Fuzzy Control for Exponential Optimal Synchronization of Chaotic Cryptosystems: Neural-Network-Based Approach

Feng-Hsiag Hsiao, Sheng-Yuan Lin and Zhe-Hao Lin
Department of Electrical Engineering
National University of Tainan, 33, Section 2, Shu Lin Street, Tainan 700, Taiwan, R.O.C.
fhhsiao@mail.nutn.edu.tw

Abstract

This paper presents a systematic design methodology for neural-network (NN) based secure communications in multiple time-delay chaotic (MTDC) systems with optimal H^{∞} performance and cryptography. First, we use the n-shift cipher and key to the original message of transmission for encryption. The encrypted message is re-encrypted by using chaotic synchronization. A robust model-based fuzzy control design is then presented to address the effects of modeling errors between the MTDC systems and the NN models. Next, a delay-dependent exponential stability criterion is derived in terms of Lyapunov's direct method to guarantee that the trajectories of the slave system can approach those of the master system. Subsequently, the stability conditions of this criterion are reformulated into linear matrix inequalities (LMIs). According to the LMIs, a model-based fuzzy controller is then synthesized to stabilize the MTDC systems. A fuzzy controller is synthesized to not only realize the exponential synchronization, but also achieve optimal H^{∞} performance by minimizing the disturbance attenuation level. Furthermore, the error of the recovered message is stated by using the n-shift cipher and key.

Keywords: *Exponential synchronization, chaotic communication, neural network, cryptography.*

1 Introduction

Stability and stabilization are particularly important factors in time-delay systems, and these factors have, to date, been the focus of many studies. Furthermore, engineering systems [1], such as the structure control of tall buildings, hydraulics, or electronic networks, often involve time delays. Notably, the introduction of a time-delay factor tends to complicate analysis. For this reason, a great deal of research has been focused on developing convenient stability checking methods. The stability criteria of time-delay systems have been traditionally approached from two main directions according to the dependence on the size of the delay. Moreover, since Mackey and Glass [2] first identified chaos phenomena in time-delay systems, time delays have received increasing interest in chaotic systems. Chaotic phenomena have been observed in numerous physical systems, and can lead to irregular performance and potentially catastrophic failures [3]. Chaos is a well-known nonlinear phenomenon; it is the seemingly random behavior of a deterministic system characterized by sensitive dependence on initial conditions [4]. Because of these properties, chaos has received a great deal of interest from scientists in various research fields [5]. One particular communication research field, chaotic synchronization, has been extensively investigated.

The chaotic synchronization of identical systems with different initial conditions was first introduced by Pecora and Carroll in 1990 [6]; it aims to lock one chaotic system to another, so that both follow the same path. Based on this concept, various synchronization approaches have been widely developed in the past two decades. Chaotic synchronization can be applied in the vast areas of physics and engineering science, and especially in secure communication [7]. The most acceptable synchronization method is the masking method which contains messages in a chaotic system and recovers the original messages from the synchronization [8]. In chaos secure communications, two identical chaotic oscillators called transmitter (master) and receiver (slave) are required. Consequently, chaotic synchronization has become a popular study [9-10]. However, most synchronization methods are focused on synchronizing two identical chaotic systems with different initial conditions [11]. In fact, experimental and even real systems are often not fully identical; in particular, there are mismatches in the parameters of the systems [11].

In general, there will always be some noise or disturbances that may cause instability. An external disturbance will negatively affect the performance of chaotic systems. Therefore, how to reduce the effect of external disturbances in

the synchronization process is an important issue for chaotic systems [12]. The H^{∞} control has been conferred for synchronization in chaotic systems over the last few years [12], and the H^{∞} synchronization problem for time-delay chaotic systems has been extensively investigated (see, for example [13-15]). Accordingly, the purpose of this study is to realize the exponential synchronization of identical multiple time-delay chaotic (MTDC) systems, and to simultaneously attenuate the effect of external disturbances on the control performance to a minimum level.

Due to the unique merits in solving complex nonlinear system identification and control problems, neural-network-based modeling has become an active research field in the past few years. Neural networks (NN) consist of simple elements operating in parallel; these elements are inspired by biological nervous systems. As in nature, the connections between elements largely determine the network function. A neural network can be trained to perform a particular function by adjusting the values of the connections (weights) between elements. Therefore, a nonlinear system can be approximated as closely as desired by an NN model via repetitive training. Some examples of successful applications of NN in recent years can be found in [15-19].

In the past few years, much research effort has been devoted to fuzzy control, which has attracted a great deal of attention from both the academia and industry, and it has been successfully used in wide variety of applications [20-24]. Despite the successes of fuzzy control, it still has many basic problems that have yet to be solved. Stability analysis and systematic design are certainly among the most important issues for fuzzy control systems. Recently, significant research efforts have been devoted to these issues [25]. All of these studies, however, ignored the modeling errors between the fuzzy combination of T–S fuzzy models and the nonlinear systems under control. In fact, the existence of modeling errors may be a potential source of instability for control designs based on the assumption that the fuzzy model exactly matches the nonlinear plant [26]. In recent years, novel approaches to overcome the influence of modeling errors in the field of model-based fuzzy control for nonlinear systems have been offered by Kiriakidis [26], Chen *et al.* [27]and Cao and Frank [28].

Cryptography has always been very important in military and business applications for maintaining the secrecy of messages and to prevent information tampering and eavesdropping. This is especially true since and the number of transactions being made via the Internet continues to increase at a pace [29]. In this regard, a direct solution to protect messages is to use symmetric encryption. Symmetric encryption uses the same key for both encryption and decryption [30]. There are two basic types of symmetric encryption algorithms, the Data Encryption Standard (DES), and the Advanced Encryption Standard (AES) algorithms [31]. There have been numerous recent reports on the success of symmetric encryption [32-34]. Therefore, the security problem of master-slave systems based on chaotic circuits needs to develop a high secure communication system, which is the other subject of this thesis.

Almost all existing research on controlling chaos has used fuzzy models to approximate chaotic systems [3-4]. Although using fuzzy models to approximate the chaotic systems is simpler than using Neural networks (NN), the NN models better approach the chaotic systems by iterative training and weight adjustment. That is to say, NN models will have fewer modeling errors will be much less than fuzzy models. In addition, this study combines the concepts of chaotic synchronization and cryptography to achieve a more security communication system. First, we use the n-shift cipher and key to the original message of transmission for encryption. The encrypted message is re-encrypted using chaotic synchronization. Consequently, an effective method is proposed via a neural-network (NN)-based technique to realize the optimal H^{∞} exponential synchronization of multiple time-delay chaotic (MTDC) systems, so that the trajectories of slave systems can approach those of master systems and the effect of external disturbance on control performance is attenuated to a minimum level. The MTDC systems are first approximated by the NN model approach. Next, in terms of Lyapunov's direct method, a delay-dependent criterion is derived to guarantee the exponential stability of the error system between the master and the slave systems. Subsequently, the stability conditions are reformulated into linear matrix inequalities (LMIs). On the basis of the LMIs, a model-based fuzzy controller is then synthesized to stabilize the MTDC systems. Based on the LMI, a fuzzy controller is synthesized not only to realize the exponential synchronization but also to achieve optimal H^{∞} performance by minimizing the disturbance attenuation level. Finally, the error of the recovered message is stated using the n-shift cipher and key.

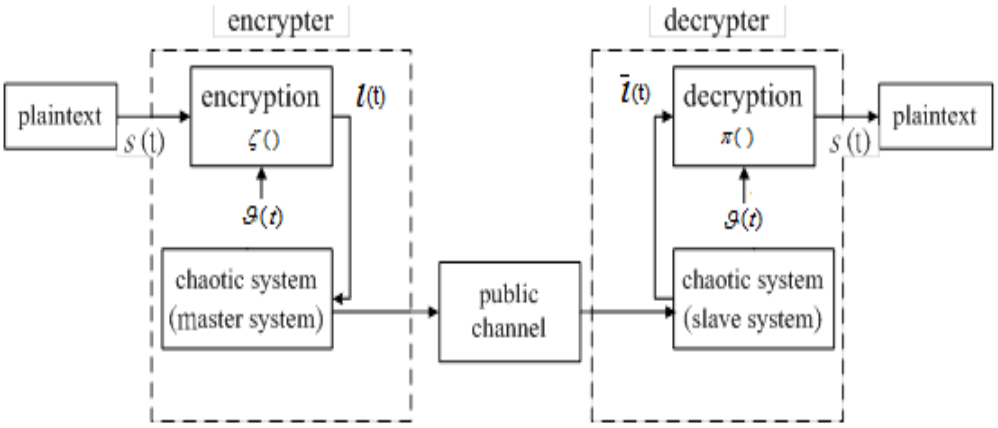

Figure 1. Block diagram of the chaotic synchronization cryptosystem

2 Problem Formulation

Consider two multiple time-delay chaotic (MTDC) systems in master-slave configuration. The dynamics of the master system (N_m) and slave system (N_s) are described as follows:

$$N_m: \dot{X}(t) = f(X(t)) + \sum_{k=1}^{g} H_k(X(t-\tau_k))$$
$$Y(t) = f(X(t)) \quad (2.1)$$

$$N_s: \dot{\hat{X}}(t) = \hat{f}(\hat{X}(t)) + \sum_{k=1}^{g} \hat{H}_k(\hat{X}(t-\tau_k)) + BU(t) + D(t)$$
$$\hat{Y}(t) = \hat{f}(\hat{X}(t)) \quad (2.2)$$

where $f(\cdot)$, $\hat{f}(\cdot)$, $H_k(\cdot)$ and $\hat{H}_k(\cdot)$ are the nonlinear vector-valued functions, τ_k ($k = 1, 2, \cdots, g$) are the time delays, $U(t)$ is the control output and $D(t)$ denotes the external disturbance.

In this section, we first use the n-shift cipher and key to the original message of transmission for encryption. The encrypted message is re-encrypted by using chaotic synchronization. A Neural-network (NN) model is then established to approximate the MTDC system. The dynamics of the NN model are then converted into a linear differential inclusion (LDI) state-space representation. Finally, based on the LDI state-space representation, a fuzzy controller is synthesized to realize the synchronization of the MTDC systems.

2.1 Chaotic Cryptosystem

A chaotic synchronization cryptosystem is shown in Figure 1. It consists of the encrypter (the master system and an encryption function $\zeta(\cdot)$) and decrypter (the slave system and a decryption function $\pi(\cdot)$. First, the message $s(t)$ and encryption key $\vartheta(t)$ form an encrypted message $\iota(t)$ via an encryption function. The encrypted message $\iota(t)$ is then combined the master system. When the chaotic systems are synchronized in the decrypter and encrypter, we can obtain the message $\bar{\iota}(t)$ in the encrypter. Next, the message $\bar{\iota}(t)$ can be decrypted by decryption key $\vartheta(t)$ in the decryption function $\pi(\cdot)$. A decryption function is then used to reveal the message.

We use an n-shift cipher for encryption [32]. The n-shift cipher is defined by

$$\iota(t) = \zeta(s(t), \vartheta(t)) = \underbrace{F(...F(F}_{n}(s(t), \underbrace{\vartheta(t)), \vartheta(t)), ..., \vartheta(t))}_{n} \quad (2.3)$$

where h is chosen such that message $s(t)$ and encryption key $\vartheta(t)$ lie within $(-h, h)$. Here, $\iota(t)$ denotes the encrypted signal, and $F(.)$ is the following nonlinear function:

$$F(s(t), \vartheta(t)) = \begin{cases} (s(t)+\vartheta(t)) + 2h, & -2h \le (s(t)+\vartheta(t)) \le -h \\ (s(t)+\vartheta(t)), & -h < (s(t)+\vartheta(t)) < h \\ (s(t)+\vartheta(t)) - 2h, & h \le (s(t)+\vartheta(t)) \le 2h \end{cases} \quad (2.4)$$

The corresponding decryption function is the same as the encryption function

$$s(t) = \pi(\bar{\iota}(t), -\vartheta(t)) = \underbrace{F(...F(F}_{n}(\zeta(s(t), \vartheta(t)), \underbrace{-\vartheta(t)), -\vartheta(t)), ..., -\vartheta(t))}_{n} \quad (2.5)$$

where $\bar{\iota}(t)$ is the recovered decryption signal,

and $\pi(\cdot)$ is the decryption function. In the n-shift cipher, the key signal $\vartheta(t)$ is used n times to encrypt the plain signal.

The encrypted message $\imath(t)$ is then combined in the master system. The dynamics of the master system (N_m) and slave system (N_s) are then described as follows:

$$N_m: \dot{X}(t) = f(X(t)) + \sum_{k=1}^{g} H_k(X(t-\tau_k)) + BS\imath(t)$$
$$Y(t) = f(X(t)) + S\imath(t) \quad (2.6)$$

$$N_s: \dot{\hat{X}}(t) = \hat{f}(\hat{X}(t)) + \sum_{k=1}^{g} \hat{H}_k(\hat{X}(t-\tau_k)) + BU(t) + D(t)$$
$$\hat{Y}(t) = \hat{f}(\hat{X}(t)) \quad (2.7)$$

2.2 Neural-Network (NN) Model

The MTDC system can be approximated by an NN model that has S layers with $J^{\sigma}(\sigma = 1, 2, \cdots, S)$ neurons for each layer, in which $x_1(t) \sim x_{\delta}(t)$ are the state variables and $x_1(t-\tau_1) \sim x_1(t-\tau_g)$, $x_2(t-\tau_1) \sim x_{\delta}(t-\tau_g)$ are the state variables with delays.

In order to distinguish among these layers, superscripts are used to identify the layers. Specifically, we append the number of the layer as a superscript to the names for each of these variables. Thus, the weight matrix for the σ th layer is written as W^{σ}. Moreover, it is assumed that $v_{\varsigma}^{\sigma}(t)$ $(\varsigma = 1, 2, \cdots, J^{\sigma};\ \sigma = 1, 2, \cdots, S)$ is the net input and $T(v_{\varsigma}^{\sigma}(t))$ is the transfer function of the neuron. Subsequently, the transfer function vector of the σ th layer is defined as:

$$\Psi^{\sigma}(v_{\varsigma}^{\sigma}(t)) \equiv [T(v_1^{\sigma}(t))\ T(v_2^{\sigma}(t))\ \cdots\ T(v_{J^{\sigma}}^{\sigma}(t))]^T \quad (2.8)$$

where $T(v_{\varsigma}^{\sigma}(t))$ $(\varsigma = 1, 2, \cdots, J^{\sigma})$ is the transfer function of the ς th neuron. The final output of NN model can then be inferred as follows:

$$\dot{X}(t) = \Psi^S(W^S\Psi^{S-1}(W^{S-1}\Psi^{S-2}(\cdots\Psi^2(W^2\Psi^1(W^1\Lambda(t)))\cdots))) \quad (2.9)$$

where $\Lambda^T(t) = [X^T(t)\ X^T(t-\tau_k)]$

with $X(t) = [x_1(t)\ x_2(t)\cdots x_{\delta}(t)]^T$,

$X(t-\tau_k) = [x_1(t-\tau_1)\cdots x_1(t-\tau_g)\ x_2(t-\tau_g)\ \cdots\ x_{\delta}(t-\tau_m)]^T$

for $k = 1, 2\ \cdots, g$.

2.3 Linear Differential Inclusion (LDI)

To deal with the synchronization problem of MTDC systems, this study establishes the following LDI state-space representation for the dynamics of the NN model, described as [35]:

$$\dot{O}(t) = A(a(t))O(t),$$
$$A(a(t)) = \sum_{i=1}^{\kappa} h_i(a(t))\tilde{A}_i \quad (2.10)$$

where κ is a positive integer, $a(t)$ is a vector signifying the dependence of $h_i(\cdot)$ on its elements, $\tilde{A}_i$ $(i = 1, 2, \cdots, \kappa)$ are constant matrices and $O(t) = [o_1(t)\ o_2(t)\ \cdots\ o_{\aleph}(t)]^T$ is the state vector. Furthermore, it is assumed that $h_i(a(t)) \geq 0$ and $\sum_{i=1}^{\kappa} h_i(a(t)) = 1$.

According to (2.10) and following the same procedure as that in Section II of [36], the dynamics of the NN model (2.11) can be rewritten as the following LDI state-space representation:

$$\dot{X}(t) = \sum_{i=1}^{\kappa} h_i(t) C_i \Lambda(t) \quad (2.11)$$

where $h_i(t) \geq 0$, $\sum_{i=1}^{\kappa} h_i(t) = 1$, κ is a positive integer and C_i is a constant matrix with appropriate dimension associated with C_{Ω}^{σ}. Moreover, the LDI state-space representation (2.11) can be rearranged as follows:

$$\dot{X}(t) = \sum_{i=1}^{\kappa} h_i(t)\{A_i X(t) + \sum_{k=1}^{g} \bar{A}_{ik} X(t-\tau_k)\} \quad (2.12)$$

where A_i and $\bar{A}_{ik}$ are the partitions of C_i corresponding to the partitions of $\Lambda^T(t)$.

2.4 Fuzzy Controller

On the basis of the state-feedback control scheme, a model-based fuzzy controller is able to ensure that the slave system can synchronize with the master system. The output error is defined as $Y_e(t) \equiv \hat{Y}(t) - Y(t) = [e_1(t), e_2(t), \cdots, e_{\delta}(t)]^T$, and the fuzzy controller is in the following form:

Control Rule l:

IF $e_1(t)$ is M_{l1} and $\cdots$ and $e_{\delta}(t)$ is $M_{l\delta}$

THEN $U(t) = -K_l Y_e(t)$

where $l = 1, 2, \cdots, m$, and m is the number of IF-THEN rules of the fuzzy controller, and $M_{l\eta}(\eta = 1, 2, \cdots, \delta)$ are the fuzzy sets. Therefore, the final output of this fuzzy controller can be inferred as follows:

$$U(t) = \frac{-\sum_{l=1}^{m} w_l(t) K_l Y_e(t)}{\sum_{l=1}^{m} w_l(t)} = -\sum_{l=1}^{m} \bar{h}_l(t) K_l Y_e(t) \quad (2.13)$$

with $w_l(t) \equiv \prod_{\eta=1}^{\delta} M_{l\eta}(e_{\eta}(t))$, and $M_{l\eta}(e_{\eta}(t))$ is the grade of membership of $e_{\eta}(t)$ in $M_{l\eta}$.

Furthermore, $\bar{h}_l(t) \equiv \frac{w_l(t)}{\sum_{l=1}^{m} w_l(t)}$ and $\sum_{l=1}^{m} \bar{h}_l(t) = 1$ for all *t*.

In the past, solving the feedback gains K_l ($l = 1, 2, \cdots, m$) was based on experience and trial-and-error. It will therefore be advantageous to develop a powerful tool for solving suitable K_l ($l = 1, 2, \cdots, m$).

From the above, the NN models of the master and slave chaotic systems are described by the following LDI state-space and a model-based fuzzy controller is designed by the state-feedback control scheme. Therefore, the master and slave chaotic systems can be rewritten as representations (2.14) and (2.15), respectively:

Master:

$$\dot{X}(t) = \sum_{i=1}^{\phi} h_i(t)\{A_i X(t) + \sum_{k=1}^{g} \bar{A}_{ik} X(t-\tau_k)\} + BS\sum_{l=1}^{m} w_l(t) K_l \iota(t)$$
$$Y(t) = CX(t) + S\iota(t) \qquad (2.14)$$

Slave:

$$\dot{\hat{X}}(t) = \sum_{j=1}^{\phi} \hat{h}_j(t)[\hat{A}_j \hat{X}(t) + \sum_{k=1}^{g} \hat{\bar{A}}_{jk} \hat{X}(t-\tau_k)] + BU(t)$$
$$\hat{Y}(t) = C\hat{X}(t) \qquad (2.15)$$

3 Stability Analysis and Chaotic Synchronization via Fuzzy Control

In this section, the synchronization of multiple time-delay chaotic (MTDC) systems is examined under the influence of modeling error. The exponential synchronization scheme of the MTDC systems is described below.

3.1 Error Systems

From Eqs. (2.1) and (2.2), the dynamics of the error system under the fuzzy control (2.5) can be described as follows:

$$\dot{Y}_e(t) = \hat{\Psi} - \Psi + D(t)$$
$$+\sum_{i=1}^{\kappa}\sum_{j=1}^{\kappa}\sum_{l=1}^{m} h_i(t)\hat{h}_j(t)\bar{h}_l(t)\Big\{ G_{il} Y_e(t) + (\hat{A}_j - A_i)\hat{X}(t)$$
$$+\sum_{k=1}^{g}(\hat{\bar{A}}_{jk} - \bar{A}_{ik})\hat{X}(t-\tau_k) + \sum_{k=1}^{g}\bar{A}_{ik} Y_e(t-\tau_k)\Big\} + D(t)$$
$$-\sum_{i=1}^{\kappa}\sum_{j=1}^{\kappa}\sum_{l=1}^{m} h_i(t)\hat{h}_j(t)\bar{h}_l(t)\Big\{ G_{il} Y_e(t) + (\hat{A}_j - A_i)\hat{X}(t)$$
$$+\sum_{k=1}^{g}(\hat{\bar{A}}_{jk} - \bar{A}_{ik})\hat{X}(t-\tau_k) + \sum_{k=1}^{g}\bar{A}_{ik} Y_e(t-\tau_k)\Big\} - D(t)$$
$$= \sum_{i=1}^{\kappa}\sum_{l=1}^{m} h_i(t)\bar{h}_l(t)\Big\{ G_{il} Y_e(t) + \sum_{k=1}^{g}\bar{A}_{ik} Y_e(t-\tau_k)\Big\} + D(t) + \Phi(t) \qquad (3.1)$$

where $G_{il} \equiv A_i - BCK_l$,

$$\hat{\Psi} \equiv \hat{f}(\hat{X}(t)) + \sum_{k=1}^{g}\hat{H}_k(\hat{X}(t-\tau_k)) + U(t),$$
$$\Psi \equiv f(X(t)) + \sum_{k=1}^{g} H_k(X(t-\tau_k)) \text{ with } U(t) = -\sum_{l=1}^{m}\bar{h}_l(t) K_l Y_e(t),$$
$$\Phi(t) \equiv \hat{\Psi} - \Psi - \Big\{\sum_{i=1}^{\kappa}\sum_{l=1}^{m} h_i(t)\bar{h}_l(t)\,[G_{il} Y_e(t) + \sum_{k=1}^{g}\bar{A}_{ik} Y_e(t-\tau_k)]\Big\}.$$

Suppose that there exists a bounding matrix ΘR_{il} such that:

$$\|\Phi(t)\| \le \Big\|\sum_{i=1}^{\kappa}\sum_{l=1}^{m} h_i(t)\bar{h}_l(t)\Theta R_{i\ell} Y_e(t)\Big\| \qquad (3.2)$$

for the trajectory $Y_e(t)$, and the bounding matrix ΘR_{il} can be described as follows:

$$\Theta R_{il} = \varepsilon_{il} R \qquad (3.3)$$

where R is the specified structured bounding matrix and $\|\varepsilon_{il}\| \le 1$, for $i = 1, 2, \cdots, \phi$; $l = 1, 2, \cdots, m$. Eqs. (3.2) and (3.3) show that:

$$\Phi^T(t)\Phi(t)$$
$$\le \sum_{i=1}^{\phi}\sum_{l=1}^{m} h_i(t)\bar{h}_l(t)\|RY_e(t)\|\,\varepsilon_{il}\,\Big\|\sum_{i=1}^{\kappa}\sum_{l=1}^{m} h_i(t)\bar{h}_l(t)\Big\|\,\varepsilon_{il}\,\|RY_e(t)\|$$
$$\le [RY_e(t)]^T [RY_e(t)] \qquad (3.4)$$

Namely, $\Phi(t)$ is bounded by the specified structured bounding matrix *R*.

Remark 3.1 [27]: The following simple example describes the procedures for determining ε_{il} and R. First, assume that the possible bounds for all elements in ΘR_{il} are:

$$\Theta R_{il} = \begin{bmatrix} \Theta r_{il}^{11} & \Theta r_{il}^{12} & \Theta r_{il}^{13} \\ \Theta r_{il}^{21} & \Theta r_{il}^{22} & \Theta r_{il}^{23} \\ \Theta r_{il}^{31} & \Theta r_{il}^{32} & \Theta r_{il}^{33} \end{bmatrix} \qquad (3.5)$$

where $-r^{qs} \le \Theta r_{il}^{qs} \le r^{qs}$ for some r_{il}^{qs} with *q*, *s* = 1, 2, 3; $i = 1, 2, \ldots, \phi$, and $l = 1, 2, \ldots, m$.

A possible description for the bounding matrix ΘR_{il} is:

$$\Theta R_{il} = \begin{bmatrix} \varepsilon_{il}^{11} & 0 & 0 \\ 0 & \varepsilon_{il}^{22} & 0 \\ 0 & 0 & \varepsilon_{il}^{33} \end{bmatrix} \begin{bmatrix} r^{11} & r^{12} & r^{13} \\ r^{21} & r^{22} & r^{23} \\ r^{31} & r^{32} & r^{33} \end{bmatrix} = \varepsilon_{il} R \qquad (3.6)$$

where $-1 \le \varepsilon_{il}^{qq} \le 1$ for $q = 1, 2, 3$. Notice that ε_{il} can be chosen by other forms as long as $\|\varepsilon_{il}\| \le 1$. The validity of (3.2) is then checked in the simulation. If it is not satisfied, we can expand the bounds for all elements in ΘR_{il} and repeat the design procedure until (3.2) holds.

3.2 Delay-Dependent Stability Criterion for Exponential H^∞ Synchronization

In this subsection, a delay-dependent criterion is proposed to guarantee the exponential stability of the error system described in (3.1). Moreover, in general, there will always be some noise or disturbances that may cause instability. The effect of the external disturbance $D(t)$ will negatively affect the performance of chaotic systems. To reduce the effect of the external disturbance, an optimal H^∞ scheme is used to design a fuzzy control such that the effect of the external disturbance on control performance can be attenuated to a minimum level. In other words, the fuzzy controller (2.5) simultaneously realizes exponential synchronization and achieves the optimal H^∞ control performance in this study.

Before examining the stability of the error system, some definitions and lemma are given below.

Lemma 1 [40]: For the real matrices A and B with appropriate dimension:

$$A^T B + B^T A \le \lambda A^T A + \lambda^{-1} B^T B$$

where λ is a positive constant.

Definition 1 [42]: The slave system (2.2) can exponentially synchronize with the master system (2.1) (i.e., the error system (3.3) is exponentially stable) if there exist two positive numbers α and β so that the synchronization error satisfies:

$$\|Y_e(t)\| \le \alpha \exp(-\beta(t-t_0)), \quad \forall t \ge 0$$

where the positive number β is called the exponential convergence rate.

Definition 2 [11]: The master system (2.1) and slave system (2.2) are said to be in exponential H^∞ synchronization if the following conditions are satisfied:

(i). With zero disturbance (i.e., $D(t)=0$), the error system (3.1) with the fuzzy controller (2.5) is exponentially stable.

(ii). Under the zero initial conditions (i.e., $E(t)=0$ for $t \in [-\tau_{\max}, 0]$, in which $\tau_{\max}$ is the maximal value of τ_k's) and a given constant $\rho > 0$, the following condition holds:

$$\Theta(Y_e(t), D(t)) = \int_0^\infty Y_e^T(t) Y_e(t) dt - \rho^2 \int_0^\infty D^T(t) D(t) dt \le 0 \tag{3.7}$$

where the parameter ρ is called the H^∞-norm bound or the disturbance attenuation level. If the minimum ρ is found to satisfy the above conditions (i.e., the error system can reject the external disturbance as strongly as possible), the fuzzy controller (2.5) is an optimal H^∞ synchronizer [11].

Theorem 1: For given positive constants a and n, if there exist two symmetric positive definite matrices P and ψ_k, as well as to positive constants ξ and ρ, so that the following inequalities hold, then the exponential H^∞ synchronization with the disturbance attenuation ρ is guaranteed via the fuzzy controller (2.5):

$$\Delta_{il} \equiv \sum_{k=1}^{g} \tau_k P G_{il} + \sum_{k=1}^{g} \tau_k G_{il}^T P + \sum_{k=1}^{g} \psi_k + ng R^T R + C^T C + I + \sum_{k=1}^{g} \tau_k^2 P^2 (\xi^{-1} + n^{-1} + ga^{-1}) < 0 \tag{3.8a}$$

$$\nabla_{ik} \equiv ga \bar{A}_{ik}^T \bar{A}_{ik} - \psi_k < 0 \tag{3.8b}$$

$$\rho > \sqrt{\xi g} \tag{3.8c}$$

where $G_{il} \equiv A_i - BCK_l$, for $i = 1, 2, \cdots, \phi$; $k = 1, 2, \cdots, g$ and $l = 1, 2, \cdots, m$.

Corollary 1: Eqs. (3.8a) and (3.8b) can be reformulated into LMIs via the following procedure:

By introducing the new variables; $Q = P^{-1}$, $F_l = K_l Q$ and $\bar{\psi}_k = Q \psi_k Q$, Eqs. (3.8a) and (3.8b) can be rewritten as follows:

$$\sum_{k=1}^{g} \tau_k \{A_i Q - B F_l + Q A_i^T - F_l^T B^T\} + \sum_{k=1}^{g} \bar{\psi}_k + ngQ R^T R Q + Q C^T C Q + QIQ + \sum_{k=1}^{g} \tau_k^2 (\xi^{-1} + n^{-1} + ga^{-1}) I < 0 \tag{3.9a}$$

$$gaQ \bar{A}_{ik}^T \bar{A}_{ik} Q - \bar{\psi}_k < 0 \tag{3.9b}$$

for $i = 1, 2, \cdots, \phi$; $k = 1, 2, \cdots, g$ and $l = 1, 2, \cdots, m$. According to Schur's complement [35], it is easy to show that the linear matrix inequalities in Eqs. (3.9a) and (3.9b) are equivalent to the following LMIs in Eqs. (3.10a) and (3.10b):

$$\begin{bmatrix} \Xi & QR^T & Q \\ RQ^T & -(ng)^{-1} I & 0 \\ Q & 0 & -I \end{bmatrix} < 0 \tag{3.10a}$$

$$\begin{bmatrix} -\bar{\psi}_k & Q \bar{A}_{ik}^T \\ \bar{A}_{ik} Q & -(ga)^{-1} I \end{bmatrix} < 0 \tag{3.10b}$$

where

$$\Xi \equiv \sum_{k=1}^{g} \tau_k A_i Q - \sum_{k=1}^{g} \tau_k B F_l + \sum_{k=1}^{g} \tau_k Q A_i^T - \sum_{k=1}^{g} \tau_k F_l^T B^T + \sum_{k=1}^{g} \bar{\psi}_k + \sum_{k=1}^{g} \tau_k^2 (\xi^{-1} + n^{-1} + ga^{-1}) I + QC^T CQ.$$

Thus, Theorem 1 can be transformed into an LMI problem, and efficient interior-point algorithms are now available in Matlab LMI Solver to solve this problem.

Corollary 2 [44]: In order to verify the feasibility of solving the inequalities in Eqs. (3.10a) and (3.10b) using the LMI Solver

(Matlab), interior-point optimization techniques are utilized to compute feasible solutions. These techniques require that the LMI systems are constrained to be strictly feasible, that is, the feasible set has a nonempty interior. For feasibility problems, the LMI Solver by *feasp* ① is shown as follows:

Find x such that the LMI $L(x) < 0$ ② (3.11a)

as

Minimize t subject to $L(x) < t \times I$ (3.11b)

where $L(x)$ is symmetric matrix and I is identity matrix.

From the above, the LMI constraint is always strictly feasible in x, t and the original LMI (3.11a) is feasible if and only if the global minimum $tmin$ ③ of (3.11b) satisfies $tmin < 0$. In other words, if $tmin < 0$ will satisfy Eqs. (3.10a) and (3.10b), then the stability conditions (3.8a) and (3.8b) in Theorem 1 can be met. The obtained fuzzy controller (2.5) can then exponentially stabilize the error system, and the H^∞ control performance is achieved at the same time.

4 Conclusion

In this paper, exponential synchronization multiple time-delay chaotic (MTDC) systems with optimal H^∞ performance and cryptography were combined to achieve a more security communication system. First, we applied the n-shift cipher and key to the original message of transmission for encryption. The encrypted message is re-encrypted using chaotic synchronization. The MTDC systems were then approximated using an NN model-based approach. Next, a robust model-based fuzzy control design was proposed to overcome the effect of modeling error between the MTDC systems and the NN models. In terms of Lyapunov's direct method, a delay-dependent stability criterion was derived to ensure that the slave system was able to exponentially synchronize with the master system. Subsequently, the stability conditions of this criterion were reformulated into linear matrix inequalities (LMIs). On the basis of the LMIs, a model-based fuzzy controller was then synthesized to stabilize the MTDC systems. According to the LMIs, we synthesized a fuzzy controller to realize the exponential H^∞ synchronization of the chaotic master-slave systems, and reduce the H^∞-norm from disturbance to synchronization error at the lowest level. On the other hand, the output error of the recovered message was stated using the n-shift cipher and key.

① *feasp* is the syntax used to test the feasibility of a system of LMIs in MATLAB.

② In this study, Eq. (3.11a) can be represented as Eqs. (3.10a) and (3.10b).

③ The global minimum $tmin$ is the scalar value returned as the output argument by feasp.

References

[1] K. R. Lee, J. H. Kim, E. T. Jeung and H. B. Park, "Output feedback robust H^∞ control of uncertain fuzzy dynamic systems with time-varying delay," *IEEE Trans. Fuzzy Systems, vol. 8, pp. 657-664, 2000*.

[2] M. Mackey and L. Glass, "Oscillation and chaos in physiological control systems," *Science, vol. 197, no. 4300, pp. 287–289, 1977*.

[3] Z. R. Tsai, Y. Z. Chang, J. D. Hwang and J. Lee, "Robust fuzzy stabilization of dithered chaotic systems using island-based random optimization algorithm," *Information Sciences, vol. 178, pp. 1171–1188, 2008*.

[4] C. Hu, H. Jiang and Z. Teng, "General impulsive control of chaotic systems based on a TS fuzzy model," Fuzzy Sets and Systems, vol. 174, pp. 66-82, 2011

[5] S. L. Lin and P. C. Tung, "A new method for chaos control in communication systems," *Chaos, Solitons & Fractals, vol. 42, pp. 3234-3241, 2009*.

[6] L. M. Pecora and T. L. Carroll, "Synchronization in chaotic systems," *Physical Review Letters, vol. 64, pp. 821-824, 1990*.

[7] H. T. Yau and J. J. Yan, "Chaos synchronization of different chaotic systems subjected to input nonlinearity," *Applied Mathematics and Computation, vol. 197, pp.775–788, 2008*.

[8] T. C. Chen and T. L. Liao, "Implementation of H-Infinite Synchronization of Switched Chaotic Systems and Its Application to Secure Communications," *Applied Mathematics and Computation, National Cheng Kung University, 2010*.

[9] H. K. Lam, W. K. Ling, H. H. C. Iu and S. S. H. Ling, "Synchronization of chaotic systems using time-delayed fuzzy state-feedback controller," *IEEE Trans. Circuit and Systems I, vol. 55, pp. 893-903, 2008*.

[10] M. Liu, “Optimal exponential synchronization of general chaotic delayed neural networks: an LMI approach,” *Neural Networks, vol. 22, pp. 949-957, 2009*.

[11] H. H. Chen, G. J. Sheu, Y. L. Lin and C. S. Chen, “Chaos synchronization between two different chaotic systems via nonlinear feedback control,” *Nonlinear Analysis, vol. 70, pp. 4393-4401, 2009*.

[12] D. Qi, M. Liu, M. Qiu and S. Zhang, “Exponential H^{∞} synchronization of general discrete-time chaotic neural networks with or without time delays,” *IEEE Trans. Neural Network, vol. 21, pp. 1358-1365, 2010*.

[13] H. R. Karimi and H. Gao, “New delay-dependent exponential H^{∞} synchronization for uncertain neural networks with mixed time delays,” *IEEE Trans. Syst. Man Cybern. B: Cybern., vol. 40, no. 1, pp. 173–185, Feb. 2010*.

[14] B. S. Chen, C. H. Chiang and S. K. Nguang, “Robust H^{∞} Synchronization design of nonlinear coupled network via fuzzy interpolation method,” *IEEE Trans. on Circuits and Systems I, vol. 58, pp. 349-362, 2011*.

[15] S. Limanond, J. Si, and Y. L. Tseng, “Production data based optimal etch time control design for a reactive ion etching process,” *IEEE Trans. Semiconductor Manufacturing, vol. 12, pp.139-147, 1999*.

[16] R. Enns and J. Si, “Helicopter trimming and tracking control using direct neural dynamic programming,” *IEEE Trans. Neural Networks, vol. 14, pp.929-939, 2003*.

[17] F. J. Lin, H. J. Shieh, P. H. Shieh, and P. H. Shen, “An adaptive recurrent-neural-network motion controller for X-Y table in CNC machine,” *IEEE Trans. Systems, Men, and Cybernetics-B, vol. 36, pp. 286-299, 2006*.

[18] H. C. Liaw, B. Shirinzadeh, and J. Smith “Robust neural network motion tracking control of piezoelectric actuation systems for micro/nanomanipulation” *IEEE Trans. Neural Networks, vol. 20, pp. 356-367, 2009*.

[19] S. Limanond, and J. Si, “Neural-network-based control design: An LMI approach,” *IEEE Trans. Neural Networks, vol. 9, pp. 1422-1429, 1998*.

[20] J. J. Wang, C. T. Lin, S. H. Liu and Z. C. Wen, “Model-based synthetic fuzzy logic controller for indirect blood pressure measurement,” *IEEE Trans. Systems, Men, and Cybernetics-B, vol. 32, pp. 306-315, 2002*.

[21] R. J. Wai, “Hybrid fuzzy neural-network control for nonlinear motor-toggle servomechanism,” *IEEE Trans. Control Systems Technology, vol. 10, pp. 519-532, 2002*.

[22] C. L. Hwang, L. J. Chang and Y. S. Yu, “Network-based fuzzy decentralized sliding-mode control for car-like mobile robots,” *IEEE Trans. Industrial Electronics, vol. 54, pp. 574-585, 2007*.

[23] A. V. Sant, “PM synchronous motor speed control using hybrid fuzzy-PI with novel switching functions,” *IEEE Trans. Magnetics, vol. 45, pp. 4672-4675, 2009*.

[24] D. H. Spatti, I. N. da Silva, W. F. Usida and R. A. Flauzino, “Fuzzy control system for voltage regulation in power transformers,” *IEEE Latin America Trans, vol. 8, pp. 51-57, 2010*.

[25] H. K. Lam, “Stability analysis of interval type-2 fuzzy-model-based control systems,” *IEEE Trans. Systems, Men, Cybernetics-B, vol. 38 pp.617-628, 2008*.

[26] K. Kiriakidis, “Fuzzy model-based control of complex plants,” *IEEE Trans. Fuzzy Systems, vol. 6, pp. 517-529, 1998*.

[27] B. S. Chen, C. S. Tseng and H. J. Uang, “Robustness design of nonlinear dynamic systems via fuzzy linear control,” *IEEE Trans. Fuzzy Systems, vol. 7, pp. 571-585, 1999*.

[28] Y. Y. Cao and P. M. Frank, “Robust H^{∞} disturbance attenuation for a class of uncertain discrete-time fuzzy systems,” *IEEE Trans. Fuzzy Systems, vol. 8, pp. 406-415, 2000*.

[29] R.C. Luo, L.Y. Chung and C. H. Lien, “A novel symmetric cryptography based on the hybrid Haar wavelets encoder and chaotic masking scheme" *IEEE Trans. on Industral Electronics, vol.49, pp. 933-944, 2002*.

[30] S. O' Melia and A. J. Elbirt, "Enhancing the Performance of Symmetric-Key Cryptography via Instruction Set Extensions,” *IEEE Trans. on Very Large Scale Integration Systems, vol. 18, pp. 1505-1518, 2010*.

[31] M. Alioto, M. Poli and S. Rocchi, "Differential Power Analysis Attacks to Precharged Buses: A General Analysis for Symmetric-Key Cryptographic Algorithms " *IEEE Trans. on Dependable and Secure Computing, vol. 7, pp. 226-239, 2010*.

[32] T. Yang, C. W. Wu and L. O. Chua, "Cryptography based on chaotic systems." *IEEE Trans. on Circuits and Systems I, vol. 44, pp. 469-472, 1997*.

[33] B. Bruhadeshwar, S. S. Kulkarni and A. X. Liu, "Symmetric Key Approaches to Securing BGP—A Little Bit Trust Is Enough," *IEEE Trans. on Parallel and Distributed Systems, vol. 22, pp. 1536-1549, 2011*.

[34] K. McCusker and N.E. O'Connor, "Low-Energy Symmetric Key Distribution in Wireless Sensor Networks," *IEEE Trans. on*

Dependable and Secure Computing, vol. 8, pp. 363-376, 2011.

[35] S. Limanond and J. Si, "Neural-network-based control design: an LMI approach," *IEEE Trans. Neural Networks, vol. 9, pp. 1422-1429, 1998*.

[36] F.H. Hsiao, S.D. Xu, C.Y. Lin and Z.R. Tsai, "Robustness Design of Fuzzy Control for Nonlinear Multiple Time-Delay Large-scale Systems via Neural-Network-Based Approach," *IEEE Trans. on Systems, Man, and Cybernetics Part B, Vol. 38, pp. 244-251,2008*.

[37] H. F. Leung, H. K. Lam and S. H. Ling, "Tuning of the structure and parameters of a neural network using an improved genetic algorithm," *IEEE Trans. Neural Networks, vol. 14, no. 1, pp. 79-88, Jan. 2003*.

[38] T. Takagi and M. Sugeno, "Fuzzy identification of systems and its applications to modeling and control," *IEEE Trans. Systems, Man, and Cybernetics, vol. 15, pp. 116-132, 1985*.

[39] C. C. Sun, H. Y. Chung and W. J. Chang, "Design the T-S fuzzy controller for a class of T-S fuzzy models via genetic algorithm," *IEEE Int. Conf. on Fuzzy Systems, vol. 1, pp. 278-283, 2002*.

[40] S. T. Pan, "Evolutionary Computation on Programmable Robust IIR Filter Pole-Placement Design," *IEEE Trans. Instrum. Meas., vol. 60, no. 4, pp. 1469-1479, Jan. 2011*.

[41] W. J. Wang and C. F. Cheng, "Stabilising controller and observer synthesis for uncertain large-scale systems by the Riccati equation approach," *IEE Proceeding D, vol. 139, pp. 72-78, 1992*.

[42] Y. J. Sun, "Exponential synchronization between two classes of chaotic systems," *Chaos, Solitons & Fractals, vol. 39, pp. 2363-2368, 2009*.

[43] S. Limanond and J. Si, "Neural-network-based control design: an LMI approach," *IEEE Trans. Neural Networks, vol. 9, pp. 1422-1429, 1998*.

[44] P. Gahinet, A. Nemirovski, A. J. Laub and M. Chilali, "LMI control toolbox user's guide," *The MathWorks, Inc., 1995*.