding, M, Yang, W: Synchronizing hyperchaos with a scalar transmitted signal. *Phys. Rev. Lett.* **76**(6), 904 (1996)
- Vicente, R, Daudén, J, Colet, P, Toral, R: Analysis and characterization of the hyperchaos generated by a semiconductor laser subject to a delayed feedback loop. *IEEE J. Quantum Electron.* **41**(4), 541-548 (2005)
- Posadas-Castillo, C, López-Gutiérrez, RM, Cruz-Hernández, C: Synchronization of chaotic solid-state Nd:YAG lasers: application to secure communication. *Commun. Nonlinear Sci. Numer. Simul.* **13**(8), 1655-1667 (2008)
- Park, JH: Chaos synchronization of a chaotic system via nonlinear control. *Chaos Solitons Fractals* **25**(3), 579-584 (2005)
- Agiza, HN, Yassen, MT: Synchronization of Rossler and Chen chaotic dynamical systems using active control. *Phys. Lett. A* **278**(4), 191-197 (2001)
- Aghababa, MP: Robust stabilization and synchronization of a class of fractional-order chaotic systems via a novel fractional sliding mode controller. *Commun. Nonlinear Sci. Numer. Simul.* **17**(6), 2670-2681 (2012)
- Aghababa, MP, Aghababa, HP: Synchronization of nonlinear chaotic electromechanical gyrostat systems with uncertainties. *Nonlinear Dyn.* **67**(4), 2689-2701 (2012)
- Mossa Al-Sawalha, M, Salmi Md Noorani, M: Anti-synchronization of two hyperchaotic systems via nonlinear control. *Commun. Nonlinear Sci. Numer. Simul.* **14**(8), 3402-3411 (2009)
- Yang, C-C: One input control of exponential synchronization for a four-dimensional chaotic system. *Appl. Math. Comput.* **219**(10), 5152-5161 (2013)
- Liao, X, Yu, P: Study of globally exponential synchronization for the family of Rössler systems. *Int. J. Bifurc. Chaos* **16**(8), 2395-2406 (2006)
- Wang, Z: Anti-synchronization in two non-identical hyperchaotic systems with known or unknown parameters. *Commun. Nonlinear Sci. Numer. Simul.* **14**(5), 2366-2372 (2009)
- Tong, D, Zhu, Q, Zhou, W, Xu, Y, Fang, J: Adaptive synchronization for stochastic T-S fuzzy neural networks with time-delay and Markovian jumping parameters. *Neurocomputing* **117**, 91-97 (2013)
- Tong, D, Zhang, L, Zhou, W, Zhou, J, Xu, Y: Asymptotical synchronization for delayed stochastic neural networks with uncertainty via adaptive control. *Int. J. Control. Autom. Syst.* **14**(3), 706-712 (2016)
- Tong, D, Zhou, W, Zhou, X, Yang, J, Zhang, L, Xu, Y: Exponential synchronization for stochastic neural networks with multi-delayed and Markovian switching via adaptive feedback control. *Commun. Nonlinear Sci. Numer. Simul.* **29**(1), 359-371 (2015)
- Yan, Z, Yu, P: Globally exponential hyperchaos (lag) synchronization in a family of modified hyperchaotic Rössler systems. *Int. J. Bifurc. Chaos* **17**(5), 1759-1774 (2007)
- Cuomo, KM, Oppenheim, AV, Strogatz, SH: Synchronization of Lorenz-based chaotic circuits with applications to communications. *IEEE Trans. Circuits Syst. II, Analog Digit. Signal Process.* **40**(10), 626-633 (1993)
- Boutayeb, M, Darouach, M, Rafaralahy, H: Generalized state-space observers for chaotic synchronization and secure communication. *IEEE Trans. Circuits Syst. I, Fundam. Theory Appl.* **49**(3), 345-349 (2002)
- Stevens, BL, Lewis, FL, Johnson, EN: *Aircraft Control and Simulation: Dynamics, Controls Design, and Autonomous Systems*. Wiley, New York (2015)
- Teschl, G: *Ordinary Differential Equations and Dynamical Systems*. Graduate Studies in Mathematics, vol. 140. Am. Math. Soc., Providence (2012)
- Narendra, KS, Annaswamy, AM: *Stable Adaptive Systems*. Dover, Mineola (2012)
- Khalil, HK: *Nonlinear Systems*, 3rd edn. Pearson, Harlow (2002)
- Shankar, S, Bodson, M: *Adaptive Control: Stability, Convergence and Robustness*. Dover, Mineola (2011)
- Aghababa, MP, Khanmohammadi, S, Alizadeh, G: Finite-time synchronization of two different chaotic systems with unknown parameters via sliding mode technique. *Appl. Math. Model.* **35**(6), 3080-3091 (2011)
- Xu, Y, Wang, Y: A new chaotic system without linear term and its impulsive synchronization. *Optik* **125**(11), 2526-2530 (2014)
- Mata-Machuca, JL, Martínez-Guerra, R, Aguilar-López, R, Aguilar-Ibañez, C: A chaotic system in synchronization and secure communications. *Commun. Nonlinear Sci. Numer. Simul.* **17**(4), 1706-1713 (2012)