Adaptive Synchronization of Lorenz System and Its Uses in Cryptanalysis

Ying Liu and Wallace K.S. Tang
Department of Electronic Engineering,
City University of Hong Kong,
Tat Chee Avenue, Kowloon, Hong Kong, P.R. China
Email: yingliu2@student.cityu.edu.hk, kstang@ee.cityu.edu.hk

Abstract— **This paper addresses the adaptive synchronization problem of Lorenz system even when its system structure is imprecise and some of its parameters are unknown. With only a single observable state, this is accomplished by a newly designed adaptive observer based on linear feedback control, where the estimated parameters are adaptively updated by some dynamical minimization algorithms. As illustrated with the numerical simulations, the observer's states can asymptotically synchronize with the targeted system, while the unknown parameters can be identified simultaneously in a fast convergence rate. Furthermore, the proposed observer is applied for providing the cryptanalysis of some Lorenz-based chaotic modulation communication systems. It is demonstrated that the covered messages can be easily estimated by such an adaptive attack. Hence, the securities of those systems are challenged.**

Keywords*—*Adaptive observer; adaptive synchronization; cryptanalysis; minimization algorithm; secure communication

I. Introduction

The importance of chaos synchronization [1] has aroused a lot of interests, not only because of its theoretical importance, but also its wide applications, such as secure communications and data encryption.

In the last two decades, a large number of chaos-based cryptosystems have been suggested based on the concept of synchronization, see Refs. [2]–[7] for example. The success of these cryptosystems is largely dependent on how resistive they are for different kinds of attacks. In additions, as pinpointed in [2], the in-use chaotic systems must also be *anti-adaptive* in order to prevent intruder from retrieving the system states and/or the parameters based on the observability of the transmitted output.

The concept of *anti-adaptiveness* is closely related with *adaptive synchronization*, which implies the synchronization of a targeted system without knowing its exact model. Currently, a variety of adaptive synchronization approaches have been reported, such as, Refs. [8]-[15], where Lorenz system is of particular interest. Lorenz system has been commonly used in practical communication system designs, as it is a well-known difficult synchronization problem when some unknown parameters are resided in all the three state equations and only the first state is measurable. As a general remark, this problem is manageable if the second state is observed [11], [12].

Recently, some static minimization approaches [16], [17] have been explored to tackle with this difficult synchronization problem. Evolutionary computation technique [18], namely particle swarm optimization, has also been successfully applied for the parameter estimations in chaotic systems. However, these methods do not serve the needs for real-time estimation as a set of fixed record is generally required.

On the other hand, designs based on adaptive rules [13], [14], [15] provide some possible solutions. In [13], an adaptive rule for parameter estimation, driven by the synchronization error, has been suggested for observer design based on the concept of system control. However, detailed design procedure is missed, and the time for synchronization is very long as presented. Similarly, a local adaptive Lyapunov function has been established in [14], where parameter adaptive control loops are designed to synchronize a given system as well as to estimate its unknown parameters. Although the construction of this local Lyapunov function is rather complex, it is considered to be a practical means to justify the design of the parametric update rules.

In this paper, a new observer based on the linear feedback control and dynamical minimization algorithm [11] is proposed to achieve the adaptive synchronization of Lorenz system. In addition, the designed observer will also be applied for the cryptanalysis of some chaos-synchronization based secure communication systems.

[†]Corresponding author: Ying Liu, Email: yingliu2@student.cityu.edu.hk

As shown from our simulations, the suggested design serves as an effective means for challenging the anti-adaptiveness of those systems.

The rest of the paper is organized as follows. In Sect. II, a design of observer system proposed for adaptive synchronization of Lorenz system is described. The design is then verified and some simulation results are also given in the same section. In Sect. III, the proposed observer system is adopted for the cryptanalysis of some Lorenz-based chaotic modulation communication systems, supported with various simulation examples. Finally, conclusions are drawn in Sect. IV.

II. Adaptive Synchronization of Lorenz System

In this section, the adaptive synchronization of Lorenz system is described. To formulate a more challenging problem, it is assumed that the exact form of Lorenz equation is unknown while the following generalized form is considered:

$$M : \begin{cases} \dot{x_1} &= p_1(x_2 - x_1) \\ \dot{x_2} &= p_2 x_1 - p_3 x_2 - x_1 x_3 \\ \dot{x_3} &= x_1 x_2 + p_4 x_2 - p_5 x_3 \end{cases} \tag{1}$$

where $\mathbf{x} = [x_1 \quad x_2 \quad x_3]^T$ is the state vector and $\mathbf{p} = [p_1 \quad p_2 \quad p_3 \quad p_4 \quad p_5]^T$ are unknown parameters but linearly depend on the system states.

In (1), an addition term $p_4 x_2$ is included in the third equation. It is expected that the exact form of the equation can be recovered if p_4 can be correctly estimated as zero.

It is also letting that the output is:

$$y = \mathbf{C}\mathbf{x} \tag{2}$$

where $\mathbf{C} = [1 \quad 0 \quad 0]$ and hence $y = x_1$ is observable. Similar to all the identification problem, the condition of persistently excitation is assumed (Note: This is generally true when the system M is in its chaotic mode).

In order to achieve adaptive synchronization, another system, known as an observer system S, is to be designed such that the states and unknown parameters can be simultaneously estimated. Motivated by a recent work [15], a new design of S is proposed as follows:

$$S : \begin{cases} \dot{\hat{x}}_1 &= q_1(\hat{x}_2 - \hat{x}_1) + k_1 e_y \\ \dot{\hat{x}}_2 &= q_2 \hat{x}_1 - q_3 \hat{x}_2 - \hat{x}_1 \hat{x}_3 + k_2 e_y \\ \dot{\hat{x}}_3 &= \hat{x}_1 \hat{x}_2 + q_4 \hat{x}_2 - q_5 \hat{x}_3 + k_3 e_y \\ \dot{q}_i &= \delta_i h_i(\hat{\mathbf{x}}, e_y) \mu_i(\hat{\mathbf{x}}) \qquad \text{for } i = 1, \cdots, 5 \end{cases} \tag{3}$$

where $\hat{\mathbf{x}} = [\hat{x}_1 \quad \hat{x}_2 \quad \hat{x}_3]^T$ is the observer state vector; $e_y = y - \hat{y}$ and $\hat{y} = \mathbf{C}\hat{x}$; $\mathbf{q} = [q_1 \quad q_2 \quad q_3 \quad q_4 \quad q_5]^T$ is the estimator for unknown parameter $\mathbf{p}$; $\mathbf{K} = [k_1 \quad k_2 \quad k_3]^T$ is the feedback gain to stabilize the linear part of the original system; $\delta_i > 0, i = 1, \cdots, 5$ are some stiffness constants; h_i and μ_i are functions to ensure the minimization of the synchronization errors and to allow the unknown parameters converging with a similar rate, respectively.

The detailed design procedures are given as follows:

1) Design $\mathbf{K}$ to stabilize the linear part of the system: Rewrite (1) as

$$M : \; \dot{\mathbf{x}} = \mathbf{A}(\mathbf{p})\mathbf{x} + \varphi(\mathbf{x}) \equiv \mathbf{F}(\mathbf{x}, \mathbf{p}) \tag{4}$$

where $\mathbf{F} = F_i(i = 1, 2, 3)$, $\mathbf{A}(\mathbf{p}) = \begin{bmatrix} -p_1 & p_1 & 0 \\ p_2 & -p_3 & 0 \\ 0 & p_4 & -p_5 \end{bmatrix}$ and the only nonlinearity $\varphi(\mathbf{x}) = \begin{bmatrix} 0 \\ -x_1 x_3 \\ x_1 x_2 \end{bmatrix}$ is Lipshitzian, i.e. there exists a positive constant $L < \infty$, such that

$$\| \varphi(\mathbf{x}) - \varphi(\hat{\mathbf{x}}) \| \leq L \| \mathbf{x} - \hat{\mathbf{x}} \|, \quad \forall \mathbf{x}, \hat{\mathbf{x}} \in \Re^n \tag{5}$$

Since $\mathbf{A}(\mathbf{p})$ is unknown, for the best estimation, $\mathbf{K}$ is chosen to have all the eigenvalues of $(\mathbf{A}(\mathbf{q}^0) - \mathbf{K}\mathbf{C})$ being negative, where $\mathbf{q}^0$ is the initial guess of the parameter $\mathbf{p}$. For example, let $\mathbf{q}^0 = [12.0 \quad 30.0 \quad 2.0 \quad 2.0 \quad 2.5]^T$, one has the feedback gain $\mathbf{K} = [60 \quad 120 \quad 0]^T$, where the eigenvalues of $(\mathbf{A}(\mathbf{q}^0) - \mathbf{K}\mathbf{C})$ are $\lambda_{1,2,3} = -49.04, -24.96, -2.50$, respectively.

2) Design the function h_i, $i = 1, \cdots, 5$:
The updating equations for unknown parameters are designed based on the dynamical minimization of the synchronization error e_y and the dependence of parameter q_i on the observable state. Details can be referred to [11], while the concept is briefly explained as follows.
The major idea is to design the dynamical equations for unknown parameters q_i so that the synchronization error:

$$E(q_i, t) = \min \left\{ (y - \hat{y})^2 \right\} \tag{6}$$

is to be minimized. With an analogy to an equation in mechanics, where an overdamped particle goes to a minimum of a potential, the following design rules are obtained:

a) if q_i appears in the dynamical evolution of $\hat{x}_1$, we have

$$h_i \propto \frac{\partial F_1(\hat{\mathbf{x}}, \mathbf{q})}{\partial q_i} e_y, \tag{7}$$

b) if q_i appears in $\hat{x}_i$, $i \neq 1$ and the evolution of $\hat{x}_1$ depends on state $\hat{x}_i$ directly, then

$$h_i \propto \frac{\partial F_1(\hat{\mathbf{x}}, \mathbf{q})}{\partial \hat{x}_i} \frac{\partial F_i(\hat{\mathbf{x}}, \mathbf{q})}{\partial q_i} e_y, \tag{8}$$

c) if q_i appears in $\hat{x}_i$, $i \neq 1$ but the dynamical function F_1 does not depend on state $\hat{x}_i$ explicitly, then a further dependence according to the dynamical evolution of the system should be considered as follows:

$$h_i \propto \left\{ \sum_k \frac{\partial F_1(\hat{\mathbf{x}}, \mathbf{q})}{\partial \hat{x}_k} \frac{\partial F_k(\hat{\mathbf{x}}, \mathbf{q})}{\partial \hat{x}_i} \right\} \frac{\partial F_i(\hat{\mathbf{x}}, \mathbf{q})}{\partial q_i} e_y \tag{9}$$

Hence, for the Lorenz system (1) and the proposed observer (3), the functions h_i can be derived as:

$$\begin{aligned} h_1 &= \mathrm{sgn}(\hat{x}_2 - \hat{x}_1) e_y \\ h_2 &= \mathrm{sgn}(\hat{x}_1) e_y \\ h_3 &= -\mathrm{sgn}(\hat{x}_2) e_y \\ h_4 &= -\mathrm{sgn}(\hat{x}_1 \hat{x}_2) e_y \\ h_5 &= \mathrm{sgn}(\hat{x}_1 \hat{x}_3) e_y. \end{aligned} \tag{10}$$

It should be noticed that a sign function is now introduced for performance improvement. As demonstrated in later simulation, not only that (10) provides a more simple structure, its convergence speed is also found to be faster. The dependence of q_1 in original functions $h_i, i = 2, 3, 4, 5$ is further omitted as it is always positive.

3) Design μ_i such that the convergence rates of the estimation errors are similar [15]:

The error convergence rate of each parameter is approximated by the case that it is the sole unknown. For example, if only p_1 is unknown, by linearizing the error dynamics of the targeted system (1) and the observer (3) evaluated on a typical trajectory, one obtains:

$$\left\{ \begin{aligned} \dot{\mathbf{e}} &= J_{11_{(1)}} \mathbf{e} + J_{12_{(1)}} r \\ \dot{r} &= J_{21_{(1)}} \mathbf{e} \end{aligned} \right. \tag{11}$$

where $\mathbf{e} = \mathbf{x} - \hat{\mathbf{x}}$, $r = p_1 - q_1$,

$$\begin{aligned} J_{11_{(1)}} &= \begin{bmatrix} -q_1 - k_1 & q_1 & 0 \\ p_2 - \hat{x}_3 - k_2 & -p_3 & -\hat{x}_1 \\ \hat{x}_2 - k_3 & p_4 + \hat{x}_1 & -p_5 \end{bmatrix} \\ J_{12_{(1)}} &= [\hat{x}_2 - \hat{x}_1 \quad 0 \quad 0]^T \\ J_{21_{(1)}} &= [-\delta_1 \mu_1(\hat{\mathbf{x}}) \mathrm{sgn}(\hat{x}_2 - \hat{x}_1) \quad 0 \quad 0]. \end{aligned} \tag{12}$$

The convergence rate of (11) is then governed by:

$$\begin{aligned} \Gamma_1 &= -J_{21_{(1)}} J_{11_{(1)}}^{-1} J_{12_{(1)}} \\ &= -\frac{\delta_1}{|J_{11_{(1)}}|} \mu_1 (p_3 p_5 + \hat{x}_1 (p_4 + \hat{x}_1)) |\hat{x}_2 - \hat{x}_1| \end{aligned} \tag{13}$$

Similarly, for having other parameters p_i, $i = 2, 3, 4, 5$ as the unknown, we have

$$\Gamma_2 = -\frac{\delta_2}{|J_{11_{(2)}}|} \mu_2 p_1 p_5 |\hat{x}_1| \tag{14}$$

$$\Gamma_3 = -\frac{\delta_3}{|J_{11_{(2)}}|} \mu_3 p_1 p_5 |\hat{x}_2| \tag{15}$$

$$\Gamma_4 = -\frac{\delta_4}{|J_{11_{(4)}}|} \mu_4 p_1 |\hat{x}_1 \hat{x}_2| \tag{16}$$

and

$$\Gamma_5 = -\frac{\delta_5}{|J_{11_{(5)}}|} \mu_5 p_1 |\hat{x}_1 \hat{x}_3| \tag{17}$$

where $|J_{11_{(i)}}| = (p_1 + k_1)[p_3 p_5 + \hat{x}_1 (p_4 + \hat{x}_1)] - p_1 [p_5 (p_2 - \hat{x}_3 - k_2) - \hat{x}_1 \hat{x}_2 + k_3 \hat{x}_1]$, in which p_i is taken place by q_i.

Obviously, the choice of $\mathbf{K}$ should also make $|J_{11_{(i)}}|_{i=1,\cdots,5} > 0$, implying k_1 and k_2 are large but k_3 is small.

By reviewing the Eqns. (13)–(17), it is noticed that the convergence of the parameter estimation is related with the estimated states $\hat{x}_i$. It can also be observed that $\Gamma_i, i = 1, 4, 5$ are dependent on higher order terms, while $\Gamma_i, i = 2, 3$ in (14) and (15) are of first order.

Therefore, in order to force all the Γ_i to have similar dynamics and convergence rate, we have $\mu_i = 1, \text{for}\, i = 1, 4, 5$ and $\mu_i = |\hat{x}_2|$ for $i = 2, 3$.

Remark 1: When there are multiple unknown parameters appearing in the dynamical equation of the non-observable states, the design solely based on the minimization algorithm [11] may not be successful. It is due to the fact that the unknown parameters may converge in different rates, causing a failure of estimation. Therefore, auxiliary functions μ_i are now introduced. It will also be shown in the later section that this design is valid by verifying some of its local Lyapunov functions.

The final adaptive observer is then constructed as:

$$S : \begin{cases} \dot{\hat{x}}_1 &= q_1(\hat{x}_2 - \hat{x}_1) + k_1 e_y \\ \dot{\hat{x}}_2 &= q_2\hat{x}_1 - q_3\hat{x}_2 - \hat{x}_1\hat{x}_3 + k_2 e_y \\ \dot{\hat{x}}_3 &= \hat{x}_1\hat{x}_2 + q_4\hat{x}_2 - q_5\hat{x}_3 + k_3 e_y \\ \dot{q}_1 &= \delta_1 \mathrm{sgn}(\hat{x}_2 - \hat{x}_1) e_y \\ \dot{q}_2 &= \delta_2 |\hat{x}_2| \mathrm{sgn}(\hat{x}_1) e_y \\ \dot{q}_3 &= -\delta_3 |\hat{x}_2| \mathrm{sgn}(\hat{x}_2) e_y \\ \dot{q}_4 &= -\delta_4 \mathrm{sgn}(\hat{x}_1\hat{x}_2) e_y \\ \dot{q}_5 &= \delta_5 \mathrm{sgn}(\hat{x}_1\hat{x}_3) e_y \end{cases} \qquad (18)$$

A. *Design Justification*

As mentioned in many reports, it is impossible to construct a global Lyapunov stability function for Lorenz system if **p** in (1) is unknown and only x_1 is observed.

To justify our design, the local Lyapunov function approach suggested in [14] is adopted. As pointed out in [14], it is possible to construct some local Lyapunov functions based on the information of a control surface if the observer system is sufficiently robust to parameter mismatches. It is required that the time average of control functions must be smooth with respect to the parameter **q** near the true value of **p**, and converge to zero when $\mathbf{p} = \mathbf{q}$.

These criteria can provide a guideline for the design of the observer S, in turns, become a method to evaluate whether it can achieve adaptive synchronization. For multiple parameters identification, the parameter adaptive control functions (i.e. $\dot{q}_i$) must not only be smooth, but also converge to zero with similar rates when **q** deviates slightly from **p**. This also explains why additional function μ_i has to be introduced.

Consider local Lyapunov functions $U_i, i = 1, \cdots, 5$ defined as follows:

$$U_i(\tau_0, T) = \frac{1}{T} \int_{\tau_0 - T}^{\tau_0} \dot{q}_i \, d\tau \qquad (19)$$

where $q_i \in [p_i - \Delta p_i, p_i + \Delta p_i]$, assuming that the other unknown parameters are set as their nominal values.

Consider the case of $\mathbf{p} = [16.0 \quad 45.6 \quad 1.0 \quad 0.0 \quad 4.0]^T$ while the system (1) is in its chaotic mode, Fig. 1 depicts the time average of $U_i(\tau_0, T)$ chosen from each state variable with $T = 250$ (denoted as U_i). For clarity, only the functions $U_{1,2,5}$ are given, and similar results can be obtained for $U_{3,4}$.

From Fig. 1, it can be observed that U_i varies smoothly when the parameter deviation Δp_i is small. Also, as illustrated by the slope of the functions, the time average of all parametric updating functions converge to zero approximately the same in each individual dimension, agreeing with our design concept.

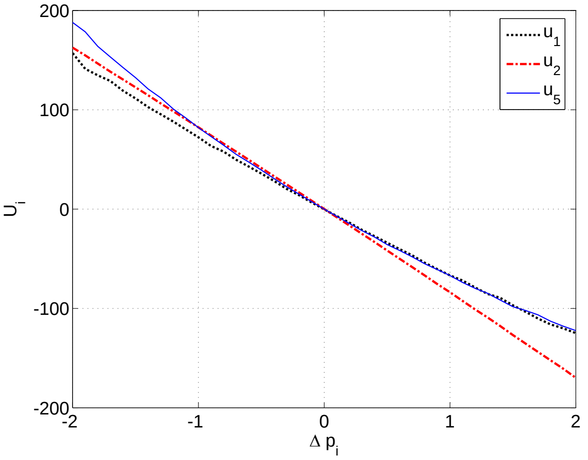


Fig. 1. $U_i, i = 1, 2, 5$ as a function of the relative deviation of the parameter error for q_i

B. *Simulation Results*

Now, consider a Lorenz system (1) with unknown parameter $\mathbf{p} = [16.0 \quad 45.6 \quad 1.0 \quad 0.0 \quad 4.0]^T$ and follow the procedures described in Sect. II, one obtains the observer (3).

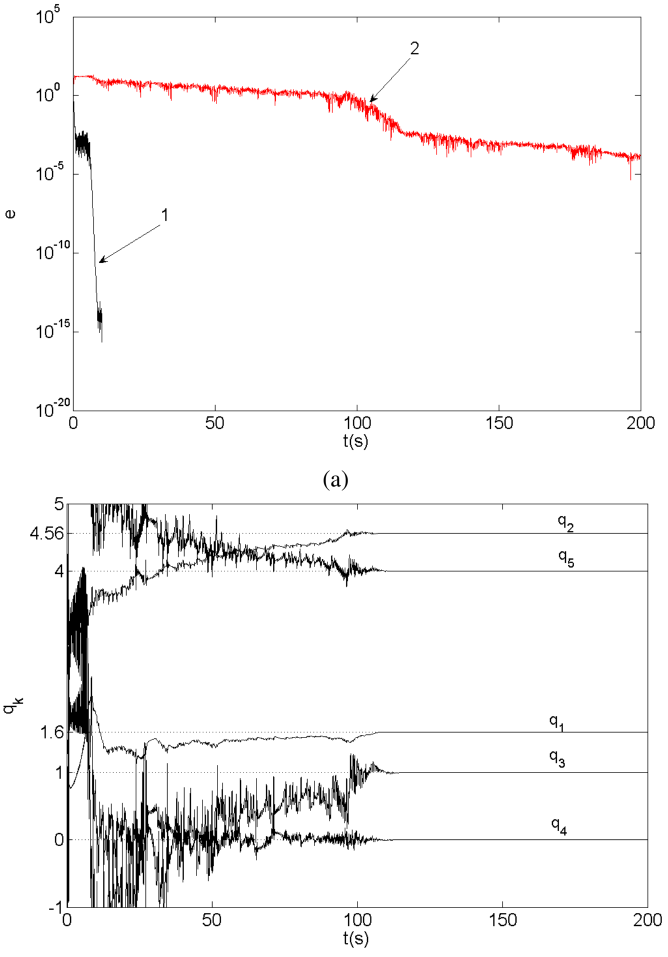
Let $\delta_{1,4,5} = 12$, $\delta_{2,3} = 2$, and assume that the initial conditions are:

$$\begin{aligned} \mathbf{x}^0 &= [1 \quad 1 \quad 1]^T, \\ \hat{\mathbf{x}}^0 &= [2 \quad 2 \quad 2]^T \qquad \text{and} \\ \mathbf{q}^0 &= [12.0 \quad 30.0 \quad 2.0 \quad 2.0 \quad 2.5]^T, \end{aligned}$$

Fig. 2 (a) shows the evolutions of the synchronization errors based on adaptive synchronization (denoted as '2'). For comparison, the same error based on identical synchronization (i.e. with **p** known) is also given and denoted as '1'.

Obviously, it takes longer time for the synchronization error to reduce to a small value when parameters are unknown. However, as illustrated in Fig. 2 (a), the error drops exponentially and reaches the order of 10^{-4} within about 120s, which is considered to be very fast. In fact, a shorter synchronization time is possible when fewer parameters are unknown. For example, if only the common system parameters $p_{1,2,5}$ are unknown, it will only takes about 40s for the synchronization error to reach the order of 10^{-4}, which is much faster than that presented in [13], [14].

The estimated parameters q_i against time are given in Fig. 2 (b). It clearly shows that all the estimators converge to their true values, and the exact Lorenz equation is identified.



(a)

(b)

Fig. 2. (a) Synchronization errors $\sqrt{\sum e_i{}^2}$ vs t, where '1' and '2' indicate the synchronization errors with normal identical synchronization and adaptive synchronization, respectively ; (b) Convergence of the recovered parameter values $q_{1,2}/10$ and $q_{3,4,5}$ of the observer (3) correspond to the true values in the master system (1)

III. Cryptanalysis of Some Chaotic Modulation Systems

In this section, it is to suggest an adaptive attack using the proposed adaptive observer, serving as the cryptanalysis of some chaos-based secure communication systems. We will only focus on those systems using Lorenz attractor as their basic units, such as [6], [7], although some other chaotic systems with unknown parameters can also be adaptively synchronized with the similar approach.

The cryptanalysis is based on the assumption that the structure of the cryptosystem is known while the system parameters, which are probably the users' specific keys, are kept secret.

A. System I

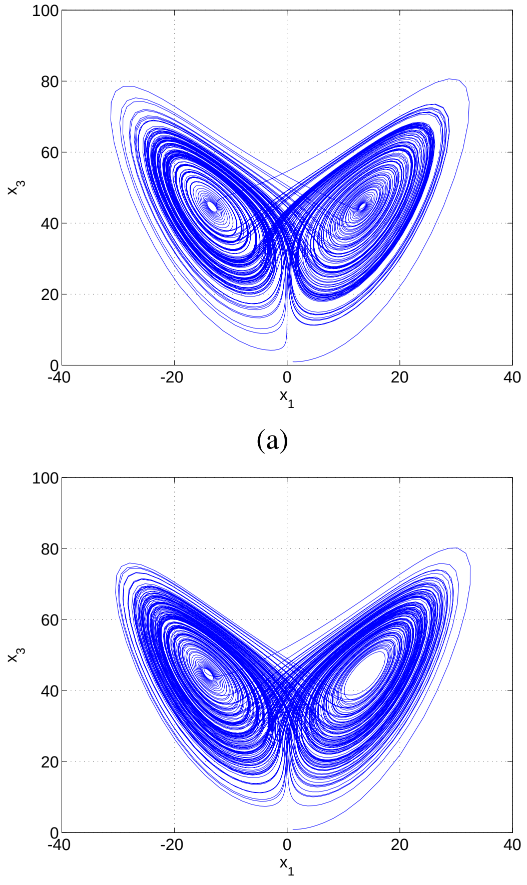
Recall the system proposed in [7], which can be expressed as:

$$M_1 : \left\{ \begin{array}{lcl} \dot{x_1} & = & p_1(x_2 - x_1) \\ \dot{x_2} & = & p_2 x_1 - x_2 - x_1 x_3 \\ \dot{x_3} & = & x_1 x_2 - \tilde{p}_3 x_3 \end{array} \right. \tag{20}$$

where $\tilde{p}_3 = p_3 + m(t) \times \Delta$, $m(t) = \pm 1$ and Δ is a constant.

The parameters p_i, $i = 1, 2, 3$ are considered to be the secret keys. The message $m(t)$ is used to modulate p_3 and the signal x_1 is transmitted.

1) Case I: In our simulation, the same parameters given in [7] and [14] are used. They are: $p_1 = 16$, $p_2 = 45.6$, $p_3 = 4.2$ and $\Delta = 0.2$. As shown in Fig. 3, the two chaotic attractors corresponding to $m(t) = \pm 1$ look very similar.



(a)

(b)

Fig. 3. (a) The chaotic attractor of Lorenz circuit for encoding (a) '-1' and (b) '1'

It should be noticed that the realization of Lorenz system in electronic circuit involves a particular time constant, and hence a transformation of time-scale is needed. As determined in [14], the new time-scale $t =$

τ/T_0, where τ is the time-scale used in simulation and $T_0 = 2505$.

When the bit duration time of $m(t)$ is sufficiently long (say 16ms), as shown in Fig. 4, the parameter q_3 can correctly follow the modulated value $\tilde{p}_3$, and the original message $m(t)$ can be obtained by estimating the medium value of q_3. Due to the transient effect, some errors are noticed in the first few milliseconds, which can be improved with the use of a moving average filter. In our simulation, a moving average filter with a length 1ms is adopted for the first 2ms.

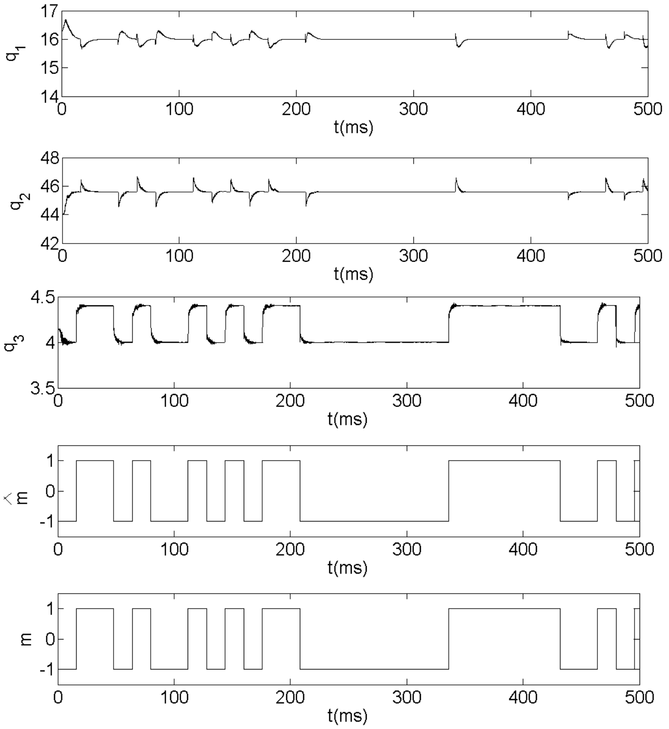


Fig. 4. Parameters q_i, recovered message $\hat{m}(t)$ and the plaintext $m(t)$ vs t

2) Case II: In the second case, the bit duration time is reduced to 4ms which is much smaller than the synchronization transient time. As compared with the attack suggested in [14] in which a wrong estimation of $\tilde{p}_3$ is obtained, the value of q_3 obtained with the proposed observer design is more accurate. By taking the average of the maximum and minimum values of q_3 after the initial transient time (in our example, 2ms), we get a coarse estimate $p_3 \approx 4.2$, which is further employed as the threshold to recover the message $m(t)$. Note that the value of the threshold is not exclusive and strict. Generally, it can be chosen as the mean of the maximum and the minimum of the modulated parameters (after the initial transient time). The simulation result is shown in Fig. 5. Again, to avoid errors caused by the initial synchronization process, a moving average filter with length of 1ms has been used for the first 2ms.

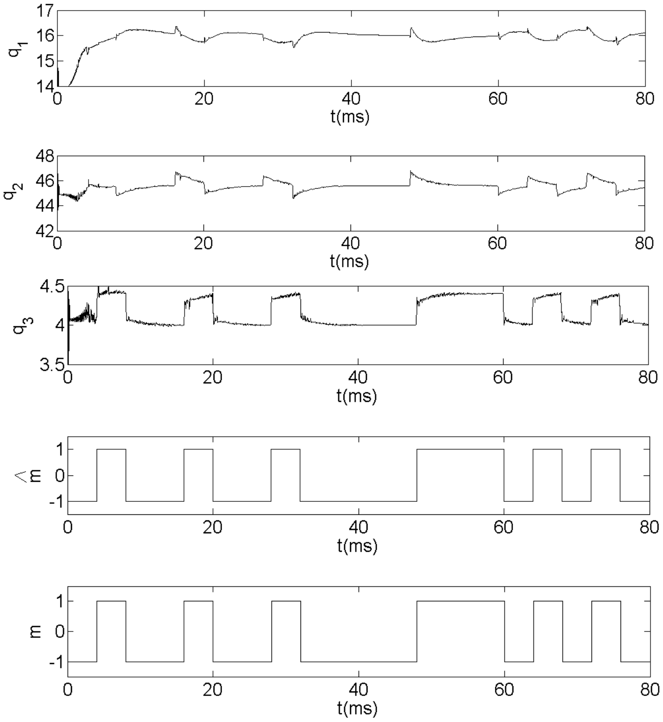


Fig. 5. Parameters q_i, recovered message $\hat{m}(t)$ and the plaintext $m(t)$ vs t

B. System II

In our second example, the system described in [6] is studied. The message is used to modulate the parameter p_2 in the cryptosystem (20), which can be described as follows:

$$M_1 : \begin{cases} \dot{x_1} &= p_1(x_2 - x_1) \\ \dot{x_2} &= \tilde{p}_2 x_1 - x_2 - x_1 x_3 \\ \dot{x_3} &= x_1 x_2 - p_3 x_3 \end{cases} \qquad (21)$$

where $\tilde{p}_2 = p_2 + m(t) \times \Delta$, $m(t) = \pm 1$ and Δ is a constant. Again, the state x_1 is used as the output signal.

1) Case I: Now, it is letting that the system true values are: $p_1 = 10$, $p_2 = 30$, $p_3 = 8/3$, and $\Delta = 2$. The same message as in the Case I of System I is to be transmitted, with the bit duration period of 16ms (again, it is based on the new time-scale). Figure 6 depicts the estimators for the unknown parameters and the decoded message from the system parameters. From the result, it can be observed that the estimator q_2 closely follows the modulation $\tilde{p}_2$, while the other two parameters also reflect the switch of the message from one value to the other. By using a simple threshold test, i.e. $p_2 = 30$ (it is determined by taking the mean of the maximum and the minimum values of q_2 after the initial transient time of 2ms.), one can easily decode the message signal $m(t)$. In this example, a moving average filter with a length 1ms is employed in the whole process for message recovery, in order to reduce the transients. Therefore, there exists a time delay, less than 1ms, in the recovered signal.

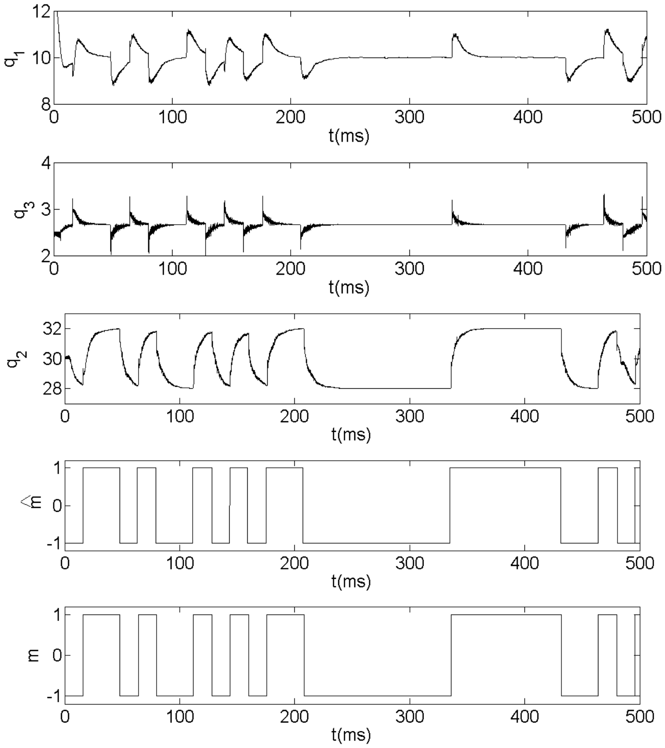


Fig. 6. Parameters q_i, recovered message $\hat{m}(t)$ and the plaintext $m(t)$ vs t

2) Case II: In this case, the bit rate of the message is increased, and the bit duration time is set as 4ms. As the bit duration time is very short, the convergence speed of the adaptive observer should be fast enough to correctly reveal the message. Therefore, in this example, a large feedback gain and stiffness constants are used.

The simulation results are shown in Fig. 7 with parameter settings: $\delta_{1,3} = 24$, $\delta_2 = 30$ and the feedback gain $\mathbf{K} = [120 \quad 300 \quad 0]^T$. It is noticed that the transient time for the System II is much longer than the System I, yet the message can still be correctly recovered by the use of a moving average filter with a length of 1ms and a simple threshold test after about 10ms.

IV. Conclusions

In this paper, the adaptive synchronization of Lorenz system with total five unknown parameters is achieved. An adaptive observer is designed for this difficult task, based on the concept of feedback control and dynamical minimization algorithm. The design is verified by the use of a local Lyapunov function approach. As shown in the simulation results, both state synchronization errors and parameter estimation errors converge to zero within a short transient, achieving the adaptive synchronization with good quality.

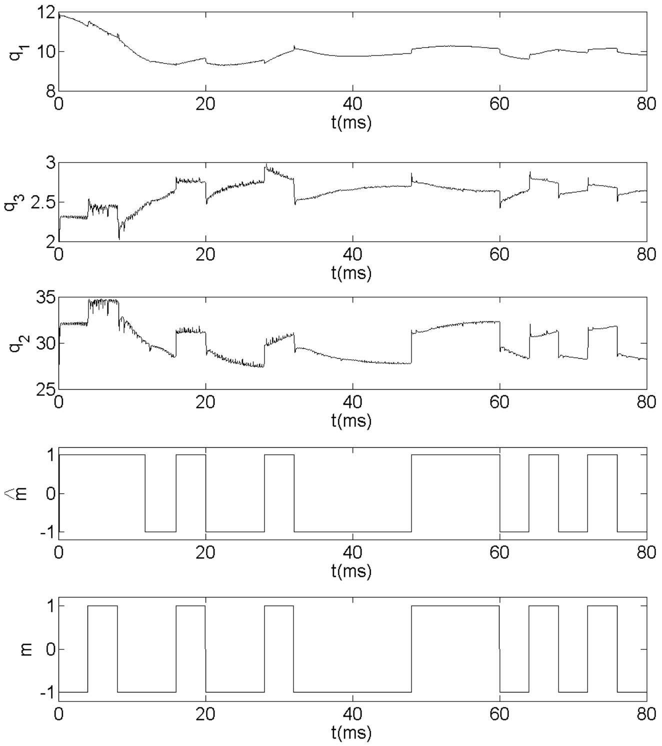


Fig. 7. Parameters q_i, recovered message $\hat{m}(t)$ and the plaintext $m(t)$ vs t

In addition, the adaptive observer is used as a means to perform the cryptanalysis of some chaos-synchronization based secure communication systems, in which one of the system parameters is used as carrier to transmit the information signal. From the view point of system adaptive control, the securities of those systems are questionable. Simulation results have shown that the transmitted message of different bit rates can be correctly extracted by an intruder, even though the exact parameter values in the transmitter are unknown.

Acknowledgment

The work described in this paper was fully supported by a grant from the Research Grants Council of the Hong Kong Special Administrative Region, China [CityU 120407].

References

[1] L.M. Pecora and T.L. Carroll, “Synchronization in chaotic systems,” *Phys. Rev. Lett*, vol. 64, pp. 821–824, 1990.

[2] S.Čelikovský and G.R.Chen, “Secure synchronization of a class of chaotic systems from a nonlinear observer approach,” *IEEE Trans on Automatic Control*, vol. 50, pp. 76–82, 2005.

[3] L. Kocarev, K.S. Halle, K. Eckert, L.O. Chua and U. Parlitz, "Experimental demonstration of secure communication via chaotic synchronization," *Int. J. Bifurc. Chaos* vol. 2, pp. 709–713, 1992.

[4] C.K. Tse and F.C.M. Lau, *Chaos-Based Digital Communication Systems: Operating Principles, Analysis Methods, and Performance Evaluation*, (Springer Verlag, Berlin,2003).

[5] M. Boutayeb, M. Darouach and H. Rafaralahy, "Generalized state-space observers for chaotic synchronization and secure communication," *IEEE Trans. Circuits Syst. I*, vol. 49, no. 3, pp. 345–349, Mar.2002.

[6] Y. Song and X. Yu, "Multi-parameter modulation for secure communication via Lorenz chaos," *Proc. IEEE Conf. Decision and Control*, pp. 42–45, 2000.

[7] K.M. Cuomo and A.V. Oppenheim, "Circuit implementation of synchronized chaos with applications to communications," *Phys. Rev. Lett.*, vol. 71, pp. 65–68, 1993.

[8] M. Feki, "An adaptive chaos synchronization scheme applied to secure communication," *Chaos, Solitons and Fractals*, vol. 18, pp. 141–148, 2003.

[9] X.J. Wu, "A new chaotic communication scheme based on adaptive synchronization," *Chaos*, vol. 16, no. 4, 043118, 2006.

[10] T. Liao and S. Tsai, "Adaptive synchronization of chaotic systems and its application to secure communications," *Chaos, Solitons and Fractals*, vol. 11,no. 9, pp. 1387–1396, 2000.

[11] A. Maybhate and R.E. Amritkar, "Use of synchronization and adaptive control in parameter estimation from a time series," *Phys. Rev. E* vol. 59, pp. 284–293, 1999.

[12] D.B. Huang, G.J. Xing and D.W. Wheeler, "Multiparameter estimation using only a chaotic time series and its applications," *Chaos*, vol. 17, no. 2, 023118, 2007.

[13] U. Parlitz, "Estimating model parameters from time series by auto-synchronization," *Phys. Rev. Lett.*, vol. 76, pp. 1232–1235, 1996.

[14] C.S. Zhou and C.H. Lai, "Decoding information by following parameter modulation with parameter adaptive control," *Phys. Rev. E*, vol. 59, no. 6, pp. 6629–6636, 1999.

[15] Y. Liu, W.K.S. Tang and L. Kocarev, "An adaptive observer design for the auto-synchronization of Lorenz system," *Int. J. Bifurc. Chaos*, scheduled on Aug. 2008.

[16] R. Konnur, "Synchronization-based approach for estimating all model parameters of chaotic systems," *Phys. Rev. E*, vol. 67, no. 4, 027204, 2003

[17] D.L. Xu and F.F. Lu, "An approach of parameter estimation for non-synchronous systems," *Chaos, Solitons and Fractals*, vol. 25, no. 2, pp. 361–366, 2005

[18] Q. He, L. Wang and B. Liu, "Parameter estimation for chaotic systems by particle swarm optimization," *Chaos, Solitons and Fractals*, vol. 34, pp. 654–661, 2007

Ying Liu received her BSc and MSc from the College of Information Engineering at Dalian Maritime University, China, in 2003 and the Department of Electrical Engineering at Shantou University, China, in 2006, respectively. She is now pursuing PhD degree from Department of Electronic Engineering of City University of Hong Kong. Her research interest is adaptive observer design and nonlinear signal processing.

Wallace Tang obtained his BSc from the University of Hong Kong in 1988, and both MSc and PhD from the City University of Hong Kong in 1992 and 1996, respectively. He is currently an Associate Professor in the Department of Electronic Engineering, City University of Hong Kong. He has published over 60 journal papers and four book chapters, and co-authored two books, focusing on genetic algorithms and chaotic theory. He is a member of Nonlinear Circuits and Systems Technical Committee in IEEE Circuits and Systems Society, IEEE SMCS Technical Committee on Soft Computing, and a member of technical committee on Optimal Control of IFAC. He was the Associate Editor for IEEE Transactions on Circuits and Systems Part II in 2004-2005 and is now an associate editor of Dynamics of Continuous, Discrete & Impulsive Systems, Series B. He is also the Distinguished Lecturer of IEEE Circuits and Systems Society in 2007/08.